

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

مدبریت و راہبردی اطلاعات

امنیت ملی و ضرورتی اطلاعات و ارتباطات

تألیف و گردآوری: بابک اخگر و سیمین باس

ترجمہ: سعید صادقی جقه و پریسا کریمی نیا



پروژه مطالعات راهبردی
نیرتای

سرشناسه: اخگر، بابک، ۱۳۵۰ -
 عنوان و نام دبیدآور: مدیریت راهبردی اطلاعات، امنیت ملی و فناوری اطلاعات و ارتباطات / نویسنده بابک اخگر، سیمئون یاتس؛
 مترجم سعید صادقی جقه، پریسا کریمی نیا.
 مشخصات نشر: تهران: پژوهشکده مطالعات راهبردی، ۱۳۹۶.
 مشخصات ظاهری: ۵۰۴ ص.
 شابک: ۹۷۸-۶۰۰-۵۲۸۲-۹۷-۹
 وضعیت فهرست نویسی: فیبا
 یادداشت: عنوان اصلی: Strategic intelligence management : national security imperatives and information and communications technologies, 2013
 یادداشت: کتابنامه: ص. [۴۴۱] - ۴۸۸.
 یادداشت: نمایه.
 عنوان دیگر: امنیت ملی و فناوری اطلاعات و ارتباطات.
 موضوع: مخابرات -- تدابیر ایمنی
 موضوع: Telecommunication -- Security measures
 موضوع: امنیت ملی -- نوآوری -- سیاست دولت
 موضوع: National security -- Technological innovations -- Government policy
 موضوع: اورژانس -- مدیریت -- نوآوری -- سیاست دولت
 موضوع: Emergency management -- Technological innovations -- Government policy
 موضوع: تروریسم -- دفاع -- پیشگیری -- نوآوری -- سیاست دولت
 موضوع: Cyberterrorism -- Prevention -- Technological innovations -- Government policy
 موضوع: تکنولوژی اطلاعات -- جنبه‌های استراتژیکی
 موضوع: Information technology -- Strategic aspects
 موضوع: تکنولوژی اطلاعات -- مدیریت
 موضوع: Information technology -- Management
 موضوع: مدیریت دانش
 موضوع: Knowledge management
 شناسه افزوده: یاتس، سیمین
 شناسه افزوده: Yates, Simeon
 شناسه افزوده: صادقی جقه، سعید، مترجم
 شناسه افزوده: کریمی نیا، پریسا، ۱۳۵۰ - مترجم
 رده بندی کنگره: الف/۸۵/۲۰۲TK۵۱۰۲۴۳۱۳۹۶
 رده بندی دیویی: ۲۵۳/۱۷۲۳۴
 شماره کتابشناسی ملی: ۴۶۸۶۵۴۹

مدیریت راهبردی اطلاعات امنیت ملی و فناوری اطلاعات و ارتباطات

تألیف و گردآوری: بابک اخگر و سیمئون یاتس

ترجمه: سعید صادقی جقه و پریسا کریمی نیا

ناشر: پژوهشکده مطالعات راهبردی

چاپ و صحافی: برتر

نوبت چاپ: اول ۱۳۹۶

شمارگان: ۲۰۰ جلد

صفحه آرا و طراح جلد: ملیحه کربلایی

قیمت: ۲۸۰,۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۵۲۸۲-۹۷-۹

* فکس: ۸۸۸۹۶۵۶۱

* تلفن: ۸۸۹۱۲۸۳۰

* روابط عمومی: ۸۸۸۰۲۴۷۷

* تلفکس انتشارات: ۸۸۸۰۲۴۷۶

* نشانی: تهران، خیابان کریم خان زند، خیابان آبان جنوبی، خیابان رودسر شرقی، شماره ۷

