مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سریع
چهل و چهارم

استراتژی ملی برای محافظت سوئیس دربرابر خطرات سایبری

National strategy to protect
Switzerland Against cyber threats

بسم الله الرحمن الرحیم

گزارش سریع

گزارش شماره ۴۴
شهریور ۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

استراتژی ملی برای محافظت سوئیس در برابر خطرات سایبری

گزارش سریع که با عنوان Rapid Report شناخته می‌شود، نوعی گزارش کوتاه است که صرفاً برای اطلاع کلی از موضوع یا پدیده‌ای خاص در بازه زمانی محدود تهیه می‌شود. هدف عمده چنین گزارش‌هایی ایجاد تصویری اجمالی برای

تهیه شده در پژوهشگاه فضاي مجازي
(گروه مطالعات بین الملل)

مترجم: فرزانه اسکندریان
ناظر: عباس قنبری باغستان

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶غربی، پلاک ۲۰
تلفن: ۸۶۱۵۱۰۶۱-۰۲۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سیدابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

مقدمه

مقدمه

سوئیس در مسیر دیجیتال‌سازی قرار دارد. در حال حاضر، ارتباط متقابل دیجیتالی فراگیر یکی از ویژگی‌های جامعه، اقتصاد و کشور ما می‌باشد و با پیشرفت سریع فناوری، پیشبرد این توسعه همچنان ادامه خواهد داشت. این روند فرصت‌های بزرگی را فراهم می‌کند و سوئیس علاقه‌مند است تا برای تضمین و گسترش رفاه طولانی مدت در کشور، از آن بهره ببرد.

با این حال، باید در نظر داشت که دیجیتال‌سازی نه تنها فرصت، بلکه مخاطراتی را نیز به همراه دارد. وابستگی روزافزون به فناوری اطلاعات و ارتباطات[1] (ICT) کشور ما را در برابر شکست‌ها، اختلالات و سوء استفاده از این فناوری آسیب‌پذیرتر می‌کند.

تا چه اندازه این میزان آسیب‌پذیری با گسترش تهدیدات در فضای سایبری، مرتبط است؟ جرایم سایبری شایع، انباشت فعالیت‌های جاسوسی به کمک حملات سایبری، موارد خرابکاری سایبری علیه زیرساخت‌های مهم مانند بیمارستان‌ها و تأمین‌کنندگان انرژی، انتشار اطلاعات سرقت شده یا دستکاری شده با هدف اطلاع‌رسانی غلط و پروپاگاندا، و افزایش حملات سایبری در قالب گونه‌های ترکیبی تعارضات برای بی‌ثبات‌سازی کشورها و

1. Information and Communication Technologies

جوامع، مشخص می‌کند که این تهدیدها در اشکال متنوع و با سرعت در حال گسترش می‌باشند.

ترکیب وابستگی روزافزون بر عملکرد ICT و وضعیت تهدید شدید بدان معناست که ریسک‌های ناشی از آن، که ما از آنها به عنوان خطرات سایبری یاد می‌کنیم، بایستی به صورت الزامی در توسعه جامعه دیجیتال درنظر گرفته شوند. به لحاظ سیاست امنیتی، باید تدابیری اتخاذ شود که استقلال و امنیت کشور در برابر تشدید و یا ظهور تهدیدها و خطرات موجود در فضای سایبری حفظ شود. از منظر سیاست‌های اقتصادی و اجتماعی، سوئیس باید از خود در برابر خطرات سایبری حفاظت کند تا بتواند به طور پیوسته از فرصت‌های ارائه شده توسط دیجیتال‌سازی بهره ببرد و از مزیت موقعیت مکانی خود به عنوان یک کشور امن و ایمن مراقبت نماید. با این‌حال، محافظت کامل در برابر خطرات سایبری تنها با اقدامات نسبی به دست نمی‌یابد. بنابراین کشور سوئیس باید انعطاف خود را در برابر حوادث سایبری افزایش دهد.

استراتژی ملی برای حفاظت از سوئیس در برابر خطرات سایبری[1] (NCS)، نحوه دستیابی به این اهداف را تا سال ۲۰۲۲ مشخص می‌کند. این راهبرد بر پایه اولین استراتژی ملی اجرایی بین سال‌های ۲۰۱۲ تا ۲۰۱۷ می‌باشد و بیشتر در راستای آسیب‌پذیری‌های سوئیس، موقعیت به شدت تهدیدآمیز و تغییریافته از سال ۲۰۱۲ و توسعه قابل پیش‌بینی در آینده ایجاد شده و سپس با اقدامات بیشتری تکمیل گردید. از این‌رو، این استراتژی چارچوبی راهبردی را برای افزایش پیشگیری، شناسایی اولیه، واکنش و انعطاف‌پذیری در همه زمینه‌های مرتبط با خطرات سایبری فراهم می‌کند.

1. National Strategy for the Protection of Switzerland Against Cyber Risks

حفاظت در برابر خطرات سایبری مسئولیت مشترک بخش خصوصی، جامعه و دولت است. این بدان معناست که اولاً همه بخش‌ها مسئول محافظت از خود هستند. NCS این تلاش‌های حفاظت فردی را پشتیبانی و هماهنگ می‌کند. افزون بر این، در مواردی که خطرات سایبری تأثیر بسزایی در توسعه و رفاه جامعه داشته باشند به تنظیم اقدامات تکمیلی نیز می‌پردازد. این مسئولیت مشترک منجر به اجرای استراتژی NCS نیز می‌شود. دولت فدرال، کانتون‌ها، بخش خصوصی و جامعه باید اقدامات NCS به صورت اشتراکی را در قالب همکاری نزدیک با یکدیگر اجرا کرده و از طریق توانش‌های[1] مربوطه خود، یاری برسانند.

چالش‌های مقابله با خطرات سایبری بسیار زیاد و پرخطر خواهند بود. ولی نکته مهم‌تر این است که همه مسئولین با هم و به صورت هماهنگ با یکدیگر، با این چالش‌ها برخورد کنند. همکاری مؤثر کلیه ارگان‌های ذی‌صلاح در حد امکان و شبکه‌سازی بین‌المللی سیستماتیک به منظور ایجاد یک فضای امن برای دیجیتال‌سازی جامعه و اقتصاد، بسیار حیاتی است. استراتژی ملی NCS ۲۰۲۲-۲۰۱۸،که به طور مشترک توسط دولت فدرال، کانتون‌ها و بخش خصوصی تهیه شده، به عنوان یک دستورالعمل و راهنما در این زمینه در نظر گرفته شده است. این نقشه اجرایی، به عنوان بخشی از استراتژی، توانش و مسئولیت‌های اجرایی برای اقدامات تعیین شده در این استراتژی را مشخص می‌کند.

۱. این ترجمه واژه Competency می‌باشد.

پیشینه

پیشینه

اولیـن گام بـرای حفاظـت مؤثر کشـور سـوئیس در برابر خطرات سـایبری، ارزیابـی وضعیـت کنونـی و آینـده تهدیـد اسـت. هـدف محاسـبه دقیـق ایـن خطـرات بـرای سـوئیس نیسـت، بلکـه مهـم این‌اسـت کـه تهدیـدات مختلف از نظـر راهبـردی ارزیابـی و دورنمایـی بـرای فراینـد احتمالـی گسـترش آنها ایجاد شـود.

عـلاوه بـر شـرایط تهدید، وضعیت فعلی حفاظت سـوئیس در برابر خطرات سـایبری دومیـن عامـل مهـم در تعیین پیشـینه می باشـد. نیاز آتی بـه اقدام، زمانـی آشـکار می‌شـود که وضعیت تهدید و پیشـرفت آن در آینـده با اقدامات موجود برای محافظت از سـوئیس در برابر خطرات سـایبری مقایسـه شـود.

1. Information and Communication Technologies

بخش اول

بخش اول

وضعیت تهدید سایبری

جهت تعیین منشأ خطرات سایبری، تهدیدات اصلی سوئیس شرح داده می‌شود. لازم به ذکر است که این تهدیدات به شکل بسیار پویا در حال پیشرفت هستند. مهمترین عامل محرک، دیجیتال‌سازی است که جامعه و اقتصاد را به طور فزاینده‌ای در معرض اختلال و نقص سیستم‌های ICT و همچنین وضعیت وخیم تهدید، به دلیل حرفه‌ای شدن مهاجمان و گسترش سیاست‌های قدرت در فضای سایبری قرار می‌دهد. با توجه به اینکه ادامه این روند پیش‌بینی می‌شود، احتمالاً وضعیت تهدید شدت خواهد گرفت.

به منظور ارزیابی این وضعیت، مهم است تا بین تهدیدهای ناشی از اقدامات عمدی غیرمجاز (حملات سایبری) و تهدیدات ناشی از حوادث غیرعمد (خطای انسانی و نقص فنی) تفکیک قائل شویم. بنابراین این تهدیدها در بخش‌های جداگانه زیر شرح داده می‌شود.

۱-۱ حملات سایبری[1]

تهدیدات ناشی از حملات سایبری طی سال‌های اخیر به شدت افزایش یافته است. حملات موفقیت‌آمیز در سوئیس و خارج از کشور با عواقب

1. Cyber Attacks

بعضاً جدی، نشان می‌دهد که نه تنها دفعات و پیچیدگی این حملات سایبری رو به رشد است، بلکه از آن‌ها به صورت هدفمند علیه دولت‌ها و شرکت‌ها نیز استفاده می‌شود.

با توجه به تعداد بالای حملات سایبری احتمالی و به منظور ارزیابی وضعیت، اهمیت دارد که پدیده‌های مختلف از یکدیگر متمایز گردند. این شاخص‌های تمیزدهنده شامل هدف حمله، عوامل حملات و همچنین مجموعه گروه‌های تحت تأثیر می‌باشند. بر این اساس، پنج نوع حمله سایبری را می‌توان مشخص کرد، در حالی که باید توجه داشت که حملات اغلب به صورت ترکیبی صورت گرفته و میان آنها همپوشانی وجود دارد.

جرم سایبری[1]: در مفهومی محدودتر، جرم سایبری به جرایمی گفته می‌شود که با کمک ICT انجام می‌شوند یا از آسیب‌پذیری‌های این فن‌آوری استفاده می‌کنند؛ از این‌رو فقط به دلیل وجود ICT امکان‌پذیرند. به معنای وسیع‌تر، جرم سایبری شامل کلیه جرایم کیفری می‌شود که از ICT به عنوان وسیله ارتکاب یا ذخیره‌سازی استفاده شده، هرچند بدون استفاده از ICT نیز همچنان امکان‌پذیر است. وجه تمایز این جرایم سایبری از طریق انگیزه ارتکاب جرم توصیف می‌شود. فضای سایبری از این جهت برای مجرمان مناسب است، زیرا خطر کمی برای آن‌ها وجود دارد ولی می‌توانند به دلیل تعداد بالای قربانیانی که به راحتی قابل دسترس‌اند، سود قابل توجهی کسب کنند. بنابراین جای تعجب نیست که در سال‌های اخیر جرایم سایبری به شدت افزایش یافته و به همان اندازه بر مشاغل، مسئولین و مردم تأثیر گذاشته است. این تهدیدی است که به احتمال زیاد رخ می‌دهد. در این میان، هدف مهاجمان تنها به خطر انداختن عملکرد جامعه، اقتصاد یا دولت نیست، بلکه تأثیر مستقیم

1. Cybercrime

آن اغلب محدود به قربانیان مربوط به همان جرم می‌شود. با این حال، مجرمان سایبری جریمه بالای خسارت را می‌پذیرند یا حتی از ترس چنین خسارتی، مبالغ بیشتری را از قربانیان اخاذی می‌کنند. به همین دلیل، حملات مجرمان سایبری پتانسیل بالایی برای آسیب رساندن توأمان به جامعه و اقتصاد دارند.

در زمینه جرایم سایبری، خطوط تجاری واقعی شکل می‌گیرند تا امکان تولید پول فراوانی را فراهم کنند. به دلیل رقابت شدید از یک‌سو و به‌روزرسانی پیوسته اقدامات دفاعی از سوی دیگر، فشار برای نوآوری میان عوامل جنایی بالا رفته است. از این‌رو، مهاجمان دائماً در حال ایجاد روش‌های نوین هستند. بر این اساس، بایستی انتظار داشت که تعداد فعالیت های مجرمانه در فضای سایبری رو به افزایش است و تخصصی‌تر نیز می‌شود.

جاسوسی سایبری[1]: جاسوسی سایبری فعالیتی برای دستیابی غیرمجاز به اطلاعات در فضای سایبری برای مقاصد سیاسی، نظامی یا اقتصادی است. این عمل توسط هر دو عوامل دولتی و غیردولتی انجام می‌شود. مهاجمان بر شرکت‌ها و همچنین نهادهای دولتی، اجتماعی و بین‌المللی تمرکز می‌کنند. اقتصاد سوئیس یکی از نوآورترین اقتصادها در جهان است و بسیاری از دفاتر اصلی و یا مراکز داده شرکت‌های بین‌المللی در اینجا مستقر می‌باشند. سوئیس همچنین میزبان بسیاری از مذاکرات و سازمان‌های بین‌المللی است. این امر سوئیس را به یک هدف جذاب برای جاسوسی اینترنتی تبدیل می‌کند. این تأثیر بسته به نوع و حجم داده‌ای که مهاجمان به آن دسترسی پیدا می‌کنند، می‌تواند بسیار متفاوت باشد. این تأثیر معمولاً بلافاصله آشکار نمی‌شود، زیرا نواقص سیاسی و اقتصادی

1. Cyber Espionage

تنهـا زمانـی مشـاهده می‌شـود که مهاجمان از دانشـی کـه به‌دسـت آورده‌اند، اسـتفاده کنند.

بـا توجـه بـه اینکـه جاسوسـی سـایبری روشـی کارآمـد بـرای جمع‌آوری اطلاعـات می‌باشـد، از جذابیـت بیشـتری برخـوردار خواهـد بـود. مهاجمـان روش‌هایـی را ایجـاد کرده‌انـد کـه تـا حد امـکان پـس از نفوذ در شـبکه‌ها نیز پنهـان بمانند. از آنجا که سـوئیس از نظر فناوری اطلاعـات و ارتباطات (ICT) وابسـتگی زیـادی بـه تولیدکننـدگان خارجـی دارد، این خطر همچنـان وجود دارد کـه ایـن تولیدکننـدگان، با همکاری سـرویس‌های اطلاعاتی کشورشـان، بـه طـور عمد فضای مناسـب بـرای مقاصد جاسوسـی را فراهـم کنند.

