

الحروب السيبرانية

في الشرق الأوسط والعالم

الحروب السيبرانية في الشرق الأوسط والعالم



المدير العام: د. خالد عكاشة
نائب المدير العام: اللواء. محمد إبراهيم الدويري
تحرير وإشراف: د. رغدة البهي
إخراج فني: إسلام علي

الطبعة الأولى، يناير 2025

رقم الإيداع: 2025/2908م

الترقيم الدولي: 8-10-9694-977-978

© حقوق الطبع محفوظة للمركز المصري للفكر والدراسات الاستراتيجية

100 شارع الميرغني مصر الجديدة - القاهرة - مصر.

الهاتف: +20226905861 - +20226905862 - +20226905863

البريد الإلكتروني: info@ecss.com.eg

www.ecss.com.eg

الحروب السيبرانية في الشرق الأوسط والعالم

تقديم: الحروب السيبرانية.. تحولات ومخاطر 7

الفصل الأول

مفهوم الحروب السيبرانية: تأصيل نظري 17

الفصل الثاني

البعد السيبراني في الحرب الروسية-الأوكرانية: وإعادة صياغة معادلة الصراع في أوروبا 37

الفصل الثالث

حدود الحرب السيبرانية بين الولايات المتحدة الأمريكية والصين 59

الفصل الرابع

"حروب التجسس": أبعاد وتداعيات التجسس السيبراني الصيني على الدول الأوروبية 77

الفصل الخامس

"حروب الظل": حدود التصعيد الإيراني-الإسرائيلي في الفضاء السيبراني 91

الفصل السادس

التصعيد السيبراني بين إسرائيل وحزب الله 109

الفصل السابع

الاستراتيجيات والأدوات الذكية في الحروب الافتراضية: دراسة في الحالة الإسرائيلية 123

الفصل الثامن

الحروب السيبرانية بالوكالة: الأبعاد والتحديات وفرص المواجهة 149

الفصل التاسع

الإرهاب الرقمي: القدرات السيبرانية للتنظيمات الإرهابية "داعش نموذجًا" 177

الفصل العاشر

اتجاهات الحروب السيبرانية: نتائج مستخلصة 195

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 حالياً 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 مستقبلاً لتشمل: شبكات الاتصالات، وأنظمة الكمبيوتر، والمعالجات المدمجة، وغير ذلك.

وعليه، تبرز أهمية هذا الكتاب كونه مرآة عاكسة لظاهرة الحروب السيبرانية التي شهدت تحولات جوهرية بالنظر إلى جملة من الحالات التطبيقية، كما تجلّى في الصراع السيبراني بين الصين والولايات المتحدة، وفي الحرب الروسية-الأوكرانية، وفي امتدادات الحرب الإسرائيلية على غزة. فقد تعددت الدول التي توظف قدراتها السيبرانية تحقيقاً 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 غير الدول 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 ، وغير ذلك . وعليه ، قدم هذا الفصل تحليلاً لمفهوم الحروب السيبرانية والمفاهيم المتداخلة معه ، وتأثيرها على الأمن القومي للدول والجهود المبذولة في مجال مكافحتها . فقد أضحت الحروب السيبرانية مجالاً معقداً 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 تهديداً ، 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 وصفت بكونها " غير مسبوقة " ضد أوكرانيا .

فقد أظهرت الحرب الروسية-الأوكرانية أن البعد السيبراني سيكون حاضراً 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 أي من طرفي الصراع، لإجبارهما على التفاوض أو القبول ببند خاصة بالتسوية قد لا تتوافق مع مصالحهما. علاوة على ذلك، من المرجح أن تشهد المرحلة المقبلة مزيداً 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 مجاًلاً رئيسياً 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 ميداناً استراتيجياً 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 وأبل 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 بعداً سيبرانياً 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 المحتمدة في المنطقة من ناحية، وأوجدت مزيداً 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 حرباً خفية بين الطرفين تُدار في رchy الفضاء السيبراني.

وقد خلاص 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 سرّاً 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 لاحقاً 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 دلت 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 والتي 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 مكن القوات الإسرائيلية من التعرف على الأشخاص من خلال كاميرات عالية الدقة على متن المَسيّرات 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. إضافةً إلى ذلك، تُسخر 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 تعتمد عليها 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 هيكالهم التنظيمي؟ وما هي تأثيرات تصاعد دور القرصنة 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 القرصنة لخدمة أهدافها القومية محوراً مهماً 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 والأيدولوجية 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 نموذجاً)" 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 المساحات 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.

وأخيراً، يُختتم الكتاب بالفصل العاشر المعنون "اتجاهات الحروب السيبرانية: نتائج مستخلصة" بتسليط الضوء على الاتجاهات المستقبلية للحروب السيبرانية وخطورة التهديدات السيبرانية التي تطل الوكالات الحكومية والمفاعلات النووية والمنظمات العالمية والمؤسسات الصحية، وتطل 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 المسؤولة 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 يُلبّي احتياجات المتخصصين والباحثين على تنوع دوائر اهتمامهم، في ظل مواكبته للتطورات الدولية والإقليمية، وفي ظل تنوع قضاياها وعمق تحليلاته، بما يواكب التطورات التكنولوجية.

مفهوم الحروب السيبرانية : تأصيل نظري

د. وفاء لطفي*

تُعد الحروب السيبرانية من أبرز معالم الصراعات السياسية والتجارية بين الدول. ومن الناحية النظرية، فهي تعني الأنشطة الخبيثة من خلال شبكة الإنترنت المدعومة من دولة ما، والتي تستهدف البنى التحتية أو المنشآت والمؤسسات الحكومية والشبكات الصناعية والأبحاث، وهي قادرة على تعطيل البنية التحتية الحيوية مع الحد من خطر اندلاع صراع أو حرب جيوسياسية، ولا سيما مع التطورات التكنولوجية المتلاحقة مثل: إنترنت الأشياء، والحوسبة السحابية والذكاء الاصطناعي، وخدمات من قبيل برنامج حماية الخصوصية أونيون روتر والشبكة الخفية. كل هذه التكنولوجيات تعتبر سلاحًا ذا حدين: فهي تجلب مزايا للدول والحكومات، ولكن تجلبها أيضًا لمرتكبي جرائم معينة.

* أستاذ العلوم السياسية المساعد، بجامعة 6 أكتوبر

وعليه، يقدم هذا الفصل تحليلاً لمفهوم الحروب السيبرانية والمفاهيم المتداخلة معه، وتأثيرها في الأمن القومي للدول والجهود المبذولة في مجال مكافحتها، حيث أصبح من الأهمية بمكان أن نبحث في السبل التي يجب اتباعها للتصدي لتلك الظاهرة العابرة للحدود، والتي تستلزم تحديد ماهيتها وخصائصها وطبيعتها وخصائص مرتكبيها وكيفية مساءلتهم.

وعليه، يُقسّم هذا الفصل إلى خمسة محاور؛ يدور أولها حول التأصيل المفاهيمي للحروب السيبرانية من خلال تناول تعريف الحروب السيبرانية، والتمييز بينه وبين المفاهيم المتداخلة معه، ثم بيان نشأة الحروب السيبرانية. فيما يدور ثانيها حول دوافع وخصائص الحروب السيبرانية، بينما يقف المحور الثالث على أنماط وأنواع الحروب السيبرانية. أما المحور الرابع، فيعرض لبعض الأمثلة الشارحة للحرب السيبرانية، فيما يأتي المحور الخامس والأخير ليعرض الجهود الدولية في مجال مكافحة الحروب السيبرانية.

أولاً: التأصيل المفاهيمي للحروب السيبرانية

1. التعريف اللغوي والاصطلاحي للحرب السيبرانية:

لغوياً، تعرف الحربُ* على أنها «قتال بين فئتين». والحرب هي نقيض السلم. وفي الاصطلاح الحديث تعني صراعاً بالقوة المسلحة بين دولتين أو أكثر، تستهدف فيه كل دولة فرض إرادتها بالقوة على الدولة الخصم⁽¹⁾. والحرب هي ظاهرة العنف الجماعي المنظم التي تؤثر في العلاقات بين مجتمعين أو أكثر أو تؤثر في علاقات القوة داخل المجتمع⁽²⁾. أما كلمة سيبرانية، فهي مشتقة من كلمة (Cybernetics) التي تم الإشارة إليها من قبل عالم الرياضيات «نوربرت وينز» (Norbert Wiener) في عام 1948 في كتابه الشهير المعنون «علم التحكم الآلي» أو كيف يتحكم الناس والحيوانات والآلات في المعلومات وينقلونها⁽³⁾.

فيما تُعرّف الحرب السيبرانية عادةً بأنها هجوم سيبراني أو سلسلة من الهجمات التي تستهدف دولة ما، ولديها القدرة على إحداث دمار في البنية الأساسية الحكومية والمدنية وتعطيل الأنظمة الحيوية؛ مما يؤدي إلى إلحاق الضرر بالدولة وحتى خسارة الأرواح⁽⁴⁾.

ويقصد بالحرب السيبرانية أساليب الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات، وتستخدم في سياق نزاع مسلح؛ أي هي الهجمات والعمليات التي ترتكب ضد أو بواسطة شبكات الحواسيب وأنظمة البيانات بين الدول أو الجماعات المسلحة المنظمة في سياق نزاع مسلح أو سياسات الردع المتبادل⁽⁵⁾.

ويعرفها مكتب الأمم المتحدة المعني بالمخدرات والجريمة على أنها الجرائم المتعلقة بالحاسوب والمرتكبة «لتحقيق مكاسب أو أذى شخصي أو مالي»⁽⁶⁾. فيما تعرفها منظمة التعاون الاقتصادي والتنمية (OCED) على أنها كل فعل أو امتناع من شأنه الاعتداء على الأصول المادية أو المعنوية بطريق مباشر أو غير مباشر من خلال استخدام تقنيات المعلومات⁽⁷⁾. أما اللجنة الدولية للصليب الأحمر، فقد عرفت أنها الأفعال التي يتخذها أطراف نزاع ما لتحقيق ميزة على خصومهم في الفضاء السيبراني باستخدام أدوات تقنية مختلفة، مثل إتلاف المعلومات أو التجسس السيبراني⁽⁸⁾. أما «جوزيف ناي» فيعرفها بأنها أعمال عدائية في الفضاء السيبراني تعادل آثارها أو تفوق العنف الحركي التقليدي⁽⁹⁾. ويعرفها «كينيث جيرز» على أنها القدرة على الهجوم على المعلومات من خلال أجهزة الكمبيوتر عبر الفضاء السيبراني مع شل قدرة الخصم على القيام بنفس الهجمات، وأهم عناصرها هي: التجسس، والحرمان من خدمة الإنترنت، والتلاعب بالبيانات والبنية التحتية⁽¹⁰⁾. كما عرفها كل من (Richard A. Clarke & Robert Knake) بأنها «أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها».

كما تعرف الحرب الإلكترونية بأنها مجموعة من الإجراءات التي تنفذ بهدف الاستطلاع الإلكتروني للنظم والوسائل الإلكترونية المعادية، والإخلال بعمل هذه النظم والوسائل الإلكترونية، ومقاومة الاستطلاع الإلكتروني المعادي، وتحقيق استقرار عمل النظم الإلكترونية الصديقة تحت ظروف استخدام العدو أعمال الاستطلاع والإعاقة الإلكترونية. كما تعرف بأنها «أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي»⁽¹¹⁾. كما أنها وسائل وأساليب الحرب التي تعتمد على تكنولوجيا المعلومات، وتستخدم في حالات النزاع المسلح. وعليه، قد تكون العمليات السيبرانية

إما هجومية وإما دفاعية، بيد أن القانون الدولي الإنساني لا ينطبق إلا على العمليات السيبرانية التي تحدث في أثناء نزاع مسلح أو التي تؤدي في حد ذاتها إلى إشعالها⁽¹²⁾.

وتتضمن الحرب السيبرانية تسليح مهارات القرصنة إما لبدء الهجمات وإما لمنع أنواع مختلفة من الهجمات السيبرانية. وعلى الرغم من أن القرصنة بدأت كهجمات محلية ومتواضعة نسبياً على أفراد وأنظمة معينة، فقد لاحظ المستفيدون وتكتلات الجريمة السيبرانية المنظمة والدول القومية الميزة الاستراتيجية الفريدة التي تخلقها الهجمات السيبرانية، فحدث المزيد والمزيد من الهجمات سيئة السمعة⁽¹³⁾. ولهذا، تعد الحروب السيبرانية ميداناً رابعاً من ميادين الحروب، فهي حروب خفية تقتحم الأنظمة الإلكترونية، وتسبق العمل العسكري، وتستهدف الأنظمة العسكرية والبنية التحتية الحيوية للدولة، فضلاً عن الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات (SCADA) التي تسمح لها بالعمل والدفاع عن نفسها⁽¹⁴⁾.

2. التفرقة بين الحروب السيبرانية ومفاهيم أخرى:

يتداخل مفهوم الحرب السيبرانية مع عدد من المفاهيم التي يأتي في مقدمتها مفهوم "الجريمة السيبرانية" التي لا يوجد تعريف محدد لها، فهناك من يعرفها على أنها "كل فعل ضار بالآخرين عبر استعمال الوسائط الإلكترونية مثل الحواسيب، وأجهزة الموبايل، وشبكات الاتصالات الهاتفية، وشبكات نقل المعلومات، وشبكة الانترنت أو عبر الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عمومًا. فيما تعرف أيضًا بأنها "نشاط إجرامي تُستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"⁽¹⁵⁾. كما أنها نشاط غير شرعي من قبل أطراف معينة، وترتكب عن طريق الشبكات الإلكترونية العالمية، أي أنها جريمة ترتكب في بيئة الفضاء السيبراني، وقد تأتي بمعنى سرقة البرمجيات، وفي إطارها قد يصبح الكمبيوتر هو مادة للجريمة أو قد يصبح أداة لها⁽¹⁶⁾.

