

قوانین امنیت سایبری

نویسنده:

دکتر حامد، حاجی ملامیرزایی

دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

مرکز انتشارات راهبردی

تهران - ۱۳۹۸

سرشناسه	: حاجی ملامیرزائی، حامد، ۱۳۵۹ -
عنوان و نام پدیدآور	: قوانین امنیت سایبری/نویسنده حامد حاجی ملامیرزایی؛ ویراستار مهدی یوسفی.
مشخصات نشر	: تهران: دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، مرکز انتشارات راهبردی، ۱۳۹۸
مشخصات ظاهری	: ۲۹۵ ص.
شابک	: ۹۷۸-۶۲۲-۶۳۵۰-۸۸-۴
وضعیت فهرست نویسی	: فیبا
موضوع	: جرایم کامپیوتری
موضوع	: Computer crimes
موضوع	: جرایم کامپیوتری -- قوانین و مقررات
موضوع	: Computer crimes -- Law and legislation
موضوع	: جرایم کامپیوتری -- قوانین و مقررات -- ایران
موضوع	: Computer crimes -- Law and legislation-- Iran
موضوع	: امنیت ملی -- قوانین و مقررات -- ایران
موضوع	: National security-- Law and legislation-- Iran
شناسه افز	: دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، مرکز انتشارات راهبردی
رده بندی کنگ	: HV۶۷۷۳
رده بندی دیویی	: ۳۴۰/۱۶
شماره کتابشناسی ملی	: ۵۷۵۱



عنوان کتاب: قوانین امنیت سایبری

نویسنده: حامد حاجی ملامیرزایی

ویراستار ادبی: مهدی یوسفی

ناظر ویراستار: مهران غلامیان

صفحه آرا: مینا مجلسی

طراح جلد: زهرا مهدوی

نوبت چاپ: اول- ۱۳۹۸

ناشر: انتشارات دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

شمارگان: ۱۰۰۰ نسخه

قیمت: ۵۵۰۰۰۰ ریال

همه حقوق چاپ و نشر این کتاب محفوظ است.

دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

مرکز انتشارات راهبردی

نشانی انتشارات: تهران، ضلع شمالی بزرگراه شهید بابایی، بعد از اتوبان هنگام،

دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، انتشارات دانشگاه عالی دفاع ملی

نشانی اینترنتی: www.sndu.ac.ir

تلفن: ۲۲۹۷۰۳۴۳

فهرست مطالب

۱۵	 مقدمه
۱۵	بخش اول: کلیات
۱۹	فصل اول: مفهوم و اهمیت فضای سایبری
۲۸	 مفهوم امنیت
۳۴	 اهمیت امنیت سایبری
۳۴	 بررسی آماری
۳۵	فصل دوم: نمودارهایی از ملات
۳۹	 استاکس نت
۳۹	 جنگ سایبری
۴۰	 آپ اسرائیل
۴۱	 حمله سراسری
۴۳	 اعتراض اینترنتی و حمله به صفحات شخصی
۴۴	 دزدی اطلاعات بانکی
۴۴	 دزدی اطلاعات کاربری
۴۵	 جاسوسی دولتی
۴۵	 باران تایتان
۴۵	فصل سوم: حملات از نگاه آمار
۵۱	بخش دوم: امنیت سایبری در قانون (خط مشی ها و حقوق بین الملل)
۵۵	 اقدامات کشورهای پیشرو در زمینه امنیت سایبری
۶۷	فصل چهارم: امنیت سایبری در قانون؛ آمریکا
۶۹	 نگاه تاریخی
۷۱	 دسته بندی قوانین
۷۷	 نمونه هایی از قوانین مرتبط با جرائم سایبری
۸۷	فصل پنجم: امنیت سایبری در قانون؛ چین
۸۹	 نگاه تاریخی
۹۱	 دسته بندی قوانین
۹۲	 حفاظت از اطلاعات شخصی
۹۴	 زیرساخت اطلاعات حیاتی

۹۵	اپراتورهای شبکه
۹۶	حفاظت از اطلاعات حساس
۹۶	گواهی برای محصولات امنیتی
۹۷	مسئولیت‌های قانونی
۹۸	قانون جرائم سایبری
۹۹	دسترسی غیر مجاز به رایانه
۱۰۰	دسترسی غیر مجاز به سیستم‌های اطلاعاتی فهرست شده
۱۰۱	تغییر غیر مجاز داده‌های ذخیره شده روی سیستم اطلاعات رایانه‌ای و کنترل غیر مجاز سیستم اطلاعات رایانه‌ای
۱۰۲	ارائه‌ی ابزارهای خاص برای دسترسی غیر مجاز، به دست آوردن غیر مجاز داده‌ها و کنترل غیر مجاز رایانه‌ها
۱۰۴	مداخله‌ی رایانه‌ای
۱۰۵	مسئولیت کیفی تأمین کننده خدمات شبکه
۱۰۶	جرائم سنتی که با رایانه تسهیل شده است
۱۰۶	استفاده غیر قانونی از شبکه‌ی اطلاعات
۱۰۷	مسئولیت فرعی، شرکت در جرم
۱۰۷	صلاحیت قانونی
۱۰۹	فصل ششم: امنیت سایبری در قانون؛ بریتانیا
۱۱۶	دفاع
۱۲۶	بازداشتن (ممانعت)
۱۲۹	توسعه
۱۴۷	فصل هفتم: راهبرد امنیت سایبری؛ استرالیا
۱۵۳	مشارکت سایبری ملی
۱۵۳	دفاع سایبری قدرتمند
۱۶۷	بخش سوم: ایران در امنیت سایبری
۱۶۹	فصل هشتم: امنیت سایبری در قانون؛ ایران
۱۷۱	نگاه تاریخی
۱۷۲	دسته‌بندی قوانین
۱۷۴	داده‌ها و سیستم‌های رایانه‌ای و مخابراتی
۱۸۴	سایر قوانین
۱۹۱	فصل نهم: سیاست‌های مرتبط با امنیت سایبری ج.ا.ایران