خرابـکاری سـایبری[1] و تروریسـم سـایبری[2]: خرابکاری سـایبری به فعالیت‌هایـی اطـلاق می‌شـود که هـدف آن ایجـاد اختلال یا تخریـب عملکرد قابـل اعتمـاد و بـدون خطای ICT در فضای سـایبری اسـت که بسـته به نوع خرابـکاری و هـدف حملـه، ممکـن اسـت اثـرات فیزیکی نیـز به‌همراه داشـته باشـد. انگیـزه چنین اقداماتـی می‌تواند به میـزان قابل توجهی متفاوت باشـد. بـه عنـوان مثـال، کارمنـدان ناامیـد ممکـن اسـت تصمیـم بگیرنـد ICT یک سـازمان را خـراب کنند. از سـوی دیگـر، اگر اقدام خرابکارانه توسـط عواملی با انگیزه تروریسـتی انجام شـود، از آن به عنوان تروریسـم سـایبری یاد می‌شود. هدف از خرابکاری و تروریسـم سـایبری نه تنها دسـتیابی به بیشـترین آسیب ممکـن اسـت، بلکه ایجـاد ارعاب و نمایش قـدرت با هدف بی‌ثبات‌سـازی یک سـازمان یـا حتـی کل جامعـه می‌باشـد. هرچند اقدامـات خرابـکاری متفاوتی در سـطح بین‌المللـی، از جملـه علیه تأمین انرژی دولت‌ها مشـاهده شـده، اما تاکنـون مـوارد عمده‌ای در سـوئیس گزارش نشـده اسـت. با ایـن حال ممکن اسـت سـازمان‌های داخلـی یـا خارجی سوئیسـی به دلایل سیاسـی، از سـوی

1. Cyber Sabotage
2. Cyber Terrorism

عوامـل دولتـی یـا غیردولتی مورد هـدف قرار گیرنـد؛ بنابرایـن احتمال چنین رخـدادی بـه میـزان قابل توجهـی افزایش یافته و آسـیب احتمالی نیز بسـیار زیاد اسـت.

ایـن تهدیـد بـا دیجیتال‌سـازی تدریجی جامعـه و اقتصاد همچنـان افزایش خواهـد یافـت. شبکه‌سـازی دیجیتـال دسـتگاه‌های فیزیکی از طریـق اینترنت، اشـکال جدیـدی از دسـتکاری دیجیتالـی را ایجاد کرده که تأثیری مسـتقیم بر دنیـای فیزیکی خواهد داشـت.

اطلاعات نادرسـت[1] و پروپاگاندا: تهدید ناشـی از انتشار هدفمند اطلاعات نادرسـت یـا اطلاعاتی که به طـور غیرقانونی از طریق حملات سـایبری با هدف بی‌اعتبـار کـردن عوامـل سیاسـی، نظامی یا جامعه مدنی به دسـت آمده اسـت، بیـش از پیـش مـورد توجـه قـرار گرفته اسـت. چنیـن فعالیت‌هایی در آسـتانه انتخابـات میـان‌دوره و اصلـی در کشـورهای مختلـف مشـاهده شـده اسـت. در کشـور سـوئیس نیـز ایـن احتمـال را بایـد در نظـر گرفت کـه عوامـل دولتی یا غیردولتـی ممکـن اسـت به دنبال تـلاش در جهـت تضعیف اعتماد شـهروندان بـه دولت و نهادها باشـند.

بـا توجـه بـه اینکـه اهمیـت رسـانه‌های اجتماعی بـه عنوان منبـع اطلاعات در حـال افزایـش اسـت، بایـد ایـن فـرض را در نظـر گرفت کـه می‌تـوان از این کانال‌ها برای مقاصد تبلیغاتی با ترکیبی کاملاً غیرشـفاف از اطلاعات نادرسـت، اسـتدلال‌های سیاسـی و اطلاعات سـرقتی بهـره برد.

حمـلات سـایبری در تعارضات: هنگامی‌کـه جنگی به طـور انحصاری در فضای سـایبری (جنگ سـایبری) رخ می‌دهد، سـناریو غیرواقعی تلقی می‌شود، حـال آنکـه از انواع حملات سـایبری به عنـوان ابزار جنـگ در تعارضات مختلف اسـتفاده شـده اسـت. معمولاً، در ایـن تعارضات ترکیبی علاوه بـر نیروی نظامی

۱. Disinformation در برخی منابع گمراه‌سازی یا دوروغ پراکنی نیز ترجمه شده است.

از ابزارهـای سیاسـی، اقتصـادی و جنایی نیز اسـتفاده می‌شـود. یکـی از اهداف جنـگ ترکیبـی، پنهـان کـردن مسـئولیت‌ها در تعـارض می‌باشـد. حمـلات سـایبری یـک ابزار اثبات شـده بـرای این منظور به‌شـمار می‌رود، زیـرا افزون بر تأثیـر فـوری و بسـیار کم‌هزینه آن‌ها عموماً به‌سـختی قابل تشـخیص هسـتند. درنتیجـه می‌تواننـد در مقیـاس بـزرگ و بـا اثـرات سیاسـی-نظامی در منطقـه خاکسـتری زیـر آسـتانه یک جنـگ واقعی بـه‌کار گرفته شـوند[1].

سـرمایه‌گذاری‌های قابـل توجـه کـه توسـط بسـیاری از دولت‌هـا بـه منظور حفاظـت و دفـاع فعالانـه در برابـر تهدیـدات سـایبری انجـام گرفته، بـر اهمیت منابـع سـایبری در تعارضـات تأکیـد می‌کنـد. بنابرایـن، انتظار مـی‌رود اهمیت حمـلات سـایبری هدفمنـد برای اهداف اسـتراتژیک بیشـتر افزایش یابـد. برای پیشـگیری از چنین فعالیت‌هایی، سوئیس بایسـتی اقدامات لازم در زمینه دفاع سـایبری و دیپلماسـی سـایبری بـرای تعارض‌هـای احتمالی را در نظـر بگیرد.

۲-۱ خطای انسانی و نقص فنی

علاوه بر حملات سـایبری هدفمند و عمدی، اقدامات غیرعمدی یا حوادث طبیعـی و فناورانـه نیـز ممکـن اسـت منجـر بـه آسـیب در فضـای سـایبری یا محیط فیزیکی شـوند. این حوادث ناشـی از خطای انسـانی در تأمین و اسـتفاده از ICT (به عنوان مثال بی‌احتیاطی یا اسـتفاده نادرسـت از سیسـتم‌های ICT، مدیریـت یـا پیکربندی معیوب، از دسـت دادن حامل‌هـای داده و غیره) یا نقص فنـی اسـت کـه خود مـی‌توانـد دلایـل مختلفی داشـته باشـد (زیرسـاخت‌های قدیمـی یـا حـوادث طبیعی، اسـتفاده بیـش از حـد، طراحی معیـوب، نگهداری ناکافـی). رویدادهایـی از ایـن دسـت غالبـاً بـا درجـات متفاوتـی رخ می‌دهـد و بخشـی از امـور روزمـره ادارات ICT در مشـاغل و مقامـات دولتی اسـت. بر این

۱. مفهوم کلی این جمله اشاره دارد به اقداماتی که می‌تواند مانند تبلیغات زیرآستانه حسی، بدون دیده شدن، همانند یک جنگ واقعی، اثرات مخرب سیاسی_نظامی داشته باشند.

اساس، به طور کلی می‌توان تأثیرات این خطاها و شکست‌ها را به خوبی کنترل کرد. با این وجود، تجربه نشان داده است که بسیاری از حوادث مهم سایبری نتیجه حملات هدفمند نیست، بلکه بیشتر ناشی از زنجیره شرایط متفاوت مانند خطای انسانی یا نقص فنی همراه با آماده‌سازی نامناسب است. اقدامات پیشگیرانه در برابر چنین رویدادهایی نباید در برنامه‌ریزی و اجرای اقدامات حفاظتی نادیده گرفته شود.

خطرات سایبری ناشی از خطای انسانی یا نواقص فنی بسیار حائز اهمیت است. پیچیدگی فزاینده به دلیل شبکه‌سازی محدوده وسیعی از مناطق، تخمین و محدودکردن، میزان تأثیر این رویدادهای ناخواسته را با دشواری روبرو می‌کند. بنابراین تمهیدات مناسب و برنامه‌ریزی پیشگیرانه برای چنین حوادثی از عناصر اصلی برای مقابله با خطرات سایبری به‌شمار می‌رود.

بخش دوم

بخش دوم

وضعیت کنونی حفاظت در برابر خطرات سایبری در سوئیس

تا به امروز، اولین استراتژی NCS، پایه و اساس کار محسوب می‌شد که در سال ۲۰۱۲ تصویب و تا پایان سال ۲۰۱۷ اجرا شد. اما مفاد استراتژیک NCS نیز باید مد نظر قرار گیرد. استراتژی‌های متفاوت دولت فدرال تأثیر مستقیمی بر چگونگی محافظت سوئیس در برابر خطرات سایبری دارد و ازاین‌رو چارچوبی برای فعالیت‌های آتی ایجاد می‌کند.

۱-۲ استراتژی ملی برای محافظت از سوئیس در برابر خطرات سایبری ۲۰۱۷-۲۰۱۲

اولین استراتژی NCS شامل ۱۶ اقدام بود که به صورت غیرمتمرکز توسط واحدهای سازمانی ذی‌صلاح در دولت فدرال با همکاری انجمن‌ها و مجریان زیرساخت‌های حیاتی اجرا شد. نتایج NCS به طور مفصل در گزارش ارزیابی[1] MCS شرح داده شده است. به منظور ارزیابی پیشینه NCS 2018-2022 ، اهدافی که توسط NCS محقق شد، حائز اهمیت است:

- **ایجاد ظرفیت‌ها، توانایی‌ها و دانش:** نگرانی اصلی NCS ایجاد ظرفیت‌ها، توانایی‌ها و دانش در سازمان‌های ذی‌صلاح بود. در سال ۲۰۱۲ مشخص شد که بسیاری از مناطق، فاقد منابع و تخصص لازم می‌باشند که با

1. https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/ncs_strategie-2012/wirksamkeitsueberpruefung.html

اجرای اقدامات NCS، اوضاع بهبود یافته است.

- **ایجاد فرایندها، ساختارها و بنیان‌ها:** از آنجا که خطرات سایبری عاملان بسیاری را تحت تأثیر قرار می‌دهد، سازماندهی همکاری بین مسئولان مختلف، تخصیص مسئولیت‌ها و توسعه بنیان‌ها بسیار اهمیت دارد. فرایندهای برنامه‌ریزی شده، ساختارها و مبانی‌ها ایجاد شده‌اند، حال بایستی مورد استفاده قرار گیرند و به طور پیوسته توسعه داده شوند.

- **تمرکز بر حفاظت از زیرساخت‌های حیاتی:** اقدامات NCS عمدتاً مربوط به حفاظت از زیرساخت‌های حیاتی می‌باشد. تحلیل‌های ریسک و آسیب‌پذیری برای زیر بخش‌های مهم، تعیین اقدامات، گسترش پشتیبانی در صورت بروز حوادث و تصویری از وضعیت تهدیدات سایبری انجام شد. با این کار هسته اصلی NCS شکل گرفت و اکنون می‌تواند تعمیق و گسترش یابد.

- **تقویت همکاری با اشخاص ثالث:** علاوه بر بهبود هماهنگی در داخل دولت، همکاری با سایر شرکا نیز مهم است. NCS همکاری با کانتون‌ها، بخش خصوصی و شرکای مختلف بین‌المللی را تقویت کرده است. ایجاد این مقدمات همکاری باعث تقویت اعتماد متقابل و ارتقای تبادل اطلاعات شده و زمینه مناسبی جهت تعمیق و گسترش بیشتر همکاری در همه سطوح را فراهم می‌کند.

۲-۲ مفاد استراتژیک

استراتژی‌های مختلف دولت فدرال، دستورالعمل‌های مرتبط با موضوع خطرات سایبری را تعریف می‌کند و مفاد استراتژیک برای حفاظت

سوئیس در برابر خطرات سایبری را تشکیل می‌دهند. استراتژی‌های اساسی عبارتند از:

- **گزارش انجمن فدرال در مورد سیاست امنیتی سوئیس:** در گزارش سیاست امنیتی سال ۲۰۱۶، انجمن فدرال، گرایش راهبردی اصلی سیاست امنیتی سوئیس را تعریف می‌کند. این گزارش اهمیت عمده و روبه‌رشد تهدیدهای سایبری برای سیاست امنیتی را توضیح می‌دهد و اصطلاحات مهمی را در مفاد موضوع تعریف می‌کند. در این گزارش، با ذکر NCS به عنوان مبنایی جهت حفاظت سوئیس در برابر خطرات سایبری تأکید می‌شود که محافظت از سیستم‌ها و زیرساخت‌های ICT باید در سیاست امنیتی آتی نقش بیشتری داشته باشند.
- **استراتژی انجمن فدرال برای سوئیس دیجیتالی:** این استراتژی نشان می‌دهد که چگونه سوئیس تمایل دارد تا از فرصت‌هایی که توسط دیجیتال‌سازی به‌وجود آمده، استفاده کند. یکی از اهداف راهبردی اصلی، ایجاد شفافیت و امنیت است تا مردم سوئیس قادر باشند از امکان خود-مختاری[1] در ارتباط با اطلاعاتی که به آن‌ها مربوط است، بهره ببرند. به عنوان پیش‌نیاز، دولت باید به وظیفه خود در زمینه محافظت از جامعه و اقتصاد در عصر دیجیتال ادامه دهد. علاوه بر این، راهبرد و برنامه عملیاتی به تعریف اهداف می‌پردازد و اقدامات لازم برای موقعیت‌یابی سوئیس در حوزه دیجیتال‌سازی و فرایندهای تحول در محیط بین‌المللی را مشخص می‌کند. در زمینه امنیت سایبری، این امر به طور خاص از طریق اجرای NCS حاصل می‌شود.

1. Self-Determination

- **استراتژی ملی برای حفاظت از زیرساخت حیاتی**[1]: استراتژی CIP به تعریف واژه «زیرساخت‌های حیاتی» می‌پردازد و مشخص می‌کند که کدام بخش‌ها و زیرشاخه‌ها در سوئیس مهم تلقی می‌شوند. این راهبرد شامل اقداماتی می‌باشد که هدف آن بهبود انعطاف‌پذیری سوئیس در برابر زیرساخت‌های حیاتی است. استراتژی NCS تمام خطرات زیرساخت‌های حیاتی در حوزه سایبری را پوشش می‌دهد.