* پست الکترونیک: info@risstudies.org

* صندوق پستی: ۱۴۱۵۵-۵۱۸۹

کلیه حقوق برای پژوهشکده مطالعات راهبردی محفوظ است

فهرست مطالب

۷	سخن ناشر
۹	قدردانی
۱۱	درباره نویسندگان
۲۱	پیش‌گفتار
۱۲	فصل اول: مقدمه: طراحی راهبرد در دوران جهانی‌شده و شبکه‌ای - بررسی مفهوم و تعریف آن
۲۷	بابک اخگر، سیمئون یاتس، الثنور لاکلی
۲۷	فصل دوم: نگرش‌های دولت: پاسخ‌های راهبردی برای دنیای وابستگی‌های متقابل
۶۹	اندرو استانیفورت
۶۹	فصل سوم: دشمن در مقابل ماست و آن خود ما هستیم: تهدید خودی و چالش‌های آن برای امنیت ملی
۸۹	گریگوری ب. ساتوف، تری ولد، کریستوفر پ. هالستگ
۸۹	فصل چهارم: عصر چالش‌های نامتقارن؛ نسل چهارم: جدای دریایی
۱۱۱	پیتر لهر
۱۱۱	فصل پنجم: امنیت بنادر و مرزها: نخستین و آخرین خط دفاع امنیت ملی
۱۳۵	اندرو استانیفورت
۱۳۵	فصل ششم: اطلاع‌رسانی، درک و رفتار در مقابل ریسک به مثابه بنیادهای امنیت ملی کارآمد
۱۴۹	ام. بروک راجرز، جولیا ام. پیترس
۱۴۹	فصل هفتم: افزایش انعطاف‌پذیری عمومی در مقابل تروریسم شیمیایی، بیولوژیکی، رادیولوژیکی و هسته‌ای
۱۴۹	کریستین کریگر، ام. بروک راجرز

۱۶۵ فصل هشتم: از محله تا جهان: انتظام محله محور و امنیت ملی

فهیمه طباطبایی، سید محمدرضا ناصرزاده، سیمون یاتس، بابک اخگر، الثور لاکلی، دیوید فور چون
فصل نهم: نقش رسانه های اجتماعی در بحران: رویکرد کل نگر اروپایی نسبت به کاربست

۱۷۷ ارتباطات آنلاین و سیار در واکنش به بحران ها و جستجو و نجات بازماندگان

مارکو مانسو، باربارا مانسو

فصل دهم: فناوری های نوظهور و حقوق بشر: چالش مرتبط با ظرفیت های گسترش یابنده

۱۹۹ دولت ها در نظارت بر شهروندان

محمد دستباز، ادوارد هلپین، استیو رایت

فصل یازدهم: تقاضاها، الزامات آموزشی کاربران در برنامه های امنیتی: روش هایی

۲۱۷ برای شناخت نیازها و تسهیل ارتباطات

الکس دباو، ستدمن، رز سایکایاسیت، کلاین لاسون، پیترو فاسی

۲۲۹ فصل دوازدهم: سیری در مدیریت بحران: مراحل مدیریت دانش

ماتس کورائوس و اریک استرن

۲۶۵ فصل سیزدهم: رویکرد معناشناسانه به منطقه است گذاری امنیتی

یان لوندروز، سیمون پولوینا

فصل چهاردهم: پروژه آتنا: استفاده از تحلیل مفهوم برای جهان واکنش پاسخ دهندگان

۲۹۱ در وضعیت بحرانی

سیمون اندروز، سیمون یاتس، بابک اخگر، دیوید فور چون

۳۱۱ فصل پانزدهم: بهره گیری از اطلاعات برای امنیت ملی

گریگور پاولین، توماس کویلینان، فرانک میگنت، پاتریک و اوود

۳۴۱ فصل شانزدهم: بازاندیشی در استاندارد سازی به اشتراک گذاری اطلاعات بین سازمانی

کلین راین

۳۶۱ فصل هفدهم: تأمین امنیت فضای مجازی: پاسخ های استراتژیک به عصر دیجیتال

اندرو استناتیفورث

۳۷۹ فصل هجدهم: استراتژی ملی دفاع سایبری

پل دو سوزا

۲۸۷ فصل نوزدهم: از تروریسم سایبری تا عملیات پنهانی سایبری بازیگران دولتی

جان کالبرگ، بهاوانی تارایزینگهام

۲۹۵ فصل بیستم: برنامه‌های امنیت سایبری برای مبارزه با تروریسم سایبری

لاکلان مک‌کینون، لیز بیکن، دایان گان، گئورگیوس لوکاس، دیوید چادویک، دیمیتریوس فرانگیسکاتوس

