بسم الله الرحمن الرحیم

راهبردهای امنیت سایبری در چین

گردآوری و تدوین
معاونت پژوهش و تولید علم

مؤسسه چاپ و انتشارات
دانشگاه اطلاعات و امنیت ملی
۱۳۹۶

عنوان و نام پدیدآور	: راهبردهای امنیت سایبری در چین/ گردآوری و تدوین معاونت پژوهش و تولید علم.
مشخصات نشر	: تهران: دانشگاه اطلاعات و امنیت ملی، مؤسسه چاپ و انتشارات، ۱۳۹۵.
مشخصات ظاهری	: ۳۳۱ ص. ش. ۳۳۳
وضعیت فهرست‌نویسی	فیپا.
عنوان دیگر	: چین و امنیت سایبری
عنوان دیگر	: جاسوسی و راهبرد و سیاست‌گذاری در حوزه دیجیتال.
موضوع	: فضای مجازی – چین – تدابیر امنیتی
موضوع	: Cyberspace – Security measures – China
موضوع	: شبکه‌های کامپیوتری – چین – تدابیر امنیتی
موضوع	: Computer networks – Security measures – China
موضوع	: سازمان اطلاعاتی – چین
موضوع	: Intelligence service – China
موضوع	: فضای مجازی - چین – سیاست دولت
موضوع	: Cyberspace – Government policy – China
موضوع	: چین – سیاست اقتصادی – قرن ۲۱م.
موضوع	: China – Economic policy – 21st century
شناسه افزوده	: دانشگاه اطلاعات و امنیت ملی. معاونت پژوهش و تولید علم
شناسه افزوده	: دانشگاه اطلاعات و امنیت ملی. مؤسسه چاپ و انتشارات
رده‌بندی کنگره	: ۱۳۹۵ ۹چ/HM۸۵۱
رده‌بندی دیویی	: ۳۰۳/٤۸۳٤
شماره کتابشناسی ملی	: ٤٦۱۷۳۰٦

مشخصات

عنوان: راهبردهای امنیت سایبری در چین

گردآوری و تدوین: معاونت پژوهش و تولید علم

ناشر: مؤسسه چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی

تاریخ انتشار: ۱۳۹٦

شمارگان: ۱۰۰۰ نسخه

نوبت چاپ: اول

قیمت: ۱۵۰۰۰۰ ریال

شابک: ۹۷۸ـ٦۰۰ـ۸٤۱۱ـ٦٦ـ٦

شماره تلفن: ۲۲٤٦۹۷۳۹

تهران: صندوق پستی ۱٤۳۸-۱٦۷٦۵

مقدمه ناشر

در حوزهٔ مطالعات امنیت روابط بین‌الملل، تعداد اندکی از انتشارات دانشگاهی در زمینهٔ امنیت سایبری فعالیت دارند و بیشتر، زمینه‌های اقتصادی دیده شده است. در زمینهٔ امنیت سایبری کشور چین نیز پژوهش‌های اندکی صورت گرفته؛ زیرا ماهیت پنهان و پیچیدگی عملیات سایبری و نیز زیادی راهبردهای بازدارندگی متقابل را پیچیده کرده و درک حقایق فنی سایبری و برات دولت‌ها را با مانع جدی مواجه کرده است.

این نوشته با هدف بر طرف کردن شکاف‌ها در حوزهٔ امنیت سایبری و مطالعات چین جمع‌آوری شده و به منظور برانگیختن حساسیت محققان و سیاست‌گذاران، دیدگاه‌های متضاد را فراهم آورده است. همچنین به دلیل کم بودن منابع تحقیقاتی عمدتاً رویکردی توصیفی دارد. این کتاب همانند رشتهٔ امنیت سایبری، کاملاً بین‌المللی و میان‌رشته‌ای است و به بررسی مواجههٔ چین با فناوری سایبری در مقابله با ناامنی اینترنتی می‌پردازد.