1. Critical Infrastructure Protection

بخش سوم

بخش سوم

اقدام مورد نیاز: توسعه بیشتر مورد نیاز: NCS

اهداف تعیین شده در اولین NCS محقق گردید و مفاد راهبردی، اساس کار بیشتر را فراهم آورد. اما مقایسه بین وضعیت تهدید فعلی و توسعهٔ مورد انتظار بر پایه تمهیدات فعلی برای حفاظت سوئیس در برابر خطرات سایبری، به وضوح نشان می‌دهد که حفظ وضعیت کنونی برای اطمینان از سطح مناسب حفاظت کافی نمی‌باشد. ازاین‌رو در سطوح مختلف نیاز به اقدام می‌باشد. از یک سو، هدف این است که ظرفیت‌ها و توانایی‌هایی موجود و بهره‌وری از فرایندها، ساختارها و مبانی‌ها، برای اجرای اقدامات گسترش یابند. از سوی دیگر، تطابق‌های استراتژیک نیز باید انجام شود. استراتژی NCS باید به عنوان یک استراتژی ملی فراتر از دولت فدرال و زیرساخت‌های مهم، به طور مؤثرتری عمل کند تا عدالت را نسبت به این واقعیت که تهدیدات سایبری بر کل اقتصاد، جامعه و حوزه سیاسی تأثیر می‌گذارد، اعمال کند. برای این منظور، باید گروه هدف NCS و همکاری‌های موجود گسترش یابد تا شبکه‌ای برای حفاظت سوئیس در برابر خطرات سایبری ایجاد شود. در نهایت، ساختار سازمانی غیرمتمرکز به واسطه مدیریت استراتژیک قوی‌تر و یک مرکز تماس برای عموم تکمیل گردد، به‌گونه‌ای که توانایی پاسخگویی به پیشرفت‌های جدید

با توجه به خطرات بسیار پویای سایبری را داشته باشد و مردم و سیاست‌گذاران بتوانند شناخت بیشتری از NCS کسب کنند.

سطح	استراتژی NCS ۲۰۱۲-۲۰۱۷	اقدام موردنیاز
ظرفیت‌ها، قابلیت‌ها و دانش	افزایش ظرفیت‌ها و دانش بهتر نسبت به سال ۲۰۱۲	گسترش بیشتر ظرفیت‌ها و دانش جهت اجرای عدالت در وضعیت وخیم تهدیدی ضروری است.
اهداف اقدامات NCS	ایجاد فرایندها، ساختارها و مبانی‌ها	استفاده سودمند از فرآیندها، ساختارها و مبانی‌ها جهت کاهش خطرات سایبری. اقدامات و خروجی‌های موردنظر بایستی پیاده‌سازی شوند، توسعه یابند و در صورت لزوم، تکمیل شوند.
ساختار سازمانی	اجرا به روش غیرمتمرکز توسط مقامات ذی‌صلاح انجام می‌شود.	افزایش ارتباط سیاسی، اقتصادی و اجتماعی و توسعه سریع خطرات سایبری، نیاز به مدیریت استراتژیک قوی‌تری از NCS را طلب می‌کند. ساختار سازمانی غیرمتمرکز باید به همین منظور تکمیل شود.
گروه‌های هدف	تمرکز بر محافظت از زیرساخت‌های حیاتی در برابر خطرات سایبری	تهدیدات سایبری کل سوئیس را تحت تأثیر قرار می‌دهد، ازاین‌رو گروه هدف NCS باید گسترش یابد.
همکاری	ایجاد همکاری با کانتون‌ها، بخش خصوصی و شرکای بین‌المللی	افزایش ارتباط متقابل، اهمیت همکاری در همه سطوح را تقویت می‌کند. جهت ایجاد شبکه‌ای برای حفاظت سوئیس در برابر خطرات سایبری، مقدمات همکاری موجود و مشارکت‌های دولتی-خصوصی باید تقویت گردند و به هم پیوند داده شوند.

جدول ۱- خلاصه‌ای از اقدام موردنیاز

هـدف دومیـن NCS ایـن اسـت کـه کار NCS اول را ادامـه، در صـورت لـزوم توسـعه داده و بـا اقدامـات جدیـد تکمیـل کنـد. افـزون بر حفـظ تـداوم کار NCS، اول می‌بایسـت اطمینـان حاصـل کرد کـه اهداف، اصـول، حوزه‌هـای عملکردی و اقدامـات آن متناسـب با تحولات از سـال ۲۰۱۲ رعایت شـوند و روندهـای آتی را حتـی الامکان پیش‌بینـی کند.

بخش چهارم

بخش چهارم

جهت‌گیری استراتژیک 2018-2022 NCS

جهت‌گیری استراتژیک بر پایهٔ اقدام مورد نیاز که در 2018-2022 NCS، شناسایی شد، مشخص می‌شود. این چشم‌انداز و اهداف استراتژیک آنچه که باید در این دوره محقق شود را تعیین می‌کند، چگونگی انجام امور توسط اصول استراتژیک شرح داده می‌شود، و بخش مربوط به گروه‌های هدف مشخص می‌کند که استراتژی باید خطاب به چه کسانی باشد.

۴-۱ چشم‌انداز و اهداف استراتژیک

از آنجا که خطرات سایبری همزمان دامنه وسیعی از اقتصاد، سیاست و جامعه را تحت تأثیر قرار می‌دهد، اقداماتی در زمینه‌های مختلف مورد نیاز می‌باشد. برای حفظ انسجام استراتژی در این تنوع، پیگیری یک چشم انداز مشترک و تدوین اهداف راهبردی اساسی بسیار حائز اهمیت است.

چشم‌انداز 2018-2022 NCS

سوئیس در بهره‌برداری از فرصت‌های دیجیتال‌سازی، به اندازه کافی در برابر خطرات سایبری حفاظت می‌شود و در برابر آنها انعطاف‌پذیر است.

ظرفیت عملکرد و تمامیت جمعیت، اقتصاد و کشور در برابر تهدیدات سایبری ایمن هستند.

اهداف استراتژیک:

این چشم‌انداز تنها در صورت تحقق هفت هدف استراتژیک NCS 2022-2018 به شرح ذیل قابل درک است:

- سوئیس از توانش‌ها، دانش و قابلیت‌های لازم برای شناسایی و ارزیابی خطرات سایبری در مراحل اولیه برخوردار است.
- سوئیس در حال تدوین اقدامات مؤثر برای کاهش خطرات سایبری است و آنها را در چارچوب پیشگیری اجرا می‌کند.
- سوئیس از ظرفیت‌ها و ساختارهای سازمانی لازم در همه شرایط برای شناسایی سریع حوادث سایبری و مقابله با آنها برخوردار است، حتی اگر در مدت زمان طولانی ادامه یابند و مناطق مختلف را به طور همزمان تحت تأثیر قرار دهند.
- سوئیس در برابر خطرات سایبری انعطاف‌پذیر است و از توانایی زیرساخت‌های حیاتی در ارائه خدمات و کالاهای اساسی حتی در صورت وقوع حوادث بزرگ سایبری نیز حراست می‌شود.
- محافظت از سوئیس در برابر خطرات سایبری مسئولیت مشترک جامعه، بخش خصوصی و دولت است. تعیین و اجرای مشخص مسئولیت‌ها و توانش‌ها نیز از سوی همه افرادی که در ارتباط هستند، صورت می‌گیرد.
- سوئیس متعهد به همکاری بین‌المللی برای افزایش امنیت سایبری است و مذاکره در زمینه سیاست خارجی و امنیتی سایبری را ترویج

می‌بخشد. همچنین به طور فعال در نهادهای متخصص بین‌المللی شرکت کرده و با سایر کشورها و سازمان‌های بین‌المللی تبادل برقرار می‌کند.

- سوئیس از حوادث سایبری در داخل و خارج کشور درس می‌گیرد. حوادث سایبری به دقت مورد تجزیه و تحلیل قرار گرفته و اقدامات مناسبی بر اساس یافته‌ها اخذ می‌شود.

۲-۴ اصول

چشم‌انداز و اهداف استراتژیک به تعیین آنچه NCS 2018-2022 درصدد دستیابی است، می‌پردازد. این اصول، چگونگی انجام این کار را مشخص می‌کند.

- NCS با رویکرد جامع مبتنی بر ریسک[1]، بهبود انعطاف‌پذیری سوئیس در برابر خطرات سایبری را مدنظر قرار داده است. این مطلب اشاره به قبول این فرض دارد که حفاظت کامل در برابر خطرات سایبری امکان‌پذیر نیست، اما تا آنجا که خطر باقی مانده قابل قبول باشد می‌توان با خطرات کنار آمد. یک رویکرد جامع تمام آسیب‌پذیری‌ها و تهدیدهای مربوطه را در نظر می‌گیرد.

- امنیت سایبری تقریباً بر تمام زمینه‌های زندگی، مشاغل و امور اداری اثر می‌گذارد. از همه درخواست می‌شود به منظور حفاظت سوئیس در برابر خطرات سایبری اقدام کنند و در مسئولیت آن سهیم باشند. استراتژی NCS به کمک مسئولین دارای توانش‌های لازم و از طریق ساختارهای موجود، این مسئولیت مشترک را تقویت می‌کند. این امر اجرای غیرمتمرکزی[2] را در پی دارد اما این اجرا از طریق شیوه‌ای متمرکز توسط مدیریت استراتژیک NCS کنترل می‌شود و بدین‌ترتیب تقسیم‌بندی مشخص وظایف و نقش‌ها را پیش‌بینی می‌کند.

1. Risk-Based,Comprehensive Approach
2. Decentralized Implementation

- NCS مبتنی بر درک نقش فرعی دولت[1] است، به این معنی که دولت فقط زمانی مداخله می‌کند که رفاه جامعه ما به طور قابل ملاحظه‌ای تحت تأثیر قرار گیرد و مسئولان خصوصی قادر نباشند یا تمایلی به حل مسئله به طور مستقل نداشته باشند. در این حالت، دولت می‌تواند از طریق وضع مقررات، به حمایت، ایجاد انگیزه یا مداخله بپردازد.
- NCS بر پایه یک رویکرد همکاری، شراکت خصوصی-عمومی[2] موجود در سطح ملی را تقویت و هماهنگ می‌کند، مقدمات همکاری دولتی-خصوصی را ارتقا داده و همکاری بین دولت فدرال، کانتون‌ها و بخش‌ها را گسترش می‌دهد.
- NCS همکاری با شرکای بین‌المللی[3] را در سطح بین‌المللی ارتقا می‌دهد.
- اجرای NCS شفاف است، مشروط بر اینکه در اثربخشی اقدامات تداخلی ایجاد نکند. این امر از طریق ارتباط فعال، متقابل و دوسویه NCS با جامعه، بخش خصوصی و سیاست‌گذاران حاصل می‌شود.

۳-۴ گروه‌های هدف

دولت فدرال از طریق NCS، متعهد به اجرای اقدامات توصیف شده با همکاری کانتون‌ها، بخش خصوصی و جامعه می‌شود. بنابراین تأثیر مورد نظر NCS مربوط به کل سوئیس است. NCS صراحتاً گروه‌های زیر را مخاطب قرار می‌دهد:

- **زیرساخت‌های حیاتی:** گروه هدف اصلی NCS، اپراتورهای زیرساخت‌های حیاتی می‌باشند که دسترسی به کالاها و خدمات ضروری

1. Subsidiary role of the state
2. Public-private partnership
3. Cooperation with international partners

را تضمین می‌کنند و عملکردشان برای جمعیت و اقتصاد سوئیس مهم است. از این‌رو حفاظت آنها از اولویت بالاتری برخوردار بوده و در تمام اقدامات NCS مورد توجه قرار گرفته است.

- **مقامات دولتی:** زیرساخت‌های حیاتی شامل خدمات ادارات و مقامات دولتی می‌باشند. دولت فدرال، کانتون‌ها و بخش‌ها مسئولیت مستقیم حفاظت از آنها را بر عهده دارند.
- **عموم مردم:** حمایت از عموم مردم هدف نهایی کلیه اقدامات NCS است (به عنوان مثال حفاظت در برابر نواقص زیرساخت‌های حیاتی). اما تمرکز به طور خاص بر روی جرایم سایبری است. استراتژی NCS از طریق اطلاعات شفاف به عموم مردم کمک می‌کند تا از ICT به عنوان روشی ایمن، آگاهانه و مطمئن استفاده شود.
- **بخش خصوصی:** یک محیط امن و قابل اعتماد، پایه و اساس مهمی برای اقتصاد به‌شمار می‌رود. خطرات سایبری نه تنها زیرساخت‌های حیاتی، بلکه کلیه شرکت‌ها به ویژه شرکت‌های تجاری کوچک و متوسط[1] را با چالش‌های اساسی مواجه می‌کند. استراتژی NCS ایمن‌ترین شرایط ممکن را برای شرکت‌های سوئیسی به‌منظور مقابله با خطرات سایبری از یک‌سو و پشتیبانی هدفمندی را از سوی دیگر در شکل شرکت تابعه[2] که توسط بازار ارائه می‌شود، فراهم می‌کند.

1. SMEs: Small and Mid-size Enterprises
2. Subsidiary Basis

بخش پنجم

بخش پنجم

حـوزه عملیـات واقدامات NCS 2018-2022

بـرای دسـتیابی بـه اهـداف اسـتراتژیک، اقدامـات بایـد در محدوده بسـیار گسـترده‌ای اجـرا شـود. NCS ۱۰ حـوزه عملیاتـی کـه جنبه‌هـای مختلـف خطرات سـایبری را بررسـی می‌کننـد، از یکدیگر تفکیک می‌کنـد. در مجموع ۲۹ اقـدام در ایـن حوزه‌هـای عملیاتـی تدوین شـده اسـت.