كما يتداخل مفهوم الحرب السيبرانية أيضًا مع مفهوم «الحرب الإلكترونية» التي يُقصد بها استخدام الطيف الكهرومغناطيسي لتشويش أو تعطيل الاتصالات وأنظمة التحكم والتوجيه الخاصة بالعدو. ويعتبر هذا النوع من الحروب أداة حيوية في العمليات

العسكرية الحديثة، فقد يُستخدم لتعطيل اتصالات العدو، وإرباك أنظمة الرادار، وحماية القوات العسكرية من الهجمات. وتشمل: التشويش الإلكتروني (Electronic Jamming) الذي يعتمد على إرسال إشارات كهرومغناطيسية بهدف تشويش أو تعطيل الإشارات اللاسلكية الخاصة بالعدو، مثل الرادارات أو الاتصالات اللاسلكية. هذا إلى جانب الاختراق الإلكتروني (Electronic Deception) من خلال إرسال إشارات كاذبة أو مضللة، بحيث يتلقى العدو معلومات خاطئة قد تقوده لاتخاذ قرارات غير صحيحة. هذا إلى جانب الحماية الإلكترونية (Electronic Protection)، وهي عبارة عن التدابير التي تتخذها الجيوش لحماية أنظمتها الخاصة من الهجمات الإلكترونية والتشويش، وذلك من خلال استخدام ترددات محمية أو أنظمة متقدمة للحماية من التشويش.

وتختلف الحرب السيبرانية في جوهرها عن الحرب الإلكترونية؛ إذ تركز على الهجمات التي تستهدف الشبكات الحاسوبية والأنظمة الرقمية. هذه الهجمات يمكن أن تتراوح بين سرقة البيانات الحساسة وتعطيل البنية التحتية الرقمية، مثل محطات الطاقة أو شبكات الاتصالات. أما أنواعها، فهي تشمل عدة أشكال من الهجمات، منها: الاختراقات (حيث يقوم الهاكرز باختراق الأنظمة الرقمية بهدف سرقة المعلومات أو تعطيلها)، والهجمات بالبرامج الخبيثة (مثل الفيروسات أو البرمجيات التي تتسبب في عطل أنظمة الحاسوب والسيطرة عليها)، والهجمات الموزعة لقطع الخدمة (التي تقوم بإغراق الشبكات الرقمية بطلبات زائفة؛ مما يؤدي إلى توقف النظام عن العمل بشكل صحيح)، وأخيرًا التجسس السيبراني، فقد تستخدم الدول أو الجماعات أدوات سيبرانية لجمع المعلومات الاستخباراتية أو التجسس على مؤسسات أو أفراد.

وبالرغم من أن الحريين تتشابهان من حيث اعتمادهما على التكنولوجيا الحديثة، فإن هناك فروقاً جوهرية بينهما، يمكن الوقوف على أبرزها بالنظر إلى النقاط التالية:

أ. المجال العملياتي: تعمل الحرب الإلكترونية ضمن الطيف الكهرومغناطيسي (مثل موجات الراديو والترددات اللاسلكية)، وتهدف إلى التشويش أو تعطيل الاتصالات المادية التي تتم عبر هذه الموجات. أما الحرب السيبرانية، فتركز

على الفضاء الرقمي، حيث تستهدف الشبكات الحاسوبية، وقواعد البيانات، وبرمجيات الحماية، باستخدام أدوات من قبيل: الفيروسات، والبرامج الخبيثة، والهجمات على الأنظمة الرقمية.

ب. الأهداف: يتمثل الهدف الأساسي من الحرب الإلكترونية في تعطيل أنظمة اتصالات العدو وأجهزة الرادار، مما يؤدي إلى إرباك العمليات العسكرية. بينما يتمثل الهدف الأساسي للحرب السيبرانية في: سرقة البيانات، والتجسس الإلكتروني، أو تعطيل البنية التحتية الرقمية مثل شبكات الطاقة أو المصارف أو أنظمة الطيران.

ج. الوسائل: تعتمد أدوات الحرب الإلكترونية على أجهزة التشويش والتداخل الكهرومغناطيسي، مثل أجهزة التشويش الموجهة التي تمنع العدو من التواصل. أما في الحرب السيبرانية، فتُستخدم البرمجيات المتقدمة مثل الفيروسات والبرامج الخبيثة لتدمير الأنظمة الرقمية أو السيطرة عليها.

د. التأثير الاستراتيجي: أصبحت الحروب الإلكترونية والسيبرانية أدوات رئيسية في الصراعات الحديثة، ففي الأولى، يتم تعطيل القدرات العسكرية للعدو من خلال تعطيل اتصالاته وأنظمة التوجيه، فالجيوش التي تمتلك قدرات حرب إلكترونية قوية غالباً ما تتمتع بتفوق تكنولوجي يُمكنها من التفوق على الخصوم في ساحات المعارك. أما التأثيرات الاستراتيجية للثانية، فتكمن في تعطيل البنية التحتية الحيوية، حيث تؤدي الهجمات السيبرانية إلى شلل كامل في الدول المستهدفة من خلال تعطيل شبكات الطاقة، والأنظمة المصرفية، وشبكات الاتصالات. كما أن الحرب السيبرانية تُستخدم بشكل واسع للتجسس على الدول الأخرى وسرقة معلومات حساسة قد تؤثر في الأمن القومي، بالإضافة إلى التأثير في الرأي العام من خلال هجمات على وسائل الإعلام أو مواقع التواصل الاجتماعي، إذ يمكن للحرب السيبرانية التأثير في تشكيل الرأي العام وتوجيهه في اتجاهات معينة⁽¹⁷⁾.

كما يتداخل مفهوم الحرب السيبرانية أيضاً مع مفهوم "الهجوم السيبراني"، وهو أي نوع من المناورة الهجومية التي تستهدف أنظمة معلومات الكمبيوتر أو البنية التحتية أو شبكات الكمبيوتر أو أجهزة الكمبيوتر الشخصية. بحيث يصبح المهاجم كل شخص أو عملية تحاول الوصول إلى البيانات أو الوظائف أو المناطق المحظورة

الأخرى في النظام دون الحصول على إذن. وتُعتبر الهجمات السيبرانية، التي تجمع بين قدرات تخريب كبيرة ونشر سريع بتكاليف سياسية واقتصادية منخفضة، مؤاتية إلى حد كبير للجهات الفاعلة التي تسعى إلى تحقيق استراتيجية جيوسياسية موسّعة ذات موارد محدودة، وتُلحق الضرر وبشكل كبير وسريع وعلى المستوى العالمي⁽¹⁸⁾.

3. نشأة الحرب السيبرانية:

تعود بداية الحروب السيبرانية إلى حقبة الحرب الباردة، وبالرغم من أنها كانت تدور في نطاق محدود نوعاً ما، فإن أول موقعة سيبرانية ذات آثار بارزة دارت بين الولايات المتحدة والاتحاد السوفيتي في عام 1982. فقد تم تخريب خط الأنابيب السوفيتي العابر لسيبيريا، حيث كانت هناك عملية ضخمة لجهاز المخابرات السوفيتي (KGB)، تسمى (Line X)، صُممت لتساعد الاتحاد السوفيتي، والذي كان متأخراً إلى حد كبير في مجال تصميم التكنولوجيا والإلكترونيات الدقيقة، على تخطي هذه الفجوة عن طريق سرقة تكنولوجيا المعلومات من الغرب. وعليه، قامت المخابرات السوفيتية بتدريب جيش من العلماء على التسلل إلى الشركات والوكالات لسرقة المخططات والرسوم للمشروعات والإنشاءات والمعلومات السرية للأبحاث، ثم تسربت معلومات إلى وكالة المخابرات المركزية الأمريكية (CIA)، والتي بدلاً من أن تشن حملات ومداهمات ضد هؤلاء العلماء-العملاء، قررت القيام بما هو أبعد من ذلك، ونصبت فخاخاً لتنفيذ عملية تجسس مضادة. فبدلاً من إلقاء القبض عليهم، تركتهم يواصلون العمل، وأمدتهم بمعلومات مغلوطة، وسمحت لهم بالولوج إلى مخططات لمنشآت يمكنهم بناءها، من بينها مخططات لبناء خطوط أنابيب للنفط والغاز الطبيعي. وقد حصل الجواسيس السوفييت على وثائق تتضمن مخططات الإنشاء، لكنها كانت تتضمن خطأ بسيطاً في الشفرة لم يتمكنوا من ملاحظته. وقد استخدم السوفييت المخططات بالفعل لبناء العمود الفقري لخطوط نقل الغاز الطبيعي والنفط القادمة من سيبيريا، ولكن بعد فترة قصيرة، تسبب الخطأ المتعمد في الشفرة في حدوث انفجار لخط الأنابيب، وكان انفجاراً يعادل ثلث حجم انفجار القنبلة النووية في هيروشيما⁽¹⁹⁾.

ثانيًا: دوافع وخصائص الحروب السيبرانية

هناك العديد من الأسباب التي قد تجعل شخصًا ما يشن هجومًا إلكترونيًا، سواء لتحقيق مكاسب مالية أو لسرقة معلومات مثل أرقام بطاقات الائتمان أو احتجاز البيانات للحصول على فدية. وقد يتطلع المهاجم إلى تعطيل العمليات أو التسبب في أضرار من خلال شن هجومات لرفض الخدمة، على نحو يؤدي إلى إغراق النظام بحركة المرور، ويقطع اتصاله بالإنترنت. وفي بعض الحالات، يمكن أن تحدث الهجمات السيبرانية برعاية دولة ما، حيث تهاجم دولة ما أنظمة الكمبيوتر في دولة أخرى لتعطيل بنيتها التحتية أو أنظمة اتصالاتها؛ حيث تشكل الهجمات السيبرانية تهديدًا خطيرًا للأفراد والشركات على حدٍ سواء. ومن المهم لكل من الشركات والأفراد أن يكونوا على دراية بالمخاطر، وأن يتخذوا خطوات لحماية أنفسهم، من خلال استخدام كلمات مرور قوية، والمصادقة متعددة العوامل (MFA)، وتحديث البرامج، وغير ذلك. ومما لا شك فيه أن تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية يتسبب في نشوء نمط جديد من الضرر الذي يمكن أن تسببه دولة لأخرى، وخاصة أن الثورة التكنولوجية الحديثة تمخضت عنها ثورة أخرى في المجالات العسكرية في ظل تطور تقنيات الحرب⁽²⁰⁾.

وتبلورت ظاهرة الحروب السيبرانية التي اتسمت بخصائص مختلفة عن نظيراتها التقليدية؛ من حيث: طبيعة الأنشطة العدائية، والفواعل، والتأثيرات في بنية الأمن الدولي. ومن أبرز خصائصها ما يلي:

1. **تراجع التكلفة:** تعتبر الحروب السيبرانية حروبًا غير تناظرية؛ إذ تتراجع تكلفة الأدوات اللازمة لشن هكذا حروب نسبيًا، مقارنة بالتكلفة التي تتكبدها الدول لتصنيع أسلحة على شاكلة حاملات الطائرات والمقاتلات المتطورة، كي تفرض تهديدًا خطيرًا وحقيقيًا على دولة أخرى⁽²¹⁾.

2. **هلامية الشكل وصعوبة الردع:** يختلف مفهوم الردع في الحرب التقليدية عن مثيله في الفضاء السيبراني. فعلى عكس الحروب التقليدية، حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان تحديد موقع الهجمات

السيبرانية، وهو ما يلغي مفعول الردع، ولا سيما مع ظل صعوبة تتبع مصدر كثير من تلك الهجمات في المقابل. وقد يمكن تتبع مصدر تلك الهجمات، ولكن إن ثبت أنها تعود لفاعلين من غير الدول، فلن يكون لديهم أصول أو قواعد للرد عليها.

3. تنوع الجوانب المستهدفة: لا تقتصر أهداف الحروب السيبرانية على استهداف المواقع العسكرية، وبخاصة مع تحول البنى التحتية المدنية والحساسة في البلدان المستهدفة على شاكلة شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة إلى أهداف محتملة، مما يعني اتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون، سواء كانوا دولاً أو فاعلين من غير الدول. فقد تشن الدول هجمات سيبرانية عبر أجهزتها الأمنية أو الدفاعية، كما قد تلجأ إلى تجنيد قراصنة أو موالين لشن هجمات ضد الخصوم بالوكالة. وبرغم عدم تطوير الجماعات الإرهابية، كفاعل من غير الدول، لقدراتها في الحرب السيبرانية، مقارنة بممارسة القوة الناعمة على الفضاء الإلكتروني لنشر الأفكار المتطرفة، فإن هناك مؤشرات على احتمال تطوير تلك الجماعات لقدراتها الهجومية مستقبلاً⁽²²⁾.

4. توظيف الفضاء الإلكتروني في تعظيم قوة الدول: من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى «الاستراتيجية السيبرانية» للدول، والتي تشير إلى القدرة على التنمية، وتوظيف القدرات للتشغيل في الفضاء الإلكتروني، وذلك بالاندماج والتنسيق مع المجالات العملية الأخرى لتحقيق أو دعم إنجاز الأهداف، عبر عناصر القوة القومية.

ثالثاً: أنماط وأنواع الحروب السيبرانية

تتعدد أنماط الحروب السيبرانية، لتشمل ما يلي:

1. الحرب السيبرانية الباردة منخفضة الشدة: وفيها يتم استخدام الفضاء السيبراني كساحة للصراع منخفض الشدة. ويعبر هذا النمط عن صراع مستمر بين الفاعلين المتنازعين، وقد يكون ذا طبيعة ممتدة وعدوانية دائمة. ولهذه الحرب السيبرانية الباردة وسائل عدة؛ منها: شن الحروب النفسية، والاختراقات المتعددة، والتجسس، وسرقة المعلومات، وشن حرب الأفكار، والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية. ويظهر هذا النمط من الحروب في الصراعات السياسية، ذات البعد الاجتماعي الديني الممتد، مثل الصراع العربي-الإسرائيلي والصراع الهندي-الباكستاني والصراع بين الكوريتين الشمالية والجنوبية، وغير ذلك. وتجدر الإشارة إلى أن في مثل هذه الصراعات، تنشط جماعات دولية للقرصنة للتعبير عن مواقف سياسية أو حقوقية، مثل جماعة «ويكيليكس» و«أنونيموس»، وأيضاً في حالات الأزمات الدولية، مثل التوتر بين استونيا وروسيا في عام 2007، والاختراقات المتبادلة بين الصين والولايات المتحدة وروسيا، وبين طهران وواشنطن⁽²³⁾.

2. نمط الحرب السيبرانية متوسطة الشدة: وفيها يتحول الصراع عبر الفضاء السيبراني إلى ساحة موازية لحرب تقليدية دائرة على الأرض. ويكون ذلك تعبيراً عن حدة الصراع القائم بين الأطراف، كما قد يمهد لعمل عسكري. وتدور حروب الفضاء السيبراني عن طريق اختراق المواقع الإلكترونية وتخريبها، وشن حرب نفسية ضد الخصوم، وغير ذلك. ويستمد ذلك النوع من الحروب السيبرانية شدته من قوة أطرافه، وارتباطها بعمل عسكري تقليدي، خاصة في ظل بعض التقديرات التي تشير إلى أن تكلفة هذه الحروب قد تشكل أربعة أضعاف نظيراتها التقليدية، مما يعني إمكانية تمويل حملة حربية كاملة عبر الإنترنت بتكلفة تصنيع دبابة واحدة فقط⁽²⁴⁾.