۲۹۷ فصل بیست و یکم: نتیجه‌گیری: امنیت ملی در جامعه شبکه‌مند

سیمئون یاتس

۲۹۹ منابع

۳۰۵ نمایه

فهرست شکل‌ها

۳۰۶ شکل ۱-۱: عناصر چهار راه‌برد ملی (جانسون و اسکولز، ۱۹۹۳)

۳۰۸ شکل ۱-۲: رابطه متقابل بین راه‌برد ملی، منافع ملی، و راهبرد امنیت ملی

۳۱۰ شکل ۱-۳: حلقه امنیت ملی

شکل ۱-۴: مدل ارزیابی آسیب‌پذیری از اقدامات تروریستی برای طراحی راهبرد

۳۱۵ پیشگیری و مدیریت بحران

۳۱۶ شکل ۲-۱: عوامل مورد توجه در برنامه‌ریزی برای مواجهه مناسب با فوریت‌ها

۳۱۸ شکل ۲-۲: اپلیکیشن موبایل پلیس یورکشایر شمالی

۳۱۹ شکل ۲-۳: جریان کنونی ارتباطات میان سازمان‌های امداد ملی و شهروندان

۳۲۰ شکل ۲-۴: جریان ارتباطاتی تقویت شده با رسانه‌های جدید موبایل و تلویزیون

۳۲۱ شکل ۲-۵: شمایی از پلتفرم جستجو و نجات مبتنی بر فناوری

۳۲۲ شکل ۲-۶: ۱۱-۱

۳۲۳ شکل ۲-۷: ۱۲-۱: فرآیند SECI

۳۲۴ شکل ۲-۸: نقش کارشناسان در مدیریت بحران

۳۲۵ شکل ۲-۹: ۱۳-۱: طبقه‌بندی و شدت ریسک در رادار

۳۲۶ شکل ۲-۱۰: ۱۳-۲: طبقه‌بندی و شدت ریسک در رادار

۳۲۷ شکل ۲-۱۱: ۱۳-۳

۳۲۸ شکل ۲-۱۲: ۱۳-۴

۲۸۵	شکل ۵-۱۳:
۲۸۵	شکل ۶-۱۳:
۲۸۸	شکل ۷-۱۳:
۲۹۵	شکل ۱-۱۴:
۲۹۲	نمودار ۵-۱۴: شبکه مفهومی بمب‌گذاری لندن بر اساس اظهارات شاهدان عینی
۲۹۲	شکل ۶-۱۴:
۲۹۵	شکل ۷-۱۴:
۲۹۶	شکل ۸-۱۴:
۲۹۲	شکل ۱-۱۵: تفاوت تحلیل با استفاده از روش تلفیق ساده داده‌ها و روش کاملاً دستی
۲۹۸	شکل ۲-۱۵: رابطه کارشناس، مدل نرم‌افزاری و سیستم تحلیل
۲۹۲	شکل ۳-۱۵: امنیت سیستم چارچوب‌محلی در DPIF
۲۹۶	شکل ۱-۱۶: شمایی از زبان استاندارد مدیریت نبرد ائتلافی
۲۹۷	شکل ۲-۱۶: الگوریتم تلفیق اطلاعات محلی به ابزار
۲۹۸	شکل ۲-۱۶: شمایی از آخرین مرحله تبدیل گزارش به BML
۲۹۲	شکل ۱-۱۷: استراتژی جدید انگلستان برای امنیت سایبری
	فهرست جدول‌ها
۲۹۷	جدول ۱-۱: تکنیک‌ها، مدل‌ها، چارچوب‌ها، و ابزارهای راهبر
۲۹۴	جدول ۱-۲: تفاوت مردم و کارشناسان در درک مخاطرات
۲۹۵	جدول ۱-۸: بررسی مطالعات انجام‌شده درباره شیوه‌های شناسایی اینترنت تاریک
۲۹۶	جدول ۱-۹: کاربردهای اصلی شبکه‌های اجتماعی اینترنتی
۲۹۷	جدول ۲-۹: اکوسیستم ابزارهای فاوا
۲۹۳	جدول ۳-۹: نحوه تأثیر رسانه‌های ارتباطی جدید در ارتباطات سازمان‌های امداد و نجات
۲۹۴	جدول ۱-۱۱: مشخصات سازمانی برای مکان X
۲۹۶	جدول ۲-۱۱: افراد مناسب برای مدیریت اتاق کنترل و کارکنان امنیتی
۲۹۹	جدول ۳-۱۱: الگوهای ارتباطی جدول‌بندی شده برای Venue X
۲۹۵	جدول ۱-۲۰: چارچوب امنیت سایبری

