الحـــروب السـيبرانية

في الشـرق الأوسـط والعـالم

الحـــروب السـيبرانية
في الشـرق الأوسـط والعـالم

المديـــر العـــام: د. **خـــالـــد عـــكاشـــة**

نائـب المديـر العـام: اللـواء. **محمـد إبراهيـم الدويـري**

تحرير وإشراف: **د. رغـــدة البـــهي**

إخـــراج فـــني: **إســـلام علـي**

الطبعة الأولى، يناير 2025

رقـم الإيـداع: 2025/2908م

الترقيم الدولي: 978-977-9694-10-8

100 شارع الميرغني مصر الجديدة– القاهرة– مصر.

الهاتف: 20226905861+ - 20226905862+ - 20226905863+

البريد الإلكتروني: info@ecss.com.eg

www.ecss.com.eg

الحـروب السـيبرانية في الشـرق الأوسـط والعـالم

تقديم

الحروب السيبرانية.. تحولات ومخاطر

يعكس هذا الكتاب الذي يحمل عنوان "**الحروب السيبرانية في الشرق الأوسط والعالم**" مخاطر الحروب السيبرانية في الحاضر والمستقبل، حيث إنها وإن كانت تقتصر حاليًّا على شبكات المعلومات والأنظمة المتصلة بالشبكة، فإنها ستتوسع بشكل كبير في المستقبل، ولن تقتصر التأثيرات السيبرانية المحتملة على شبكات الكمبيوتر، بل ستشمل جميع أنظمة معالجة المعلومات الإلكترونية. لذا، فإن التهديدات السيبرانية المتسارعة التي سوف تتبلور ملامحها طيلة عقد ممتد، سوف تُحدد كيفية تدريب القوات الجوية والقواعد الحاكمة لانتشارها في ساحات المعارك المستقبلية. ومن المتوقع أن تمتد الحرب السيبرانية مستقبلًا لتشمل: شبكات الاتصالات، وأنظمة الكمبيوتر، والمعالجات المدمجة، وغيرذلك.

وعليه، تبرز أهمية هذا الكتاب كونه مرآة عاكسة لظاهرة الحروب السيبرانية التي شهدت تحولات جوهرية بالنظر إلى جملة من الحالات التطبيقية، كما تجلى في الصراع السيبراني بين الصين والولايات المتحدة، وفي الحرب الروسية-الأوكرانية، وفي امتدادات الحرب الإسرائيلية على غزة. فقد تعددت الدول التي توظف قدراتها السيبرانية تحقيقًا لأهدافها، ليركز الكتاب من بينها على بعض الحالات التي أتى في مقدمتها الولايات المتحدة والصين وروسيا وإسرائيل. هذا إلى جانب الاهتمام بعدد من الفاعلين من غيرالدول على شاكلة جماعات القرصنة والتنظيمات الإرهابية.

وعليه، شارك في هذا الكتاب كوكبة من الخبراء ورؤساء الوحدات والعسكريين والباحثين الأوائل ممن تنوعت خلفياتهم على اختلاف تخصصاتهم؛ فكان منهم

الأكاديميون والعسكريون والباحثون المتخصصون من داخل المركز المصري للفكر والدراسات الاستراتيجية ومن خارجه. وقد رسموا باقتدار ملامح ظاهرة الحروب السيبرانية واتجاهاتها المستقبلية بالتركيز على منطقة الشرق الأوسط في المقام الأول، ولكن مع اهتمام مماثل بحالات دولية وعالمية أخرى. وفي ضوء ذلك، ينقسم الكتاب الذي أعده كوكبة من المؤلفين، وقامت بتحريره والتقديم له د. **رغدة البهي** (رئيس وحدة الأمن السيبراني بالمركز المصري للفكر والدراسات الاستراتيجية) إلى 10 فصول.