حوزهٔ سایبری مستعد اغراق و گزافه‌گویی است و نیاز دارد به دیدگاه‌هایی چندجانبه و تجربی نیاز دارد؛ به همین دلیل از نوشته‌های تحقیقاتی پژوهشگران و تحلیلگران چین، ایالات‌متحده، کانادا و انگلستان استفاده شده است. نویسندگان پیشرفته با یکدیگر توافق ندارند؛ برخی تهدیدات سایبری را بسیار خطرناک می‌دانند، در حالی که سایرین آن را بی‌اهمیت جلوه می‌دهند. فناوری شمشیری دو لبه است و نهادهای اطلاعاتی از فضای مجازی به منظور نظارت بر تهدیدات داخلی و خارجی بهره‌برداری می‌کنند. جمع‌آوری سایبری، بسیاری از خطرهای مرتبط با فناوری‌های سنتی را از میان برمی‌دارد و دسترسی بسیار بیشتری را فراهم می کند؛ به همین دلیل است که زیرساخت‌های ارزشمند اطلاعاتی و داده‌های ذخیره‌شده، هدف جذابی برای سارقان و جاسوسان و نظامیان محسوب می‌شوند. چین نیز، نظیر بسیاری از کشورهای صنعتی پیشرفته، منبع فناوری و هدف

حمله‌های سایبری؛ شامل جرائم مالی و جاسوسی است. از نظر مخاطبان چینی، اتهام‌هایی که آمریکا علیه چین مطرح می‌کند اغلب نظیر دزدی است که از دزدی دیگر گلایه می‌کند. مدارک افشاشده نزد مطبوعات، توسط پیمانکار اطلاعاتی ایالات‌متحده، شاهد رویکرد به شدت تهاجمی سرویس‌های اطلاعاتی غربی در قبال شبکه‌های چینی است.

«یه ژنگ» استراتژیست آکادمی علوم نظامی چین معتقد است: «هدایت و توسعهٔ جنگ سایبری به دست ایالات‌متحده است و سایر کشورها آن را شبیه‌سازی کرده‌اند. همان‌طور که جنگ هسته‌ای جنگ راهبردی عصر صنعتی بود، جنگ سایبری نیز جنگ راهبردی عصر اطلاعات است. چین باید قابلیت‌های سایبری خود را به منظور حفاظت از بی‌ثباتی‌هایی که توسط ایالات‌متحده ایجاد می‌شود توسعه دهد.»

جنگ سایبری ممکن است به خصوص برای قدرت‌های ضعیف‌تر و رو به رشد که در جستجوی توسعهٔ ابزارهایی برای مقابله با برتری نظامی سنتی رقبای قوی‌تر هستند جذاب باشد. این کتاب نشان می‌دهد که بسیاری از نهادهای چینی باور دارند جنگ سایبری راه مقرون به صرفه‌ای برای فلج کردن دشمنی نظیر ایالات‌متحده است.

در واقع با خواندن این کتاب می‌آموزیم دولت چین از اطلاعات جمع‌آوری شده چه استفاده‌های کاربردی می‌کند؛ توانایی‌اش در استفاده از فناوری سایبری به عنوان یاریگر منبع انسانی چقدر است و نحوهٔ مدیریت فضای داخلی، امنیت شبکه و برخورد با مجرمان اینترنتی چگونه است. همچنین با مفاهیم چینی امنیت اطلاعات و تلاش منسجم این کشور در دفاع از خطرهای متصور، نظیر تروریسم، جدایی‌طلبی و افراط‌گرایی آشنا می‌شویم. خواندن این کتاب به دانشجویان و کارشناسان حوزهٔ چین و آی‌تی توصیه می‌شود.

معاونت پژوهش و تولید علم

فهرست مطالب

فصل اول: چین و امنیت سایبری: مباحث و زمینه ۱۳

ورای لفاظی‌ها ۱۷

ساختار امنیت سایبری چین ۲۰

سازماندهی ابعاد ۲۹

جاسوسی و جرائم سایبری ۳۰

راهبرد نظامی و نهادها ۳۲

سیاست‌گذاری امنیت سایبری ملی ۳۵

مفاهیم نظری و کاربردی ۳۷

نتیجه‌گیری ۳۹

بخش یک: جاسوسی و جرم سایبری ۴۷

فصل دوم: سرویس‌های اطلاعاتی چین:
تکامل و توانمندسازی در فضای سایبری ۴۹

جمع‌آوری محدود اطلاعات خارجی ۵۰

ساختارهای اطلاعاتی کنونی چین ۵۳

ترفندهای پیشرفته اطلاعاتی چین ۵۵

جمع‌آوری علوم و فناوری ٥٦
تکنیک‌های منابع انسانی ٥٧
سرویس‌های اطلاعاتی چین و جامعه سیاست‌گذار ٦٠
استفاده جامعه اطلاعاتی چین از قابلیت‌های سایبری ٦٥
نتیجه‌گیری ٧٢

