سلسلة كتب المستقبل

الحرب السيبرانية

الاستعداد لقيادة المعارك العسكرية في الميدان الخامس

د. إيهاب خليفة

المستقبل
للأبحاث والدراسات المتقدمة

العربي
للنشر والتوزيع

الحرب السيبرانية

الاستعداد لقيادة المعارك العسكرية
في الميدان الخامس

د. إيهاب خليفة

العربي للنشر والتوزيع

المستقبل
للأبحاث والدراسات المتقدمة

الحرب السيبرانية
الاستعداد لقيادة المعارك العسكرية في الميدان الخامس
د. إيهاب خليفة

الطبعة الأولى: 2020
رقم الإيداع: 2020/8635
الترقيم الدولي: 9789773195755
الإخراج الفني: عبدالله خميس

60 شارع قصر العيني - 11451 - القاهرة
ت: 27921943 - 27954529 فاكس: 27947566
www.alarabipublishing.com.eg

بطاقة فهرسة
خليفة، إيهاب

الحرب السيبرانية: االاستعداد لقيادة المعارك العسكرية في الميدان الخامس، القاهرة: العربي للنشر والتوزيع، 2020 - ص؛ سم.
تدمك: **9789773195755**
1- ثورة المعلومات – الجوانب الاجتماعية
2- الحروب
أ- العنوان 306.42

المستقبل
للأبحاث والدراسات المتقدمة

عن المستقبل:

مركز تفكير (Think Tank) مستقل، أنشئ عام 2014، في أبوظبي، بدولة الإمارات العربية المتحدة، للمساهمة في تعميق الحوار العام، ومساندة صنع القرار، ودعم البحث العلمي، فيما يتعلق باتجاهات المستقبل، التي أصبحت تمثل إشكالية حقيقية بالمنطقة، في ظل حالة عدم الاستقرار وعدم القدرة على التنبؤ، خلال المرحلة الحالية، من خلال رصد وتحليل وتقدير "المستجدات" المتعلقة بالتحولات السياسية والاتجاهات الأمنية، والتوجهات الاقتصادية والتطورات التكنولوجية، والتفاعلات المجتمعية والثقافية، المؤثرة على مستقبل منطقة الخليج، وفي نطاق الشرق الأوسط عموماً.

للاتصال والمعلومات:
البرج الدولي، شارع الكرامة، منطقة مركز المعارض، الطابق (24)
ص.ب 111414 أبوظبي, الإمارات العربية المتحدة
هاتف: 24444513-971+, فاكس: 24444732-971+
العلاقات العامة: 999 657 502 971+
Email: info@futureuae.com
www.futureuae.com

الفهرس

مُقدِّمة:

في صباح صيف أحد الأيام الصحوة استيقظ سكان أحد المدن المزدهرة ذات ناطحات السحاب الشاهقة والمشهورة بتقدمها التكنولوجي الكبير، على أصوات ارتطام وانفجارات كبيرة، وألسنة نيران مشتعلة هنا وهناك، وكأنه عمل إرهابي قد أصاب المدينة بأكملها، أو حرب بأسلحة فتاكة قد بدأت تضرب المدينة، ماذا يحدث؟ هل هي «بيرل هاربر» أمريكية جديدة أم «11 سبتمبر» مرة أخرى؟ الكهرباء لا تعمل؛ لا يوجد مصدر لمعرفة الأخبار، خدمات البث الرقمي والهوائي متوقفة وخدمة الاتصالات الهاتفية والإنترنت لا تعمل أيضًا وكأن المدينة الأكثر ازدحامًا والأكثر تطورًا عادت إلى العصور القديمة.

ما هذه الأصوات وما هذه النيران؟ المنظر مرعب؛ السماء تمطر قطعًا معدنية وإلكترونية واسلاكًا؛ إنها أقمار صناعية تتهاوى من السماء وطائرات مسيّرة ومدنية تسقط في شكل قنابل موجهة نحو الأرض، ما الذي أسقطها؟، الكهرباء منقطعة في المدينة بأكملها، خدمات الرعاية الصحية للمرضى في المستشفيات توقفت بعد نفاذ بطاريات الطاقة الاحتياطية، حركة القطارات السريعة والمترو متوقفة، الشوارع في حالة شلل تام، فالسيارات الكهربائية قد فرغت شحناتها، وإشارات المرور لم تعد تعمل، وخدمة الـGPS متوقفة، وهناك صعوبة في السيطرة على السيارات الذكية ذاتية القيادة، القتلى والجرحى في كل مكان وسيارات الإسعاف حبيسة الطرقات، الموت يحاصر الجميع من كل اتجاه.