وقد حمل الفصل الأول منه عنوان "**مفهوم الحروب السيبرانية: تأصيل نظري**"، والذي أوضح كيف باتت تلك الحروب من أبرز معالم الصراعات السياسية والتجارية بين الدول، وكيف باتت قادرة على تعطيل البنية التحتية الحيوية، ولا سيما مع التطورات التكنولوجية المتلاحقة مثل: إنترنت الأشياء، والحوسبة السحابية، والذكاء الاصطناعي، وغيرذلك. وعليه، قدم هذا الفصل تحليلًا لمفهوم الحروب السيبرانية والمفاهيم المتداخلة معه، وتأثيرها على الأمن القومي للدول والجهود المبذولة في مجال مكافحتها. فقد أضحت الحروب السيبرانية مجالًا معقدًا وسريع التطور وله آثار كبيرة على المواطنين والحكومات والشركات في جميع أنحاء العالم. وقد فرضت بالفعل تحديات عديدة تواجه دول العالم، حيث أصبح المجال الافتراضي بمنزلة ساحة قتال جديدة تشكل تهديدًا، يضاف إلى قائمة التهديدات التقليدية التي تواجه العالم، وتتجاوز في أبعادها وآثارها الحدود الجغرافية والسياسية، وتلقي بتداعياتها على مستقبل الأمن القومي والحيوي للدول.

فيما حمل الفصل الثاني عنوان "**البعد السيبراني في الحرب الروسية-الأوكرانية: وإعادة صياغة معادلة الصراع في أوروبا**" الذي أوضح كيف كشفت ديناميكيات المواجهة العسكرية المباشرة بين روسيا وأوكرانيا عن أوجه أخرى للحرب المتواصلة بينهما، كانت أبرز مظاهرها تصاعد توظيف القدرات السيبرانية في إطار ما يعرف باسم "الحروب الهجينة" التي أسهمت في إعادة تشكيل معادلة الصراع وعدم الاستقرار بين روسيا وأوكرانيا، وذلك بالتوازي مع استخدام القوة العسكرية التي عززت من قدرة روسيا على إضعاف واستنزاف الدفاعات المدنية والعسكرية الأوكرانية في بداية الحرب التي كانت الضربة الأولى فيها مرتكزة على توجيه هجمات سيبرانية وُصفت بكونها "غير مسبوقة" ضد أوكرانيا.

فقد أظهرت الحربُ الروسية-الأوكرانية أن البعد السيبراني سيكون حاضرًا وذا تأثير ممتد حتى لو تم التوصل إلى تسوية حول اليوم التالي في أوكرانيا، مع احتمالية تنامي اللجوء إليه خلال أي مسار تفاوضي في المستقبل باعتباره إحدى آليات الضغط على أيٍّ من طرفي الصراع، لإجبارهما على التفاوض أو القبول ببنود خاصة بالتسوية قد لا تتوافق مع مصالحهما. علاوة على ذلك، من المرجح أن تشهد المرحلة المقبلة مزيدًا من الدعاية الروسية التي تستهدف بشكل مباشر الحكومة الأوكرانية، للتشكيك في شرعية الرئيس الحالي، وذلك قبل بدء التفاوض المحتمل بالتزامن مع تولي الإدارة الأمريكية الجديدة برئاسة "دونالد ترامب" السلطة في يناير 2025 للنيل المعنوي من أوكرانيا، ولممارسة المزيد من الضغوط عليها للقبول بوقف الحرب الراهنة بأي تكلفة.

ثم يأتي الفصل الثالث بعنوان **"حدود الحرب السيبرانية بين الولايات المتحدة الأمريكية والصين"** ليؤكد على خطورة التهديدات السيبرانية التي تواجهها الولايات المتحدة الأمريكية، والتي تأتي من الدول التي تمتلك توظيف هذا النوع من التهديد، وفي مقدمتها الصين التي تعمل على سرقة المعلومات التجارية الأمريكية والأسرار العسكرية، مع توجيه هجمات سيبرانية تهدف إلى تعطيل المنظومة الإلكترونية لشبكات الدفاع والاستخبارات الأمريكية. فيما تسعى الصين إلى تحقيق تفوق نسبي على خصومها في المجال التكنولوجي والمعلوماتي. وفي ظل المتغيرات السريعة في بيئة الفضاء السيبراني، بوصفه مجالًا رئيسيًا للحرب، ظهرت الحاجة إلى إعادة النظر في مفهوم السيادة السيبرانية وفق استراتيجية الأمن السيبراني الصينية، والاستفادة من أدوات الثورة الرقمية بطرق متطورة وحديثة.

