

فضای مجازی و روابط بین‌الملل

(جلد دوم)

مترجمان:

مهدی اوریا

اکبر اصغرزاده بناب



انتشارات دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

۱۴۰۳

عنوان و نام پدیدآور	فضای مجازی و روابط بین‌الملل / اویراستاران [جان- فردریک کرمر، Benedikt Müller]؛ مترجمان مهدی اوریا، اکبر اصغرزاده بناب
مشخصات نشر	تهران: ارتش جمهوری اسلامی ایران، دانشگاه فرماندهی و ستاد، انتشارات دافوس، ۱۴۰۳.
مشخصات ظاهری	ج: ۲؛ جدول.
شابک	ج: ۱: ۹۷۸-۶۲۲-۸۳۳۰-۳۸-۹؛ ج: ۲: ۹۷۸-۶۲۲-۸۳۳۰-۳۹-۶؛ دوره: ۲-۴۰-۹۷۸-۶۲۲-۸۳۳۰
وضعیت فهرست نویسی	فیبا
یادداشت	عنوان اصلی: Cyberspace and International Relations : Theory, Prospects and Challenges, ۲۰۱۴.
یادداشت	کتابنامه.
موضوع	اینترنت و روابط بین‌المللی Internet and international relations تکنولوژی و روابط بین‌المللی Technology and international relations فضای مجازی -- جنبه‌های سیاسی Cyberspace -- Political aspects
شناسه افزوده	کریمر، یان-فردریک Kremer, Jan-Frederik
شناسه افزوده	مولر، بندیکت Müller, Benedikt
شناسه افزوده	اوریا، مهدی، ۱۳۵۳
شناسه افزوده	اصغرزاده بناب، اکبر، ۱۳۶۳، مترجم
شناسه افزوده	دانشگاه فرماندهی و ستاد آجا، انتشارات دافوس
اطلاعات رکورد کتابشناسی:	فیبا

عنوان: فضای مجازی و روابط بین‌الملل (دوم)

مؤلف: جان- فردریک کرمر

مترجمان: مهدی اوریا و اکبر اصغرزاده بناب

طراح جلد: علیرضا اکبرپور

صفحه‌آرایی: امیرحسین رضایی

ناشر: دافوس

شمارگان: ۱۰۰۰

تعداد صفحه: ۳۲۲ ص

نوبت چاپ: چاپ اول

تاریخ انتشار: ۱۴۰۳

چاپ و صحافی: مدیریت چاپ، انتشارات و فصلنامه دانشگاه فرماندهی و ستاد آجا

قیمت: ۳۴۵۰،۰۰۰ ریال

نشانی: تهران، میدان پاستور، خیابان دانشگاه جنگ، دانشگاه فرماندهی و ستاد، انتشارات دافوس

تلفن: ۶۶۴۱۴۱۹۱ - ۰۲۱، ۶۶۴۷۰۴۸۶ - ۰۲۱

مسئولیت صحت مطالب بر عهده مترجمان می‌باشد.

کلیه حقوق برای دافوس آجا محفوظ است. (نقل مطالب با ذکر مأخذ بلامانع است).

فهرست مطالب

عنوان مطلب صفحه

فصل اول: شفاف سازی بحث بین المللی در مورد استاکس نت: استدلال هایی برای

استاکس نت به عنوان یک اقدام جنگی ۱۱

چکیده ۱۲

مقدمه ۱۳

تعریف اقدام جنگی ۱۴

استاکس نت به عنوان یک اقدام جنگی ۱۶

موضوع تعارض ۱۶

قربانی ۱۷

مهاجم ۱۹

خواسته مهاجم ۲۰

اقدام خشونت آمیز ۲۱

نتیجه گیری ۲۳

فصل دوم: روشی جدید برای رهبری جنگ: جنگ سایبری، آیا واقعی است؟ ... ۲۷

مقدمه ۲۹

تعاریف جنگ ۳۲

کاربرد مفروضات کلاوزویتز در جنگ سایبری ۳۷

نتیجه گیری ۴۹

فصل سوم: حفظ صلح ۴۰: بهره برداری حداکثری از پتانسیل کلان داده، رسانه های

اجتماعی و فناوری های سایبری ۵۷

مقدمه ۵۹

سایبری سازی پیشگیری از درگیری، اقدام بشردوستانه و توسعه ۶۵

توسعه حفظ صلح مدرن ۷۱

تلاش‌ها برای اصلاح حفظ صلح ۷۴

چالش‌ها و فرصت‌ها ۷۹

نتیجه‌گیری و پیشنهادات ۸۷

فصل چهارم: رهبری ایالات متحده در فضای سایبری: امنیت سایبری فراملیتی و حکمرانی جهانی ۹۹

چکیده ۱۰۰

مقدمه ۱۰۲

آسیب‌پذیری سایبری، سیاست امنیت سایبری ایالات متحده، و محدودیت‌های بازدارندگی

سایبری ۱۰۴

سیاست امنیت سایبری ایالات متحده ۱۰۶

محدودیت‌های بازدارندگی سایبری ۱۰۸

امنیت سایبری فراملیتی ۱۱۴

نیاز به رهبری ایالات متحده ۱۱۸

امنیت سایبری به عنوان یک مسئله حکمرانی جهانی ۱۲۵

نتیجه‌گیری ۱۲۹

فصل پنجم: لسله مراتب شبکه‌ها: ترکیب‌های نوظهور شبکه‌ها و سلسله مراتب ایجاد امنیت در اینترنت ۱۳۷