3. الحرب السيبرانية الساخنة مرتفعة الشدة: ويقصد به نشوء حروب في الفضاء السيبراني منفردة وغير متوازية مع الأعمال العسكرية التقليدية. ولم يشهد العالم هذا النوع من الحروب، وإن كانت احتمالات حدوثها واردة في المستقبل مع تطور القدرات التكنولوجية، وتنامي الاعتماد على الفضاء السيبراني. وهذا النمط من الحروب ينطوي على سيطرة البعد التكنولوجي على إدارة العمليات الحربية، فقد يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو أو اللجوء إلى الروبوتات الآلية في الحروب والطائرات دون طيار وإدارتها عن بعد، بخلاف تطوير القدرات في مجال الدفاع والهجوم السيبراني، والاستحواذ على القوة الإلكترونية⁽²⁵⁾. فقد شهدت الأسلحة السيبرانية تطوراً أكبر في قدرتها على التأثير في الخصوم، مثل أسلحة الميكروويف عالية القدرة، والهجمات السيبرانية عبر الفيروسات، مثل شن إسرائيل هجمات فيروس ستاكسنت ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة في عام 2010.

أما عن أنواع هجمات الحرب السيبرانية، فيمكن القول إن هناك العديد من أنواع هجمات الحرب السيبرانية التي يمكن استخدامها لتعطيل أو سرقة المعلومات الحساسة من أنظمة الكمبيوتر والشبكات والأجهزة. وهذا وتشمل بعض الأسلحة السيبرانية ما يلي⁽²⁶⁾:

- استخدام البرامج الضارة: مثل الفيروسات أو الفيروسات المتنقلة أو أحصنة طروادة، للتسلل إلى الأنظمة وإتلافها أو سرقة المعلومات الحساسة.
- رفض الخدمة الموزعة (DDoS): أي إغراق الشبكة أو موقع الويب بحركة المرور أو الطلبات؛ مما يجعلها غير متاحة للمستخدمين الشرعيين.
- التصيد الاحتيالي: بمعنى إرسال رسائل بريد إلكتروني مزيفة أو رسائل تبدو وكأنها من مصادر مشروعة في محاولة لخداع المستلم للكشف عن معلومات حساسة أو النقر فوق رابط ضار.
- هجمات الرجل في الوسط: أي اعتراض وتغيير الاتصالات بين طرفين دون علمهما.
- هجمات حقن SQL: أي حقن تعليمات برمجية ضارة في قاعدة بيانات موقع الويب من خلال ضعف في عملية التحقق من صحة إدخال موقع الويب.

- هجمات برامج الفدية: تشفير ملفات الضحية والمطالبة بفدية لاستعادة الوصول إليها.
- هجمات سلسلة التوريد: أي اختراق سلسلة التوريد الخاصة بشركة أو مؤسسة للوصول إلى أنظمتها أو بياناتها.

رابعاً: بعض الأمثلة الشارحة لهجمات الحروب السيبرانية

يمكن للتجسس السيبراني جمع المعلومات الاستخبارية التي من شأنها أن تساعد دولة ما في الاستعداد للإعلان عن هجوم مادي أو حرب إلكترونية أو حرب هجينة على دولة أخرى. كما يمكن استخدام الهجمات السيبرانية على أنظمة الكمبيوتر الحكومية لتعطيل العمليات الحيوية ومساعدة جهود الحرب التقليدية. ولا شك أن إتلاف البنية التحتية الرقمية الحيوية يضر بالخدمات أو العمليات الحيوية الحديثة. وفي هذا الإطار، نعرض بعض هجمات القراصنة البارزة عبر التاريخ والتي كان لها تأثيرات كبيرة في الأفراد والمنظمات والدول، وهي كالتالي:

1. هجوم برنامج الفدية WannaCry: في مايو 2017، أثر هجوم برنامج الفدية المعروف باسم (WannaCry) على أكثر من 200 ألف جهاز كمبيوتر في 150 دولة. وقد استغل الهجوم ثغرة أمنية في نظام التشغيل (Windows)، وقام بتشفير البيانات الموجودة على أجهزة الكمبيوتر المصابة، وطالب بالدفع مقابل مفتاح فك التشفير، وتسبب في اضطراب واسع النطاق؛ مما أثر بشكل خاص في المستشفيات وأنظمة النقل.
2. اختراق (SolarWinds): في ديسمبر 2020، قامت مجموعة من المتسللين باختراق شركة البرمجيات (SolarWinds) وإدخال برامج ضارة في تحديثات برامجها، والتي تستخدمها العديد من الوكالات الحكومية والشركات الكبرى. ولا تزال السلطات تحقق في الأضرار الناجمة عن الاختراق، ولكن كان هناك إجماع على أن المتسللين يمكنهم الوصول إلى البيانات الحساسة في المستقبل وربما تعطيل العمليات.
3. اختراق بيانات (Equifax): في عام 2017، عانت شركة التقارير الائتمانية (Equifax) من اختراق بيانات أثر في أكثر من 147 مليون شخص، حيث تمكن القراصنة من الوصول إلى المعلومات الدقيقة، مثل: أرقام الضمان الاجتماعي، وتواريخ الميلاد

والعناوين. وهو ما أثر بشكل كبير في الأفراد المتضررين وعلى سمعة الشركة واستقرارها المالي.

4. اختراق شركة (Sony Pictures) في عام 2014، أدى هذا الهجوم، الذي نُسب لاحقًا إلى كوريا الشمالية، إلى نشر معلومات حساسة للشركة، بما في ذلك رسائل البريد الإلكتروني وبيانات الموظفين والأفلام التي لم يتم إصدارها. وتسبب الهجوم في خسائر مالية كبيرة لشركة (Sony Pictures)، وأدى إلى استقالة العديد من كبار المسؤولين التنفيذيين.

5. اختراق شركة (Yahoo Inc): في 2016، تعرضت شركة الويب العملاقة (Yahoo Inc) إلى هجوم كبير، حيث قام المتسللون بسرقة بيانات شخصية مرتبطة بما لا يقل عن 500 مليون حساب.

6. اختراق بيانات (Uber Data Ransom): في عام 2022، اعترفت شركة "أوبر" بالتستر على خرق ضخم للبيانات في عام 2016. واختارت الشركة التزام الصمت بشأن هجوم كشف البيانات السرية الذي طال 57 مليون عميل وسائق.

ومما لا شك فيه أن مثل هذه الهجمات السيبرانية تؤدي إلى خسائر مالية مباشرة، مثل تكلفة دفع فدية لفتح البيانات المشفرة في هجوم برامج الفدية أو إصلاح الأنظمة التالفة أو استبدالها. ويمكن أن تؤدي أيضًا إلى خسائر مالية غير مباشرة، مثل فقدان الإيرادات بسبب التوقف أو فقدان العملاء بسبب انتهاك معلوماتهم الشخصية.

كما يمكن أن تؤدي الهجمات السيبرانية إلى تعطيل عمليات الشركات؛ مما يتسبب في توقف العمل، ويجعل من الصعب على الموظفين الوصول إلى الأنظمة والموارد التي يحتاجونها للقيام بعملهم. وهذا يمكن أن يؤدي إلى تراجع الإنتاجية والإيرادات.

وكلما شهدت البنية التحتية للدول تقدمًا ملحوظًا في مجال تكنولوجيا المعلومات، فإن أمنها الوطني سوف يظل عرضة للمخاطر، إلا أن الأمر الذي يجب أن

توليه الدول اهتمامًا هومدي قدرة الجماعات الإرهابية على شن هجمات سيبرانية على قطاعي الدفاع والأمن بصفة خاصة. وحتى الآن، يؤكد الخبراء أن أنظمة الجيوش لا تزال في مأمن من تلك المخاطر، إلا أنه تجدر الإشارة إلى أنها مستهدفة، والأمثلة على ذلك عديدة، ومنها إعلان وزير الدفاع الفرنسي أن الأنظمة الأمنية الفرنسية قد أحبطت 24 ألف هجوم سيبراني خارجي استهدف أجهزة الدفاع خلال عام 2016. وفي عام 2017، تعرضت العديد من الدول لسلسلة من الهجمات السيبرانية، حيث وقع أكثر من 45 ألف هجمة سيبرانية لأكثر من 99 دولة، وذلك وفقًا لخبراء الأمن المعلوماتي. كما أعلنت شركة «كاسبرسكاى لابز» (Kaspersky Labs) أن من ضمن الدول التي تعرضت لذلك الهجوم من خلال «الفيروس العالمي الذي يطلق عليه انتزاع الفدية» (Grab the Ransom) كلاً من: بريطانيا، وألمانيا، وتركيا، واليابان، والهند، ومصر، والصين، وفرنسا، وإسبانيا، والفلبين، والمكسيك، وروسيا⁽²⁷⁾.

وفي عام 2018، اتهم وزير الخارجية البريطاني «جريمي هانت» الاستخبارات العسكرية الروسية بالوقوف خلف هجمات سيبرانية في جميع أنحاء العالم، واستهداف وسائل إعلامية وسياسية، كالتدخل في الانتخابات الأمريكية في عام 2016 بناء على نتائج المركز الوطني البريطاني للأمن السيبراني. كما تعرضت بريطانيا في عام 2018 كذلك لهجمات الفدية التي استهدفت قطاع الصحة بهدف جمع الأموال، وقد اتهمت روسيا وكوريا الشمالية. وقد سبق ذلك في عام 2012 تعرض شركة أرامكو السعودية لأكبر هجوم سيبراني عندما تم تدمير أكثر من 30 ألف جهاز باستخدام فيروس «شامون»⁽²⁸⁾.

خامساً: الجهود الدولية في مجال مكافحة الحروب السيبرانية

يتمخض عن الحروب السيبرانية تهديدات سياسية واقتصادية عدة، ولا سيما في حالة الاستخدام غير المشروع للمعلومات السرية أو نظم التشغيل، فضلاً عن التهديدات الإلكترونية من قبل التنظيمات الإرهابية، والتعدي على أموال الغير بالوسائل الإلكترونية، والسطو على أموال البنوك⁽²⁹⁾. وانطلاقاً من تلك المخاطر وغيرها، تتعدد الجهود التي تبذلها الدول في مجتمع المعلومات العالمي من أجل

العمل على تنظيم عملية وضع السياسات المثلى للتعامل مع الهجمات السيبرانية من قبل الحكومات، ومن أجل حماية البنية التحتية الكونية للمعلومات من خطر التعرض لمثل تلك الأخطار. كما اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني أو الثنائي أو الإقليمي⁽³⁰⁾.

وفي ظل التحولات الرقمية التي يعيشها العالم، ظهر نوع جديد من التهديدات الأمنية التي تعتبر البيئة الرقمية عاملاً مهماً في انتشارها، وقد أصبحت هذه التهديدات تمس ليس فقط أمن المؤسسات، وإنما أيضاً أمن الأفراد، وبذلك تكون شكلت تحدياً للدولة في سعيها لتحقيق أمنها القومي. ومما شك فيه أن الاعتماد على أنظمة المعلومات الرقمية يجلب معه نقاط الضعف والمخاطر المتزايدة، ولا سيما للبنية التحتية للمعلومات الوطنية الحرجة (CNII)، والتي تشمل من بين أمور أخرى الجرائم الإلكترونية مثل القرصنة والتطفل والاحتيال والمضايقة والرموز الضارة وهجمات الحرمان من الخدمة، وهو ما يزيد من التهديدات السيبرانية التي تهدد السيادة السيبرانية للدول⁽³¹⁾.

وعليه، هناك العديد من الخطوات التي يمكن اتخاذها للحماية من المخاطر السيبرانية، تتمثل في التالي:

1. إجراء تقييمات المخاطر باستخدام (Cyber Wargames): إن أفضل طريقة لتقييم مدى استعداد الدولة للحرب السيبرانية هي إجراء تدريب أو محاكاة واقعية، والمعروفة أيضاً باسم «لعبة الحرب السيبرانية»، وهي بمثابة تدريب على كيفية استجابة الحكومات والمنظمات الخاصة لسيناريو الحرب السيبرانية، وكشف الثغرات في الدفاعات، وتحسين التعاون بين الكيانات. والأهم من ذلك، يمكن أن تضمن «لعبة الحرب السيبرانية» المدافعين السرعة والفاعلية في التصرف من أجل حماية البنية التحتية الحيوية وحماية الأرواح. كما يمكن أن تساعد ألعاب الحرب السيبرانية البلدان على تحسين استعدادها للحرب السيبرانية من خلال:

- اختبار المواقف المختلفة: مثل اكتشاف الهجمات في المراحل المبكرة، أو التخفيف من المخاطر بعد تعرض البنية التحتية الحيوية للخطر بالفعل.

- اختبار السيناريوهات الخارج عن المألوف: الهجمات السيبرانية لا تتم حسب القواعد المتعارف عليها، في هذه الحالة يعمل فريق كمهاجم بواسطة طرق مبتكرة لاختراق النظام المستهدف، وبهذا يتعلم المدافعون كيف يخففون أو يمنعون التهديدات الحقيقية عندما تحدث.
- تقسيم العمل وآليات التعاون: تتطلب الحرب السيبرانية تعاون العديد من الأفراد من مختلف المنظمات والوحدات سواء أكانت حكومية أو مستقلة في آليات عملها عن الجهاز الرسمي. ومن الممكن أن تجمع «لعبة الحرب السيبرانية» هؤلاء الأشخاص الذين قد لا يعرفون بعضهم البعض، وتساعدهم على تحديد كيفية العمل معًا في حالة وقوع أزمة.
- تحسين السياسات: قد تضع الحكومات سياسات للحرب السيبرانية، ولكنها تحتاج إلى اختبارها عمليًا. ومن الممكن أن تختبر «لعبة الحرب السيبرانية» مدى فاعلية السياسات، وتوفر الفرصة لتحسينها.