فصل سوم: از سرمایه‌برداری تا نوآوری: اکتساب، جذب و کاربرد ٧٧
ارزیابی خسارات نامطمئن ٧٨
یک مدل اثربخش جاسوسی ٨٠
اکتساب غیرقانونی داده‌های خارجی ٨٤
تهدید پایدار پیشرفته ٨٦
انتساب به چین ٨٩
سوزن‌هایی در انبار کاه ٩١
زیرساخت کلان برای جذب داده‌های خارجی ٩٢
تحقیقات دفاعی، توسعه و اکتساب ٩٣
جذب کردن ٩٨
نوآوری مجدد ٩٩
عدم اطمینان از کاربرد در رقابت بین‌المللی ١٠١
نتیجه‌گیری: درس‌های اتحاد جماهیر شوروی برای چین؟ ١٠٤

فصل چهارم: بررسی اقتصاد زیرزمینی آنلاین چین ١١٧
جرائم سایبری در چین و غرب ١١٨
تحلیل ساختاری اقتصاد زیرزمینی آنلاین ١٢٠
زنجیره ارزش سرقت دارایی‌های واقعی ١٢٢
زنجیره ارزش سرقت دارایی‌های مجازی سایبری ١٢٤

زنجیره ارزش سوءاستفاده از خدمات و منابع اینترنتی ۱۲۶
زنجیره ارزش تکنیک‌ها، ابزارها و آموزش بلک هت ۱۲۶
تحلیل تجربی اقتصاد زیرزمینی آنلاین ۱۲۸
برآورد خسارات ناشی از اقتصاد زیرزمینی آنلاین ۱۳۱
خسارات برآوردشده از زنجیره ارزش سرقت دارایی‌های واقعی ۱۳۱
برآورد خسارات ناشی از زنجیره ارزش سرقت دارایی‌های مجازی شبکه ۱۳۲
برآورد خسارات ناشی از زنجیره ارزش سوءاستفاده از خدمات و منابع اینترنتی ۱۳۳
برآورد خسارات ناشی از زنجیره ارزش تکنیک‌ها، ابزارها و آموزش بلک هت ۱۳۴
چکیده خسارات اقتصاد زیرزمینی ۱۳۴
تحلیل بازارهای زیرزمینی ۱۳۴
رفتار بازار ۱۳۵
مشارکت‌کنندگان در بازار ۱۳۶
توزیع جغرافیایی شرکت‌کنندگان ۱۳۶
رفتار شرکت‌کنندگان ۱۳۷
رفتار توزیع کالاها و خدمات ۱۳۸
نقش‌های مشارکت‌کنندگان ۱۳۹
تحلیل و استخراج قیمت ۱۴۰
تقلب در بازار زیرزمینی ۱۴۰
ارتباط بین موارد جرائم سایبری و فعالیت بازار زیرزمینی ۱۴۱
بحث و نتیجه‌گیری ۱۴۲

بخش دوم: راهبرد نظامی و نهادها ۱۵۳

فصل پنجم: آثار چینی درمورد جنگ سایبری و قهرآمیز ۱۵۵
عملیات شبکه رایانه‌ای ۱۵۷

دکترین زمینه ۱۵۹
شناسایی رایانه‌ای ۱۶۲
ضربه به شبکه رایانه‌ای ۱۶۳
دفاع شبکه‌ای ۱۶۵
اضطرار سایبری ۱۶۷
توسعه تسلیحات «برگ برنده» ۱۶۹
اضطرار حمله شبکه ۱۷۰
جنگ روانی ۱۷۱
نتیجه‌گیری ۱۷۲
ترجیحات هدف‌گیری ۱۷۴
پویایی اضطرار ۱۷۵
حملات سایبری: پتانسیل تحقیر ۱۷۸
تهاجمی یا تدافعی: از نگاه بیننده ۱۷۹

فصل ششم: امنیت سایبری و ادغام نظامی ـ غیرنظامی
مطالعه‌ای در تخریب جنگ اطلاعاتی چین ۱۸۹
رویکرد پژوهشی ۱۹۲
روابط تدارکات رسمی ۱۹۳
برون‌سپاری رسمی ۱۹۳
برون‌سپاری اضطراری و مبادلاتی ۱۹۴
«خودمنبعی» عملیاتی ۱۹۴
سامانه شبه‌نظامی ۱۹۵
واحدهای شبه‌نظامی جنگ اطلاعاتی ۱۹۸
ساختار واحدهای شبه‌نظامی جنگ اطلاعاتی ۱۹۹
دامنه اطلاعات ۱۹۹

