سومین همایش ملی تحقیقات میان رشته ای در علوم مهندسی و مدیریت
3rd Interdisciplinary Research Conference in Engineering & Management Sciences
25 February 2022-Tehran
۶ اسفند ۱۴۰۰
محل برگزاری: تهران

استراتژی امنیت سایبری

سهیل انوشا
کارشناس ارشد مهندسی کامپیوتر، شرکت آب و فاضلاب استان کرمانشاه، کرمانشاه، ایران
soheil.anousha@gmail.com

مهنوش نیکجو
کارشناس ارشد مدیریت بازرگانی، شرکت آب و فاضلاب استان کرمانشاه، کرمانشاه، ایران
M.Nikjou1372@gmail.com

روح اله کولیوند
کارشناس ارشد حقوق جزا و جرم شناسی، شرکت آب و فاضلاب استان کرمانشاه، کرمانشاه، ایران
rohollah.koolivand@gmail.com

چکیده

بطور کلی کسب اطلاعات یک جنبه بسیار مهم در دیپلماسی و حتی در یک درگیری مسلحانه می باشد. با این حال، از دهه ۱۹۹۰ و با گسترش روزافزون فناوری ، نقش و اهمیت اطلاعات در امنیت و روابط بین الملل و در جهت نیل به اهداف سیاسی افزایش یافته است. امنیت سایبری یک مؤلفه مهم در زیرساخت های کشور است. موفقیت در امنیت فضای سایبری به توانایی یک کشور در محافظت از اطلاعات اختصاصی و داده های خود در مقابل افراد، نهادها و کشورهایی که قصد سوء استفاده از آن را دارند، بستگی دارد. یک استراتژی امنیت سایبری قوی می‌تواند وضعیت مناسبی را در مقابل حملات خرابکارانه که برای دسترسی، تغییر، حذف، تخریب و یا بدست گرفتن سیستم‌های کاربران یا سازمان ها و داده‌های حساس طراحی شده‌اند، فراهم نماید. امنیت سایبری همچنین در جلوگیری از حملاتی که هدفشان از کار انداختن یا اخلال در عملیات‌های دستگاه یا سیستم است، مفید می باشد. مجموعه ای از کشورها استراتژی امنیت سایبری ملی خود را منتشر کرده اند. علی رغم اینکه هریک از این کشورها با تهدیدات مشابهی در زمینه امنیت سایبری مواجه هستند، اما تفاوت های بنیادین زیادی در روش ها و رویکردهای سایبری آن ها در زیرساخت های حساس و حیاتی آن ها مشاهده می شود. این مقاله قصد دارد اهمیت ارائه یک استراتژی امنیت سایبری منطبق بر سیاست های بالادستی را ارائه داده و مراحل ایجاد آن را شرح دهد تا در نهایت به یک رویکردی بومی جهت توسعه امنیت سایبری و در نهایت امنیت ملی برسد.

واژگان کلیدی: امنیت سایبری، زیرساخت های حیاتی، حملات خرابکارانه، استراتژی ملی، رویکرد بومی

۱- معرفی

مفهوم امنیت تحت تاثیر تحولات سطح کلان بین الملل دستخوش تغییر شده و با شروع روند جهانی شدن و تحت تاثیر فناوری اطلاعات و ارتباطات[1] مفهومی چند بعدی یافته است. با شکل گیری فضای سایبر و رشد سریع آن مفاهیم عرصه زندگی نیز به سمت تغییر ماهوی گام برداشت. امنیت در پارادایم[2] فضای سایبری تابع دو عنصر کلیدی انسان و فضای سایبر است.[3] مسئله اول انسان ویژگی ها و قابلیت هایش است و مسئله دوم ابعاد، قابلیت ها و مبانی شکل گیری فضای سایبری است. استراتژی امنیت سایبری[4] می تواند یک طرح و برنامه برای ایمن نمودن یک شرکت، سازمان، نهاد و یا کشور جهت حفاظت از دارایی های خود باشد. از آنجایی که فناوری و تهدیدات سایبری می توانند به طور غیرقابل پیش‌بینی تغییر کنند، در بسیاری از مواقع باید استراتژی خود را بسرعت به روزرسانی کنید. همچنین ذکر این نکته ضروری است که قرار نیست استراتژی امنیت سایبری کامل باشد، در واقع این یک حدس و پیش بینی کاملاً آموزش دیده در مورد آنچه باید انجام دهید است. همانطور که سازمان و دنیای اطراف شما تکامل می یابد، استراتژی امنیت سایبری ما نیز باید تکامل یافته و تغییر کند. نتیجه در نظر گرفته شده از توسعه و اجرای استراتژی امنیت سایبری این است که دارایی های شما امنیت بهتری داشته باشد. امنیت سایبری به طور کلی شامل تغییر رویکرد امنیتی از اقدام واکنشی به اقدام پیشگیرانه است، جایی که شما بیشتر بر پیشگیری از حملات و حوادث سایبری متمرکز هستید تا اینکه بعد از رخداد امنیتی[5] به آنها واکنش نشان دهید. البته یک استراتژی امنیت سایبری مستحکم سازمان شما را برای پاسخگویی به حوادثی که رخ می‌دهند، آماده تر می‌کند. با جلوگیری از بزرگتر شدن حوادث جزئی، سازمان شما می تواند ضمن حفظ اعتبار خود، از آسیب رسیدن به سازمان، کارکنان، مشتریان، شرکا و دیگران جلوگیری نماید.