وقد خلص الفصل إلى أن الحرب السيبرانية بين الولايات المتحدة والصين تتسم بتعقيداتها المتزايدة وتوسعها لتشمل مجالات متعددة تتجاوز التجسس التقليدي أو الهجمات التقنية. فقد أصبحت هذه الحرب ميدانًا استراتيجيًا للصراع على النفوذ العالمي والتحكم في الفضاء السيبراني. ومع ذلك، فإن حدود هذه الحرب لا تزال غامضة نتيجة غياب إطار قانوني دولي ينظم هذا النوع من الصراعات بشكل واضح. ومن أبرز مظاهر الحرب السيبرانية بين البلدين تصاعد الهجمات المستهدفة للأنظمة الحكومية والمؤسسات الاقتصادية، حيث تعمل الصين على تعزيز قوتها السيبرانية من خلال

عمليات تجسس منسقة تستهدف القطاعات الحيوية في الولايات المتحدة. وتشير تقارير إلى تورط مجموعات سيبرانية صينية مدعومة من الدولة في سرقة بيانات متعلقة بالأمن القومي والتكنولوجيا الحساسة، وهو ما دفع الولايات المتحدة إلى اتخاذ خطوات استباقية لتعزيز أمنها السيبراني، وتقليل نقاط الضعف في بنيتها التحتية.

فيما استُهل الفصل الرابع الذي حمل عنوان "**حروب التجسس: أبعاد وتداعيات** التجسس السيبراني الصيني على الدول الأوروبية" بمناقشة كيف تتصاعد الاتهامات الغربية للجانب الصيني بشأن ممارساته المتعلقة بالتجسس السيبراني، وهو جزء من مجموعة من الاتهامات التي يتم توجيهها للصين بداية من ممارساتها المتعلقة بعدم الالتزام بقواعد السوق حتى انتهاكها لحقوق الإنسان. وبشكل عام، تقود الولايات المتحدة المعسكر الغربي فيما يخص الاتهامات الموجهة للصين على اختلاف أشكالها، ومنها السيبرانية. وهو ما يُمكن فهمه في ظل رغبة الولايات المتحدة في احتواء الصعود الصيني المهدد الرئيسي لها، وكذلك بسبب تقدمها على مختلف المستويات الاقتصادية والتكنولوجية، والتي تجعلها في مرمى الاهتمام الصيني فيما يتعلق بالاستحواذ على تلك المعارف المختلفة، التي تُعد السبب الرئيسي وراء تقدم الغرب وبخاصة الولايات المتحدة عن أي من القوى الأخرى.

وعليه، تتزايد مخاوف القطاعين العام والخاص من التجسس السيبراني الصيني على الأسرار التجارية الأوروبية، والذي يصل إلى 94٪ من جميع الهجمات السيبرانية في قطاع الصناعات التحويلية فحسب، ليكلف أوروبا ما يصل إلى 60 مليار يورو، وهو رقم سيرتفع مع قيام الشركات الأوروبية برقمنة خدماتها. فقد تمكنت الصين من زرع رقاقات بالغة الصغر في أجزاء من الخوادم التي تشق طريقها إلى السوق العالمية وإلى مراكز خوادم خدمات أمازون السحابية وآبل وغيرها من شركات التكنولوجيا، ما يمكنها من الوصول إلى البيانات الموجودة ضمن تلك الخوادم. ولذا، سعت حكومات عدة إلى عقد صفقات مع الصين لوقف تلك الممارسات، في الوقت الذي تتكرر فيه التصريحات الأوروبية المحذرة من خطورة تلك الممارسات، التي من غير المتوقع أن تتوقف في القريب.

أما الفصل الخامس فقد جاء بعنوان "**حدود التصعيد الإيراني-الإسرائيلي في الفضاء السيبراني**"، وقد أوضح كيف أن لعدد كبير من الصراعات التقليدية في منطقة الشرق الأوسط بعدًا سيبرانيًا في ظل صعوبة حسم كثير منها على المستوى العسكري، ومن ثم يجد أطراف تلك الصراعات في الفضاء السيبراني ساحات موازية يمكنها تحقيق بعض الاختراقات الاستراتيجية والمكاسب الفعلية، وهو ما يعني أن تعدد الصراعات العسكرية المسلحة والمفاوضات السلمية الفاشلة ساهمت في تشكيل مشهد التهديدات السيبرانية المحتدمة في المنطقة من ناحية، وأوجدت مزيدًا من الأسباب الهيكلية التي أفضت إلى استمرار الصراعات العسكرية من ناحية ثانية. وفي هذا الإطار، برزت خصوصية الصراع السيبراني بين إسرائيل وإيران، والذي بات يرقى في نظر كثير من التحليلات إلى حد "الحرب السيبرانية". فلم يعد الصراع بين الجانبين يعتمد فقط على الصراع العسكري المحتمل بين الطرفين، بل تطور الأمر إلى أن أصبح حربًا خفية بين الطرفين تُدار في رحى الفضاء السيبراني.