سخن ناشر

تهدیدهای ناشی از انسان‌ها و یا طبیعت اغلب به بحران‌هایی منجر می‌شود که افراد، اجتماعات، کسب و کارها و جمع‌ها را با پیامدهای قابل تأملی مواجه می‌سازند. پیشگیری، تخفیف، یا کمک به انعطاف‌پذیری در مقابل بحران‌هایی کماکان از وظایف اصلی دولت - ملت‌ها به شمار می‌رود. با این حال، در جهان کنونی ملت‌ها به تدریج جای خود را به شبکه‌ها داده، و تهدیدات نیز جهان‌شمول می‌شوند. حال سخن این است که کارکردهای سیاست‌گذارانه و حاکمیتی دولت - ملت‌ها چگونه به این تغییرات راسخ‌شان می‌دهند؟ آنها چگونه می‌توانند راهبردهایی را طراحی کنند تا بتوانند با تهدیداتی که متوجه خودشان یا همسایگان‌شان است مقابله کنند؟ مهم‌تر اینکه، فناوری‌هایی که این دنیای جهانی شده و شبکه‌ها را ایجاد کرده‌اند - یعنی فناوری اطلاعات و ارتباطات (فائو) - چگونه می‌توانند ابزاری برای پشتیبانی از چنان راهبردهایی ارائه کنند؟ و اینکه، آیا این شبکه‌ها دریچه‌های جدیدی از تهدیدات و خطرهای به‌دری می‌گشایند؟

مدیریت بحران‌های مختلف و کنترل تهدیدات امنیتی با هدف بسیار از شهروندان نیازمند رویکردی پیشگیرانه و اطلاعات‌محور است. در دوره پس از ۱۱ سپتامبر اشتقاق برای گردآوری و ضبط گسترده اطلاعات توسط سازمان‌ها و نهادهای گوناگون دولتی افزایش یافته است که این کار، در کنار دستاوردهای راهبردی و ضدتروریستی، چالش‌های جدیدی را در حوزه مدیریت اثربخش بانک‌های اطلاعاتی ایجاد کرده است. کتاب حاضر مجموعه‌ای استثنایی از تجربیات میدانی کارشناسان را در کنار نظریات دانشگاهی و مهارت‌های بخش خصوصی گرد هم آورده است تا پاسخی جامع برای چگونگی استفاده از فناوری اطلاعات و ارتباطات در طراحی راهبرد امنیت ملی شهروندمحور فراهم سازد. کتاب حاضر موضوع تمایل و عزم دستگاه‌های امنیتی دولتی برای گردآوری گسترده اطلاعات جدید را به بحث می‌گذارد. ایجاد دسترسی، دریافت، ذخیره‌سازی، و جستجوی موثر در بانک‌های اطلاعاتی فزاینده‌ای که در میان ادارات و سازمان‌های مختلف

دولتی پراکنده شده است، از جمله چالش‌های مورد بحث در کتاب به شمار می‌رود. کتاب همچنین درباره اضافه‌شدن داده‌های به‌دست آمده از شبکه‌ها و رسانه‌های اجتماعی و فناوری جدید تلفن‌های هوشمند، و پیچیده‌تر شدن امر مدیریت اثر بخش اطلاعات مزبور بحث می‌کند.

کتاب به بررسی این واقعیت می‌پردازد که همه سلول‌های تروریستی در یک زمینه مخرب و درهم‌تنیده بین‌المللی فعالیت کرده و دستیابی به ظرفیت و توان انجام حملات شیمیایی، بیولوژیکی، رادیواکتیو، یا هسته‌ای را نیز مد نظر دارند. حملات سایبری به بخش‌های دولتی، خصوصی، و نیز شهروندان عادی از دیگر مباحث مورد توجه کتاب است که توأمان از جانب دولت‌های متخاصم و مجرمین صورت می‌گیرد.