2. الدفاع الطبقي: تحت ضغط الحرب السيبرانية، أقرت حكومات العديد من البلدان سياسات أمنية وطنية عملية لحماية البنية الأساسية للمعلومات. وتستخدم هذه السياسات عادة نهجًا دفاعيًا متعدد الطبقات، والذي يتضمن: تأمين النظام البيئي السيبراني، ورفع مستوى الوعي السيبراني، وتعزيز المعايير المفتوحة لمكافحة التهديدات السيبرانية، وتنفيذ إطار ضمان الأمن السيبراني الوطني، والعمل مع المنظمات الخاصة لتحسين قدراتها في مجال الأمن السيبراني.
3. تأمين القطاع الخاص: إن العامل الاستراتيجي في الحرب السيبرانية يتمثل في قدرة الشركات المحلية على الصمود في مواجهة الهجمات السيبرانية. وتحتاج الشركات إلى تشديد إجراءاتها الأمنية للحد من التداعيات المحتملة للهجوم⁽³²⁾.

وفيما يلي مجموعة من التدابير لضمان الأمن السيبراني للشركات، والتي يمكن أن تعزز الأمن الوطني:

- استخدام كلمات مرور قوية: استخدم كلمات مرور معقدة يصعب على المهاجمين تخمينها، واستخدم كلمات مرور مختلفة لحسابات مختلفة مع تمكين المصادقة الثنائية كلما أمكن ذلك.
- تحديث البرامج وأنظمة الأمان: القيام بتحديث البرامج وأنظمة الأمان بانتظام لإصلاح نقاط الضعف التي يمكن أن يستغلها المتسللون.
- تثقيف الموظفين: بمعنى تدريب الموظفين على تحديد وتجنب هجمات التصيد الاحتيالي والتهديدات السيبرانية الشائعة الأخرى.
- استخدام جدران الحماية وبرامج مكافحة الفيروسات: وذلك بهدف الحماية من البرامج الضارة والتهديدات الأخرى.
- استخدام شبكات آمنة: مثل الشبكات الخاصة الافتراضية (VPN)، لحماية البيانات عند الوصول إلى الإنترنت عبر شبكة (Wi-Fi) عامة.
- تنفيذ إجراءات النسخ الاحتياطي للبيانات واستعادتها: يجب إجراء النسخ الاحتياطي للبيانات المهمة بانتظام، ولا بد من وجود خطة لاستعادتها في حالة وقوع أي هجوم فعلي.
- استخدام البروتوكولات الآمنة: مثل (HTTPS) لحماية البيانات المنقولة عبر الإنترنت.
- إجراء تقييمات أمنية منتظمة: أي تقييم واختبار أمان الأنظمة بانتظام لتحديد نقاط الضعف وإصلاحها قبل أن يتم استغلالها.

خاتمة:

مما سبق، يتضح أن الحروب السيبرانية مجاًلاً معقداً وسريع التطور وله آثار كبيرة في المواطنين والحكومات والشركات في جميع أنحاء العالم. وقد فرضت بالفعل تحديات عديدة تواجه دول العالم، حيث أصبح المجال الافتراضي بمنزلة ساحة قتال جديدة تشكل تهديداً، يضاف إلى قائمة التهديدات التقليدية التي تواجه العالم، وتتجاوز في أبعادها وآثارها الحدود الجغرافية والسياسية، وتلقي بتداعياتها على

مستقبل الأمن القومي والحيوي للدول . كما أصبحت عمليات الاختراق التي يقوم بها «الهكرز» قادرة على إغراق أجهزة خوادم برسائل من أنظمة متعددة تشل سير عملها وتوقف نظم الإنتاج .

ومع استمرار تطوّر التكنولوجيا، يُتوقّع أن تشهد الحروب الإلكترونية والسيبرانية تطوّرات أكبر، مما يطرح تحديات جديدة. فمع زيادة استخدام الذكاء الاصطناعي وإنترنت الأشياء (IoT)، سيصبح من الصعب حماية الأنظمة الرقمية والبنية التحتية من الهجمات السيبرانية. ومع تزايد الاعتماد على الشبكات الرقمية والاتصالات اللاسلكية في العمليات العسكرية، سيزداد الضغط على الجيوش لحماية أنظمتها من الهجمات الإلكترونية والسيبرانية. والأخطر من ذلك، أنّ القوانين الدولية المتعلقة بكلتا الحريين لا تزال غير واضحة بشكل كافٍ؛ مما يزيد من احتمالات نشوب صراعات بين الدول بسبب هجمات من هذا النوع.

ومن الجدير بالذكر أن الهجمات السيبرانية قد تشكل مصدر خطر لا يستهان به، ولها عدة أنواع؛ منها الفيروسات التي تعتبر مثلاً للأسلحة الحالية من خلال إصابة برامج البيانات وأنظمة التشغيل وإعطابها بشكل دوري بواسطة الثغرات المبينة، وكذلك نظام الاختراق وبرامج التدمير عبر وسائل الهواتف الذكية أو أنظمة التشغيل المعتمدة قانونياً لدى الأجهزة الأمنية.

المصادر:

1. نبيلة عبد الفتاح، الحرب السيبرانية وسبل مواجهتها، مجلة شؤون استراتيجية، العدد 17، مارس 2024، ص. 487.
2. حرب، القاموس العملي للقانون الإنساني، متاح على: <https://ar.guide-humanitarian-law.org/content/article/5/> /hrb
3. Miranda Green, 'Cyber' is everywhere, but what does the prefix mean and where did it come from?, **Wmar2 News**, Oct 14, 2014, Available at: <https://shorturl.at/aMm0c>
4. Cyber Warfare, Available at: <https://www.imperva.com/learn/application-security/cyber-warfare/>
5. هالة أحمد الرشدي، هل من حرب سيبرانية بين الولايات المتحدة وروسيا؟، جريدة الأهرام، 4 يناير 2021.
6. Computer-related offences, **UNODC**, Available at: <https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/computer-related-offences.html>
7. فرد كابلان، المنطقة المعتمدة: التاريخ السري للحرب السيبرانية، ترجمة: لؤي عبد المجيد (الكويت: المجلس الوطني للثقافة والفنون والآداب، 2019)، ص. 66.
8. هريت لين، النزاع السيبراني والقانون الدولي الإنساني، مجلة اللجنة الدولية للصليب الأحمر، المجلد 94، 2012، ص. 505.
9. Joseph Nye, **Nuclear Lessons for Cyber Security? Strategic Studies Quarterly**, No. 4, (USA - Virginia: Air University Press, 2011), pp. 18-38.
10. Kenneth Geers, **Cyberspace and the changing of warfare**, (Estonia-Tallinn: The NATO Cooperative Cyber Defence Centre, 2008), p. 28.
11. انصر سفاح كريم، الحروب الإلكترونية وأثرها على الأمن القومي، مركز النهرين للدراسات الاستراتيجية، 26 ديسمبر 2023، متاح على: https://www.alnahrain.iq/post/1031#_edn1
12. Cyber warfare, **Casebook**, Available at: https://casebook.icrc.org/a_to_z/glossary/cyber-warfare
13. History Of Cyber Warfare And The Top 5 Most Notorious Attacks, **Fortinet**, Available at: <https://www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare>
14. تورية حمدون، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، 2011، ص. 9-8.
15. وفاء لطفى، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجاً، مجلة كلية الاقتصاد والعلوم السياسية، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، 2022، ص. 160.
16. الجرائم الإلكترونية، متاح على: <https://www.business.hsbc.com.eg/ar-eg/cybercrime>
17. فيولا مخزوم، ما الفرق بين الحرب الإلكترونية والحرب السيبرانية؟، الميادين نت، 19 أيلول، متاح على: <https://shorturl.at/08svB>
18. مايكل يونغ، ما الأهمية التي باتت تتمتع بها الحرب السيبرانية (الإلكترونية) في دول الشرق الأوسط؟، مركز كارنيغي للشرق الأوسط، 1 فبراير 2028، متاح على: <https://carnegieendowment.org/middle-east/diwan/2018/02/how-important-has-cyber-warfare-become-to-the-states-of-the-middle-east?lang=ar>
19. الحروب السيبرانية.. نتائج ملموسة لمعارك غير مرئية، مجلة الجندي، 1 أبريل 2021، متاح على: <https://shorturl.at/4DdEV>
20. Jennie M. Williamson, **Information Operations: Computer Network Attack in the 21st Century**, Strategy Research Project (Pennsylvania: U.S. Army War College. Carlisle Barracks, 2002) pp. 15-22.
21. William J. Lynn, Defending a New Domain: The Pentagon's Cyberstrategy, **Foreign Affairs**, September-October 2010, p. 98.
22. Martin C. Libicki, Cyber deterrence and cyberwar, Rand, 2009, pp. 39-64.
23. David E. Sanger, Confront and Conceal: Obama's Secret Warsand Surprising Use of American Power (New York: Crown, 2012), p. 188. "RalphLangner: Cracking Stuxnet, a 21 st Century Cyber Weapon", **TED**, Available at: http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon
24. Florian Bieber, Cyber war or Sideshow the Internet and the Balkan Wars, **Current History**, Vol. 99, No. 635, Mar 2000, pp. 124-128, Available at: <http://search.proquest.com/docview/200751259accountid=7180>
25. عادل عبد الصادق، هل يمثل الإرهاب الإلكتروني شكلاً جديداً من أشكال الصراع، مركز الأهرام للدراسات السياسية والاستراتيجية، 2017، ص. 6.
26. المرجع السابق، مصدر إلكتروني.
27. هبة أحمد عبد الدايم، منار محمد شعبان، الهجمات السيبرانية، دراسات دورية، بنك الاستثمار القومي، قطاع الاستثمار والموارد الدعم الفني للاستثمار، يوليو 2017، ص. 9.

28. محمد فرج، جرائم القرصنة... تهديد متزايد يستنفر جهود المجتمع الدولي، سكاي نيوز، 3 يوليو 2021، متاح على: <https://shorturl.at/BvBql>
29. وفاء لطفى، تأثير الإرهاب الإلكتروني على الأمن القومي للدول في ظل جائحة كورونا (كوفيد-19)، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، جامعة الإسكندرية، المجلد 7، العدد 13، يناير 2022، ص. 454.
30. عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق (القاهرة: الهيئة العامة للكتاب، 2018)، ص. 485.
31. Mohd Shamir B. Hashim, Malaysia's National Cyber Security Policy: The country's cyber defence initiatives, **IEEE**, Available at: <https://ieeexplore.ieee.org/document/5978782>
32. سميرة طوق، ما هي الحرب السيبرانية؟، بيروت تايم، 22 أيلول 2024، متاح على: <https://beiruttime.com/Article/20527>

البعد السيبراني في الحرب الروسية - الأوكرانية: وإعادة صياغة معادلة الصراع في أوروبا

آية عبد العزيز*

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 وصفت بكونها "غير مسبقة" ضد أوكرانيا؛ ذلك أن جوهرها قائم على تحقيق مجموعة من الأهداف منها تدمير البنية التحتية الحيوية لأوكرانيا، وشل قدراتها على الرد أو الدفاع، والقيام بمزيد من عمليات التجسس

* باحث أول بوحدة الدراسات الأوروبية، بالمركز المصري للفكر والدراسات الاستراتيجية

خارج أوكرانيا، والتأثير في الرأي العام العالمي من خلال حملات للدعاية ونشر المعلومات المضللة⁽¹⁾.

وهو ما تجلّى في استهداف المؤسسات الأوكرانية، بحسب مركز استخبارات التهديدات التابع لشركة "مايكروسوفت" (Microsoft)، باستخدام مجموعة من البرامج الخبيثة التي تُعرف باسم "الممسحة" (wiper) والتي أُطلق عليها اسم "فوكس بيلد" (FoxBlade) بعد تفكيكها⁽²⁾. كما قدمت الشركة معلومات استخباراتية ونصائح دفاعية للمسؤولين حول الهجمات التي استهدفت الجيش الأوكراني والعديد من الوكالات الحكومية، بحسب ما أوضحه "براد سميث" (نائب رئيس مجلس إدارة "مايكروسوفت" ورئيسها).

اتصلاً بذلك، كشف أيضًا باحثو شركة "إسيت" (ESET) - المتخصصة في مجال الأمن الرقمي - أن الأنظمة الحكومية تعرضت لهجوم ثانٍ بواسطة برنامج (IsaacWiper) الأقل تطوراً والمختلف عن برنامج (HermeticWiper)، من حيث الأكواد، رغم تقارب نتائج الهجومين، كما لم يستطع باحثو الشركة تحديد جهة التهديد المباشرة التي استخدمت برنامج (IsaacWiper). لذا فقد تم التعامل مع هذه التهديدات باعتبارها ناشئة من جهات مختلفة بحسب ما أوضحه "إيان بوتين" رئيس قسم أبحاث التهديدات في الشركة⁽³⁾.

وقد توالى العمليات السيبرانية الروسية ذات الطابع المدني والعسكري ضد أوكرانيا والدول الغربية التي تبنت استجابة مُنسقة قائمة على دعم القدرات الدفاعية الأوكرانية في مواجهة روسيا، إلى جانب انتهاج العديد من الاستراتيجيات الاستباقية والنوعية لتعزيز قدراتهم على الردع دون الدخول في تصعيد عسكري مباشر مع روسيا؛ الأمر الذي جعل البعد السيبراني حاضراً بقوة؛ كونه أصبح عنصراً أساسياً في إعادة صياغة معادلة الحرب بين روسيا وأوكرانيا من ناحية، والقوى الغربية من ناحية أخرى.

كما أسهم التوظيف المتزايد للقدرات السيبرانية في وصف الحرب الراهنة بكونها "الحرب السيبرانية العالمية الأولى" بحسب ما صرح به وزير التحول الرقمي

الأوكراني "ميخايلو فيدوروف" في خطابه الذي ألقاه في بولندا في أثناء حضوره مؤتمر (CYBERSEC) لأمن التكنولوجيا، الذي عُقد في مايو 2022، وحصل خلاله على جائزة (CYBERSEC 2022)، مُشيرًا إلى قدرة أوكرانيا على مجابهة الحرب السيبرانية التي تشنها روسيا عليها قائلًا: "كما دمر جيشنا البطل أسطورة روسيا باعتبارها القوة العسكرية الثانية في العالم، دمرت حربنا السيبرانية أسطورة القوة السيبرانية لروسيا"⁽⁴⁾.

وبرغم صعوبة رصد إجمالي عدد الهجمات السيبرانية الروسية على أوكرانيا، أشارت تقديرات إلى نحو 2194 هجومًا تمت الاستجابة لهم منذ اندلاع الحرب في فبراير 2022 وحتى حلول عام 2023، من قبل فريق الاستجابة للطوارئ الحاسوبية الأوكرانية (CERT-UA)⁽⁵⁾.