۲- استراتژی ملی

بنا به تعریف، استراتژی به عنوان یک برنامه عملی که برای دستیابی به یک چشم انداز خاص طراحی شده است، تعریف می گردد. این تعریف از استراتژی شامل جنبه هایی مانند رهبری[6] اهداف، آینده مطلوب و یک جهت یا مسیر که دستیابی به چشم انداز[7] را ممکن می سازد، می باشد.

براین اساس استراتژی ملی به این صورت تعریف می گردد: *"یک برنامه اقدام ملی مدون مبتنی بر چشم انداز ملی بمنظور دستیابی به مجموعه ای از اهداف که به امنیت حوزه فضای مجازی کمک کند"*

به طور کلی، یک استراتژی ملی اهداف متفاوتی را دنبال می کند:

۱. هماهنگی نمودن کل ارکان دولت (حکومت)

[1] ICT (Information and Communication Technology)
[2] Paradigm
[3] Cyberspace
[4] Cybersecurity Strategy
[5] Security incident
[6] Leadership
[7] Vision

۲. منسجم نمودن نقش ها، مسئولیت ها و روابط بین همه ذینفعان (دولت، سازمان های مدنی، نهادهای نظارتی، زیرساخت های حیاتی، صنعت و تجارت، شرکت ها ، سازمان های تحقیق و توسعه، دانشگاه ها، تک تک شهروندان و به طور کلی همه جمعیت.)

۳. انتقال علایق استراتژی ملی به سایر ملت ها

۳- فضای سایبری

فضای سایبر در معنا به مجموعه هایی از ارتباطات درونی انسان ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظرگرفتن جغرافیای فیزیکی گفته می شود. طبق تعریف، فضای سایبری به دنیایی مجازی گفته می‌شود که با متصل کردن کامپیوترها، دستگاه‌های با قابلیت اتصال به اینترنت، سرورها، روترها و سایر مولفه‌هایی که زیرساخت اینترنت را شکل می‌دهند پدید می‌آید. فضای مجازی، برخلاف خود اینترنت، موجودیتی است که توسط این پیوندها پدید می‌آید.

۳-۱- امنیت سایبری

امنیت سایبری یعنی محافظت از سیستم‌ها، شبکه‌ها، برنامه‌ها و سامانه های نرم افزاری در برابر حملات دیجیتالی. هدف از امنیت سایبری، محافظت از اطلاعات در برابر سرقت و آسیب است. بدون وجود امنیت سایبری، سازمان‌ها نمی‌توانند از خود در برابر نقض‌های داده‌ای و حمله‌های هکرها[8]دفاع کنند و به هدفی ساده برای مجرمان سایبری تبدیل می‌شوند. مخاطرات امنیتی به دلیل گسترده‌تر شدن ارتباطات در مقیاس جهانی و استفاده از سرویس‌های ابری[9]برای ذخیره‌سازی اطلاعات حساس و شخصی رو به افزایش است.