جدول ۲- لیست حوزه‌های عملیات و اقدامات NCS 2018-2022

حوزه عملیات	اقدامات
ایجاد توانش‌ها و دانش	۱. شناسایی اولیه روندها و فناوری‌ها و تولید دانش ۲. گسترش و ارتقای توانش‌های پژوهشی و آموزشی ۳. ایجاد چارچوبی مطلوب برای اقتصاد نوآورانه امنیت ICT در سوئیس
وضعیت تهدید	۴. گسترش قابلیت‌های ارزیابی و ارائه وضعیت تهدیدات سایبری
مدیریت مقاومتی (انعطاف‌پذیر)	۵. بهبود انعطاف‌پذیری ICT در زیرساخت‌های حیاتی ۶. بهبود انعطاف‌پذیری ICT در دولت فدرال ۷. تبادل تجربه و ایجاد مبانی‌ها برای بهبود انعطاف‌پذیری ICT در کانتون‌ها
استانداردسازی/مقررات	۸. ارزیابی و معرفی حداقل استانداردها ۹. بررسی الزام گزارش حوادث سایبری و تصمیم در مورد معرفی ۱۰. حاکمیت جهانی اینترنت ۱۱. ایجاد تخصص در مورد مسائل استانداردسازی مربوط به امنیت سایبری

حوزه عملیات	اقدامات
مدیریت حوادث	۱۲. گسترش MELANI به عنوان شراکت خصوصی-عمومی برای اپراتورهای زیرساخت‌های حیاتی ۱۳. توسعه خدمات برای همه شرکت‌ها ۱۴. همکاری بین دولت فدرال و عاملیت‌های ذی ربط و مراکز توانش ۱۵. فرآیندها و مبانی مدیریت حوادث دولت فدرال
مدیریت بحران	۱۶. ادغام دفاتر مسئول امنیت سایبری در تیم‌های بحران فدرال ۱۷. تمرینات مشترک مدیریت بحران
پیگرد قانونی	۱۸. تصویری از وضعیت جرایم سایبری ۱۹. شبکه پشتیبانی برای رسیدگی به اجرای قانون دیجیتال ۲۰. آموزش ۲۱. دفتر مرکزی برای دفاع سایبری جرایم سایبری
دفاع سایبری	۲۲. گسترش قابلیت‌های جمع‌آوری اطلاعات و انتساب ۲۳. قابلیت اجرای اقدامات پویا در فضای سایبری تحت IntelSA و ArmA ۲۴. اطمینان از آمادگی عملیاتی نیروهای مسلح در همه اوضاع موجود در فضای سایبری و تعیین نقش کمکی آنها در حمایت از مقامات غیرنظامی
موضع‌گیری پویای سوئیس در سیاست بین‌المللی امنیت سایبری	۲۵. شکل‌گیری فعال و مشارکت در فرایندهای سیاست امنیت سایبری خارجی ۲۶. همکاری بین‌المللی جهت ایجاد و گسترش ظرفیت‌های امنیت سایبری ۲۷. رایزنی‌های سیاسی دو جانبه و گفتگوی چند جانبه در مورد سیاست امنیت سایبری خارجی
افزایش آگاهی و اثربخشی بر عموم	۲۸. ایجاد و اجرای یک مفهوم ارتباطی برای NCS ۲۹. افزایش آگاهی عموم از خطرات سایبری

در ادامه، حوزه‌های عملیاتی و اقدامات با جزئیات بیشتری شرح داده شده است. در حال حاضر این سؤال که کدام ارگان باید مسئولیت اقدامات را بپذیرد و آیا مبانی قانونی اقدامات قبلاً وجود داشته یا لازم است ایجاد شوند، از این موضوع مستثنی هستند. این سؤالات قرار است در برنامه اجرایی مطرح شوند.

۵-۱ ایجاد توانش‌ها و دانش

مروری بر حوزه عملیات	
شرح	شناسایی در اسرع وقت و ارزیابی صحیح خطرات سایبری پیش‌شرط کاهش این خطرات می‌باشد. جهت انجام کار، ذینفعان بخش خصوصی، جامعه و مسئولین دولتی، توأمان به توانش‌های اساسی و تخصص خاص نیاز دارند. قرار است توانایی‌های مربوطه به صورت میان‌رشته‌ای از طریق مؤسسات آموزشی و پژوهشی موجود ایجاد، انتقال و توسعه یابد. تنوع و ماهیت بسیار پویای خطرات سایبری به ویژه در این زمینه چالش‌برانگیز است.
پیشینه	سوئیس میزبان شبکه‌ای با عملکرد بالا از مؤسسات آموزشی و پژوهشی در تمام سطوح است. به دلیل توسعه سریع خطرات سایبری، نیاز به توانش‌ها و دانش متناظر به طور چشمگیری افزایش یافته است. در حال حاضر، دانش و نیروی متخصص خاص در زمینه‌های مختلف مرتبط با خطرات سایبری با کمبود روبرو می‌باشد. این امر محافظت در برابر خطرات سایبری را دشوار کرده و فرصت‌های بخش خصوصی را به منظور قرارگرفتن در بازار ایمن رو به رشد ICT، محدود می‌سازد. به طور کلی، شناسایی روندها و فناوری‌های مهم در مراحل اولیه همچنان یک چالش اساسی به‌شمار می‌رود. تاکنون، با در نظر گرفتن جنبه‌های بین‌المللی، هیچ ارزیابی سیستماتیک و هماهنگی از این روندها و فناوری‌ها صورت نگرفته است.
اهداف و اقدام مورد نیاز	سوئیس به عنوان یک مرکز آموزشی و پژوهشی باید بر موضوع خطرات سایبری توجه درخوری داشته باشد و توانش‌های لازم و یافته‌های تحقیقاتی را در اختیار جامعه، بخش خصوصی و مقامات دولتی قرار دهد. روندها و فن‌آوری‌های جدید در زمینه امنیت سایبری باید از همان ابتدا مشخص شود تا با آماده‌سازی سوئیس برای خطرات احتمالی بتواند در اسرع وقت اقدامات مناسب را انجام دهد. بخش خصوصی باید با همراه داشتن دانش کافی و متخصصانی در این حوزه بتواند به

مروری بر حوزه عملیات	
اهداف و اقدام مورد نیاز	طور صحیح با خطرات سایبری مقابله کند و از فرصت های ارائه شده توسط بازار ایمن ICT در حال ظهور بهره ببرد. در این زمینه، باید بررسی شود که آیا با تقویت همکاری بین بخش خصوصی، مؤسسات تحقیقاتی و دولت، می‌توان راه‌حل‌های روبه‌رشد امنیت ICT را در سوئیس تولید کرد، تا بدین‌ترتیب چارچوب راه‌حل‌های نوآورانه در زمینه امنیت ICT و همچنین تولید و توزیع آنها بهبود بخشد. اساس دستیابی به این اهداف با تحقیق در زمینه امنیت سایبری فراهم می‌شود. چنین تحقیقاتی نه تنها برای ایجاد دانش تخصصی و شناسایی زود هنگام روندها و فن‌آوری‌ها اهمیت دارد، بلکه به کمک تبادل دانش بین مؤسسات تحقیقاتی و بخش خصوصی، فضای قابل توجهی برای پرسنل متخصص و شرکت‌های خلاق ایجاد می‌کند. از این‌رو، تحقیقات در زمینه بین رشته‌ای باید به بهترین شکل ممکن انجام گردد.

اقدامات
۱) شناسایی اولیه روندها و فناوری‌ها و تولید دانش روندها و فن‌آوری‌ها در بخش ICT و فرصت‌ها و خطرات ناشی از آن باید در فواصل منظم و در مراحل اولیه شناسایی شوند. نتایج این نظارت به ذینفعان در بخش‌های تحقیقاتی، خصوصی، دولتی و جامعه ابلاغ می‌شود. تحقیقات پایه و کاربردی در صورت لزوم و در حد امکان در چارچوب روش‌ها و فرایندهای موجود (به عنوان مثال از طریق برنامه‌های تحقیقاتی ملی) ارتقا می‌یابند.
۲) گسترش و ارتقای توانش‌سازی در تبادلی بین بخش خصوصی، دانشگاه‌ها، دولت فدرال و کانتون‌ها، نیاز به ایجاد توانش در خطرات سایبری مورد تجزیه و تحلیل قرار می‌گیرد. به‌ویژه، بر این مطلب نیز تأکید می‌شود که چگونه موضوع خطرات سایبری به‌طور روزافزونی در واحدهای درسی فعلی وارد می‌شود.
۳) ایجاد چارچوبی مطلوب برای اقتصاد نوآورانه امنیت ICT در سوئیس سوئیس باید مکانی جذاب برای شرکت‌ها در زمینه امنیت ICT باشد. افزایش تبادل بین بخش خصوصی و تحقیقاتی باید به ارتقای شرکت‌های استارت‌آپ نوآور در این زمینه کمک کند. برای این منظور، روش‌های موجود فعلی در اقدام یک نیز قابل دسترس است. با همکاری انجمن‌ها و دانشگاه‌ها، اقدامات آتی برای بهبود چارچوب اقتصاد امنیت ICT در صورت لزوم بررسی و اجرا می‌شود.

۲-۵ وضعیت تهدید

مروری بر حوزه عملیات	
شرح	همانطور که در بخش پیشینه توضیح داده شد، وضعیت تهدید سایبری از طریق طیف گسترده‌ای از تهدیدات ممکن مشخص می‌شود. این تهدیدها بسته به نوع هدف حملات، عوامل پشت حملات و مجموعه افراد آسیب دیده از یکدیگر متمایز می‌شوند. با توجه به اینکه مهاجمان می‌توانند همزمان اهداف مختلفی را دنبال کرده و یا ماهیت و اهداف حمله را با یکدیگر ترکیب کنند، مرزها بین تهدیدهای مختلف اغلب مشخص نیست. علاوه بر ماهیت بسیار پویای گسترش خطرات سایبری، پیچیدگی و پراکندگی آن، دستیابی به یک نمای کلی از وضعیت تهدید سایبری را با چالش روبرو می‌سازد. با این حال، چنین مروری عنصری اصلی برای محافظت در برابر خطرات سایبری به‌شمار می‌رود. همچنین این بازبینی می‌تواند پایه و اساسی برای انتخاب، اولویت‌بندی اقدامات پیشگیرانه و واکنشی باشد و افزون‌بر این برای تصمیم‌گیری صحیح در صورت وقوع حوادث و شرایط بحرانی ضروری است. بدین ترتیب، ارزیابی تهدیدات موجود و تحولات آینده مورد نیاز می‌باشد (شرح و ارزیابی وضعیت).
پیشینه	به‌عنوان بخشی از اجرای NCS از سال ۲۰۱۳ تا ۲۰۱۷، قابلیت‌های توصیف و ارزیابی وضعیت، شناسایی اولیه و ویژگی آنها تعیین شد. فرایندهای مورد نیاز برای ایجاد یک تصویر کلی از وضعیت آماده و اطلاعات مربوط به وضعیت تهدید از طریق یک ردیاب موقعیت تعاملی و پویا خلاصه شد و در اختیار مسئولین دولتی و مجریان زیرساخت‌های حیاتی قرار گرفت.
اهداف و اقدام مورد نیاز	کشور همچنان به یک تصویر کلی از وضعیت سایبری، به منظور حفاظت سوئیس در برابر خطرات سایبری وابسته است. با توجه به وضعیت وخیم تهدید، بایستی توانایی‌های موجود گسترش یابند و تبادل اطلاعات با بخش خصوصی و کانتون‌ها بیشتر تقویت شود. با توجه به اینکه منابع موجود به شدت جذب تجارت روزانه می‌شوند، ارزیابی و تدوین سیستماتیک حوادث سایبری در حال حاضر تضمینی ندارند. هدف این است که به ارزیابی عمیق و با جزئیات بیشتر در تهدیدهای مربوط به سوئیس دست یافت. افزون‌بر این، یافته های مربوط به وضعیت تهدید نه تنها باید در اختیار مقامات و مجریان زیرساخت‌های حیاتی باشد، بلکه به شکل مناسب در اختیار سایر شرکت‌ها و عموم مردم سوئیس نیز قرار گیرد.

اقدامات
۴) گسترش قابلیت‌های ارزیابی و ارائه وضعیت تهدید سایبری قابلیت‌های دستیابی، ارزیابی و تأیید اطلاعات در مورد وضعیت تهدید در سرویس اطلاعاتی بایستی بیشتر گسترش یابد. این امر مستلزم استفاده سیستماتیک از هوش منبع باز[1] و تخصص مرتبط، استفاده از کمک‌های فنی، نگهداری، و گسترش شبکه شرکای ملی و بین‌المللی است. یافته‌های به دست آمده از وضعیت تهدید باید پردازش سیستماتیک و به‌روزرسانی منظم شوند و با استفاده از موقعیت‌یاب، در اختیار گروه هدف قرار گیرند. نسخه‌ای از وضعیت‌یاب نیز باید برای عموم تهیه شود.

۳-۵ مدیریت انعطاف‌پذیر

مروری بر حوزه عملیات	
زیرساخت‌های حیاتی[2] وابستگی زیادی به عملکرد و ایمنی سیستم‌ها و زیرساخت‌های ICT دارند. اقدامات کاهش آسیب‌پذیری ICT در زیرساخت‌های حیاتی از اهمیت بالایی جهت حفاظت سوئیس در برابر خطرات سایبری برخوردار است. این اقدامات نه تنها به تقویت پیشگیری مربوط می‌شود، بلکه اقدامات برای مهار خسارت و کاهش زمان خرابی در صورت بروز حوادث می‌باشد. هدف این است که قابلیت انعطاف‌پذیری و بازسازی زیرساخت‌های حیاتی در سوئیس بهبود یابد. بخش عمده‌ی زیرساخت‌های حیاتی در سوئیس توسط شرکت‌های خصوصی اداره می‌شود. این شرکت‌ها اقدامات بهبود انعطاف‌پذیری ICT را اجرا می‌کنند. با این وجود، دولت به عنوان بخشی از وظیفه اساسی خود برای حفظ امنیت کشور، مسئولیت حفاظت از زیرساخت‌های حیاتی و در نتیجه تضمین در دسترس بودن کالاها و خدمات حیاتی برای عموم و اقتصاد را بر عهده دارد. این کشور باید این وظیفه را به صورت تابعه و با همکاری نزدیک با بخش خصوصی انجام دهد. از این‌رو، دولت فدرال در تعریف اقدامات لازم برای بهبود انعطاف‌پذیری ICT در زیر بخش‌های مهم نقش فعالی دارد و همچنین بر اجرای آنها نظارت می‌کند. بسته به اقدامات، اجرای آن ممکن است در سطوح مختلف (در سطح شرکت یا بخش) انجام شود. زیرساخت‌های مهم ICT مسئولین دولتی خود، یک مورد ویژه است. در اینجا دولت فدرال و کانتون‌ها، خود مسئول اجرای اقدامات می‌باشند.	شرح
بین سال‌های ۲۰۱۳ و ۲۰۱۷، FOCP و FONES با همکاری مقامات ذیربط، انجمن‌ها و نمایندگان اپراتورهای زیرساخت‌های حیاتی، خطرات و موارد آسیب‌پذیر	پیشینه

1. Open Source Intelligence (OSINT)
2. Critical Infrastructures (CI)

مروری بر حوزه عملیات	
پیشینه	ICT را در ۲۸ زیر بخش حیاتی شناسایی کردند و به طور مشترک برای بهبود انعطاف‌پذیری ICT اقداماتی (که قبلاً نیز به طور جزئی اجرا شده‌اند) را پیشنهاد دادند. دولت فدرال برای محافظت از زیرساخت‌های ICT خود، به واسطه مفهومی جدید، تجزیه و تحلیل منظم آسیب‌پذیری سیستم‌های ICT دولت فدرال را توصیف می‌کند. کانتون‌ها به عنوان بخشی از دو پروژه SSN تجزیه و تحلیل خطر را برای ادارات خود انجام داده‌اند.
اهداف و اقدام مورد نیاز	بر اساس تجزیه و تحلیل دوره‌ای و به‌روز خطر و آسیب‌پذیری، اقدامات تعیین شده برای بهبود انعطاف پذیری ICT در زیر بخش‌های حیاتی و ادارات اجرا شده و بسط می‌یابند. این کار با هماهنگی اقداماتی که در حوزه عمل استانداردسازی و مقررات تعیین شده‌اند، بهره‌گیری از اثر هم‌افزایی کار مداوم دولت فدرال در رابطه با حفاظت زیرساخت‌های حیاتی، مدیریت بحران، حفاظت مدنی (شبکه امن داده +SDN)، تأمین اقتصادی ملی، مدیریت ریسک دولت فدرال، امنیت ICT و سایر نهادهای درگیر انجام می‌شود.