وبناءً على ذلك، أثار هذا المشهد المُركب العديد من التساؤلات حول أسباب ودوافع روسيا للجوء إلى الاستخدام المتنامي لقدراتها السيبرانية في أوقات السلم وفي سياق حربها العسكرية على أوكرانيا، بالإضافة إلى كيف تمكنت كييف من تعزيز قدراتها على الردع والدفاع والاستجابة لمثل هذه التهديدات السيبرانية المُتتالية بالاعتماد على القوى الغربية لإعادة توجيه هجمات مماثلة لروسيا؟ وإلى أي مدى أصبحت القوى الغربية طرفًا غير مباشرًا في هذه الحرب؟

أولاً: التصور الروسي لتوظيف القدرات السيبرانية ضد الخصوم

يتداخل تصور روسيا بشأن الحرب السيبرانية مع المواجهة المعلوماتية أو «حرب المعلومات»؛ إذ لا تفرق بينهما في إطار استهدافها لأنظمة ومؤسسات الدول التي تعتبرها خصومًا لها؛ كون هذه العمليات مرتبطة بشكل أساسي بالسمات النفسية والمادية للصراع بين الدول في الفضاء المعلوماتي. لذا، تُعرّف روسيا «حرب المعلومات» التي تنظر إليها من منظور أوسع عن الحرب السيبرانية بكونها: «الصراع بين دولتين أو أكثر في الفضاء المعلوماتي بهدف إلحاق الضرر بأنظمة المعلومات والعمليات والموارد، فضلاً عن الهياكل المهمة للغاية وغيرها من الهياكل، وتقويض الأنظمة السياسية والاقتصادية والاجتماعية، وتنفيذ حملات نفسية جماعية ضد

سكان الدولة من أجل زعزعة استقرار المجتمع والحكومة، فضلاً عن إجبار الدولة على اتخاذ قرارات لصالح خصومها». وذلك بحسب ما أوضحته وثيقة صادرة عن وزارة الدفاع الروسية في عام 2011⁽⁶⁾.

وعليه، يتم اللجوء إلى هذا النوع من العمليات في الفضاء المعلوماتي كنهج استباقي للمواجهة العسكرية المباشرة؛ فوفقاً للعقيدة العسكرية لروسيا لعام (2010)، على سبيل المثال، فإن إحدى سمات الصراعات العسكرية الحديثة هي: «التنفيذ المُسبق لتدابير حرب المعلومات من أجل تحقيق أهداف سياسية دون اللجوء إلى القوة العسكرية، ومن ثمّ لصالح تشكيل استجابة مواتية من جانب المجتمع الدولي لاستخدام القوة العسكرية»⁽⁷⁾.

وهو ما يعكس أهمية حرب المعلومات من وجهة نظر روسيا في التعاطي مع التهديدات الأمنية الخارجية، وتحديدًا عبر استخدام الإنترنت الذي بات إحدى أدوات هذه الحرب في نشر الرواية الروسية بشأن التفاعلات الدولية أو الداخلية المؤيدة لتحركاتها وسياساتها نحو الآخر، علاوة على نشر عدم الاستقرار داخل الدول التي تعتبرها ذات توجهات معادية لها، وإضعاف ثقة الشعوب في هذه الحكومات ومؤسساتها، وذلك من خلال عمليات التجسس السيبراني، والتصيد عبر الإنترنت المرتكز على إنشاء مدونات وهمية وملفات تعريف تقوم بنشر الدعاية المضللة أو الأخبار الكاذبة والتي تُعرف باسم «متصيدي الإنترنت»⁽⁸⁾.

كانت أبرز مظاهر هذه الحرب المعلوماتية واضحةً في تعاطي روسيا مع أوكرانيا في مرحلة ما قبل التصعيد العسكري المباشر عليها. فعلى سبيل المثال، بحلول نهاية عام 2015 قامت مجموعة من القراصنة الروس باستخدام برامج خبيثة تستهدف تعطيل المواقع الإلكترونية للحكومة الأوكرانية للحصول على وثائق وخطط حكومية وتسريبها، والتأثير المعنوي في الجيش الأوكراني عبر تشجيع أفرادهِ على الانشقاق من خلال إرسال رسائل نصية من قبل القراصنة، علاوة على تعطيل الأنظمة المرتبطة بالبنية التحتية الحيوية بواسطة هجمات سيبرانية إلى جانب عمليات التجسس السيبراني⁽⁹⁾.

وقد سبق أن تعرضت إستونيا لهجمات سيبرانية - يُعتقد أن مصدرها هو روسيا - استهدفت المواقع الإلكترونية الحكومية والإعلامية وأيضًا البنكية، عقب نقل نصب تذكاري روسي يعود إلى الحقبة السوفيتية، والمُعرف باسم «الجندي البرونزي»، وقد اعتبر بعض المحللين أن هذه الهجمات كانت البداية الفعلية لما يمكن تسميته «الحروب الإلكترونية الحقيقية». وقد أعقب ذلك الهجوم على جورجيا عام 2008 الذي تزامن مع التدخل العسكري الروسي في البلاد⁽¹⁰⁾.

وهنا، اتضحت نقطة مهمة، ألا وهي أن هذه العمليات رغم أنها لا تصل إلى عتبة التدمير الذي قد ينجم عن استخدام القوة العسكرية، فإن تكلفتها وتبعاتها ذات تأثيرات ممتدة سواء على الحكومات أو المجتمعات التي وقع عليها العدوان أو الهجوم السيبراني، لما لها من قدرة على إكراه الخصوم قسريًا عبر هجمات الحرمان من الخدمة، وإضعاف الروح المعنوية للشعوب، وهو الأمر الذي جعل البعض يشبه فاعلية الهجمات السيبرانية بفاعلية الضربة الجوية الأولى التي تسبق عمليات الاشتباك بالأسلحة الثقيلة، وقد أطلق عليها أيضًا من قبل مؤرخين الحرب بأنها «القصف المعنوي للنيل من معنويات الجنوب»⁽¹¹⁾.

وبالتطبيق على الحالة الأوكرانية، يمكن القول إن روسيا جمعت بين إضعاف الإرادة السياسية والشعبية من خلال عمليات «القيمة المضادة» إلى جانب استنزاف القدرات الأوكرانية العسكرية، وتقويض الدعم الغربي لها، والحد من فاعليته في عمليات الدفاع أو شن الحرب أو تطوير قدرته على تطوير الهجوم المضاد بواسطة عمليات «القوة المضادة». لذا فقد ركزت الهجمات الروسية على أوكرانيا باستهداف البنية التحتية المدنية وبدرجة أقل البنية العسكرية⁽¹²⁾. ولكن هذا الأمر قد تطور وفقًا لمقتضيات الوضع على جبهة القتال، وما فرضته قواعد الاشتباك مع الخصوم، وأيضًا مقاومة أوكرانيا على صد مثل هذه الهجمات وقدراتها على تطوير هجمات مضادة.

ثانيًا: التهديدات السيبرانية الروسية ضد أوكرانيا والقوى الغربية

تمتلك روسيا العديد من الأدوات السيبرانية التي توظفها بأشكال مختلفة تتوافق مع سياساتها الخارجية، وبما يخدم مصالح الأمن القومي الروسي، رغم اتجاهها - في كثير من الأحيان - إلى إنكار علاقتها بمثل تلك الهجمات، مُستغلة صعوبة إسنادها إليها، وهي إشكالية ليست مقصورة على الهجمات الروسية تحديدًا، ولكنها مرتبطة بتكتيكات الحروب السيبرانية التي أطلق عليها البعض «حروب الظل» عمومًا؛ نظرًا لخطورة تداعياتها، وعدم القدرة على تتبع الجهات الفاعلة، وهو ما يتضح على النحو التالي:

1. الاستخبارات العسكرية الروسية (GRU): أسهمت الوكالة في تحقيق أهداف الأمن القومي الروسي إزاء الجهات المُعادية لروسيا من خلال عمليات التجسس والاختراق التي تقوم بها الفرق والوحدات من القراصنة الذين يُعتقد أنهم تابعون لها. إذ كشفت وكالة الاستخبارات الداخلية الألمانية (BfV) في سبتمبر 2024 بالتعاون مع الجهات النظرية التابعة للشركاء الدوليين أن المجموعات التابعة لوحدة (GRU 29155) والمعروفة أيضًا باسم (Cadet Blizzard) أو (Ember Bear) كانت «مسئولة عن عمليات الشبكة الحاسوبية ضد أهداف عالمية لأغراض التجسس والتخريب والإضرار بالسمعة منذ عام 2020 على الأقل»، بجانب الهجمات التي تعرضت لها أوكرانيا قبل الحرب في يناير 2022 بواسطة مجموعة من البرامج الخبيثة (WhisperGate). كما أوضحت وكالة الاستخبارات الداخلية الألمانية أن الوحدة (29155) قامت بهجمات أيضًا على «شبكات في دول أعضاء في الناتو في أوروبا وأمريكا الشمالية وكذلك دول في أمريكا اللاتينية وآسيا الوسطى»، مُحذرة من خطورة النشاط التي تقوم به⁽¹³⁾.

لم تكن هذه الوحدة هي فقط من ترتبط بوكالة الاستخبارات الروسية؛ إذ يُعتقد أن مجموعات القراصنة المُعروفة باسم (APT 28) أو (Fancy Bear) و(Sofacy) و(APT 29) (المُعروفة أيضًا باسم Cozy Bear) تابعين لها؛ حيث يشتهر أن المجموعة الأولى كانت مسؤولة عن استهداف أبحاث اللجنة الوطنية الديمقراطية حول «دونالد ترامب»، وهو ما يراه البعض نموذجًا على التدخل الروسي في الانتخابات

الأمريكية عام 2016. فيما يُعتقد أيضًا أن الهجوم الذي تعرضت له البنية التحتية المرتبطة بالانتخابات في أوكرانيا خلال عام 2014 كان من قبل (CyberBerkut)⁽¹⁴⁾.

كما كشفت لألحة اتهام أصدرت من قبل هيئة محلفين كبرى فيدرالية في بيتسبرج في أكتوبر 2020 بحق ستة قراصنة جميعهم في روسيا، وهم مواطنون وضباط في الوحدة (74455) التابعة لمديرية الاستخبارات الرئيسية الروسية (GRU)، عن مزيد من الهجمات التي تعرضت لها أوكرانيا والقوى الغربية من قبل الوكالة؛ حيث قام هؤلاء بعمليات اختراق دعمًا للحكومة الروسية خلال الفترة من نوفمبر 2015 حتى أكتوبر 2019 بالاعتماد على عدّة برامج خبيثة، وقد تمثلت أبرز هذه الحالات فيما يلي:

- الحالة الأوكرانية: إذ استُهدفت شبكة الكهرباء ووزارة المالية وخدمة الخزنة الحكومية خلال الفترة من ديسمبر 2015 إلى ديسمبر 2016 بواسطة مجموعة من البرامج الخبيثة أطلق عليها اسم (BlackEnergy) و (Industroyer) و (KillDisk).
- الحالة الفرنسية: في مرحلة ما قبل الانتخابات الرئاسية لعام 2017، تم استهداف السياسيين الفرنسيين وحزب الرئيس "إيمانويل ماكرون"، بحملات "التصيد الاحتيالي".
- الحالة الجورجية: حيث تم استهداف شركة إعلامية كبرى بحملات تصيد احتيالي خلال عام 2018، إلى جانب محاولات اختراق شبكة البرلمان الجورجي في عام 2019، وإطلاق حملة تشويه عبر مواقع الويب في العام نفسه.
- الحالة البريطانية: تم استهداف التحقيقات المرتبطة بجائحة تسمم العميل "سيرجي سكريبال" وابنته وبعض المواطنين البريطانيين بغاز الأعصاب، التي كانت تجريها منظمة "خطر الأسلحة الكيميائية" ومختبر العلوم التكنولوجية الدفاعية في المملكة المتحدة بواسطة عمليات تصيد احتيالي في أبريل 2018.
- دورة الألعاب الأولمبية الشتوية: تم استهداف المواطنين والمسؤولين والرياضيين ومسؤولي اللجنة الأولمبية الدولية خلال دورة الألعاب التي عقدت في بيونج تشانج بكوريا الجنوبية في الفترة من ديسمبر 2017 وحتى فبراير 2018 من خلال حملات "التصيد الاحتيالي".

▪ البنية التحتية الحيوية: تعرضت أجهزة الكمبيوتر على مستوى العالم إلى هجمات خبيثة بواسطة برامج (NotPetya) في يونيو 2017 لا سيما المستشفيات والمرافق الطبية الأخرى في نظام (Heritage Valley) الصحي في المنطقة الغربية من ولاية بنسلفانيا، وشركة تابعة لشركة (FedEx Corporation)، وشركة تصنيع أدوية أمريكية، والتي تكبدت معًا خسائر بلغت نحو مليار دولار من الهجمات، بحسب ما أوضحت لأحة الاتهام⁽¹⁵⁾.

2. فرق القراصنة الروس: لعب القراصنة الروس دورًا محوريًا في إلحاق الضرر بالمؤسسات المدنية والعسكرية لخصوم روسيا خلال الحرب الروسية-الأوكرانية؛ الأمر الذي فرض المزيد من التحديات على استجابة أوكرانيا لصد مثل هذه الهجمات المتتالية خاصة في ضوء عدم القدرة على ملاحقاتهم أو كشف علاقاتهم الارتباطية المباشرة بروسيا لاعتمادهم على التواصل عبر قنوات مشفرة⁽¹⁶⁾، علاوة على تكوينهم لفرق تعمل على استهداف خصوم روسيا على غرار ما قامت به مجموعة «كونتي» التي دعمت الرئيس الروسي بشكل مُعلن، وتعهدت بالرد على أي هجوم مُحتمل أو قائم قد تتعرض له روسيا من قبل خصومها⁽¹⁷⁾. كما وظفت مجموعة من القراصنة المرتبطة بموسكو العديد من البرامج الخبيثة لاستهداف الدول المعادلة للسياسة الروسية. فعلى سبيل المثال، استطاعت مجموعة (DarkSide) في عام 2021 اختراق نظام نقل الوقود الأمريكي المعروف باسم «كولونيال بايبلاين» (Colonial Pipeline) عبر برامج «الفدية» التي تم نشرها ضده⁽¹⁸⁾.