فرمان و کنترل ۲۰۲
عملکردها، نقش‌ها و مأموریت‌ها ۲۰۳
بسیج ۲۰۴
عملیات زمان صلح ۲۰۵
عملیات زمان جنگ ۲۰۶
تحلیل فعالیت‌های شبه‌نظامی جنگ اطلاعاتی ۲۰۶
انجمن‌ها ۲۰۷
نرخ ایجاد ۲۰۸
پراکندگی جغرافیایی ۲۰۸
مطالعات موردی ۲۰۹
مورد تلفن همراه چین ۲۱۰
واحدهای شبه‌نظامی جنگ اطلاعاتی مستقر در دانشگاه ۲۱۰
نتیجه‌گیری، زمینه‌هایی برای تحقیقات بیشتر و پیامدهای سیاست‌گذاری ۲۱۱
ادغام نظامی ـ غیرنظامی در دامنه شبکه بدون نتیجه‌گیری ۲۱۲
زمینه‌هایی برای تحقیقات بیشتر ۲۱۳
مفاهیم سیاست‌گذاری ۲۱۴

بخش سوم: سیاست‌گذاری امنیت سایبری ملی ۲۲۳

فصل هفتم: وضعیت امنیت سایبری چین و پتانسیل همکاری بین‌المللی ۲۲۵
وضعیت امنیت فضای سایبری در چین ۲۲۶
توسعه سیاست‌گذاری امنیت سایبری چین ۲۲۹
نقایص در حفاظت امنیت فضای سایبری چین ۲۳۲
وقفه‌ها در توسعه فناوری امنیت اطلاعات ۲۳۳
فقدان بنیان حقوقی برای امنیت سایبری ۲۳۴

مشکلات در سطح کسب‌وکارهای تجاری ۲۳۵
چالش‌ها در سطح اجتماعی ۲۳۶
مشکلات امنیت شبکه بین چین و ایالات متحده ۲۳۶
نقش سازمان‌های غیردولتی ۲۳۹
شکل‌گیری اجماعی در سطح پایه امنیت سایبری ۲۴۱
نتیجه‌گیری ۲۴۳

فصل هشتم: تحول چارچوب‌های حقوقی برای حفاظت از حریم خصوصی کاربران در چین ۲۴۷
خاستگاه حقوق حریم خصوصی در چین ۲۴۸
راهنمای اساسی و پنج فضیلت دات ۲۴۹
ریشه‌های حقوقی ۲۴۹
حریم خصوصی در اینترنت ۲۵۲
چارچوب حقوقی کنونی برای حفاظت از حریم خصوصی اینترنت ۲۵۴
قانون اساسی جمهوری خلق چین ۲۵۴
قانون مدنی چین ۲۵۵
قانون کیفری جمهوری خلق چین ۲۵۵
قانون آیین دادرسی چین ۲۵۶
قانون اداری چین ۲۵۶
قوانین و مقررات محلی ۲۵۷
توضیح تحولات حریم خصوصی اینترنت ۲۵۷
نتیجه‌گیری: چالش‌های حریم خصوصی اینترنت ۲۵۹

فصل نهم: «نیروهای متخاصم خارجی»: ابعاد حقوق بشر در کارزار سایبری چین ۲۶۷
حقوق بشر در جهان آنلاین ۲۶۹

مبانی ایدئولوژیک امنیت در چین ۲۷۱
«نفوذ اینترنت» ۲۷۳
مفهوم چین از «نیروهای متخاصم خارجی» ۲۷۶
هدف قرار دادن «نیروهای متخاصم خارجی» در فضای سایبری ۲۷۸

بخش چهارم: مفاهیم نظری و عملی ۲۹۵

فصل دهم: چین و تهدیدات امنیت اطلاعات: پاسخ‌های سیاست‌گذاری در ایالات متحده ۲۹۷
گسترش داده‌های دیجیتال و سامانه‌های کنترل شبکه ۲۹۸
بهمن داده‌های دیجیتال ۲۹۸
ازدیاد و اهمیت زیرساخت سایبری ۲۹۹
ماهیت تهدیدات سایبری ۲۹۹
وسعت تهدیدات ۲۹۹
نقش دولت چین ۳۰۰
نقش ایالات متحده ۳۰۰

فصل یازدهم: نتیجه‌گیری: ظهور چین و آینده امنیت سایبری ۳۱۱
تقاطعی در مباحثات مفهومی ۳۱۲
محرک‌های امنیت سایبری؟ ۳۱۶
وضعیت بی‌ثبات کنونی اینترنت ۳۱۸
فضای سایبری به‌طور فزاینده رقابتی ۳۲۰
ابهام در جنگ سایبری ۳۲۰