اقدامات
۵) بهبود انعطاف‌پذیری ICT در زیرساخت‌های حیاتی تمرکز بر اجرای اقدامات برای بهبود انعطاف‌پذیری ICT در زیربخش‌های حیاتی، شامل مراجع نظارتی مربوطه و دفاتر تخصصی است. مبانی این امر شامل تحلیل ریسک و آسیب‌پذیری موجود به‌همراه پیشنهادات برای اقدامات مرتبط با آن است. علاوه بر اجرای اقدامات تعیین شده، تحلیل و اقدامات باید به طور منظم به روز شده و در صورت لزوم، با یافته‌ها و تحولات جدید مطابقت داده شوند.
۶) بهبود انعطاف‌پذیری ICT در دولت فدرال بهبود انعطاف‌پذیری ICT دولت فدرال به واسطه تدوین مفهومی برای تحلیل و مقابله با موارد آسیب‌پذیر ICT در دولت فدرال حاصل می‌شود. این مفهوم نتایج مشخصی از آسیب‌پذیری‌های شناسایی شده را فراهم می‌کند تا اقدامات امنیتی ICT که به طور منطقی قابل اجرا هستند، انتخاب شوند. به منظور بهبود انعطاف‌پذیری ICT، آموزش و آگاهی‌بخشی هدفمند در این بخش‌ها برای افراد مسئول حفاظت زیرساخت‌های ICT و رسیدگی به حوادث فراهم می‌شود و از تبادل اطلاعات مربوط به آسیب‌پذیری‌ها یا حوادث امنیتی در بین ارگان‌های ذی صلاح اطمینان حاصل می‌شود.

اقدامات
۷) تبادل تجربه و ایجاد مبانی برای بهبود انعطاف‌پذیری ICT در کانتون‌ها شبکه‌ای از مسئولین دولتی جهت تبادل تجربیات و ایجاد مبانی‌های مشترک به‌منظور تقویت انعطاف‌پذیری ICT در کانتون‌ها ایجاد خواهد شد (یا از شبکه‌های موجود استفاده می‌گردد). هدف در این مرحله، حمایت متقابل و اقدام هماهنگ مسئولین فدرال و کانتون می‌باشد.

۵-۴ استانداردسازی/مقررات

مروری بر حوزه عملیات	
استانداردسازی و مقررات ICT ابزار مهمی برای حفاظت در برابر خطرات سایبری است. حداقل الزامات اقدامات حفاظتی پیشگیری را تقویت می‌کند و دستورالعمل‌های برخورد با حوادث (به عنوان مثال الزام گزارش) می‌توانند در پاسخ بهتر یاری برسانند. استانداردسازی و مقررات نیز در زمینه بین‌المللی با توجه به ایجاد شفافیت و اعتماد بیشتر در جامعه جهانی دیجیتال حائز اهمیت است. با این حال، هنگام تعریف استانداردسازی و مقررات، تفاوت‌های عمده بین بخش‌های اقتصادی و شرکت‌ها در ابعاد مختلف باید در نظر گرفته شود. بخش‌ها به طور یکسان در معرض خطرات سایبری نیستند و منابع مالی و انسانی شرکت‌ها بسیار متفاوت است. بنابراین استانداردسازی و مقررات باید با همکاری نزدیک بین بخش خصوصی و دولت تدوین و معرفی شوند. علاوه بر این، زمینه بین‌المللی باید همیشه در نظر گرفته شود. استانداردها و مقررات در فضای سایبری فرامرزی باید تا حد امکان مطابق با محیط بین‌المللی باشند. بنابراین کارکرد نهادهای استانداردسازی بین‌المللی و تحولات نظارتی مربوط به سوئیس باید لحاظ گردند. فرایندهای مختلف حاکمیت اینترنتی که توسط اجلاس جهانی سازمان ملل متحد در مورد جامعه اطلاعاتی (WSIS) ایجاد شده است و نیز در محدوده استانداردسازی و مقررات قرار دارد. این فرایندها به توسعه اصول، هنجارها، قوانین و سازوکارهای تصمیم‌گیری برای ایجاد و استفاده از اینترنت در سطح بین‌المللی می‌پردازد. در اجرای WSIS Action Line C5 (ایجاد اطمینان و امنیت)، ITU به عنوان مجری انواع مختلف پروژه‌ها و مشاغل استفاده می‌شود. علاوه بر این، سایر عاملان بین‌المللی مانند OECD و WEF فرایندها و فعالیت‌هایی را جهت بهبود امنیت در زمینه دیجیتال آغاز کرده‌اند. هدف اصلی WSIS در مورد الزام همه ذینفعان (رویکرد چند-سهامدار) این است که	چالش

مروری بر حوزه عملیات	
شرح	برای توسعه باید هنجارها و قوانین دنیای دیجیتال که به طور روزافزون توسط عاملان جهانی در بخش خصوصی تعیین می‌شوند، درنظر گرفته شوند ازاین‌رو همکاری بین عاملان دولتی و خصوصی از اهمیت ویژه‌ای برخوردار است.
پیشینه	استانداردهای کلی و جزئی (بخش‌بندی) گوناگونی برای امنیت سایبری وجود دارد. در همکاری با بخش خصوصی، ارزیابی اولیه برای نیاز به استانداردسازی و مقررات در بخش‌های مختلف صورت گرفت. آشنایی با تحولات در نهادهای استانداردسازی بین‌المللی و در زمینه تنظیم مقررات در سایر کشورها موجود است. دستورالعمل امنیت شبکه و اطلاعات اتحادیه اروپا (دستورالعمل NIS) در سطح اروپا به تصویب رسیده است و اکنون توسط کشورهای عضو در حال اجرا است. این دستورالعمل معرفی حداقل استانداردها و الزام گزارش حوادث سایبری را در نظر گرفته است. در زمینه حاکمیت اینترنت، ارگانها ، فرایندها و رویدادهای ویژه مربوط به سوئیس مشخص شده، مسئولیت‌های دولت فدرال توضیح داده شده و به کمک فرایندهای مصوب NCS، از هماهنگی با همه عوامل درگیر اطمینان حاصل شده است.
اهداف و اقدام مورد نیاز	اهمیت روزافزون استانداردسازی و مقررات ICT باید در نظر گرفته شود. حداقل استانداردهای ICT الزام‌آور و قابل تأیید برای امنیت و اطمینان در اقتصاد دیجیتال و جامعه اهمیت دارد، باید با همکاری بخش خصوصی ارزیابی شوند و در صورت لزوم معرفی گردند. همچنین باید بررسی شود که آیا و چگونه باید تعهدی برای گزارش حوادث سایبری معرفی شود؟ این اقدامات زمینه بین‌المللی را در نظر می‌گیرند، که تأثیر قابل توجهی بر آنها دارد، به همین دلیل است که باید بر پیشرفت‌ها نظارت شود. از این‌رو، سوئیس از منافع و ارزش‌هایش برای فرایندهای بسیار مهم یاری می‌گیرد.

اقدامات
۸) ارزیابی و معرفی حداقل استانداردها بر اساس تحلیل ریسک و آسیب‌پذیری، حداقل استانداردهای ICT قابل تأیید ارزیابی شده و با همکاری نزدیک بین مقامات متخصص، بخش خصوصی و انجمن‌ها معرفی می‌شوند. اگر دسترسی فراهم باشد، ترجیحاً از استانداردهای موجود استفاده می‌گردد و یا درصورت لزوم با شرایط تطبیق داده می‌شوند. با توجه به نتایج تجزیه و تحلیل

اقدامات
آسیب‌پذیری، مقامات ذی‌صلاح بررسی می‌کنند که استانداردها برای کدام سازمان‌ها و فعالیت‌ها اجباری است.
۹) بررسی الزام گزارش حوادث سایبری و تصمیم در مورد معرفی به منظور بهبود تصویری از تهدیدات سایبری، معرفی الزام گزارش حوادث سایبری باید مورد بررسی و تصمیم‌گیری قرار گیرد. اولین مسائلی که باید روشن شوند این است که چه کسانی باید متعهد به گزارش‌دهی باشند، چه حوادثی مربوط به این الزام گزارش می‌شود، به چه کسانی باید گزارش داده شود و آیا الزام گزارش می‌تواند به طور قابل توجهی تصویر وضعیت را در مقایسه با امروز بهبود بخشد. اشکال متنوعی از ارائه این گزارش‌ها در بخش‌های مختلف طرح و مبانی قانونی لازم تعریف می‌شود. این امر با مشارکت مقامات مربوطه، بخش خصوصی و انجمن‌ها، با هماهنگی استراتژی ملی برای حفاظت از زیرساخت‌های حیاتی و در نظر گرفتن تحولات بین‌المللی انجام می‌شود. بر اساس این توضیحات، سپس در مراحل آتی در مورد معرفی الزام گزارش تصمیم‌گیری شده و در صورت لزوم اقدامات لازم انجام می‌گردد.
۱۰) حاکمیت جهانی اینترنت سوئیس باید فعالانه و به صورت هماهنگ در جهت ارتقای یک چارچوب نظارتی بین‌المللی برای استفاده و توسعه بیشتر اینترنت عمل کند که با ایده‌آل‌های آزادی، دموکراسی و مسئولیت‌پذیری (شخصی)، تأمین خدمات اساسی، فرصت‌های برابر، امنیت، حقوق بشر و حاکمیت قانون سوئیس سازگار باشد. برای این منظور، ذینفعان ملی باید درگیر شوند و تحولات مربوطه به آنها ارائه شود.
۱۱) ایجاد تخصص در مورد مسائل استانداردسازی مربوط به امنیت سایبری دولت فدرال مجموعه‌ای از تخصص‌ها را در مورد مسائل استانداردسازی مربوط به امنیت سایبری فراهم می‌کند تا ناظران مرتبط با توسعه و اجرای استانداردها، مقررات و دستورالعمل‌های موضوع‌محور را راهنمایی کند. در صورت لزوم، این گروه متخصص با پشتیبانی از کانتون‌ها، تحولات بین‌المللی مربوط به استانداردسازی و مقررات را پایش می‌کنند و در این زمینه با بخش خصوصی ارتباط برقرار می‌کند. با این کار، مجموعه متخصصان به یک رویکرد هماهنگ متناسب با تحولات بین‌المللی کمک می‌کنند.

۵-۵ مدیریت حوادث

مروری بر حوزه عملیات	
شرح	از آنجا که هیچ حفاظت کاملی در مقابل حوادث سایبری وجود ندارد و تعداد حملات هدفمند روبه افزایش است، یکی از وظایف اصلی در مقابله با خطرات سایبری، ایجاد و راه‌اندازی سازمانی برای رسیدگی به حوادث می‌باشد (مدیریت حوادث). مدیریت حوادث شامل شناسایی حوادث در اسرع وقت، شناسایی و اجرای اقدامات متقابل مناسب و تحلیل حوادث برای کسب نتایج جهت بهبود پیشگیری است. این وظیفه به مهارت‌های تخصصی، ابزارهای تحلیلی، سازمان هموارکننده عملیات و همکاری قوی بین کلیه بخش‌های مربوطه نیاز دارد. تبادل اطلاعات بین شرکای قابل اعتماد در مورد حوادث و اقدامات متقابل احتمالی بسیار مهم است. با توجه به این که حوادث غالباً به طور همزمان بر عاملیت‌های مختلف تأثیر می‌گذارد اگر همه آن‌ها اطلاعات مربوطه را در اختیار بگذارند، می‌توان سریعتر و مؤثرتر رسیدگی کرد. مسئولیت‌ها و فرایندها باید مشخص و کارآمد باشد و روال‌های مناسبی ایجاد شود. تبادل و ارزیابی اطلاعات باید به صورت متمرکز هماهنگ گردند تا در کوتاه‌ترین زمان، اهمیت استراتژیک یک حادثه و اولویت آن برای سیاست‌های امنیتی شناخته شود، عاملیت‌های مربوطه و ارگان‌های ذی‌صلاح نیز مطلع شوند - در دولت فدرال، اینها بسته به نوع و دامنه رویداد، شامل گروه هسته امنیت[1] (SCG) و کمیته شورای امنیت فدرال[2] (FCSC) می‌شوند.
پیشینه	تیم‌های تخصصی در بسیاری از سازمان‌ها در سوئیس مأمور شده‌اند تا به مقابله با حوادث سایبری، بپردازند. این تیم‌ها با اسامی مختلف (به عنوان مثال مراکز عملیات امنیتی، تیم‌های واکنش اضطراری رایانه‌ای، تیم‌های واکنش حوادث امنیتی رایانه) و توانش‌های متناسب با حوزه مسئولیت مربوطه تعریف شده‌اند. بسیاری از کانتون‌ها و همچنین دولت فدرال چنین تیم‌هایی را در اختیار دارند. مدیریت حوادث در درجه اول از طریق این تیم‌ها انجام می‌شود. دولت فدرال برای پشتیبانی از اپراتورهای زیرساخت‌های حیاتی، مرکز گزارش و تحلیل برای تضمین اطلاعات[3] (MELANI) را اداره می‌کند. MELANI به عنوان مرکز تماس در سطح دولتی، به پشتیبانی در زمینه تحلیل فنی و اطلاعاتی حوادث، از جمله بستر تبادل اطلاعات مرتبط می‌پردازد. مرکز MELANI همچنین نقش هماهنگ‌کننده اصلی را در دولت فدرال در برخورد با حوادث دارد. به طور معمول، دفاتر مرتبط با فدرال به MELANI اطلاع می‌دهند که گزارش‌ها را ارزیابی کرده و سپس به عاملیت‌های فدرال مربوطه می‌فرستند. با این حال،