دسترسی، نابودی و تغییر در اطلاعات مهم، دریافت پول از کاربران و در نهایت ایجاد وقفه در روال کسب‌وکارها از اهداف حملات سایبری است. حفاظت از سامانه‌های اطلاعات در برابر آسیب رساندن به سخت‌افزار، نرم‌افزار و اطلاعات سامانه ها و محافظت در برابر این حملات، نمونه پارامترهایی هستند که امنیت رایانه‌ای را مورد سنجش قرار می دهند. تهدیدات سایبری با سرعت زیادی رشد می‌کند و هر ساله تعداد زیادی نفوذ به سیستم ها در حال رخ دادن است. برخی مفاهیم در تهدیدات سایبری دنیای امروز بسیار مورد استفاده قرار می گیرد عبارت است از :

۳-۱-۱- جرایم سایبری:[10]

عبارت است از فرد یا گروهی که سیستم‌ها را مورد هدف قرار داده تا از آن طریق درآمد کسب کنند و یا موجبات خرابکاری در سیستم ها را فراهم نمایند.

۳-۱-۲- حمله سایبری:[11]

اغلب با هدف جمع‌آوری هدفمند اطلاعات و با انگیزه های سیاسی رخ می دهد.

[8] Hackers
[9] Cloud Services
[10] Cybercrime
[11] Cyberattack

۳-۱-۳- تروریست سایبری:[12]

با هدف ایجاد رعب و وحشت به وسیله خراب کردن سیستم‌های الکترونیکی انجام می گیرد.

۳-۲- تهدیدات سایبری

تهدیدات فضای سایبری که کاربران، تجهیزات و شبکه‌ها را مورد حمله قرار می دهند، می توانند به صورت ذیل دسته‌بندی می‌شوند:

۳-۲-۱- تهدیدات شبکه ای

کاربران، تجهیزات و کانال‌های ارتباطی (شبکه‌های بی‌سیم و سیمی) در معرض انواع مختلفی از تهدیدات سایبری نظیر نفوذ،[13] حمله انکار سرویس،[14] حمله انکار سرویس توزیع شده،[15] حمله سیلابی، باتنت‌ها،[16] ویروس‌ها، باج‌افزارها[17] و... قرار دارند.

۳-۲-۲- تهدیدات مرتبط با برنامه‌های کاربردی

تمامی برنامه‌های کاربردی از سامانه‌های مدیریت بانک‌های اطلاعاتی گرفته تا برنامه‌های دسکتاپ، موبایل و سرور ممکن است به آسیب‌پذیری‌هایی آلوده باشند که به هکرها اجازه دهند به واسطه آن‌ها به سامانه‌ها حمله کنند.

۳-۲-3- تهدیدات دستری از راه دور[18]

دسترسی از راه دور یکی از ارکان اجتناب‌ناپذیر کسب‌وکارهای امروزی است. همین مسئله شکاف امنیتی بزرگی به وجود می‌آورد که در نهایت نقض داده‌ای را باعث می‌شود. در این تهدید هکرها می‌توانند رمز عبور و نام حساب کاربری یک کارمند را سرقت نموده و به شکلی کاملاً مشروع به شبکه سازمانی نفوذ کنند.

۳-۲-۴- تهدیدات دستکاری داده‌ها[19]

گاهی اوقات حمله‌های هکری با هدف دستکاری اطلاعات پایگاه‌های داده‌ای انجام می‌شوند. در این نوع تهدید هکرها پس از نفوذ به یک پایگاه داده، سعی می‌کنند با ارتقای سطح دسترسی خود به ویرایش اطلاعات درون پایگاه‌های داده و نسخه‌های پشتیبان آن بپردازند.

4- طراحی استراتژی امنیت سایبری

با افزایش حجم و پیچیدگی حملات سایبری، شرکت‌ها و سازمان‌ها به ویژه آن‌هایی که وظیفه حفاظت از اطلاعات محرمانه مربوط به امنیت ملی و یا سوابق مالی را بر عهده دارند، باید اقدامات لازم بمنظور محافظت از این اطلاعات حساس را انجام دهند. ایجاد یک استراتژی امنیت سایبری منسجم برای یک سازمان ایده ای مناسب برای این منظور است که البته نیاز به تلاش بسیار زیادی دارد و از مراحل و گام های مختلفی تشکیل می شود. این گام ها عبارتند از :

۴-۱- گام اول: درک چشم انداز تهدیدات سایبری

[1] Cyberterrorism
[2]
[1] Penetration
[3]
[1] Denial of Service (DoS)
[4]
[1] Distributed Denial of Service (DDoS)
[5]
[1] Botnets
[6]
[1] Ransomware
[7]
[1] Remote Access Threats
[8]
[1] Data Manipulation Threats
[9]