چکیده ۱۳۸

مقدمه	۱۳۹
امنیت، شبکه‌ها و سلسله مراتب در روابط بین الملل	۱۴۰
مدل‌های امنیت بین المللی	۱۴۰
سلسله مراتب در امنیت شبکه	۱۴۵
سلسله مراتب در پاسخ‌های بات نت	۱۵۳
نزدیکی جوامع امنیت ملی و امنیت فنی	۱۶۰
لیگ دفاع سایبری استونی	۱۶۰
تحولات در ایالات متحده	۱۶۳
نتیجه‌گیری	۱۶۹
فصل ششم: چگونه حمله سال ۲۰۰۷ به گوگل تصور تهدید دولت آمریکا از جاسوسی سایبری اقتصادی را تغییر داد؟	۱۷۷
چکیده	۱۷۸
مقدمه	۱۷۹
سیاست تهدید	۱۸۶
چارچوب تهدید	۱۸۹
بازیگران چارچوب‌ساز	۱۹۰
پنجره سیاست (خط مشی)	۱۹۲
همخوانی و اقدامات متقابل	۱۹۲
عملیات شفق قطبی	۱۹۳
برداشت دولت ایالات متحده از جاسوسی سایبری اقتصادی قبل و بعد از عملیات شفق قطبی	۱۹۵

۱۹۶	چارچوب تهدید قبل از شفق قطبی
۲۰۴	چارچوب تهدید پس از شفق قطبی
۲۱۱	چگونه شفق قطبی منجر به اقدامات متقابل جاسوسی سایبری اقتصادی شد
۲۱۲	پنجره سیاست: عملیات شفق قطبی
۲۱۳	بازیگران چارچوب ساز ← چارچوب تهدید پیچیده
۲۲۰	چارچوب تهدید گسترش یافته ← اقدامات متقابل
۲۲۲	نتیجه گیری

فصل هفتم: رویکردهای مشارکتی بین‌المللی برای امنیت شبکه: درک و ارزیابی تلاش‌های سازمان توسعه و همکاری اقتصادی و اتحادیه بین‌المللی مخابرات برای ارتقای امنیت سایبری مشترک

۲۳۱	چکیده
۲۳۲	مقدمه
۲۳۴	امنیت شبکه و امنیت سایبری در فضای اطلاعات
۲۳۸	دیدگاه‌ها در مورد مطلوبیت و امکان‌پذیری همکاری‌های بین‌المللی در زمینه امنیت شبکه

۲۴۷	سازمان توسعه و همکاری اقتصادی (OECD)
۲۵۵	اتحادیه بین‌المللی مخابرات
۲۶۲	بحث و نتیجه گیری

فصل هشتم: روش ارتباط مؤثر: ارتباطات معیوب در طبقه روشنفکر سایبری

۲۷۴	چکیده
۲۷۶	مقدمه

۲۷۸	 بررسی عیوب در بخش‌های دانش
۲۷۹	 فنی
۲۸۰	 سیاسی
۲۸۲	 دولتی
۲۸۴	 اقتصادی
۲۸۶	 تشابه‌های گمشده در چارچوب‌های تحلیلی مختلف
۲۸۷	 شکاف خط مشی-محقق در تروریسم سایبری
۲۸۸	 شکاف راهبردی-عملیاتی در امور سایبری نظامی
۲۸۸	 شکاف اندازه‌گیری-انتزاعی-ضمنی در معیارهای سایبری
۲۸۹	 شکاف مختلف کنکره در انتقال‌گذاری امنیت سایبری
۲۹۰	 بارقه‌های امید در چارچوب
۲۹۲	 در خط مقدم علم: موارد مثبت و منفی
۲۹۲	 پروژه مشترک هاروارد-MIT «کاوش در روابط بین‌الملل سایبری»
۲۹۴	 بیانیه دانشمندان اتمی
۲۹۵	 نتیجه‌گیری
	فصل نهم: تأملاتی در مورد مجازی به واقعی: تکنیک مدرن، مطالعات امنیت
۳۰۱	 بین‌المللی و محیط امنیت سایبری
۳۰۲	 چکیده
۳۰۳	 یک نقطه شروع: امنیت و فناوری در عصر اطلاعات
۳۰۵	 مارتین هایدگر و پرسش در مورد تکنیک: مقدمه‌ای بر تکنیک مدرن و تفکر اقتضایی

- تغییر شکل زمان و مکان: معضلات مفهومی در نظریه روابط بین الملل ۳۰۶
- سرعت سالاری پل ویریلیو و انقباض زمان ۳۰۶
- زمان و مکان در دیدگاه زیگمونت باومن ۳۰۸
- مانوئل کاستلز و جامعه اطلاعاتی: فراتر از مرزها ۳۰۹
- امنیت سایبری و نظریه روابط بین الملل: مکتب کپنهاگ ۳۱۰
- از طریق یک روش روش شناختی «جدید»: امنیتی سازی ۳۱۱
- مکتب کپنهاگ و امنیت سایبری ۳۱۲
- امنیت سایبری و اصول «جدید» برای قرن بیست و یکم ۳۱۴
- بخش ها، اشیاء مرجع و امنیت سایبری ۳۱۷
- امنیتی سازی در شبکه های اجتماعی: واقعی به مجازی ۳۱۸