1. The Security Core Group
2. The Federal Council Security Committee
3. The Reporting and Analysis Centre for Information Assurance

مروری بر حوزه عملیات	
پیشینه	فرایندها استاندارد نیستند و مشخص نمی‌باشد که مرکز MELANI در چه زمانی SCG و یا FCSC را مطلع می‌سازد. به عنوان بخشی از NCS ۲۰۱۲-۲۰۱۷، ظرفیت‌های پرسنل MELANI تقویت شد و همکاری با تیم‌های تخصصی در داخل و خارج از دولت فدرال بیشتر گسترش یافت. این امر امکان افزایش تعداد شرکت‌ها با دسترسی به بستر تبادل اطلاعات و پشتیبانی فنی را فراهم کرد. حال آن‌که پس از این توسعه، خدمات MELANI به بخش خصوصی بیشتر بر اپراتورهای زیرساخت‌های حیاتی متمرکز ماند.
اهداف و اقدام مورد نیاز	با گسترش گروه هدف NCS، باید در صورت بروز حوادث پشتیبانی لازم به دیگر بخش‌ها نیز تسری یابد. هنگام انجام این کار، کیفیت پشتیبانی موجود در شناسایی، مدیریت و تجزیه و تحلیل حوادث بایستی حفظ شود و تبادل مطمئن اطلاعات با اپراتورهای زیرساخت‌های حیاتی همچنان تضمین گردد. همکاری نزدیک فعلی با مراکز توانش مربوطه باید به صورت هدفمند تقویت شود تا بتوان از منابع تخصصی محدود در سوئیس در حد امکان و به طور مؤثر استفاده کرد. علاوه بر گسترش و تشدید همکاری با اشخاص ثالث، فرایندهای داخلی فدرال برای مدیریت حوادث نیز باید بهبود یابند. هر بخش باید توانایی رسیدگی به حوادث را به شیوه مناسب داشته باشد، با این‌حال مرکز MELANI باید با آمادگی زیر نظر واحد فناوری اطلاعات فدرال[1] (FITSU)، پشتیبانی لازم را ارائه دهد. در مورد حوادثی که چندین بخش را تحت تأثیر قرار می‌دهند ویا در ارزیابی MELANI تهدیدی برای امنیت داخلی یا خارجی است، حوادث باید به طور یکنواخت و به صورت متمرکز توسط FITSU با مشارکت بخش‌های آسیب‌دیده مدیریت شود. واحد FITSU بلافاصله با کمک بخش‌ها، سیاست امنیتی و اثر استراتژیک حادثه را ارزیابی می‌کند.

اقدامات
۱۲) گسترش MELANI به عنوان شراکت خصوصی-عمومی برای اپراتورهای زیرساخت‌های حیاتی بایستی پشتیبانی از اپراتورهای زیرساخت‌های حیاتی گسترش یابند. هدف این است که همه بخش‌های حیاتی در تبادل اطلاعاتی و فعالیت بین تمام قسمت‌ها دخیل باشند. هنگام گسترش PPP، باید از حفظ کیفیت خدمات موجود اطمینان حاصل شود. همچنین نوع برخورداری از خدمات برای هر یک از اعضای حوزه انتخابیه مشخص گردد.

اقدامات
۱۳) توسعه خدمات برای همه شرکت‌ها MELANI گروه هدف را گسترش داده و خدمات را در زمینه پیشگیری و مدیریت حوادث برای یک گروه هدف گسترده‌تر که محدود به اپراتورهای زیرساخت‌های حیاتی نیست، توسعه می‌دهد. بخش خصوصی سوئیس و به‌ویژه شرکت‌های کوچک و متوسط توسط MELANI پشتیبانی می‌شوند. پشتیبانی به صورت تابعه از خدمات حفاظت و مدیریت حوادث موجود در بازار ارائه می‌شود.
۱۴) همکاری بین دولت فدرال و عاملیت‌های ذیربط و مراکز توانش همکاری نزدیک MELANI با سایر عاملیت‌های فدرال و کانتون باید بیشتر تقویت شود. با توجه به وجود تعداد محدودی متخصص در سوئیس، برای استفاده کاراتر و مؤثرتر از منابع محدود، باید همکاری با مراکز توانش منتخب تقویت و هماهنگ شود.
۱۵) فرایندها و مبانی مدیریت حوادث در دولت فدرال به منظور استانداردسازی مدیریت حوادث در داخل دولت فدرال، فرایندی برای روشن شدن کانال‌ها و مسئولیت‌های گزارش‌دهی و اطمینان از مشارکت مقامات دادسرا و - در مورد حوادث مربوط به سیاست یا استراتژی امنیتی - SCG یا FCSC ایجاد شده است. بخشها یک مرکز تماس برای هماهنگی مدیریت حوادث تعیین می‌کنند و به FITSU اختیار لازم برای ارائه دستورالعمل به مدیریت حوادث داده می‌شود. دبیرخانه فدرال ارتباطات را در صورت بروز حوادث سایبری در چندین بخش تحت تأثیر هماهنگ می‌کند.

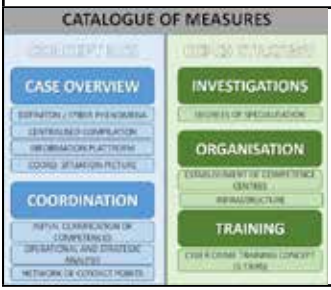
۵-۶ مدیریت بحران

مروری بر حوزه عملیات	
شرح	حوادث سایبری می‌تواند با پیامدهای جدی همراه باشد و به سطحی برسد که نیاز به مدیریت بحران در سطح ملی ضروری شود. تصویری به‌روز، یک‌دست و جامع از وضعیت، همچنین تعریف فرایندهای تصمیم‌گیری کارآمد و استراتژی ارتباطی برای کنترل بحران‌ها بسیار مهم است.
پیشینه	بر اساس نتایج تمرین رهبری استراتژیک ۲۰۱۳، مفهومی برای مدیریت بحران با جنبه‌های سایبری در سطح فدرال تدوین شد. این مفهوم متعاقباً با همکاری کانتون‌ها و نمایندگان مشاغل به مفهومی برای مدیریت ملی بحران خطرات سایبری، گسترش

مروری بر حوزه عملیات	
پیشینه	یافت. این مفهوم مورد آزمایش قرار گرفت و تمرینات ارزیابی شدند. دسترسی به تصویری از وضعیت که تا حد امکان دقیق و به‌روز باشد، یکی از عناصر حیاتی و مهمترین چالش در مدیریت بحران با جنبه‌های سایبری تلقی می‌شود.
اهداف و اقدام مورد نیاز	این تمرینات نشان داده است که قابلیت‌های هماهنگی در سطح عملیاتی و توصیف وضعیت باید گسترش یابد. دفاتر مسئول امنیت سایبری باید مستقیماً درگیر مدیریت بحران در سطح فدرال باشند. این مدیریت توسط تیم‌های بحران فعلی یا موقت انجام می‌شود. همکاری با کانتون‌ها و بخش خصوصی نیز باید به طور منظم تمرین شود تا افراد درگیر مسئولیت‌ها و مراکز تماس خود را بدانند.

اقدامات
۱۶) ادغام دفاتر مسئول امنیت سایبری در تیم‌های بحران فدرال تیم‌های بحران موجود (هیئت‌مدیریت بحران فدرال برای حفاظت مدنی و تیم بحران FONES) برای مقابله با بحران‌های سایبری به‌کار گرفته شده و یا تیم‌های بحرانی موقت تشکیل می‌شوند. دفاتر مسئول امنیت سایبری باید در تیم‌های بحران ادغام شده و علاوه بر توانایی تقبل هماهنگی تخصصی در بحران سایبری، پیشنهاداتی نیز به تیم بحران ارائه بدهند. در صورت بروز بحران، همچنین باید مشخص شود که چه قدرتی برای ارائه دستورالعمل در سطح سازمان تخصصی مورد نیاز است.
۱۷) تمرینات مشترک مدیریت بحران مدیریت بحران با توجه به جنبه‌های سایبری در تمرینات مشترک دولت فدرال، کانتون‌ها و نمایندگان زیرساخت‌های حیاتی آزمایش می‌شود. جنبه‌های سایبری باید در این تمرینات کلی قرار گیرند و تمرینات ویژه‌ای برای مدیریت بحران‌های سایبری نیز برگزار شود. ارزیابی این تمرین‌ها در بهینه‌سازی رویه‌های مدیریتی وارد می‌شوند.

۷-۵ پیگرد قانونی

مروری بر حوزه عملیات	
شرح	زیرساخت‌های دیجیتالی موجود از طریق اینترنت، فرصت‌های جدیدی برای مجرمان با پتانسیل بالای ایجاد خسارت عظیم برای جامعه و اقتصاد فراهم می‌کند. دیگر، برای جرایم جنایی محدودیت زمانی و مکانی وجود ندارد. جرایم سایبری پویا با چرخه‌های نوآوری کوتاه‌مدت از مرزهای منطقه‌ای عبور می‌کنند. هرچه ارتباط دیجیتالی بیشتر باشد، خطر شروع حوادث سایبری در دنیای مجازی بیشتر می‌شود اما تأثیر مخربی در دنیای واقعی دارد. علیرغم جنبه این پیشرفت، نیاز مبرم به رویکردهای جدید در زمینه پیگرد قانونی دیده می‌شود. هدف این است که قابلیت همکاری و پاسخگویی در سراسر سوئیس، همکاری با شرکای بین‌المللی و هماهنگی بین توانش‌های تخصصی، فنی و پرسنلی بدون تخصیص مجدد اختیارات بین مقامات و سطوح مختلف دولت ارتقا یابد.
پیشینه	یک گام مهم در مبارزه با جرایم سایبری، انجام مطالعه موردی جامع در سطح ملی است. یک مفهوم تلفیقی که همراه با کانتون توسعه یافته برای این منظور در دسترس می‌باشد. همچنین تدابیری برای گردآوری یکسان، هماهنگی و انتشار اطلاعات وضعیت؛ اقدامات پلیسی برای تعیین صلاحیت قضایی محلی و گردآوری و تحلیل پدیده‌محور از داده های جرایم سایبری تعیین شده است. با این حال، مطالعه موردی ملی و هماهنگی موردی بین کانتون، تنها دو جنبه جزئی از چالش جرایم سایبری به‌شمار می‌رود. جنبه‌های مهمی مانند تحقیقات واقعی، ساختارهای ملی و آموزش متناسب با سطح هنوز بایستی مشخص شوند. ازاین‌رو، کنفرانس فرماندهان پلیس کانتون سوئیس (CCPCS) در حال تهیه کاتالوگ ملی از اقدامات مرتبط با جرایم سایبری و دادگاه‌های فناوری اطلاعات است. این کاتالوگ، همراه با تخصیص منابع لازم، مسائل سازمانی و زیربنایی را به طور کامل بررسی می‌کند.
اهداف و اقدام مورد نیاز	 کاتالوگ ملی CCPCS اقدامات مقابله با جرایم سایبری و برنامه اجرایی آن را در نظر گرفته، تمامی جنبه‌های مبارزه با جرایم سایبری (مطالعه موردی، هماهنگی موردی، آموزش، تحقیقات) را پوشش داده و مراحل اجرای اقدامات و مفاهیم در حال انجام را نشان می‌دهد.

1. The Conference of Cantonal Police Commanders of Switzerland

اقدامات
۱۸) تصویری از وضعیت جرایم سایبری دولت فدرال (Fedpol) و کانتون‌ها (CCPCS) چارچوب فنی را آزموده و طراحی می‌کنند تا به تصویر کنونی در سطح ملی از وضعیت جرایم سایبری برای اهداف پلیسی دست یابند. این کار با همکاری برنامه هماهنگی فناوری اطلاعات پلیس[1] (HPI) انجام می‌شود.
۱۹) شبکه پشتیبانی برای رسیدگی به اجرای قانون دیجیتال (ISNDLE) دولت فدرال (Fedpol) و کانتون‌ها (CCJPD) توافق‌نامه اداری را در زمینه همکاری و هماهنگی بین مرکز ملی توانش سایبری[2] (NC3) و مراکز منطقه‌ای توانش سایبری[3] (RC3) در ISNDLE فراهم می‌کنند.
۲۰) آموزش مقابله با جرایم سایبری باهمکاری کنفرانس فرماندهان پلیس کانتون (CCPCS) و کنفرانس دادستان‌های سوئیس[4] (CSP)، مفاهیم آموزشی خاصی برای توسعه پایدار توانش‌های لازم در پیگرد قانونی در حال ایجاد است.
۲۱) دفتر مرکزی جرایم سایبری به منظور ایجاد یک دفتر مرکزی برای جرایم سایبری و زمینه لازم برای همکاری با کانتون‌ها جهت مبارزه با جرایم سایبری، Fedpol بازنگری قانون دفاتر مرکزی[5] (COA) را آغاز می‌کند.

۸-۵ دفاع سایبری

مروری بر حوزه عملیات	
حملات سایبری گسترده یا بسیار هدفمند به زیرساخت‌های حیاتی سوئیس می‌تواند امنیت مردم و اقتصاد را به خطر بیندازد. علاوه بر طیف وسیعی از اقدامات برای تقویت حفاظت در برابر خطرات سایبری، به منظور جلوگیری از حملات مداوم و شناسایی عوامل مسئول، قابلیت‌ها و منابع در همه شرایط مورد نیاز می‌باشد. در مورد حملاتی که عملکرد زیرساخت‌های حیاتی را به مخاطره می‌اندازد، در صورت لزوم باید اقدامات متقابل فعالی جهت حصول اطمینان از ادامه عملیاتشان انجام شود. دفاع سایبری شامل اقداماتی است که به طور کلی برای محافظت از سیستم‌های حیاتی و دفاع در برابر حملات در فضای سایبری در همه شرایط، یعنی از جمله زمان‌های درگیری و جنگ، انجام می‌شود.	