وقد خلص هذا الفصل إلى أن الصراع السيبراني قد لا يتصدر عناوين الأخبار بقدر ما يتصدر الصراع المادي، لكن الفضاء السيبراني سيظل ساحة موازية للحرب الإسرائيلية على غزة والصراع الإسرائيلي-الإيراني، بعد أن غيرت الحرب الإسرائيلية على غزة من طبيعة الصراع الإيراني-الإسرائيلي الذي دار سرًا وفي الخفاء طيلة سنوات عدة ليتحول إلى ساحات مفتوحة. فقد تضاعف عدد الهجمات السيبرانية منذ اندلاع الحرب الإسرائيلية على غزة خلال الربع الأول من عام 2023 على أقل تقدير مقارنة بالفترة نفسها من العام الماضي. وفي الربع الأول من عام 2024، تضاعف عدد تلك الهجمات ثلاث مرات. وفي بداية الحرب، استهدفت معظم الهجمات إسرائيل وفلسطين، لكنها انتشرت لاحقًا إلى الدول المجاورة، واجتذبت المتسللين وجماعات القرصنة من جميع أنحاء العالم، حتى أعلن بعضها أنها ستشن هجمات سيبرانية بشكل متكرر على أحد جانبي الصراع أو الآخر.

وقد سلّط الفصل السادس الذي حمل عنوان "**التصعيد السيبراني بين إسرائيل وحزب الله**" الضوء على حادثة تفجير أجهزة البيجر (PAGER) المستخدمة في اتصالات مقاتلي حزب الله والتي تعد سابقة لم يسبق استخدامها أو التفكير في استخدامها في

الصراعات العسكرية قديمًا أو حديثًا. فقد دللت تلك الحادثة على بداية عصر جديد من الحروب بعد أن أضحت التكنولوجيا قادرة على تصعيد صراعات عسكرية قائمة بالفعل، وبعد أن تحولت إلى وسيلة لتنفيذ عمليات اغتيال جماعية. بيد أن تحليل تلك الحادثة اقتضى النظر إليها في سياق الصراع المحتدم بين حزب الله وإسرائيل، على نحو يصعب معه فصل تلك الحادثة عن سياق الأحداث التي سبقتها أو التي تلتها. وقد أكد الفصل أن فاعلية الوسائل التجسسية لن تكون حاسمة وبهذه الدقة لولا وجود اختراق بشري كبير، ليتكامل العنصر البشري مع الوسائل التكنولوجية ومنها تقنيات مراقبة الهواتف المحمولة التي شكلت جزءًا من استراتيجية إسرائيل لتحديد مواقع قادة حزب الله، إضافةً إلى أن تكنولوجيا التعرف على الوجه شهدت تقدمًا كبيرًا مكّن القوات الإسرائيلية من التعرف على الأشخاص من خلال كاميرات عالية الدقة على متن المُسيّرات أو الأقمار الاصطناعية.