الأمر لا ينقصه شيء حتى يقول الناس إنه يوم القيامة، سوى رؤية السحب الدخانية على شكل فطر عيش الغراب ترتفع إلى عنان السماء؛ أنه الشكل المألوف لانفجار القنبلة النووية، ولكن من أين جاءت ومن أطلقها؟ وما هذا الصفير الذي كاد أن يصم الآذان؟ إنه انفجار لمفاعل نووي قرب المدينة، نجم عنه غبار ذري ارتفع إلى أعلى في شكل مظلة غطت سماء المدينة، تَبعه سكون تام وكأن المدينة في حالة سُبات عميق، فالحياة تقريبًا قد انتهت.

إنه سيناريو افتراضي لحرب المستقبل، الحرب السيبرانية، تلك الهجمات الدقيقة والمعقدة للغاية عبر نظم وشبكات الكمبيوتر والأجهزة الذكية، تستهدف البنية التحتية المدنية والعسكرية للدول، من محطات الطاقة والكهرباء، ونظم الاتصالات والمواصلات والأقمار الصناعية، وخدمات تحديد الموقع الجغرافي والسيارات ذاتية القيادة وإنترنت الأشياء، فضلًا عن المفاعلات النووية والسدود والخزانات المائية، هي دقائق أو ساعات قليلة حتى تصبح الحياة المزدهرة بالتكنولوجيا الذكية الغناء، مصدرُ السعادة والرخاء للبشرية، مُجردَ كومة من الأجهزة الإلكترونية والأجساد البشرية الممزقة تعلو فوق بعضها، إنها الحرب السيبرانية حيث التدمير الشامل دون إطلاق رصاصة واحدة.

من يقف خلف ذلك التأثير المدمر الذي يمكن أن يحدث في لمح البصر، هم مجموعة من محترفي اختراق شبكات الحاسب الآلي، يشكلون جيشًا سيبرانيًا عسكريًا، يقاتل ضمن صفوف القوات العسكرية المسلحة، ولكنه يتكون من مجموعة من المبرمجين والباحثين الأمنيين ومكتشفي الثغرات ومحللي الشفرات ومطوري البرمجيات، أو كما يطلق عليهم قراصنة المعلومات، يعملون خلف شاشات وأجهزة الكمبيوتر، مسلحين ببرمجيات وفيروسات فتّاكة يمكن أن تحقق ما لم تحققه الدبابات والطائرات على أرض المعركة.

ويعتبر الفضاء السيبراني هو ميدان المعركة الرئيس لهذه الجيوش السيبرانية، ولكنه ليس الميدان الوحيد، فكما تقاتل القوات المسلحة في الميادين الأربعة التقليدية-الأرض والبحر والجو والفضاء الخارجي-فإن الجيوش السيبرانية تقاتل في جميع هذه الميادين مشتركة، إلى جانب قتالها في الميدان الخامس الافتراضي وهو الفضاء السيبراني.

وفي وقت السلم، فإن المهمة الرئيسة للجيوش السيبرانية هي تقديم الدعم المعلوماتي واللوجستي؛ فيقومون بالتجسس على العدو عبر اختراق شبكاته لكشف أسراره وسرقة تصميمات الأسلحة المتقدمة التي يمتلكها والخطط

الاستراتيجية والاقتصادية في حالة الحرب، ونوع التسليح الذي يمتلكه ومناطق توزيعه وانتشاره، والأهداف التي يسعى إلى تدميرها في حالة الحرب، ومناطق تواجد القوات وعددهم ومواعيد نومهم ونشاطهم والوجبات التي يأكلونها بل والمتعاقد الذي يورد لهم هذه الوجبات، فكل معلومة في وقت الحرب مهمة.