۱۹۳ مطابق برنامه پنجم توسعه

۱۹۸ مطابق برنامه ششم توسعه

بخش چهارم: تحلیل و ارزیابی حقوقی کشورها در امنیت سیاسی..... ۲۰۷

۲۰۹ فصل دهم: وضعیت ایران در شاخص بین‌المللی امنیت سایبری

۲۱۵ فصل یازدهم: تحلیل و ارزیابی حقوقی کشورها در امنیت سایبری

۲۱۷ ایالات متحده آمریکا

۲۱۹ اتحادیه اروپا

۲۲۱ فرانسه

۲۲۲ استرالیا

۲۲۵ فصل دوازدهم: مطالعه تطبیقی قانون کشورها

بخش پنجم: مدل ماندگار امنیت سایبری..... ۲۲۹

فصل سیزدهم: تهدیدکننده‌ها

۲۳۳ سایبری

۲۳۵ جرم سایبری

۲۳۶ تهدیدکننده‌های امنیت سایبری

۲۴۱ فصل چهاردهم: آسیب‌پذیری‌های سایبری

۲۴۳ محدوده‌ی روبرو افزایش تجهیزات

۲۴۴ سلامت و مطلوبیت ضعیف سایبری

۲۴۵ آموزش و مهارت ناقص

۲۴۵ سیستم‌های موروثی و بدون وصله

۲۴۵ دسترسی‌پذیری منابع هک

۲۴۶ جمع‌بندی

۲۴۷ فصل پانزدهم: انواع تهدیدها در امنیت سایبری

۲۴۹ موضوعات مورد تهدید در فضای سایبری

۲۵۰ ارائه مدل مفهومی ساماندهی امنیت سایبری

۲۶۱ فصل شانزدهم: مدل مفهومی ساماندهی امنیت سایبری

۲۶۳ نیازهای راهبردی کشور در امنیت سایبری

۲۶۵ سیاست‌ها و اقدامات پیشنهادی

۲۶۷ جمع‌بندی

۲۶۹ پیوست

اصطلاحات مرتبط با امنیت سایبری ۲۶۹

مراجع ۲۷۰

www.ketab.ir

مقدمه

امروزه با توسعه فضای سایبری، برقراری امنیت در این فضا به یکی از دغدغه‌های اساسی کشورها تبدیل شده است. نوظهور بودن این فضا به همراه سرعت بسیار بالای پیشرفت و توسعه فناوری‌های مرتبط با این فضا، کار کشورها و دولت‌ها را برای برقراری امنیت به چالش کشیده است. علاوه بر موارد ذکر شده، چالش‌هایی نظیر محدود نبودن فضای سایبری به مرزهای فیزیکی کشورها باعث شده تا برای برقراری کامل امنیت در این فضا نیاز به یک همکاری بین‌المللی قوی نیز وجود داشته باشد. فقدان قوانین و مقررات کامل در کشور در زمینه مدیریت امنیت سایبری، باعث ناشناس ماندن این فضا شده و کار را برای برقراری امنیت سایبری در کشور پیش‌ازپیش چالش‌برانگیز کرده است. نگاهی به حملات سایبری صورت پذیرفته در سال‌های اخیر نشان می‌دهد که در صورت عدم توجه کافی به برقراری امنیت در این فضا کشور در اندک زمانی با چالش‌های بسیار بزرگی روبرو خواهد شد. توجه به این نکته نیز ضروری است که مرموزان سایبری برخلاف دیگر مجرمان افرادی خیره در این عرصه هستند و می‌توانند تهدیدات جدی برای کشور محسوب شوند.

در این کتاب سعی شده است تا با بررسی جامع فضای سایبری، شناخت کاملی از تمام جنبه‌های آن صورت گرفته و تمامی چالش‌ها و کمبودهای مدیریتی و حقوقی برای برقراری امنیت سایبری در کشور شناخته شود. علاوه بر این‌ها، تجربیات کشورهای پیشرو در این عرصه نیز مورد شناخت، ارزیابی و تحلیل قرار گرفته و با انجام مقایسه تطبیقی بین قوانین دیگر کشورها با قوانین مرتبط موجود در ایران، نقص‌ها و کاستی‌های حقوقی موجود در قوانین کشور در این زمینه شناسایی شود.