وفي محاولة لدعم العمليات العسكرية الروسية، تم تنفيذ هجمات سيبرانية ضد شبكات محطة «زابوريجيا» النووية بالتزامن مع توجه القوات الروسية للاستيلاء عليها في أبريل 2022. فضلًا عن استهداف مقر القوات الجوية الأوكرانية المتمركز في مدينة فينيتسا عبر تعطيله. كما استهدفت منشآت حكومية وعسكرية في مدينة دينبرو بهجمات مماثلة، علاوة على التوجه العام لهذه الهجمات منذ اندلاع الحرب القائم على تدمير البنية التحتية الأوكرانية المرتبطة تحديدًا بقطاع الطاقة

والاتصالات خلال الفترة من فبراير 2022 وحتى أكتوبر من العام نفسه⁽¹⁹⁾، ولا تزال متواصلة حتى الآن.

إذ تم، على سبيل المثال، اختراق نظام شركة الاتصالات الأوكرانية «كييف ستار»، في مايو 2023 من قبل مجموعة من القراصنة الروس؛ مما نتج عنه تدمير آلاف الخوادم الافتراضية وأجهزة الكمبيوتر، وذلك بحسب ما أوضحه «إيليا فيتوك» رئيس قسم الأمن السيبراني في جهاز الأمن الأوكراني (SBU)، في مقابلة مع وكالة «رويترز» أجريت في ديسمبر 2023، واصفًا الهجوم بقوله: «ربما يكون أول مثال على هجوم سيبراني مدمر تمامًا جوهر شركة اتصالات». وفيما يتعلق بجهة التهديد الصادر عنها الهجمات قال «فيتوك» إنه: «متأكد إلى حد كبير» من أن مجموعة القراصنة «سندوورم» (Sandworm) هي التي نفذت الهجوم، موضحًا أن جهاز الأمن الأوكراني «أحبط أكثر من 4500 هجوم سيبراني كبير على الهيئات الحكومية الأوكرانية والبنية التحتية الحيوية عام 2022»⁽²⁰⁾.

وفي محاولة للرد على الدعم الغربي المتزايد لأوكرانيا من قبل روسيا، تعرضت القوى الأوروبية لهجمات سيبرانية بواسطة برامج خبيثة لا سيما «الفدية». ووفقًا لصحيفة «آي» البريطانية، فقد تم اختراق أنظمة الاتصالات التي تستخدمها خدمة الإسعاف البريطانية من قبل قراصنة روس بواسطة برامج «الفدية»، فضلًا عن استهداف الشركات الخاصة التي تقدم خدمات الدفاع وغيرها من الخدمات وذلك في أكتوبر 2024⁽²¹⁾.

يُضاف إلى ذلك، اتهام «ريتشارد مور» رئيس جهاز المخابرات السرية البريطاني (MI6) خلال زيارته لفرنسا في نوفمبر 2024 روسيا بشنّها حملات تخريبية في أوروبا، قائلًا: «لقد كشفنا مؤخرًا عن حملة متهورة بشكل مذهل من التخريب الروسي في أوروبا، حتى مع لجوء "بوتين" وأتباعه إلى التهديد النووي لبثّ الخوف بشأن عواقب مساعدة أوكرانيا"، مضيفًا: "أن تكلفة دعم أوكرانيا معروفة جيدًا، ولكن تكلفة عدم القيام بذلك ستكون أعلى بلا حدود، وإذا نجح بوتين فإن الصين سترنّ العواقب، وستشجع كوريا الشمالية وستصبح إيران أكثر خطورة»⁽²²⁾.

وعليه؛ من الواضح أن استراتيجية روسيا ضد القوى الغربية تقوم على استهدافها سبيرانياً دون الدخول في مواجهة عسكرية مباشرة، لكي تتراجع عن دعم أوكرانيا، أو ممارسة المزيد من التأثير في المجتمعات الغربية لإقناعهم بوقف الحرب؛ مما يدفعهم للضغط على حكوماتهم لوقف الدعم المقدم لأوكرانيا.

3. حملات التضليل والحجب والتقييد: لم تتوقف الجهود الروسية عند حد الاختراق والهجوم السبيراني بل امتدت إلى توظيف وسائل التواصل الاجتماعي في حربها ضد أوكرانيا والقوى الغربية؛ حيث عملت موسكو على تقييد الوصول إلى مواقع التواصل الاجتماعي منذ اليوم التالي للحرب الروسية على أوكرانيا في فبراير 2022؛ ردًا على القيود التي فرضها "فيسبوك" على حسابات خاصة بوسائل إعلام موالية للكرملين، وأخرى مدعومة من قبله⁽²³⁾. كما حجبت الوصول إلى المنصات الأخرى مثل "تويتر". بجانب وقف وكالات الأنباء التي تعمل من خارج روسيا، مثل "بي بي سي"، و"دويتشه فيله"، و"صوت أمريكا"، و"ميدوزا". وكذا حظر بعض وسائل الإعلام المحلية الروسية، مثل: "نوفي إزفستيا"، و"أوست كوت 24"، و"كافكازسكي أوزيل". فيما قامت شركة "ياندكس" للبحث التابعة لروسيا بتقليص مرتبة المحتوى المنتقد لروسيا، بجانب الترويج لروايتها حول شرعية هذه الحرب عبر إنساء مواقع وهمية تقوم بذلك⁽²⁴⁾.

وفي هذا السياق، استهدفت موسكو من خلال عمليات التضليل واسعة النطاق، والتي قامت بها جهات موالية لها، تحقيق مجموعة من الأهداف منها: زعزعة الثقة في الحكومات داخل المجتمعات المعادية، وإثارة الانقسامات بين المواطنين وتحديدًا بشأن الحرب التي تم الترويج لها من منظور روسيا بأنها مجرد "عملية خاصة محددة الأهداف" لتبرير هجومها العسكري على أوكرانيا أمام الرأي العام الروسي والدولي بالأساس⁽²⁵⁾.

ثالثاً: آليات الاستجابة الأوكرانية المدعومة من القوى الغربية ضد روسيا

منذ اندلاع الحرب الروسية-الأوكرانية، تعرضت أوكرانيا العديد من الهجمات السيبرانية الروسية المتتالية التي استهدفت مؤسساتها وبنيتها التحتية الحيوية؛ الأمر الذي دفعها إلى الاشتباك المباشر مع مثل هذه الهجمات سواء بشكل منفرد أو من خلال الاعتماد على الحلفاء لتعزيز قدرتها ومرونتها على الاستجابة والمجابهة والدفاع، وهو ما تمثل على النحو التالي:

1. انخراط وزارة التحول الرقمي في الحرب: دفعت الحرب الروسية على أوكرانيا وزارة التحول الرقمي لإعادة مراجعة الخدمات التي تقدمها بما يتوافق مع المتطلبات الحرب عبر المشاركة في الدفاع المدني والعسكري لضمان حماية المدنيين والمساعدة في إجلاء السكان من المناطق التي تدمرت، علاوة على مجابهة وإحباط الهجمات السيبرانية الروسية على البنية التحتية الحيوية في البلاد. ووفقاً لتقرير صادر عن مركز (StrategEast) بعنوان: "المقاومة الرقمية الأوكرانية للعدوان الروسي"، سعت الوزارة إلى تأمين كل البيانات المرتبطة بالدولة والمواطنين من خلال مستويات عالية من الحماية، فضلاً عن مساعدات الأوكرانيين خلال الحرب. كما شاركت الوزارة مع وزارة الثقافة وسياسة المعلومات في أوكرانيا (MinCult) في إنشاء جيش تكنولوجيا المعلومات خاص بشن هجمات سيبرانية على المواقع الروسية وجيش الإنترنت، لمجابهة الدعاية الروسية، وقد بلغ عدده حوالي 500 ألف مُطور ومصمم وكاتب نصوص ومسوق وغيرهم من المهنيين.

وفي سياق جهود حماية الدولة الأوكرانية من الهجمات السيبرانية، تم إدخال مجموعة من التعديلات التشريعية وتحديداً على المادتين (361) و(361-1) من القانون الجنائي الأوكراني التي "تسمح للمتخصصين الخارجيين بالمشاركة في البحث عن الأخطاء والثغرات الأمنية في منتجات البرامج الحكومية وأنظمة المعلومات والاتصالات، ومعالجة أي عيوب وثغرات أمنية على الفور". إلى جانب زيادة مرونة مؤسساتها رقمياً مع وضع الحرب عبر اتخاذ مجموعة من التدابير منها: نقل المعدات والنسخ الاحتياطية لقواعد البيانات إلى مناطق أكثر أماناً في أوكرانيا والتي لا يمكن

للقوات الروسية الوصول إليها، وإنشاء نظام متعدد الطبقات للدفاع السيبراني للبنية التحتية لتكنولوجيا المعلومات في الدولة، وإنشاء خط ساخن لخدمة الأمن في أوكرانيا للاستجابة السريعة لتهديد الهجمات السيبرانية على أنظمة تكنولوجيا المعلومات في البنية التحتية الحيوية⁽²⁶⁾.

وإلى جانب هذا، ساعدت وزارة التحول الرقمي في توزيع عملية المساعدات الإنسانية عبر التعاون مع برنامج الأمم المتحدة الإنمائي في أوكرانيا لدعم وزارة السياسة الاجتماعية الأوكرانية في إنشاء منصة (eDopomoga) كي تكون قادرة على تجميع كل المعلومات المتعلقة بالمساعدات الإنسانية، إلى جانب تسهيل عمليات نقل المعلومات والإبلاغ عن تحركات القوات المعادية من قبل الأوكرانيين دون الاتصال بالإنترنت عبر إنشاء روبوت للدردشة أطلق عليه (eVorog)⁽²⁷⁾.

2. نشر الدعاية المضادة للرواية الروسية: استهدفت كيف الرأي العام الدولي إلى جانب الأوكراني والروسي لكشف المزاعم الروسية المنشورة عن الحرب على أوكرانيا عبر نشر الدعاية والمعلومات والصور للضحايا الأوكرانيين ومقاطع للمناطق المدمرة على وسائل التواصل الاجتماعي للوصول إلى أكبر قاعدة جماهيرية على مستوى العالم. وبمعنى أدق، يمكن القول إن أوكرانيا خلال الحرب "حاولت مخاطبة شعوب العالم لكسب تعاطفهم ودعمهم في حربها ضد روسيا"⁽²⁸⁾.

فعلى سبيل المثال، نشر الرئيس الأوكراني "فولوديمير زيلينسكي" مقطع فيديو يحمل شعار "نحن هنا" للرد على الدعاية الروسية التي روجت لفراره من البلاد. ولم يقصر الأمر على ذلك، فقد شهد حساب وزارة الدفاع الأوكرانية على "تويتر" تفاعلاً كبيراً من قبل العديد من المتابعين، في ضوء حرص الوزارة على الوصول إلى أكبر قاعدة جماهيرية، وهو ما تجلّى في تفاعل المتابعين من اليابان مع أحد المنشورات الذي أظهر طول خط المواجهة الأوكراني على خريطة لليابان تضم جزر الكوريل، المُتنازع عليها بين طوكيو وموسكو على سبيل المثال. كما اتجهت مجموعة من منظمات المجتمع المدني في أوكرانيا إلى نشر المزيد من الدعاية حول حقيقة الحرب التي تمر بها بلادهم، علاوة على الترويج للثقافة الأوكرانية على المواقع الإلكترونية، ووسائل التواصل الاجتماعي بالعديد من اللغات⁽²⁹⁾.

3. استهداف روسيا بعمليات التخريب السيبراني: أسهمت عمليات التخريب الأوكرانية التي قامت بها بعض الفرق الأوكرانية في التأثير في القدرات العسكرية والمدنية الروسية. فعلى سبيل المثال، تم توظيف مجموعة من البرامج الخبيثة لا سيما برامج "الفدية"، والوصول عن بعد مثل (Ozone RAT) و(Rhadamanthys) (Stealer) من قبل فرق سيبرانية مختلفة مثل: (PhantomCore)، و(BlackJack)، و(Twelve) للوصول إلى معلومات استخباراتية عن المؤسسات العسكرية الروسية، ثم تدمير بياناتها لتخريب العمليات الروسية. بالإضافة إلى ذلك استهدفت مجموعة القراصنة الداعمين لأوكرانيا (Lifting Zmiy) خلال الفترة من سبتمبر 2023 إلى يونيو 2024 البنية التحتية لتكنولوجيا المعلومات للحكومة الروسية والمنظمات الخاصة.

ويذكر أن مجموعة (BlackJack) الموالية لأوكرانيا، والتي يُشتبه أنها قد تكون تابعة للاستخبارات الأوكرانية، استهدفت شركة مرافق المياه (Rosvodokanal) من خلال برامج "الفدية" ومحو البيانات. وقد أعلنت المجموعة بعدها عن مسؤوليتها عن الهجوم عبر قنواتها على "تليجرام" في ديسمبر 2023. وردًا على الهجوم السيبراني على شركة الاتصالات الأوكرانية (Kyivstar)، قام قراصنة تابعون للمجموعة بعدة هجمات من نوع (DDoS) على مزود خدمة الإنترنت الروسي (ISP M9 Com Ltd) في يناير 2024. وفي هذا السياق، يمكن القول إن الهجمات من نوع (DDoS) تم استخدامها لقطع خدمات الإنترنت مؤقتًا في منطقة كورسك الروسية، وقد تم الإبلاغ عن ذلك بعد نحو يومين من التوغل الأوكراني المفاجئ فيها في السادس من أغسطس 2024⁽³⁰⁾.

وبالفعل فقد تم تعزيز هذا الهجوم العسكري الأوكراني -الذي يعتبر الأول من نوعه منذ بداية الحرب- عبر هجمات سيبرانية استهدفت تعطيل القدرات العسكرية الروسية⁽³¹⁾. وهو ما أكدته السلطات الروسية، حيث أوضح بيان صادر من مسئولين في المنطقة أن «كورسك تعرضت لهجوم «ضخم» من هجمات الحرمان من الخدمة الموزعة بالتزامن مع الهجوم الأوكراني»⁽³²⁾.

وهنا يمكن توضيح أن أوكرانيا حاولت من خلال هذا التوغل تحقيق جُملَة من الأهداف منها: نقل ساحة القتال إلى الأراضي الروسية، والتغلب على التحديات

المتتالية التي واجهتها منذ فشل هجومها المضاد في يونيو 2023، بجانب احتمالية الرغبة في خلق أهداف جديدة لتعزيز قدراتها على التفاوض، عبر الاستحواذ على أكبر قدر من الأراضي الروسية، والمزيد من الأسرى، بما يتوافق مع النهج الروسي الذي يشترط أخذ الواقع على الأرض في الاعتبار في أي مسار مُحتمل للتسوية. لذا فقد قامت بتوظيف كل مواردها وقدراتها المدعومة من القوى الغربية خلال هذا الهجوم كي تتمكن من التعاطي مع نقاط التفشي والتحصينات الميدانية، والتغلب على أنظمة المراقبة والاستطلاع والاستخبارات الروسية⁽³³⁾.