وفي وقت الحرب، يقومون بمهمتي الهجوم والدفاع على حد سواء، فضلًا عن مهمة تقديم الدعم للوحدات العسكرية المقاتلة في الميادين المختلفة، فيقومون بمهمة الهجوم عن طريق محاولة شن هجمات سيبرانية تستهدف نظم التحكم والسيطرة الخاصة بالعدو عن طريق تعطيل نظم الدفاع الجوي، ومنصات إطلاق الصواريخ، والسيطرة على الأسلحة ذاتية التشغيل كالدرونز Drones والربوتات العسكرية، وقطع شبكات الاتصال بين الوحدات العسكرية، فضلًا عن القيام بعمليات الخداع والتشويش الرقمي على أجهزة العدو، ومن ناحية أخرى العسكرية هم مسئولون عن الدفاع من خلال تأمين الاتصالات بين الوحدات العسكرية الصديقة المقاتلة، ومنع أي محاولات لاختراقها أو التجسس عليها، ويقومون بدور الضمان لسلامة وسهولة التواصل بين الوحدات المقاتلة، وتأمين القوات العسكرية خلف خطوط العدو عبر تعطيل نظمه العسكرية وكشف الكمائن التي ينصبها لهم.

وبالتالي فإن «سلاح الحرب السيبرانية» لا يقل أهمية عن غيره من الأسلحة التقليدية الموجودة في القوات المسلحة، كسلاح الطيران والمدفعية والإشارة والمشاة والمهندسين والحرب الإلكترونية وغيرهم، بل إنه سلاح سابق لعمل الأسلحة السابقة، يقوم بدور «الكشافة» قبل بدء المعركة، والحامي لهم من هجمات العدو أثناء ذلك، كما أنه سلاح شامل أيضًا يعمل بالتزامن مع جميع الأسلحة الأخرى في نفس التوقيت، ويضمن عملية التنسيق بينهم جميعًا، ويقدم الدعم لها على قدم المساواة، فيعمل بالتقاطع مع الميادين الأربعة التقليدية للقتال، إلى جانب عمله التقليدي في الميدان الخامس، أو الفضاء السيبراني.

المثير في الأمر أنه حتى الأسلحة التقليدية مثل الدبابات والطائرات والمدفعية والصواريخ الباستية وغيرها أصبح لها جميعًا جوانب سيبرانية، وتعتمد على بنية تحتية مرتبطة بالفضاء السيبراني والأقمار الصناعية، مثل نظم تحديد الموقع الجغرافي GPS ونظم تحديد التوقيت Timing Systems ونظم الإدارة والتحكم عن بعد Command And Control Systems، وأصبحت تتطلب نظم حماية وتأمين متخصصة في صد الهجمات السيبرانية والاختراق الخارجي والتلاعب عن بعد، وليس فقط دروعًا تحميها من الاختراق من القذائف، وبالتالي فالتقاطع بين الأسلحة التقليدية والفضاء السيبراني أصبح كبيرا، للدرجة التي يمكن من خلالها القول إن الفضاء السيبراني هو البنية التحتية الحديثة للحرب التقليدية والسيبرانية معًا.

فإذا تم اختراق النظم الأمنية لهذه الأسلحة التقليدية أو إرسال معلومات خاطئة لها عبر الأقمار الصناعية مثل معلومات مضللة عن المواقع الجغرافية للأهداف العسكرية، فإن ذلك قد يتسبب في ضرب أهداف صديقة، أو إخراج عدد كبير من المعدات العسكرية عن العمل وتعطيلها.

إن تطور شكل الحرب عبر التاريخ من الحجارة والرماح إلى السهام والسيوف إلى المسدسات والبنادق إلى طبيعة الصواريخ والقاذفات ثم إلى الدبابات والطائرات والغواصات وصولًا إلى القنابل النووية والهيدروجينية، ينذر بالقول: إن من لا يدرك جيدًا تغير طبيعة وعصر وسلاح المعركة القادمة ويسارع بالحصول عليه وتطويره، سوف ينتهي به الأمر مهزومًا تابعًا لغيره ضعيفًا بين الأمم، وكلما ازدادت الدول علمًا وتقدمًا ازدادت معها القدرة التدميرية للأسلحة المستخدمة، وسلاح الحرب القادمة سوف يكون أقوى وأبشع من القنابل النووية والهيدروجينية، فالجنود المقاتلون في هذه المعركة هم من الربوتات والدرونز، والأسلحة عبارة عن شفرات وفيروسات وديديان مبرمجة، لا يتعدى حجمها بضعة كيلوبايتس، ولكنها قادرة على إحداث تأثير يفوق في قوته الأسلحة التقليدية.