قبل از اینکه بتوانید چشم انداز تهدیدات سایبری خود را درک کنید، باید درک درستی از این تهدیدات و انواع حملات سایبری را که امروزه سازمان شما با آن مواجه است را داشته باشید. این امر می تواند به این شکل نمایان شود که در حال حاضر کدام نوع از این تهدیدات بیشتر و شدیدتر بر سازمان شما تأثیر می‌گذارند:

بدافزار،[20] فیشینگ،[21] تهدیدات داخلی یا چیز دیگری؟ آیا سازمان ها و شرکت های مشابه شما اخیراً حوادث بزرگی داشته اند و اگر چنین است، چه نوع تهدیدهایی باعث آنها شده است؟

در مرحله بعد، با روندهای پیش بینی شده تهدیدات سایبری که بر سازمان شما تأثیر می گذارد، خود را آماده کنید. به عنوان مثال، بسیاری از محققان امنیتی احساس می‌کنند که با رونق گرفتن کسب‌وکارها، باج‌افزارها به تهدید بزرگ‌تری تبدیل می‌شوند. همچنین نگرانی‌های فزاینده‌ای در مورد تهدیدات در حوزه زنجیره اطلاعات وجود دارد، به این صورت که اطلاعات آسیب‌دیده و استفاده از آن در منابع اطلاعاتی می تواند منجر به دریافت اطلاعات غیرواقعی و نادرست از سامانه ها شود. درک چشم انداز تهدیدات سایبری می تواند بطور فزاینده ای سازمان را در برابر این تهدیدات مقاوم سازد.

۴-۲- گام دوم: ارزیابی بلوغ امنیت سایبری سازمان متبوع

هنگامی که متوجه شدید با چه چیزی روبرو هستید، باید یک ارزیابی کامل و دقیق از بلوغ امنیت سایبری سازمان خود انجام دهید. یک چارچوب امنیت سایبری را انتخاب نموده و از آن برای ارزیابی میزان بلوغ سازمان خود در دسته‌بندی و زیرمجموعه مختلفی از خط‌مشی‌ها و حاکمیت گرفته تا فناوری‌های امنیتی و قابلیت‌های بازیابی حوادث استفاده کنید. این ارزیابی باید شامل تمام فناوری‌های شما، از فناوری اطلاعات سنتی گرفته تا فناوری عملیاتی، اینترنت اشیا[22] و سیستم‌های فیزیکی سایبری باشد. در مرحله بعد، از همان چارچوب امنیت سایبری استفاده کرده و تعیین نمایید که سازمان متبوع شما در سه تا پنج سال آینده از نظر بلوغ برای هر یک از آن دسته‌ها و زیرمجموعه‌ها در کجا قرار گیرد.

اگر به عنوان مثال باج‌افزار بزرگ‌ترین مشکل امنیتی شماست، اطمینان از اینکه قابلیت‌های پشتیبان‌گیری و بازیابی شما بسیار بالغ هستند، ممکن است کلیدی باشد. اگر خط‌مشی‌های دسترسی از راه دور ناشی از همه گیری ویروس کرونا دائمی شوند، ابزارهای موقتی که در طول همه‌گیری استفاده می‌شوند باید قابلیت های امنیتی سخت تری داشته باشند یا اگر، حملات انکار سرویس توزیع شده یک تهدید بزرگ باشد، ممکن است بخواهید قابلیت های امنیتی شبکه شما به طور ویژه بالغ شود.

۴-۳- گام سوم: تعیین نحوه بهبود برنامه امنیت سایبری

اکنون که می‌دانید کجا هستید و می‌خواهید کجا باشید، باید ابزارهای امنیت سایبری و بهترین روش‌هایی را که به شما در رسیدن به اهدافتان کمک می‌کنند، پیدا کنید. در این مرحله، شما تعیین می کنید که چگونه برنامه امنیت سایبری خود را بهبود بخشید تا به اهداف استراتژیکی که تعریف کرده اید دست یابید. هر بهبودی در برنامه مذکور مستلزم صرف هزینه و منابع بوده لذا باید مزایا و معایب رسیدن به اهداف هر گزینه را بررسی نموده و تفکر لازم را در انتخاب آن انجام دهید. بطور مثال ممکن است به این نتیجه برسید که برخی یا همه وظایف امنیتی خود را برون سپاری کنید، در اینصورت مقدار هزینه و منابع صرف شده در این تصمیم را باید درنظر گرفته و سپس اقدامات خود را در آن راستا انجام دهید. هنگامی که مجموعه‌ای