متخصصان و دانشگاهیانی که فصول مختلف این کتاب را نگاشته‌اند همگی از سرآمدان حوزه مدیریت اطلاعات و امنیت ملی به شمار می‌روند؛ نگهبانان بی‌نام و نشانی که وظیفه تحلیل وضعیت و یا حفظ امنیت ملی را به عهده دارند. با توجه به اهمیت روزافزون امنیت سایبری به عنوان یکی از مهمترین اولویت‌های امنیت ملی، انتشار اثر حاضر ضمن پر کردن جای خالی آن در ادبیات مدیریت اطلاعات، چارچوبی برای محققان حوزه امنیت سایبری فراهم کرده و یادآور چالش‌های آینده‌ی امنیت ملی است.

پژوهشکده مطالعات راهبردی ضمن تکرار از مترجمین محترم، کتاب حاضر را منبعی آگاهی‌بخش دانسته و مطالعه آن را برای دستگاران، کارشناسان و دانشگاهیان شاغل یا علاقمند به حوزه امنیت ملی، مدیریت اطلاعات و ارتباطات و فضای مجازی ضروری می‌داند.

معاون پژوهشی

پیشگفتار

برای من واقعاً مایه افتخار است که پیشگفتار کتابی را بنویسم که فصول آن توسط متخصصان و دانشگاهیانی داشته شده است، که همگی از سرآمدان حوزه مدیریت اطلاعات امنیت ملی به شمار می‌روند. به عنوان رئیس ستاد قتل قوانین مبارزه با تروریسم در بریتانیا به مدت ۹ سال، و بازیمن مستقل سیاست امنیت ملی در ایرلند شمالی، رمان قابل توجهی را با نیروهای عملیاتی سپری کرده‌ام که در راستای تأمین امنیت برای ملت، به مدیریت اطلاعات مشغول هستند. این کار، یک وظیفه پیچیده بود و هنوز هم پیچیده هست. بخش اعظم این کار در مرکز تمام توسط تعداد زیادی از متخصصان بسیار توانمند انجام شده است، نگهبانان بی‌نام و نشان، و بعضاً با نازل امنیت ملی و امنیت عمومی. بدون تلاش این مردان و زنان، خیابان‌های ما، و به‌ویژه مکان‌های عمومی، از امنیت بسیار کمتری برخوردار می‌بود.

صیانت از یک ملت و نابودی یا کنترل طیف وسیعی از تهدیدات امنیتی نیازمند رویکردی پیشگیرانه و اطلاعات‌محور است. در دوره پس از ۱۱ سپتامبر، اشتیاق برای گردآوری و ضبط اطلاعات بسیار افزایش یافته است. علیرغم اینکه تمایل به عدم رای گردآوری اطلاعات جدید توسط دستگاه‌های امنیتی دولتی باعث غلبه بر بسیاری از چالش‌های امنیتی شده است، اما همزمان چالش‌های جدیدی را نیز به دنبال داشته است. ایجاد دسترسی، دریافت ذخیره سازی، و کندوکاو موثر در بانک‌های اطلاعاتی فزاینده‌ای که در میان ادارات و سازمان‌های مختلف دولتی پراکنده است، یکی از چالش‌های مزبور به شمار می‌رود. با اضافه شدن داده‌های به دست آمده از شبکه‌ها و رسانه‌های اجتماعی و فناوری جدید تلفن‌های هوشمند، امر مدیریت اثر بخش اطلاعات پیچیده‌تر می‌شود.