أما الفصل السابع، المعنون **"الاستراتيجيات والأدوات الذكية في الحروب الافتراضية: دراسة في الحالة الإسرائيلية"**، فقد أوضح كيف يمثل الذكاء الاصطناعي بالنسبة لإسرائيل مجالًا تكنولوجيًا ذا أهمية بالغة على الصعيد الأمني، وهو ما دفعها إلى اعتماد توظيفه في استراتيجيتها العسكرية في السنوات الأخيرة للحصول على ميزة تنافسية على أعدائها؛ وذلك لامتلاكها عددًا من التقنيات الفريدة في الحروب الذكية. ولذلك، تمثل الحروب الافتراضية أداة رئيسية في الصراعات التي تخوضها إسرائيل، حيث توظف مزيجًا من العمليات الهجومية والدفاعية التي تعتمد بدورها على: توظيف تقنيات الذكاء الاصطناعي، وبرمجيات الأمن السيبراني، وتحليل البيانات الضخمة، بما يجعلها واحدة من أبرز القوى العسكرية اعتمادًا على الحروب الذكية. إضافة إلى ذلك، تُسخّر إسرائيل تقنيات الذكاء الاصطناعي في عملياتها النفسية وحروبها الإعلامية على شبكات التواصل الاجتماعي، مما يمنحها تأثيرًا يتجاوز المجال العسكري التقليدي ليصل إلى الرأي العام العالمي وصناع القرار السياسي في المجتمع الدولي.

وقد خلص هذا الفصل إلى أنه من خلال تحليل الحروب الافتراضية التي تعتمدها إسرائيل باستخدام تقنيات الذكاء الاصطناعي، يمكن ملاحظة تطور ملحوظ في استخدام هذه التقنيات في الصراعات الحديثة. وقد أثبتت إسرائيل قدرتها على

توظيف الذكاء الاصطناعي بشكل مبتكر لتحقيق التفوق في ميادين الحرب المختلفة، سواء كانت عسكرية أو نفسية أو إعلامية. تقنيات الذكاء الاصطناعي التي تستخدمها إسرائيل في الحروب الافتراضية، بما في ذلك التزييف العميق والتحليل السيبراني وتحليل البيانات الضخمة، ساهمت في تشكيل استراتيجية دفاعية وهجومية فعالة تركز على التأثير في الرأي العام الدولي، بالإضافة إلى تحسين القدرات العسكرية التقليدية.

أما الفصل الثامن، المعنون "**الحروب السيبرانية بالوكالة: الأبعاد والتحديات وفرص المواجهة**"، فقد ناقش تصاعد نمط الحرب السيبرانية بالوكالة، وظهور نمط جديد غير مباشر لممارسة الدولة لحقها في استخدام القوة وفق القانون الدولي. وكان لها تأثيرات مختلفة على أنماط الصراع السيبراني في السباق نحو الاستحواذ على الثروة والهيمنة والمكانة، وكان لتلك الجهود الأحادية من جانب الدول تأثيرات كبيرة على الأمن السيبراني للدولة القومية من جهة، وعلى الأمن الجماعي الدولي من جهة أخرى. وهو ما طرح تساؤلات عن ماهية حركات القرصنة الدولية وخصائصهم وأهدافهم وطبيعة هيكلهم التنظيمي؟ وما هي تأثيرات تصاعد دور القراصنة المدعومين من الدولة على الأمن السيبراني العالمي؟ وما هي الأبعاد النظرية لظهور نمط الحروب السيبرانية بالوكالة؟ وما هي محفزات تصاعد عملية توظيف هذا النمط في القوة السيبرانية للدولة؟ وما هي المؤشرات الكمية لتصاعد هذا الدور؟ وما هي تحديات وفرص المواجهة على المستوى الوطني والإقليمي والعالمي؟ وما هي اتجاهات مستقبل الحرب السيبرانية بالوكالة في ظل تطبيقات الذكاء الاصطناعي التوليدي؟

إذ يرتبط نمط الحروب السيبرانية بالوكالة ضمن غيره من أنماط الصراع السيبراني بالسباق نحو الاستحواذ على تطبيقات الثورة الصناعية الرابعة والذكاء الاصطناعي ودورها في امتلاك القوة الشاملة للدولة. ويمثل لجوء الدولة إلى تجنيد القراصنة لخدمة أهدافها القومية محورًا مهمًا على أجندة الأمن الدولي نتيجة لما يضيفه من عنصر قوة جراء ذلك التحالف، ناهيك بوجود تحالفات دولية سيبرانية صاعدة بين الدول والتي تحركها الأبعاد السياسية والأيديولوجية بما يعزز من حالة الاستقطاب الدولي. ومن ثم فمن شأن ممارسة الجهود الدبلوماسية وإيجاد حلول أو تسويات أو توافق

على الأرض أن تمنع نقل الأزمات عبر المجال السيبراني وامتداد تأثيره على المجتمع الدولي، وتخفيف حدة التوتر بين القوى الدولية للحد من الظاهرة وتأثيراتها المختلفة.