[20] Malware
[21] Phishing
[22] IoT (Internet of Tools)

از گزینه‌ها را انتخاب نمودید، آن‌ها را برای بررسی، دریافت بازخورد[۲] و احتمالا در جهت حمایت بیشتر به مدیریت ارشد سازمان خود ارائه دهید. تغییرات در برنامه امنیت سایبری ممکن است بر نحوه انجام امورات سازمان تأثیر بگذارد، بنابراین باید شرایطی ایجاد گردد که مدیران نه تنها باید آن را بخوبی درک نمایند بلکه آن را به عنوان ضرورتی اجتناب ناپذیر بپذیرند تا به اندازه کافی از شرکت در برابر تهدیدات سایبری محافظت کنند. همچنین مدیر ارشد سازمان باید بخوبی از برنامه‌های دیگری که برای سال‌های آینده در زمینه امنیت سایبری درنظر گرفته شده است نیز آگاه باشد تا به بهبود مستمر آن کمک نماید. این امر به شکل فزاینده ای به گام اول طراحی استراتژی امنیت سایبری سازمان وابسته می باشد.

۴-۴- گام چهارم: مستند نمودن استراتژی امنیت سایبری

پس از تأیید مدیریت ارشد سازمان، باید اطمینان حاصل کنید که استراتژی امنیت سایبری شما به طور کامل مستند شده است. مستندسازی استراتژی امنیت سایبری شامل نوشتن یا بروزرسانی ارزیابی‌های ریسک، برنامه‌های امنیت سایبری، سیاست‌ها، دستورالعمل‌ها، رویه‌ها و هر چیز دیگری است که برای تعریف آنچه برای دستیابی به اهداف استراتژیک مورد نیاز یا توصیه می‌شود، نیاز دارید. روشن کردن وظایف هر فرد کلیدی است.

مطمئن باشید که هنگام نوشتن و به روز رسانی این اسناد، مشارکت فعال و بازخوردی از افرادی دریافت می کنید که کار مرتبط را انجام خواهند داد. همچنین باید برای آنها توضیح دهید که چرا این تغییرات ایجاد شده است و این تغییرات چقدر دارای اهمیت می باشد تا مردم بیشتر آن را پذیرفته و حمایت نمایند. همه افراد در سازمان نقشی در کاهش مسائل امنیتی و بهبود برنامه امنیت سایبری دارند. فراموش نکنید که استراتژی امنیت سایبری سازمان شما نیازمند به روز رسانی آگاهی و تلاش های آموزشی در مورد امنیت سایبری است و همانطور که مشخصات ریسک شما تغییر می کند، فرهنگ امنیت سایبری شما نیز باید تغییر کند.

۵- چشم انداز امنیت سایبری ملی در برخی کشورها

جدول ۵-۱ چشم انداز امنیت سایبری برخی از کشورهای جهان را نشان می دهد. علی رغم اینکه هریک از این کشورها با تهدیدات مشابهی در زمینه امنیت سایبری مواجه هستند، اما تفاوت هایی در روش ها و رویکردهای سایبری آن ها علی الخصوص در زیرساخت های حساس و حیاتی آن ها مشاهده می شود. نکته جالب توجه و مشترک در بررسی جدول ۱-۵ این می باشد که کشورهای یادشده به شدت به ایمن سازی محیط فضای مجازی اهتمام ورزیده و چشم اندازهای ارائه شده توسط خود را بر حفظ منافع سایبری متمرکز نموده اند.