1. The Harmonisation of Police Information Technology
2. The National Cyber Competence Center
3. The Regional Cyber Competence Centers
4. The Conference of Swiss Prosecutors
5. The Central Offices Act

مروری بر حوزه عملیات	
پیشینه	طبق قانون سرویس اطلاعات[1] (IntSA) و قانون بازنگری شده نیروهای مسلح[2] (ArmA)، دولت فدرال مبانی قانونی لازم جهت گسترش و اخذ تدابیر و اقدامات متقابل فعال به عنوان بخشی از دفاع سایبری را در اختیار دارد. با این حال، توسعه حملات سایبری طی سال‌های گذشته و پیچیدگی رو به رشد آنها، منابع را به مدت طولانی‌تری درگیر می‌کند. درنتیجه این خطر وجود دارد که حملات همزمان به دلیل تمرکز متخصصان موجود در دفاع مقابل سایر حوادث به موقع تشخیص داده نشوند. منابع اندک همچنین انجام پیگیری‌های لازم و جامع در مورد حوادث را دشوارتر می‌سازد. در برنامه عملیاتی دفاع سایبری[3] (APCD)، DDPS اقدام موردنیاز و منابع را در زمینه دفاع سایبری شناسایی، وظایف عاملیت‌های مختلف (به ویژه نیروهای مسلح) را تعریف کرده و اقدامات انجام شده برای مدیریت وظایف را شرح داده است.
اهداف و اقدام مورد نیاز	سرویس اطلاعاتی باید در موقعیتی باشد که بتواند با جمع‌آوری و ارزیابی منظم اطلاعات، الگوهای جدید حمله را در اسرع وقت شناسایی کند. همچنین باید بتواند منبع حملات را با حداکثر دقت ممکن تعیین کرده (انتساب)، به طوری‌که آزادی عمل مقامات سیاسی و قضایی حفظ شود. در صورت حمله به اپراتورهای زیرساخت‌های حیاتی، سرویس اطلاعاتی باید بتواند وظیفه خود را با مشارکت واحدهای پشتیبانی تحت INTSA انجام دهد. نیروهای مسلح به عنوان جایگزین استراتژیک برای پشتیبانی کمکی واحدهای اداری مدنی و به‌هنگام بسیج‌سازی عموم، نقشی اساسی دارند. بنابراین نیروهای مسلح باید بتوانند آمادگی عملیاتی را در همه شرایط در زمینه دفاع سایبری تضمین کنند.

اقدامات
۲۲) گسترش قابلیت‌های جمع‌آوری اطلاعات و انتساب قابلیت‌های جمع‌آوری اطلاعات و دانش تخصصی موجود جهت شناسایی اولیه حملات سایبری و تألیف آنها بیشتر توسعه یافته، همکاری بین کنفدراسیون و کانتون تقویت می‌شود و تبادل اطلاعات با بخش خصوصی گسترش می‌یابد. سرویس اطلاعاتی فدرال تحلیل‌های عمیق محیطی و انسانی را انجام می‌دهد؛ کمک‌های فنی، نظارت ارتباط از راه دور و روش‌های هوش انسانی را به کارگرفته و توسعه می‌دهد. به این ترتیب حملات سایبری به طور سیستماتیک پردازش و ردیابی می شوند.

1. The Intelligence Service Act
2. The Armed Forces Act
3. Action Plan for Cyber Defence

اقدامات
۲۳) قابلیت اجرای اقدامات پویا در فضای سایبری تحت IntSA و ArmA DDPS (FIS و نیروهای مسلح) از توانش و ظرفیت‌های کیفی و کمی مطلوب جهت ایجاد اختلال، جلوگیری یا کاهش سرعت حملات به زیرساخت‌های حیاتی را برخوردار است. این اقدامات مطابق با الزامات قانونی IntSA و ArmA استفاده می‌شود.
۲۴) اطمینان از آمادگی عملیاتی نیروهای مسلح در همه اوضاع موجود در فضای سایبری و تعیین نقش کمکی آنها در حمایت از مقامات غیرنظامی به عنوان بخشی از به‌روزرسانی نیروهای مسلح[1] (UAF)، نیروهای مسلح اطمینان حاصل می‌کنند که در موقعیت فوق العاده در فضای سایبری، از امکانات، منابع و توانایی کافی برای انجام وظیفه خود در چارچوب ArmA برخوردار هستند. نیروهای مسلح همچنین باید آماده حمایت از مقامات غیرنظامی به عنوان یک راهبرد جایگزین در قالب تابعه باشند. براین اساس، افسران و پرسنل خود را آموزش داده و همراه با مقامات غیرنظامی دولت فدرال و کانتون‌ها، چارچوبی برپایه پشتیبانی کمکی در صورت بروز حوادث سایبری ارائه می‌دهند، و همچنین به تعیین وظایف و نحوه آغاز عملیات می‌پردازند.

۹-۵ موضع‌گیری پویای سوئیس در سیاست بین‌المللی امنیت سایبری

مروری بر حوزه عملیات	
شرح	فضای سایبری بُعد جدیدی از سیاست امنیتی خارجی را ایجاد کرده که به طور فزاینده جهت اعمال قدرت و دستیابی به اهداف سیاسی، پروژه‌های اطلاعاتی و اهداف نظامی توسط مسئولین دولت استفاده می‌شود. علاوه بر استفاده از منابع سایبری در تعارضات مسلحانه مرسوم، درگیری‌های بیشتری نیز در فضای دیجیتال رخ می‌دهد. بر این اساس، همکاری بین‌المللی در سطوح دیپلماتیک و فنی/عملیاتی جهت کاهش خطرات سایبری ضروری است. حفاظت از منافع سیاست خارجی و امنیتی سوئیس نیز باید در فضای سایبری تضمین شود. بنابراین سوئیس در سطوح دیپلماتیک و فنی/عملیاتی جهت تقویت همکاری بین‌المللی برای به حداقل رساندن خطرات سایبری فعالیت می‌کند.
پیشینه	قبلاً در NCS ۲۰۱۲، بر اهمیت همکاری بین‌المللی تأکید شده بود. فرایندها و ساختارهای یک سیاست هماهنگ و منسجم امنیت سایبری خارجی مشخص شده است. استراتژی «سوئیس دیجیتالی» که در سال ۲۰۱۶ توسط شورای فدرال تصویب

1. The Upgrading of the Armed Forces

مروری بر حوزه عملیات	
پیشینه	شد، ملاحظات سیاست امنیتی را نیز در نظر می‌گیرد. در فرایندهای بین‌المللی مربوطه، سوئیس به عنوان یک شریک فعال، قابل اطمینان و قابل اعتماد شناخته می‌شود. سوئیس به شدت درگیر توسعه و اجرای اولین اقدامات اعتمادسازی بین دولت‌ها در زمینه سایبری بوده است. سوئیس به طور فعال به شکل‌گیری فرایندهای چندجانبه مربوط به امنیت سایبری کمک می‌کند و همکاری خود را با کشورها و سازمان‌های منتخب تعمیق می‌بخشد.
اهداف و اقدام مورد نیاز	سیاست منسجم امنیت سایبری خارجی برای به حداقل رساندن خطرات سایبری ضروری است. هدف اصلی چنین سیاستی، فضای سایبری آزاد، باز و ایمن می‌باشد. سوئیس برای حفاظت از منافع خود در مقابل دولت‌ها و سازمان‌های بین‌المللی، ارتقای صلح، ثبات و امنیت بین‌المللی از ابزارهای مختلفی بهره می‌برد. اولاً، این امر به رسمیت شناختن، رعایت و اجرای قوانین بین‌المللی در زمینه امنیت سایبری را ترویج می‌کند و به توصیف چگونگی اعمال قوانین بین‌المللی موجود در فضای سایبری کمک می‌کند. ثانیاً، سوئیس فعالانه اقدامات اعتمادسازی را بین دولت‌ها ارتقا می‌دهد. و سوم اینکه، طرح‌هایی را برای گسترش توانایی‌های ملی و ایجاد ظرفیت در کشورهای ثالث پشتیبانی و توسعه می‌بخشد. هدف بعدی این است که تا حد امکان از حضور همه ذینفعان در مذاکرات بین‌المللی جهت ارتقا امنیت سایبری اطمینان کسب کنند. در تمام فعالیت ها، سوئیس به ارتقای کشورش و ژنو بین‌المللی به عنوان بستری برای مذاکره در مورد سیاست امنیت سایبری خارجی توجه دارد.

اقدامات
۲۵) شکل‌گیری فعال و مشارکت در فرایندهای سیاست امنیت سایبری خارجی در زمینه سیاست امنیت سایبری خارجی، سوئیس تعهد دارد تا مجموعه قوانینی برای استفاده مسئولانه از فناوری‌های اطلاعاتی و ارتباطی تدوین کند. این کار را در سازمان ملل، سازمان امنیت و همکاری اروپا[1] OSCE و سایر مجامع بین‌المللی مرتبط انجام می‌دهد. این امر به رسمیت شناختن جامع‌تر قانون بین‌المللی را توسعه می‌دهد و همچنین به روشن شدن مسائل خاص در مورد کاربرد آن کمک می‌رساند (به عنوان مثال گروه متخصص و فرایندهای پیگیری سازمان ملل، روند دستی تالین[2] و سایر موارد). سوئیس از اصل حقوق بشر به‌صورت آفلاین و آنلاین حمایت می‌کند. بنابراین متعهد می‌شود که از حفاظت حقوق بشر در زمینه تعاملات سیاست امنیتی در فضای سایبری نیز اطمینان حاصل کند.

1. Organization for Security and Co-Operation in Euroupe
2. Tallinn Manual Process

اقدامات
سوئیس علاوه بر این در OSCE و سایر مجامع مربوطه برای اجرا و توسعه بیشتر اقدامات اعتمادسازی همکاری دارد. در نهایت، به‌عنوان رابط میان امنیت سایبری و کنترل تسلیحات به طور فعالانه در مذاکرات شرکت می‌کند، و توسعه تخصص و ظرفیت‌ها را در این زمینه ارتقا می‌بخشد.
۲۶) همکاری بین‌المللی جهت ایجاد و گسترش ظرفیت‌های امنیت سایبری از طریق همکاری و تبادل با سایر کشورها، سازمان‌های بین‌المللی و مراکز تحقیقاتی تخصصی (به عنوان مثال مرکز تعالی دفاع سایبری تعاونی[1])، سوئیس بایستی از دانش فنی خارجی برای گسترش توانایی‌های ملی در جهت به حداقل رساندن خطر استفاده کند. سوئیس از پروژه‌ها و برنامه‌های مبتکرانه برای ایجاد ظرفیت‌های امنیت سایبری در سایر کشورها پشتیبانی می‌کند (به عنوان مثال تبادل کارشناسان در زمینه ایجاد نهادها و ساختارهای امنیتی سایبری خارجی، کارگاه‌های آموزشی در مورد فرایندهای بین‌المللی، پشتیبانی از مجمع جهانی تخصص سایبری[2])
۲۷) رایزنی‌های سیاسی دو جانبه و گفتگوی چندجانبه در مورد سیاست امنیت سایبری خارجی سوئیس در مورد سیاست امنیت سایبری خارجی، به ویژه در مورد وضعیت تهدید و روندها، با کشورهای منتخب رایزنی می‌کند که به طور فعال به شکل‌گیری گفتگوهای چندجانبه یاری می‌رساند (به عنوان مثال گفتگوی سایبری و اروپایی چین).

۱۰-۵ افزایش آگاهی و اثربخشی بر عموم

مروری بر حوزه عملیات	
گسترش سریع و افزایش خطرات سایبری باعث ایجاد عدم اطمینان میان عموم مردم و اقتصاد می‌شود. برای افراد و مشاغل دشوار است که بتوانند خطرات سایبری که در معرض آن هستند را ارزیابی کرده و اقدامات محافظتی معقولانه‌ای را به‌کار برند. علاوه بر مشکل ارزیابی خطرات سایبری برای خودشان، اغلب مشخص نیست که چه حمایتی می‌توان از دولت انتظار داشت. سابقه گسترده NCS و اجرای غیرمتمرکز آن، درک اینکه دولت چه اقداماتی برای بهبود حفاظت سوئیس در برابر خطرات سایبری انجام می‌دهد را برای افراد دشوار می‌سازد. ارتباطات فعال در مورد اقدامات انجام شده و همچنین پیشرفت حاصل شده یکی از وظایف اجرای استراتژی است.	

1. Cooperative Cyber Defence Centre of Excellence
2. Global Forum on Cyber Expertise

مروری بر حوزه عملیات	
شرح	علاوه بر برقراری ارتباط در مورد NCS، دولت فدرال باید به افزایش آگاهی در مورد خطرات سایبری کمک کند. اطلاع‌رسانی به مردم در مورد خطرات سایبری و اقدامات حفاظتی احتمالی به پیشگیری و بهبود انعطاف‌پذیری و کاهش عدم اطمینان یاری می‌رساند.
پیشینه	تاکنون نتایج NCS از طریق گزارش‌های سالانه، جلسات سالانه (کنفرانس NCS و Cyber Landsgemeinde) و وب سایت به اطلاع عموم رسیده است. با این حال، بازخورد مردم، بخش خصوصی و سیاست‌گذاران نشان داده است که نیاز به اطلاعات در مورد ابزارهای موجود به اندازه کافی برآورده نشده است. همچنین حوادث جدید نشان می‌دهد که همچنان لازم است مردم را نسبت به خطرات سایبری حساس کرد و درباره گزینه‌های حفاظت اساسی آگاهی داد.
اهداف و اقدام مورد نیاز	در آینده، مردم به طور فعالانه‌تری در مورد اجرای NCS مطلع خواهند شد، به طوری‌که مشخص می‌شود فراتر از حلقه متخصصان دولت فدرال برای محافظت از سوئیس در برابر خطرات سایبری چه اقداماتی انجام می‌دهد. به منظور پیشگیری، دولت فدرال همچنین باید سهم بیشتری در افزایش آگاهی از خطرات سایبری در میان مردم، مشاغل و سیاست گذاران و اطلاع‌رسانی آنها در مورد اقدامات حفاظتی احتمالی داشته باشد.

اقدامات
۲۸) ایجاد و اجرای یک مفهوم ارتباطی برای NCS راهنماها، مسئولیت‌ها و فرایندهای ارتباطی در یک مفهوم تعریف شده‌اند. تعادل بین محرمانه بودن و نیاز به اطلاعات نیز مورد بحث قرار گرفته است. اجرای این مفهوم از طریق رسانه‌ها و روابط عمومی باید مرتبط با گروه‌های هدف باشد و تبلیغ شود.
۲۹) افزایش آگاهی عموم از خطرات سایبری دولت فدرال قصد دارد به افزایش آگاهی عمومی درباره خطرات سایبری کمک کند. این امر، به تقویت ارتباطات در مورد خطرات سایبری می‌پردازد و از ظرفیت‌های موجود انجمن‌ها و مقامات فعال در این زمینه استفاده می‌کند.