وقد ركز الفصل التاسع المعنون "**الإرهاب الرقمي: القدرات السيبرانية للتنظيمات الإرهابية (داعش نموذجًا)**" على كيفية استخدام التنظيمات الإرهابية للتكنولوجيا من أجل تعزيز نفوذها وإيجاد مساحات جديدة لنشاطها، حيث سعت تلك التنظيمات إلى استخدام سبل الابتكار المتاحة لتجاوز الرقابة الأمنية المكثفة من جهة، والوصول إلى قطاعات واسعة من الفئات المستهدفة من جهة أخرى، والتغلب على الحواجز المكانية من جهة ثالثة. ومن ثمّ لا يمكن إغفال الدور الذي لعبه التطور التكنولوجي في إتاحة العديد من الآليات التي تم استغلالها من قبل تلك التنظيمات للتوسع في الإرهاب الرقمي المرتبط بالقدرات السيبرانية لتلك التنظيمات. وقد ركز هذا الفصل على القدرات السيبرانية للتنظيمات الإرهابية بالتركيز على تنظيم "داعش" الذي استغل الإعلام الرقمي ووسائل التواصل الاجتماعي من أجل تعزيز سمعته الجهادية، بجانب الطائرات بدون طيار والعملات الافتراضية وألعاب الفيديو وتطبيقات الذكاء الاصطناعي.

وقد أكد هذا الفصل في خاتمته على مرونة التنظيمات الإرهابية التي دفعتها إلى توظيف التطورات التكنولوجية من أجل تعزيز نفوذها في الساحات المادية والافتراضية، حيث استغلت وسائل التواصل الاجتماعي من أجل نشر أفكارها والترويج لأيديولوجيتها المتطرفة، كما استخدمت الطائرات بدون طيار في عمليات الاستطلاع والدعاية وتنفيذ الهجمات، كما وظفت العملات الافتراضية في التمويل وألعاب الفيديو في التجنيد، وتتخذ في الوقت الراهن خطوات من شأنها الاستفادة من التطبيقات المختلفة للذكاء الاصطناعي من أجل تطوير قدراتها.

وأخيرًا، يُختتَم الكتاب بالفصل العاشر المعنون "**اتجاهات الحروب السيبرانية: نتائج مستخلصة**" بتسليط الضوء على الاتجاهات المستقبلية للحروب السيبرانية وخطورة التهديدات السيبرانية التي تطال الوكالات الحكومية والمفاعلات النووية والمنظمات العالمية والمؤسسات الصحية، وتطال الأفراد والشركات والدول الصغرى والمتوسطة والكبرى، في ظل تطور برمجيات الفدية وسبل الاختراق والقرصنة والمتاجرة بالبيانات وبيعها، وبروز نمط الحروب اللا متماثلة، وتزايد الاعتماد على الفضاء السيبراني في

عدد واسع من الاستخدامات المدنية والعسكرية. فمع تزايد الاعتماد على الشبكات الإلكترونية لإدارة الأنظمة المسئولة عن توجيه وإدارة البنية التحتية الحيوية بجانب الأنظمة العسكرية، ازدادت بالتبعية احتمالات استهدافها في ضوء صعوبة تأمينها من مختلف التهديدات السيبرانية بشكل مطلق، وذلك على الرغم من إنفاق الدول مليارات الدولارات لتأمين تلك الشبكات.

وعليه، مع تحول الفضاء السيبراني إلى ساحة للتفاعلات الدولية بل وساحة للصراعات المختلفة، تبلورت ظاهرة الحروب السيبرانية ذات السمات المتباينة عن نظيراتها التقليدية، من حيث طبيعة الأنشطة العدائية، والفاعلون، والتأثيرات في بنية الأمن العالمي. وفي هذا الإطار، يقدم هذا الكتاب إضافة علمية رصينة للمكتبة المصرية، في ظل تفرد طابعه بما يُلبي احتياجات المتخصصين والباحثين على تنوع دوائر اهتمامهم، في ظل مواكبته للتطورات الدولية والإقليمية، وفي ظل تنوع قضاياه وعمق تحليلاته، بما يواكب التطورات التكنولوجية.