4. دعم الشركات التكنولوجية: طالبت أوكرانيا شركاءها الغربيين بأهمية الاستجابة السريعة للتطورات التي تمر بها كييف منذ اندلاع الحرب، لا سيما توفير الخدمات الحيوية المرتبطة بالإنترنت بعد أن عرقلت روسيا اتصال كييف بالإنترنت بعد تعرضها لهجمات سيبرانية في مارس 2022، فضلاً عن تعزيز قدراتها على الرد والحد من محاولات الاختراق المتتالية التي تواجهها من قبل موسكو. في المقابل، تلقت أوكرانيا استجابة مباشرة من قبل شركة (سبيس إكس - SpaceX) برئاسة "إيلون ماسك" وهي شركة رائدة في تقديم خدمات إنترنت الفضاء بدون بنية تحتية للاتصالات سواء من كانت أسلاك كهربائية أو الكابلات البحرية عبر الاعتماد على مجموعة من الأقمار الصناعية مزودة بأنظمة توجيه تعرف باسم (ستارلينك - Starlink) التي تعمل كوسيط بين الشبكة العالمية والمستخدمين، ورغم ذلك فإنها تحتاج إلى منصات استقبال أرضية متصلة بأجهزة لنقل الإشارات لا سلكياً إلى المناطق التي يتعرّف فيها وصول خدمات الإنترنت.

واتصالاً بذلك، أتاحت شركة "سبيس إكس" خدمات إنترنت الفضاء عبر تزويد أوكرانيا بالمحطات الطرفية اللازمة بعد أقل من عشر ساعات من طلب "ميخايلوفيدوروف" (نائب رئيس الوزراء ووزير الشؤون الرقمية الأوكراني) بتزويد كييف بمحطات "ستارلينك"، وتم تفعيلها سريعاً في أوكرانيا. الأمر الذي جعل "ماسك" في مواجهة مباشرة مع روسيا؛ حيث اعتبرت موسكو موقفه بمثابة تدخل في الحرب. فعلى سبيل المثال، حذره مدير وكالة الفضاء الروسية "ديمتري روجوزين" قائلاً: "إن ماسك يزود القوات الأوكرانية بالاتصالات العسكرية، وعليه تحمل

مسئولية تصرفه". لم يتوقف الأمر عند هذا الحد، فقد تعرضت شبكات الأقمار الصناعية الخاصة بشركته التي يتجاوز عددها نحو أكثر من ألفين قمر صناعي على مدار منخفض إلى هجمات تشويش من قبل روس، وهو ما أحبطته شبكة "سبيس إكس" بحسب ما أوضحه تقرير صادر عن وزارة الدفاع الأمريكية "البنتاجون" في أبريل 2022⁽³⁴⁾.

يُضاف إلى ذلك، دعم بعض شركات التكنولوجيا الأخرى لأوكرانيا كان عن طريق وقف خدماتها ونشاطها في روسيا أو المشاركة في الدفاع عنها ضد روسيا في مقدمتها "أبل"، و"جوجل"، و"ميتا"، إلى جانب شركة "كليرفيو" التي أتاحت خدماتها التقنية لأوكرانيا لاستفادة منها في حربها ضد موسكو؛ وذلك في ضوء امتلاكها قاعدة بيانات تتضمن حوالي عشرة مليارات وجه⁽³⁵⁾. إلى جانب شركة "مايكروسوفت" التي كشفت عن تعرض أوكرانيا لمزيد من الهجمات السيبرانية تجاوزت الـ 200 هجوم سيبراني منسوب إلى روسيا بدايةً من أبريل 2022⁽³⁶⁾.

5. الدعم الغربي لبناء القدرات السيبرانية: عملت القوى الغربية على توجيه جزء من دعمها لأوكرانيا لتقوية قدراتها الدفاعية على المستوى السيبراني تمثل ذلك في مشاركة الاتحاد الأوروبي في بناء القدرات السيبرانية الأوكرانية عبر "التعاون الهيكلي الدائم" (Permanent Structured Cooperation, PESCO). إلى جانب ذلك وقعت المملكة المتحدة اتفاقية مع أوكرانيا في مجال حماية المعلومات، حيث قامت دائرة الأرشفة الحكومية الأوكرانية بالتعاون مع نظيرتها البريطانية للنقل المؤقت لتخزين البيانات السحابية ونسخ احتياطية من المواد الرقمية للمؤسسات الأرشفية الحكومية الأوكرانية في حالة خسارتها المحتملة. فيما عملت الولايات المتحدة على دعم القدرات الأوكرانية على المستوى الاستخباراتي⁽³⁷⁾. علاوة على الدعم السيبراني المتواصل في إطار ما يُعرف باسم «الحوار السيبراني الأمريكي» المعني بإجراء نقاشات سنوية حول قضايا السياسة السيبرانية، والذي يعتبر بمثابة مؤشر واضح على التزام واشنطن بدعم الدفاع السيبراني الأوكراني ضد روسيا؛ إذ يُقدر حجم الإسهامات الأمريكية الرقمية والسيبرانية منذ اندلاع الحرب حوالي 82 مليون دولار، ونحو أكثر من 120 مليون دولار منذ عام 2016⁽³⁸⁾.

واستكمالاً للجهود الغربية لدعم أوكرانيا سيبرانياً، قام مركز التميز التعاوني للدفاع السيبراني التابع لحلف شمال الأطلسي، في يناير 2023، بتوقيع اتفاقية مع كييف تستهدف انضمامها إليه، حيث يختص المركز بإجراء أبحاث حول السياسة السيبرانية، وينسق التعليم والتدريب في مجال الدفاع السيبراني لجميع هيئات حلف «الناتو»، كما ينظم أكبر مناورة دولية للدفاع السيبراني عالمياً والتي تُسمى (Locked Shields)⁽³⁹⁾.

إلى جانب ذلك وقعت أوكرانيا مجموعة من الاتفاقيات الأمنية مع بعض القوى الأوروبية لإكسابها المزيد من الدعم السيبراني مثل: الاتفاقية الأمنية التي أبرمت بين الدنمارك وأوكرانيا في فبراير 2024، تستهدف مساعدة كييف في منع وكشف ومكافحة العدوان السيبراني الروسي والتجسس السيبراني والحرب الهجينة، و”تعزيز الدبلوماسية السيبرانية، وتقديم المساعدة الفنية لأوكرانيا، وتعزيز مرونتها السيبرانية”. أما الاتفاقية الموقعة مع ألمانيا -خلال الشهر نفسه- فقد ركزت على تأمين البنية التحتية الأوكرانية من الهجمات السيبرانية، وتقديم تدريب لخبراء الأمن السيبراني الأوكرانيين ”بناءً على معايير الاتحاد الأوروبي في مجال أمن تكنولوجيا المعلومات”. وكجزء من هذه الاتفاقية ستدعم برلين كييف في الاستجابة للتهديدات المتعلقة بأمن المعلومات ”بما في ذلك الدعاية وغيرها من أشكال التدخل الأجنبي الخبيث، مثل التضليل“⁽⁴⁰⁾.

الخاتمة:

تتجه الحرب الروسية-الأوكرانية إلى مزيد من التعقيد والتشابك نتيجة تنامي محفزات استمرار التصعيد بين روسيا وأوكرانيا من ناحية، وروسيا والغرب من ناحية أخرى؛ إثر التوظيف المتزايد للقدرات السيبرانية بصور مختلفة، ومن قبل جهات فاعلة عدّة في هذه الحرب؛ حيث أضحت شركات التكنولوجيا الغربية طرفاً فيها أيضاً. وبالرغم من أن الحرب الراهنة، التي قاربت على الثلاث سنوات بدون آفاق محتملة للتسوية، نتيجة إصرار كل طرف على إلحاق الهزيمة بالطرف الآخر، فإنها برهنت على أن البعد السيبراني لم يحسم الحرب على الأرض، لكنها كانت كاشفة لحجم الخسائر الفادحة الناجمة عن تدمير البنية التحتية الحيوية لطرفي الصراع.

واتصلاً بذلك، حاول هذا الفصل من خلال محاوره الإجابة عن تساؤل رئيسي مفاده: هل أسهم البعد السيبراني في الحرب الروسية-الأوكرانية في إعادة صياغة معادلة الصراع بين روسيا وأوكرانيا المدعوم من الغرب؟ وللإجابة عنه ينبغي الأخذ في الاعتبار ما أشار إليه كل من «بيل بيرنز» (مدير وكالة الاستخبارات المركزية الأمريكية)، و«ريتشارد مور» (رئيس جهاز الاستخبارات السرية في المملكة المتحدة)، في مقالهما المنشور على موقع «فايننشال تايمز» حول هذا الصراع، والذي دفعاً فيه بأن التكنولوجيا، إذا ما استُخدمت جنباً إلى جنب مع الشجاعة غير العادية والأسلحة التقليدية، من شأنها أن تُغيّر مسار الحرب.

ووفقاً لهما، «كانت أوكرانيا أول حرب من نوعها تجمع بين البرمجيات مفتوحة المصدر وتكنولوجيا ساحة المعركة المتطورة، وتسخير صور الأقمار الصناعية التجارية والعسكرية، وتكنولوجيا الطائرات بدون طيار، والحرب السيبرانية عالية ومنخفضة التطور، ووسائل الإعلام الاجتماعية، والاستخبارات مفتوحة المصدر، والمركبات الجوية والبحرية غير المأهولة، والعمليات المعلوماتية - فضلاً عن الاستخبارات البشرية والإشارات - بهذه السرعة والنطاق المذهلين»⁽⁴¹⁾.

وبناءً على ذلك يمكن توضيح بعض الاستنتاجات التي توصل إليها هذا الفصل، تتمثل أبرزها فيما يلي:

- منحت القدرات السيبرانية الروسية الكرملين القدرة على المناورة السياسية في تحركاته الخارجية، والتعاطي الاستباقي عبر أدوات الحرمان والإكراه والتجسس والاختراق مع الخصوم والمنافسين دون الدخول في مواجهات عسكرية مباشرة في مرحلة ما قبل اندلاع الحرب في أوكرانيا عام 2022.
- سعت روسيا من خلال توظيفها للأنماط المختلفة من الأدوات السيبرانية إلى توجيه ضربات مدمرة للحكومات التي تعتبرها معادية لها، دون أن تصل تداعياتها التدميرية إلى عتبة الصراع المسلح، ولكنها أسهمت في إلحاق الضرر ببنيتها التحتية الحيوية، وزعزت الثقة في الإدارات الحاكمة.
- لم يكن استخدام روسيا للهجمات السيبرانية على أوكرانيا والقوى الغربية منذ اندلاع الحرب الراهنة مجديداً؛ إذ يأتي كجزء لا يتجزأ من الاستراتيجية الروسية إزاء

خصومها، تستهدف من خلالها إضعاف الثقة في حكومات هذه الدول وزعزعة الاستقرار السياسي، فضلاً عن تدمير بنيتها التحتية الحيوية؛ مما يكبد هذه الدول المزيد من الخسائر التي ترقى إلى مستوى تكتيكات "المنطقة الرمادية".

▪ عكست المواجهة السيبرانية بين روسيا وأوكرانيا تغييرات واضحة سواء فيما يتعلق بديناميكيات وتكتيكات الحرب أو الجهات الفاعلة؛ إن تلك المواجهة لم تعد حكراً على الدول، بل بات هناك المزيد من الفاعلين من غير الدول (سواء شركات التكنولوجيا أو فرق القراصنة)؛ ممن يتم الاعتماد عليهم لتحقيق أهداف أطراف الصراع دون التعرف عليهم أو الوصول إلى هويته أو كشف صلاتهم بأطراف الصراع.

▪ يُكمن جوهر الحرب السيبرانية بين روسيا وأوكرانيا في تحقيق جُملة من الأهداف المتمثلة في استنزاف القدرات المدنية والعسكرية لكل طرف، بما يمنح الطرف الآخر ميزة عسكرية تمكنه من تعزيز موقعه على جبهة القتال بأقل تكلفة وأسرع آلية دون إسناد العواقب الناجمة عن حجم الخسائر المحتملة إليه. فضلاً عن القدرة على اختراق الشعوب والتأثير في توجهاتها وهز ثقتها في حكوماتها، بما يؤدي إلى التآكل التدريجي في شرعية النظم القائمة، ويهدد استقرارها السياسي عبر إطلاق المزيد من حملات التضليل المعلوماتي والروايات المُوجهة التي تخدم مصالح كل طرف، وتبرر حجته في التعاطي مع الحرب.

▪ لا تصل تبعات الحروب السيبرانية إلى عتبة التدمير الناجمة عن الصراعات المسلحة، ولكنها باتت ذات تأثير مباشر في تماسك المجتمعات. وبالتطبيق على الحكومات الأوروبية، وبالرغم من قدرتها على تنسيق استجاباتها لمواجهة روسيا ودعم أوكرانيا سيبرانياً، فإنها لا تزال متأثرة بتداعيات هذا النهج من الحروب السيبرانية الذي قد يُمثل تحدياً متصاعداً يفرض عليها اتخاذ مواقف قد يكون لها ارتدادات عكسية على دعم أوكرانيا وخاصة في ظل ما تشهده العديد من القوى الأوروبية من صعود متنامٍ لقوى اليمين المتطرف واليسار الشعبوي التي تروج إلى أهمية وقف الحرب والتراجع عن العقوبات المفروضة على روسيا.

▪ بالرغم من أن البعد السيبراني لا يزال حاضراً في علاقة روسيا بأوكرانيا والقوى الغربية، فإنه يحمل مآلات مزدوجة على روسيا؛ ففي حين يدعم قدرتها على

الردع والدفاع والمواجهة ضد خصومها، فإنها تعرضت لهجمات مماثلة عرضت بنيتها التحتية الحيوية المدنية والعسكرية الروسية لمزيد من التهديدات السبيرانية.

وأخيرًا، أظهرت الحرب الروسية-الأوكرانية أن البعد السبيرانتي سيكون حاضرًا وذا تأثير ممتد حتى لو تم التوصل إلى تسوية حول اليوم التالي في أوكرانيا، مع احتمالية تنامي اللجوء إليه خلال أي مسارات تفاوضي في المستقبل باعتباره إحدى آليات الضغط على أي من طرفي الصراع، لإجبارهم على التفاوض أو القبول ببندود 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 بأي تكلفة وقف الحرب الراهنة.