بخش ششم

بخش ششم

اجرای استراتژی

اقداماتی که شرح داده شد در ۱۰حوزه عملیاتی تا سال ۲۰۲۲ اجرا خواهد شد. برای موفقیت، باید مشخص شود که چه کسی مسئول چه اقداماتی است، اقدامات بر اساس چه مبانی قانونی اجرا شده و چه زمانی کدام اهداف محقق می‌شود. اولاً، پیش فرض این است که دولت فدرال شایستگی‌های واحدهای اداری درگیر را مشخص کرده و تعیین کند که چه کسی مسئولیت کلی اجرای NCS را بر عهده دارد. ثانیاً، با تشریح مبانی قانونی، هرگونه طرح قانونی لازم آغاز شود. ثالثاً، باید مشخص شود که چگونه دولت فدرال با کانتون‌ها، بخش خصوصی و جامعه همکاری می‌کند و آنها در اجرای اقدامات فردی چه نقشی دارند. چهارم، پیشرفت اجرای NCS باید شفاف باشد. برای این منظور، باید برای همه اقدامات اهداف عملکردی قابل اندازه‌گیری تعریف شود و همچنین زمان دستیابی به این اهداف مشخص باشد. پنجم و در آخر، در صورتی‌که تحولات جدید پیوست‌ها یا تغییرات لازم را قبل از پایان سال ۲۰۲۲ ایجاد کند، NCS چگونه و توسط چه کسی به‌روز می‌شود.

از آنجا که این نکات به مسئله اجرا مربوط است و نه جهت استراتژیک،

به همین ترتیب آنها در یک برنامه اجرایی جداگانه شرح داده شده‌اند. برنامه اجرایی باید به عنوان بخش پیوسته با NCS در نظرگرفته شود که اهداف استراتژیک را با اهداف عملیاتی تکمیل و مسئولیت‌ها و توانش‌ها را توصیف می‌کند. عناصر اصلی مربوط به این سؤالات به شرح ذیل خلاصه شده و نحوه اجرای NCS را بیان می‌کند.

۱-۶ وظایف و مسئولیت‌ها در دولت فدرال

با تصویب NCS، در درجه اول خود دولت فدرال متعهد به اجرای اقدامات مندرج در آن می‌شود. از آنجا که NCS طیف گسترده‌ای از اقدامات را پوشش می‌دهد، دفاتر مختلف فدرال مستقیماً در اجرای NCS تحت یک رویکرد غیرمتمرکز نقش دارند. وظایف دولت فدرال را می‌توان تقریباً به سه بخش تقسیم کرد:

- **امنیت سایبری:** این بخش تمام اقدامات با هدف پیشگیری، مدیریت حوادث و بهبود انعطاف‌پذیری در برابر خطرات سایبری و همچنین تقویت همکاری‌های بین‌المللی را شامل می‌شود. دولت فدرال اقدامات لازم را برای افزایش امنیت سایبری خود انجام می‌دهد و با در نظر گرفتن اصل تابعیت، با تأکید ویژه بر زیرساخت‌های حیاتی، به بهبود امنیت سایبری بخش خصوصی و جامعه کمک می‌رساند. این اقدامات همچنین شامل ارتقای همکاری بین‌المللی در زمینه امنیت سایبری می‌باشد.
- **دفاع سایبری:** شامل تمام اقدامات اطلاعاتی و نظامی برای حفاظت سیستم‌های حیاتی، دفاع در برابر حملات در فضای سایبری، اطمینان از آمادگی عملیاتی نیروهای مسلح در همه شرایط و ایجاد ظرفیت‌ها و

توانایی‌ها برای پشتیبانی کمکی مقامات غیرنظامی است. این بخش به ویژه اقدامات فعال برای شناسایی تهدیدها و مهاجمان و ایجاد اختلال و سرکوب حملات را در بر می‌گیرد.

- **پیگرد قانونی جرایم سایبری:** اقداماتی که پلیس و دادستان‌ها برای مقابله با جرایم سایبری انجام می‌دهند.

۶-۲ همکاری با اشخاص ثالث

اطمینان از همکاری مشترک برای حفاظت سوئیس در برابر خطرات سایبری، هدف استراتژیک NCS است. بر این اساس، مهم است که کانتون‌ها، بخش خصوصی و جامعه به طور مستقیم در کارهای اجرایی دخیل باشند. در حالی که دولت فدرال در مورد برنامه‌های اجرایی مرتبط با توانش‌ها و وظایف دفاتر فدرال، مشخصات لازم را ارائه می‌دهد، همچنین باید تعیین شود که کانتون‌ها و همچنین سازمان‌های تجاری و اجتماعی چه وظایفی را بر عهده دارند. از این‌رو، کانتون‌ها و سازمان های تجاری و اجتماعی در تهیه نقشه اجرایی برنامه مشارکت می‌کنند.

۶-۲-۱ مشارکت کانتون‌ها در اجرا

به منظور اطمینان از مشارکت مستقیم کانتون‌ها در اجرای اقدامات NCS 2018-22 که بر آنها تأثیر گذارد، CCJPD همراه با SSN یک طرح اجرایی کانتون را تهیه می‌کند. بر این اساس، برنامه اجرای NCS اقداماتی را که کانتون‌ها در آنها مستقیماً درگیر هستند و اهداف قابل دستیابی در این زمینه را مشخص می‌کند.

۵-۲-۲ مشارکت بخش خصوصی و جامعه

طرح اجرای NCS مشخص می‌کند کدام سازمان‌های تجاری و اجتماعی متعهد به اجرای کدام اقدامات هستند. لیست سازمان‌های تجاری و اجتماعی کامل نیست و شرکت توسط سایر سازمان‌ها در هر زمان ممکن است.

۵-۲-۳ هماهنگی اجرا

همه مشارکت‌کنندگان فعالیت‌های خود را تحت مدیریت کلی پروژه هماهنگ کرده و به طور منظم در زمینه کار اجرایی توافق می‌کنند. افزون بر این بررسی می‌شود که آیا اقدامات تکمیلی برای دستیابی به اهداف NCS لازم است. برای این منظور، یک نهاد هماهنگ‌کننده متشکل از نمایندگان دولت فدرال، کانتون‌ها و بخش خصوصی تشکیل می‌شود.

۵-۳ اهداف عملکرد برای اجرای اقدامات

به منظور ارزیابی پیشرفت اجرا، باید اهداف عملکردی قابل اندازه‌گیری برای همه اقدامات تعریف شود. بدین‌ترتیب باید مشخص شود که چه اهدافی تا چه زمانی محقق می‌شوند. به عنوان مثال، اهداف عملکردی تعیین می‌کنند که چه زمان محصولات خاصی تولید می‌شوند، کدام پروژه‌ها یا مراحل پروژه باید تکمیل گردند و کدام فرایندها نیاز به اجرا و یا توسعه بیشتری خواهند داشت.

۵-۴ به‌روزرسانی NCS

این استراتژی در پایان سال ۲۰۲۲ به روز خواهد شد. در حالی که اجرا

به طور منظم مورد بررسی و تنظیم قرار می‌گیرد، به‌روزرسانی زودهنگام NCS تنها در صورت وجود تحولات غیر منتظره در وضعیت تهدید یا در صورت بروز سایر عواملی که فرضیات اساسی (که در بخش پیشینه ارائه شد) را زیر سوال می‌برند، پیش‌بینی می‌شوند. در صورت به‌روزرسانی زودهنگام، نسخه جدید NCS به شورای فدرال، دفاتر فدرال، کانتون‌ها و نمایندگان بخش خصوصی ارائه می‌شود.

بخش هفتم

بخش هفتم

لیست اختصارات

Action Plan for Cyber Defence	APCD	برنامه عملیاتی دفاع سایبری
Federal Office for Civil Protection	FOCP	دفتر حفاظت مدنی فدرال
Federal Office for National Economic Supply	FONES	دفتر تأمین اقتصاد ملی فدرال
Computer Emergency Response Team	CERT	تیم واکنش اضطراری رایانه‌ای
Federal Department of Finance	FDF	اداره سرمایه‌گذاری فدرال
European Union	EU	اتحادیه اروپا
EU Network and Information Security Directive	EU NIS	بخشنامه امنیت اطلاعات و شبکه اتحادیه اروپا
Federal Office of Police	fedpol	دفتر پلیس فدرال
Human Intelligence	HUMINT	هوش انسانی
Information and Communication Technologies	ICT	فناوری‌های اطلاعات و ارتباط
Federal IT Steering Unit	FITSU	واحد فرمان فناوری‌های اطلاعات فدرال
Information Technologies	IT	فناوری‌های اطلاعات

International Telecommunication Union	ITU	واحد ارتباطات از راه دوربین‌المللی
Conference of Cantonal Justice and Police Directors	CCJPD	کنفرانس مسئولان قضائی کانتون و پلیس
Conference of Cantonal Police Commanders of Switzerland	CCPCS	کنفرانس فرماندهان پلیس کانتون سوئیس
Reporting and Analysis Centre for Information Assurance	MELANI	مرکز گزارش و تحلیل برای تضمین اطلاعات
Armed Forces Act	ArmA	قانون بازنگری شده نیروهای مسلح
National strategy for the protection of Switzerland against cyber risks	NCS	استراتژی ملی برای حفاظت سوئیس در مقابل خطرات سایبری
Intelligence Service Act	IntSA	قانون سرویس اطلاعات
Investigation Support Network for Digital Law Enforcement	ISNDLE	شبکه پشتیبانی رسیدگی به اجرای قانون دیجیتال
National Research Programmes	NRP	برنامه‌های تحقیقات ملی
National Thematic Networks	NTN	شبکه‌های موضوعی ملی
Organisation for Economic Co-operation and Development	OECD	سازمان توسعه و همکاری اقتصادی
Open Source Intelligence	OSINT	اطلاعات منبع باز
Organization for Security and Co-operation in Europe	OSCE	سازمان امنیت و همکاری اروپا
Public-Private Partnership	PPP	شراکت خصوصی-عمومی
Regional Cyber Competence Centres	RC3	مراکز توانش سایبری منطقه‌ای

Secure Data Network	SDN+	شبکه داده امن
Federal Council Security Committee	FCSC	کمیته شورای امنیت فدرال
Critical Infrastructure Protection	CIP	حفاظت زیرساخت‌های حیاتی
Security Operations Centers	SOC	مراکز اقدامات امنیتی
Swiss Security Network	SSN	شبکه امنیت سوئیس
United Nations	UN	ملل متحد
Federal Department of Defence, Civil Protection and Sport	DDPS	اداره دفاع، حفاظت مدنی و ورزش فدرال
Upgrading of the Armed Forces	UAF	به‌روزرسانی نیروهای مسلح
World Economic Forum	WEF	انجمن اقتصاد جهانی
World Summit on the Information Society	WSIS	نشست جهانی جامعه اطلاعاتی
For Example	e.g.	برای مثال
Central Offices Act	COA	قانون دفاتر مرکزی

بخش هشتم

بخش هشتم

واژه‌نامه

حمله سایبری	اقدام غیرقانونی و بین‌المللی فرد یا گروه در فضای سایبری برای به‌خطر انداختن یکپارچگی، محرمانه بودن و دسترسی اطلاعات و داده بر اساس نوع حمله امکان اثرات فیزیکی هم وجود دارد.
خطرات سایبری	نتیجه احتمال رخداد و وسعت خسارتی که توسط حوادث سایبری ایجاد می‌شود.
جرم سایبری	در معنایی محدودتر، جرم سایبری به جرایمی اشاره دارد که با کمک ICT انجام می‌شوند یا از آسیب‌پذیری‌های این فن‌آوری بهره‌برداری می‌کنند به معنای وسیع‌تر، استفاده از اینترنت به‌عنوان ابزار ارتباطی، سوء استفاده از فرصت‌ها مانند ترافیک ایمیل یا تهیه و تبادل فایل برای اهداف خطرساز. این اقدامات مجرمانه جدید نیستند، اما ابزار ارتکاب یا ذخیره‌سازی رسانه استفاده‌شده، (ایمیل، اسنپ‌چت، واتساپ، اینستاگرام، تلگرام و حاملان داده الکترونیکی به¬جای کاغذ، خدمات ابری و غیره) جدید هستند.
فضای سایبری	تمام زیرساخت‌های ارتباطی و اطلاعاتی (سخت‌افزار و نرم‌افزار) که به تبادل، جمع‌آوری، ذخیره‌سازی و پردازش داده می‌پردازد یا داده را به اعمال (فیزیکی) تبدیل می‌کند و امکان تعامل میان اشخاص، سازمان‌ها و دولت‌ها را فراهم می‌سازد.
خرابکاری سایبری	فعالیت‌هایی که برهم‌زدن یا تخریب عملکرد بدون خطا و قابل اعتماد زیرساخت‌های ارتباطی و اطلاعاتی در فضای مجازی را هدف قرار می‌دهند. بسته به نوع خرابکاری، می‌تواند این عمل همراه با اثرات فیزیکی نیز همراه باشد.

جاسوسی سایبری	فعالیت‌های برای دسترسی غیرمجاز به اطلاعات محافظت‌شده اقدامات اقتصادی، نظامی و سیاسی در فضای مجازی.
دفاع سایبری	تمام اقدامات اطلاعاتی و نظامی برای اختلال، سرکوب یا کاهش سرعت حملات سایبری، اطمینان از آمادگی عملیاتی نیروهای مسلح در تمامی اوضاع، ایجاد ظرفیت و قابلیت پشتیبانی کمکی به مسئولین غیرنظامی.
حادثه سایبری	رویدادی عمدی یا غیرعمدی در فضای مجازی که بر یکپارچگی، محرمانه‌بودن و دسترسی داده‌ها و اطلاعات اثر سوء بگذارد و منجر به اختلال در عملکرد آن‌ها شود.
زیرساخت‌های حیاتی	فرایندها، سیستم‌ها و امکاناتی که برای عملکرد اقتصاد و رفاه مردم ضروری است.
انعطاف‌پذیری (مقاومت)	توانایی یک سیستم، سازمان یا جامعه برای مقاومت و پایداری در برابر اختلالات و حفظ قابلیت عملکرد تا حد ممکن یا بازیابی سرعت عملکرد.
امنیت‌سایبری	وضعیت مطلوب در فضای مجازی که تبادل داده و ارتباط بین زیرساخت‌های اطلاعاتی و ارتباطی بر اساس آنچه مورد نظر است، انجام می‌شود. این وضعیت از طریق اقدامات امنیت اطلاعات و دفاع سایبری به دست می‌آید.
امنیت اطلاعات/امنیت ICT	امنیت اطلاعات (یا امنیت ICT)، عدم اختلال در اعتبار، محرمانه‌بودن، یکپارچگی و در دسترس بودن سیستم فناوری اطلاعات و ارتباطات می‌باشد که داده‌ها در آن پردازش و ذخیره می‌شوند.
تهدیدسایبری	فرایندی که می‌تواند منجر به یک حادثه سایبری شود.

csri.majazi.ir

حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانه پر از آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان تر می شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت. اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم می‌شود یک تهدید.

csri.majazi.ir