البته در حوزه امنیت ملی توجهات همواره (و به درستی) بر تروریسم متمرکز می‌شود. تعداد تروریست‌ها معدود است، و خوشبختانه بسیاری از آنها نمی‌توانند آرزوهای خود را تحقق ببخشند. با این حال، شناسایی تروریست‌هایی که واقعاً خطرناک هستند، کاری دشوار است، چرا که این عده نسبت به امور امنیتی هشیار بوده و به همین دلیل خطرات عظیمی برای جامعه در بر دارند. رویدادهای تروریستی بین‌المللی کماکان زمینه‌ی جغرافیایی-سیاسی نگران‌کننده و تشویش‌آوری ایجاد می‌کنند. امروزه دیگر این واقعیت از نظر همگان پذیرفته شده است که جهادیون خشن در سرتاسر دنیا بر علیه نظم مستقر

در حال همکاری بوده، و به استثنای مواردی معدود، شواهد موید این نکته هستند که همه سلول‌های تروریستی در یک زمینه مخرب و درهم‌تنیده بین‌المللی فعالیت می‌کنند. اگر اشتیاق گروه‌های تروریستی برای دستیابی به ظرفیت و توان انجام حملات شیمیایی، بیولوژیکی، رادیواکتیو، یا هسته‌ای را نیز در نظر بگیریم، خواهیم پذیرفت که امنیت شهروندان و امنیت ملی با نگرانی‌های عمیقی مواجه است.

علاوه بر این، در سطح داخلی، در سال‌های اخیر آگاهی‌های زیادی درباره تهدیدات داخلی کسب کرده‌ایم که از القاعده الهام می‌گرفته‌اند. مهمتر اینکه شکل‌گیری دیدگاه‌های افراطی و تروریستی معمولاً از محلی‌ترین سطح شروع می‌شود. بنابراین، امنیت ملی و پیشگیری از تروریسم در سرچشمه خود، به طور روزافزونی به امنیت محله‌ای و آن گونه از اطلاعات وابسته می‌شود که از اجتماعات محلی گردآوری شده‌اند.

همانند تروریسم، حملات سایبری نیز صرفاً مخاطراتی مربوط به آینده نیستند. امروزه دولت، بخش خصوصی، و شهرها، تحت حملات مداوم سایبری هستند که توانان از جانب دولت‌های متخاصم و مجرمین صورت می‌گیرد. آنها دارایی‌های معنوی، اطلاعات حساس تجاری و حکومتی، و حتی هویت‌های ما را به سرقت می‌برند تا از آنها برای انحراف اذهان افراد، سازمان‌ها، و دولت‌ها استفاده کنند. در حال حاضر، امنیت سایبری به عنوان یکی از مهمترین اولویت‌های امنیت ملی برای بریتانیا محسوب می‌شود چرا که فصلی سایبری، سایش در قالب اینترنت و رسانه‌های شبکه اجتماعی با جامعه‌مان درهم‌تنیده شده است. بنابراین، از آنجایی که فضای سایبری به ابزاری برای جاسوسی، جرم و جنایت، و تروریسم تبدیل شده است، فعالیت در این فضا در آینده قابل تصور، تهدیدی مستقیم برای امنیت ملی و اقتصادی محسوب می‌شود.

در مواجهه با این چالش‌های معاصر برای امنیت ملی، مجموعه مقالات، حاضر ترکیبی استثنایی است که تجربیات میدانی کارشناسان را در کنار نظریات دانشگاهی و مهارت‌های بخش خصوصی گرد هم آورده است. آن دسته از افرادی که به صورت روزانه با حوزه امنیت ملی سروکار دارند، این اثر را منبعی روشنگرانه خواهند یافت که مطالعه آن برای سیاست‌گذاران، کارشناسان، دانشگاهیان شاغل و علاقمند به حوزه امنیت ملی لازم است. انتشار این اثر، که به موقع جای خالی آن را در ادبیات مدیریت اطلاعات پر می‌کند، مدیون تشویق و کمک‌های مرکز تحقیقات درباره ارتقای مبارزه با تروریسم، انعطاف‌پذیری، اطلاعات و جرایم سازمان‌یافته است که یک مرکز تحقیقاتی چندرشته‌ای و کاربرمحور بوده و در موسسه تحقیقات فرهنگی، ارتباطاتی و محاسباتی در دانشگاه شفیلد هالام مستقر است. فراهم کردن چارچوبی برای محققان حوزه امنیت، مهمترین مأموریت آنها می‌باشد که در مطالب مجموعه حاضر نیز تبلور یافته است. مطالعه کتاب حاضر یادآور این نکته است که ما امروزه نسبت به چگونگی مواجهه با چالش‌های آینده‌ی امنیت ملی آگاه‌تر شده‌ایم.

لرد کارلایل