ومع توجه العالم أجمع نحو تزايد الاعتماد على التقنيات الذكية والحديثة وتبني نماذج الحكومات والمدن الذكية، فإنه يصبح أكثر انكشافًا وعرضة للحروب السيبرانية، ومع تزايد الاعتماد على الإنترنت أثناء جائحة كورونا لتيسير مهام العمل والتعليم عن بعد تزايد معها نشاط القراصنة مستغلين ضعف الثقافة الأمنية بكثير من مستخدمي الإنترنت حول العالم، وهو ما يتسبب في تهديد الأمن القومي وتعريض مصالح الأفراد والدول للخطر.

وهو ما يعني أن الحرب السيبرانية قادمة لا محالة، بصورة قد تكون أكثر شراسة عن غيرها من الحروب، لذا بات من الضروري على جميع الدول التي تسعى للحفاظ على أمنها القومي أن تطور آليات للمواجهة وأن تستعد للمعركة القادمة.

ومن هنا جاءت أهمية هذا الكتاب، ليلقي الضوء على مفهوم الحرب السبيرانية والمقصود بها وتحديد أبعادها وخصائصها والأسلحة المستخدمة فيها، ويوضح كيفية قياس التهديدات السيبرانية والتي يمكن من خلالها التفريق بين حالة الخطر وحالة التهديد وحالة الحرب، ويستعرض أهم نماذج الجيوش السيبرانية في العالم، كما يستعرض مفاهيم الأمن والدفاع والردع السيبراني.

ويتكون الكتاب من خمسة فصول رئيسة: الفصل الأول وهو فصل نظري إلى حد كبير يناقش مفهوم الأمن القومي السيبراني Cyber National Security وذلك من واقع نظريات العلاقات الدولية، ورغم أهمية هذا الفصل في فهم التحديات النظرية التي باتت تواجه عملية تحليل التحديات غير التقليدية للأمن القومي إلا إنه يمكن للقارئ تخطي هذا الفصل دون أن يعوق ذلك من إمكانية متابعة باقي فصول الكتاب، فهذا الفصل يَهُم الأكاديميين والمتخصصين في نظريات العلاقات الدولية أكثر من غيرهم من القراء، وقد يجده غير الأكاديميين فصلًا ثقيلًا أو مملًا إلى حد ما وهو ما وجب التنويه عنه مقدمًا.

ويناقش الفصل الثاني المقصود بالحرب السيبرانية Cyber Warfare والخلاف الأكاديمي حولها عما إذا كانت حقيقة أم مجرد سيناريوهات افتراضية، ويحدد كذلك الفواعل الرئيسة فيها والمحفزات التي قد تدفع نحو نشوب حرب سيبرانية على المدى المنظور، ويدرس الفصل الثالث العناصر والأدوات اللازمة للاستعداد للحرب السيبرانية القادمة مثل بناء الجيوش والأسلحة السيبرانية وإنشاء التحالفات الأمنية السيبرانية، ويدرس الفصل الرابع اقترابات ونماذج قياس التهديدات السيبرانية، بما يساعد في النهاية على التمييز بين حالة الخطر وحالة التهديد وحالة الحرب السيبرانية، ويتطرق الفصل الخامس إلى آلية تحقيق الدفاع السيبراني Cyber Defence لحماية الأمن القومي السيبراني، وكذلك المؤسسات المسئولة عن تحقيق هذا المفهوم، كما يدرس أيضًا إشكالية تحقيق الردع في الفضاء السيبراني والآليات المقترحة لتدعيم حالة الأمن السيبراني.

وفي النهاية أتوجه بخالص الشكر إلى مركز المستقبل للأبحاث والدراسات المتقدمة وعلى رأسه الأستاذ الدكتور محمد عبد السلام رئيس المركز، على توفير الموارد المادية والأكاديمية لإصدار سلسلة متميزة من «كتب المستقبل» تصدر من المركز بالتعاون مع دار العربي للنشر والتوزيع بالقاهرة، كما أتوجه بخالص الشكر أيضًا إلى كل من ساهم معي في إتمام هذا الكتاب، وعلى رأسهم المهندس عادل عبدالمنعم، خبير الأمن السيبراني بالاتحاد الدولي للاتصالات، والأستاذ الدكتور أحمد مصطفى، الأستاذ بكلية الحسابات والمعلومات بالجامعة البريطانية بالقاهرة، والأستاذ إبراهيم غالي، نائب رئيس مركز المستقبل للأبحاث والدراسات المتقدمة للشؤون الأكاديمية، وذلك على الملحوظات القيمة التي كانت بمثابة إثراء لهذا العمل.

مؤلف الكتاب

إيهاب خليفة