[2] Feedback

[3]

جدول ۵-۱ : چشم انداز سایبری برخی از کشورها

اتریش	نگهداری ایمن، انعطاف پذیر و قابل اعتماد از محیط عملیاتی الکترونیکی کشور که در آن از امنیت ملی حمایت شود و منافع اقتصاد دیجیتال را به حداکثر برساند
کانادا	طرح ملی برای امن تر کردن فضای مجازی برای همه کانادایی ها
چک	منافع و مقاصد جمهوری چک را در زمینه سایبری تعریف کرده و برای تأمین امنیت برای یک جامعه اطلاعاتی معتبر با ضمانت های حقوقی قوی مناسب که در آن سازمان ها متعهد به انتقال امن سایبری و پردازش اطلاعات در تمامی حوزه های فعالیت های انسانی بوده و اطمینان حاصل می کند که اطلاعات را می توان آزادانه و ایمن استفاده نموده و به اشتراک گذاشت.
آلمان	هدف و چشم انداز دولت فدرال آلمان پیاده سازی فضای سایبری امن در کشور می باشد که نتیجه آن حفظ و ارتقای اقتصادی، اجتماعی و رفاه کشور است
اسپانیا	تضمین امنیت کشور، شهروندان و ساکنان آن در دامنه فضای مجازی.
بریتانیا	چشم انداز بریتانیا این است که ارزش اقتصادی و اجتماعی عظیمی از فضای سایبری بدست آورد، ایجاد محیطی امن و انعطاف پذیر که ارزش های اصلی کشور مانند آزادی، عدالت، شفافیت و حاکمیت قانون بر آن حاکم بوده و موجب افزایش رفاه، امنیت ملی و قدرتمند شدن جامعه می شود و اقدامات دولت توسط آن هدایت می شود.
آمریکا	هدف از این استراتژی توانمندسازی آمریکایی ها برای تامین امنیت بخش‌های مختلف از فضای مجازی است که یا مالک آن می باشند و یا تحت کنترل خود دارند و به نوعی با آن در تعامل هستند
ژاپن	دولت مسئول غلبه بر خطرات مربوط به استفاده از فناوری اطلاعات و ارتباطات می باشد. این امر از طریق تقویت حفاظت از زیرساخت های حیاتی و حمایت از فعالیت های اجتماعی-اقتصادی که ارتباط تنگاتنگ و نزدیکی با زندگی روزمره مردم دارد با تضمین امنیت ملی و مدیریت موثر بحران انجام می گیرد.

۶- نتیجه گیری

توسعه و اجرای استراتژی امنیت سایبری یک فرآیند مداوم است و چالش های زیادی را به همراه خواهد داشت. بسیار مهم و ضروری است که بلوغ امنیت سایبری سازمان خود را به طور دوره‌ای و مداوم مورد نظارت و ارزیابی مجدد قرار داده تا پیشرفت هایی که در راستای اهداف خود بدست آورده اید را مورد سنجش قرار دهید. هرچه زودتر قسمت هایی که ضعف بیشتری را دارند شناسایی کنید، در این صورت زودتر می توانید به آن ها رسیدگی نموده و به عقب برگردید. اندازه‌گیری پیشرفت باید شامل ممیزی‌های داخلی و خارجی، آزمایش‌ها و تمرین‌هایی باشد که آنچه را که در شرایط مختلف اتفاق می‌افتد، مانند یک حادثه بزرگ باج‌افزار، را شبیه‌سازی کند. در نهایت، هر لحظه آماده باشید که در صورت بروز یک تهدید جدید، در استراتژی امنیت سایبری خود تجدید نظر کنید. به خاطر داشته باشید که چابکی در امنیت اهمیت فزاینده ای دارد.

از به روز رسانی استراتژی خود هراسی نداشته باشید زیرا تهدیدات سایبری و فناوری های امنیتی مداوم تغییر می کنند و سازمان شما انواع جدیدی از دارایی ها را به دست می آورد که نیاز به محافظت دارند.

۷- منابع

Deibert, R. and Rohozinski, R. (2010) 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology* 4 / 1: 15–32. An intelligent account of the threat discourse that differentiates between risks to cyberspace and risks through cyberspace.

The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, Cabinet Office, London, UK, available at https://update.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategyfinal.pdf (accessed on May 5, 2012).

Dunn Cavelty, M. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London: Routledge. Examines how, under what conditions, by whom, for what reasons, and with what impact cyber-threats have been moved on to the political agenda in the USA.

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, The White House, Washington DC, USA, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed on May 5, 2012).

Information Systems Defence and Security: France's Strategy, Secrétariat général de la défense et de la sécurité nationale, Paris, France, (accessed on May 5, 2012).

Convention on Cybercrime, Council of Europe, ETS No. 185, available at http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm (accessed on May 5, 2012).

Wikipedia (2012) available at http://en.wikipedia.org/wiki/Strategy (accessed on June 2, 2012).