المصادر:

1. Brad Smith, Defending Ukraine: Early Lessons from the Cyber War, **Microsoft**, 22 June 2022, Available at: <https://blogs.microsoft.com/on-the-issues/2022/06/defending-ukraine-early-lessons-from-the-cyber-war/>
2. David E. Sanger, Julian E. Barnes and Kate Conger, As Tanks Rolled into Ukraine, So Did Malware. Then Microsoft Entered the War, **The New York Times**, 28 February 2022, Available at: <https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html>
3. David Jones, New wiper, worm attacks emerge in Ukraine targeting government and industry, **Cybersecurity Dive**, 1 March 2022, Available at: <https://www.cybersecuritydive.com/news/wiper-worm-attacks-ukraine/619597/>
4. Bartosz Sieniawski, "First cyber world war". Ensuring security in times of digital warfare, **Euractiv**, 24 May 2022, Available at: <https://www.euractiv.pl/section/bezpieczenstwo-i-obrona/news/first-cyber-world-war-ensuring-security-in-times-of-digital-warfare/>
5. Matthias Schulze and Mika Kerttunen, Cyber Operations in Russia's War against Ukraine, **German Institute for International and Security Affairs**, 23 April 2023, p. 4, Available at: https://www.swp-berlin.org/publications/products/comments/2023C23_CyberOperations_UkraineWar.pdf
6. Gavin Wilde, Cyber Operations in Ukraine: Russia's Unmet Expectations, **Carnegie Endowment for International Peace**, December 2022, pp. 3-4, Available at: https://carnegie-production-assets.s3.amazonaws.com/static/files/202212-Wilde_RussiaHypotheses-v2.pdf
7. Michael Connell and Sarah Vogler, Russia's Approach to Cyber Warfare, **The Center for Naval Analyses**, March 2017, p. 3, Available at: https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf
8. **I bid**, pp. 23-24.
9. **I bid**, p. 19.
10. Russia-Ukraine: The first full-scale cyberwar?, **London's Global University- UCL**, 11 November 2024, p. 9, Available at: https://www.ucl.ac.uk/steapp/sites/steapp/files/12_individual_final_report_-_russia-ukraine_cyberwar.pdf
11. Gavin Wilde, Russia's Countervalue Cyber Approach: Utility or Futility?, **Carnegie Endowment for International Peace**, 5 February 2024, Available at: <https://carnegieendowment.org/research/2024/02/russias-countervalue-cyber-approach-utility-or-futility?lang=en>
12. **I bid**.
13. Germany blames Russian GRU unit for EU, NATO cyberattacks, **DW**, 9 September 2024, <https://www.dw.com/en/germany-blames-russian-gru-unit-for-eu-nato-cyberattacks/a-70167641>
14. Michael Connell and Sarah Vogler, **Op. Cit**, pp. 23-24.
15. Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace, **U.S. Department of Justice**, 19 October 2020, Available at: <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>
16. رغبة البهي، حرب موازية: البُعد السيبراني في الحرب الروسية-الأوكرانية، المركز المصري للفكر والدراسات الاستراتيجية، 27 فبراير 2022، متاح على: <https://ecss.com.eg/18707/>
17. رغبة البهي، تقنيات "موسكو": أبعاد التطور في القدرات السيبرانية الروسية عقب الحرب الأوكرانية، مركز إنترريجنال للتحليلات الاستراتيجية، 18 يوليو 2023، متاح على: <https://www.interregional.com/article/%D8%AA%D9%82%D9%86%D9%8A%D8%A7%D8%AA-%22%D9%85%D9%88%D8%B3%D9%83%D9%88%22:/456/Ar>
18. Grace B. Mueller, Benjamin Jensen, Brandon Valeriano and Others, Cyber Operations during the Russo-Ukrainian War, **Center for Strategic and International Studies**, 13 July 2023, Available at: <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war>
19. Eyal Pinko, The Cyber Domain in the Russo-Ukrainian War, **Begin-Sadat Center for Strategic Studies**, 22 June 2023, Available at: <https://besacenter.org/the-cyber-domain-in-the-russo-ukrainian-war/>
20. Tom Balmforth, Exclusive: Russian hackers were inside Ukraine telecoms giant for months, **Reuters**, 5 January 2024, Available at: <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/>
21. Peter Apps, Russia's suspected sabotage campaign steps up in Europe, **Reuters**, 21 October 2024, Available at: <https://www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/>

22. Michael Holden, Gabriel Stargardter, UK spy chief says Russia behind 'staggeringly reckless' sabotage in Europe, **Reuters**, 29 November 2024, Available at: <https://www.reuters.com/world/europe/russia-behind-staggeringly-reckless-sabotage-europe-uk-spy-chief-says-2024-11-29/>
23. أنظر رغدة البهي، حرب موازية: البعد السيبراني في الحرب الروسية-الأوكرانية، مرجع سبق ذكره.
24. Todd C. Helmus, Khrystyna Holynska, Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict, **Rand**, 3 September 2024, pp. 26-27, Available at: https://www.rand.org/pubs/research_reports/RRA2771-1.html
25. Sergio Delgado, Cyber espionage in wartime: how Russia plays its cards, **The Diplomat in Spain**, 18 September 2024, Available at: <https://thediplomatinspain.com/en/2024/09/18/cyber-espionage-in-wartime-how-russia-plays-its-cards/>
26. Ukrainian Digital Resistance to Russian Aggression, **StrategEast Center for a New Economy**, April 13, 2022, pp. 5-6, Available at: https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf
27. **Ibid**, pp. 9-10.
28. Bartosz Sieniawski, **Op.Cit.**
29. Todd C. Helmus, Khrystyna Holynska, **Op.Cit.**, pp. 35-40.
30. Kursk Offensive Unveiled: Ukraine's Strategic Planning and Cyber-Kinetic Convergence, **Cyble**, 29 August 2024, Available at: <https://cyble.com/blog/kursk-offensive-unveiled-ukraines-strategic-planning-and-cyber-kinetic-convergence/>
31. Ashish Khaitan, Researchers Reveal the Kursk Offensive: Ukraine's Strategic Campaign for 2024, **The Cyber Express**, 29 August 2024, Available at: <https://thecyberexpress.com/kursk-offensive/>
32. Daryna Antoniuk, Russia's Kursk region suffers 'massive' DDoS attack amid Ukraine offensive, **Recorded Future News**, 8 August, 2024, Available at: <https://therecord.media/kursk-military-offensive-ddos-russia-ukraine>
33. آية عبد العزيز، ثغرة كورسك: هل يؤدي التوغل الأوكراني في روسيا إلى إعادة صياغة معادلة الحرب؟، المركز المصري للفكر والدراسات الاستراتيجية، 4 سبتمبر 2024، متاح على: <https://ecss.com.eg/47837/>
34. رغدة البهي، «ستارلينك»: إنترنت الفضاء والحرب الروسية-الأوكرانية، المركز المصري للفكر والدراسات الاستراتيجية، 25 مايو 2022، متاح على: <https://ecss.com.eg/19502/>
35. رغدة البهي، حدود الدور: تأثير الشركات التكنولوجية في الحرب الروسية-الأوكرانية، المركز المصري للفكر والدراسات الاستراتيجية، 7 مايو 2022، متاح على: <https://ecss.com.eg/19296/>
36. Sharon Rollins, Defensive Cyber Warfare Lessons from Inside Ukraine, **U.S. Naval Institute**, Vol. 149/6/1,444, June 2023, Available at: <https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine>
37. Gregory F. Treverton and Pari Esfandiari, Will the Ukraine War Reshape the Internet?, **Center for Strategic and International Studies**, 20 October 2022, Available at: <https://www.csis.org/analysis/will-ukraine-war-reshape-internet>
38. The 2024 U.S.-Ukraine Cyber Dialogue Media Note, **U.S. Department of State**, 16 August 2024, Available at: <https://www.state.gov/the-2024-u-s-ukraine-cyber-dialogue/>
39. Daryna Antoniuk, Ukraine signs agreement to join NATO cyber defense center, **Recorded Future News**, 20 January 2023, Available at: <https://therecord.media/ukraine-signs-agreement-to-join-nato-cyber-defense-center>
40. Daryna Antoniuk, Ukraine signs security deals with Western allies to help counter Russian cyberattacks, **Recorded Future News**, 23 February 2024, <https://therecord.media/ukraine-signs-security-deals-with-western-allies-over-russian-cyberattacks>
41. Bill Burns, Richard Moore, Bill Burns and Richard Moore: Intelligence partnership helps the US and UK stay ahead in an uncertain world, **Financial Times**, 7 September 2024, Available at: <https://www.ft.com/content/252d7cc6-27de-46c0-9697-f3eb04888e70>

حدود الحرب السيبرانية بين الولايات المتحدة الأمريكية والصين

د. فرح زعاطرة*

نتيجة للمتغيرات التي أحدثتها ثورة المعلومات والتكنولوجيا، ظهر مفهوم «الحروب السيبرانية» التي عرفها البعض على أنها أعمال تقوم بها دول تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها أو سرقة المعلومات. لذلك، أصبحت الحرب السيبرانية شكلاً من أشكال الصراع السيبراني، كما أصبح سلاح المعلومات أحد أهم الأسلحة التي تستخدمها الدول، ولا سيما الدول المتقدمة لتحقيق أهدافها الاستراتيجية. وفي رؤية «ديفيد جومبرت»، فإن أحد الآثار المهمة لثورة المعلومات هو احتمال الوقوع الوشيك للحرب السيبرانية، أي الحرب التي يتم خوضها بالمعلومات بوصفها سلاحاً أو هدفاً رئيساً.

* خبير الأمن السيبراني

أولاً: الأمن السيبراني في الاستراتيجيات والقوانين الأمريكية

أطلق الرئيس الأمريكي الأسبق «جورج دبليو بوش» الاستراتيجية القومية لتأمين الفضاء السيبراني في عام 2003، والتي تضمنت الجهود اللازمة لتقليل المخاطر والتهديدات الناجمة عن الفضاء السيبراني، والتي قد تؤدي إلى تدمير الأنظمة الخاصة بالبنية التحتية الأمريكية. وقد أشارت الاستراتيجية إلى أن البنية التحتية الأمريكية تتكون من مؤسسات عامة وخاصة في مجالات متعددة؛ منها: الأغذية والزراعة، والمياه، والصحة العامة، والطوارئ، والدفاع، والخدمات الحكومية، والاتصالات، والمعلومات، والطاقة، والنقل، والصرافة، والمعاملات المالية، والبريد، والملاحة، والصناعات الكيماوية⁽¹⁾. هذا، ويُعد الفضاء السيبراني عصب هذه المجالات، فهو نظام التحكم الخاص بالدولة. ومن ثمّ، فإن تأمينه والقدرة على التحكم فيه وإدارته من العوامل الرئيسية التي تدعم الاقتصاد والأمن القومي الأمريكي. ولتحقيق ذلك، تتطلب الاستراتيجية شراكة وتعاوناً مع القطاع الخاص، كما تهدف الاستراتيجية إلى تحقيق ثلاثة أهداف رئيسية⁽²⁾، وهي: (1) منع الهجمات السيبرانية (2) تقليل نقاط الضعف التي يمكن اختراقها (3) سرعة التعامل مع الهجمات السيبرانية لتقليل إمكانية تدمير الأنظمة والبيانات واستعادتها بسرعة.

ويمكن تحقيق هذه الأهداف من خلال تبني نظام وطني متكامل يعمل على تنسيق الجهود المشتركة لضمان سرعة الاستجابة للهجمات السيبرانية وحماية البيانات، بالإضافة إلى تنفيذ برنامج قومي يهدف إلى تقليل المخاطر السيبرانية والحد من نقاط الضعف في الأنظمة. وهو ما يشمل: إطلاق برنامج توعية وتدريباً شاملاً يهدف إلى تعزيز أمن الفضاء السيبراني، وتحسين المؤسسات الحكومية ضد التهديدات السيبرانية، مع تعزيز التعاون الدولي في هذا المجال. وتسعى هذه المحاور إلى دعم استراتيجية الأمن السيبراني من خلال توجيه دور الحكومة الفيدرالية نحو ضمان بيئة إلكترونية آمنة ومستدامة⁽³⁾.

كما وضعت الاستراتيجية بعض المسؤوليات على الحكومة الفيدرالية، وخصوصاً وزارة الأمن الداخلي، التي تم استحداثها بقرار رئاسي عام 2002، ومن هذه المسؤوليات⁽⁴⁾: (1) تطوير خطة قومية شاملة لتأمين البنية التحتية الحرجة

ومصادرها (2) تقديم نموذج لإدارة الأزمات للرد على محاولات الهجوم على أنظمة المعلومات (3) توفير المعونة الفنية للقطاع الخاص والجهات الحكومية في حالة حدوث أي هجوم سيبراني (4) التنسيق بين مختلف المؤسسات والوكالات الرسمية وغير الرسمية، وتقديم النصائح والمعلومات لتعزيز الأمن السيبراني.

وفي عام 2008، أطلقت إدارة «بوش» مبادرة وطنية للأمن السيبراني في الولايات المتحدة، تهدف إلى مواجهة التهديدات السيبرانية الحالية والمستقبلية، وتقليل نقاط الضعف في مجالي الاتصالات والأمن السيبراني. وقد ركزت المبادرة على تحقيق ثلاثة أهداف رئيسية هي: (1) إنشاء خطوط دفاع متقدمة لمواجهة التهديدات اليومية والفورية من خلال تعزيز الوعي بمخاطر الفضاء السيبراني (2) صد جميع أنواع التهديدات السيبرانية عبر تعزيز قدرات مكافحة التجسس وتحسين أمن تكنولوجيا المعلومات (3) دعم مستقبل الأمن السيبراني من خلال نشر ثقافة التعليم السيبراني، وتعزيز الجهود البحثية، وتطوير التنسيق بين مختلف الجهات المعنية⁽⁵⁾.

وفي عام 2015، أصدر الرئيس الأسبق «باراك أوباما» وثيقة بعنوان «الاستراتيجية السيبرانية لوزارة الدفاع»، والتي حددت ثلاث مهام رئيسية تمثل جوهر عمل الوزارة في مجال الأمن السيبراني، وهي: (1) دعم القيادات القتالية للولايات المتحدة (2) حماية شبكات وزارة الدفاع (3) تأمين البنية التحتية الحيوية. وقد أوضحت الوثيقة أن وزارة الدفاع - بالتعاون مع وكالات حكومية أخرى - طوّرت خيارات وأساليب تهدف إلى عرقلة الهجمات السيبرانية ذات التأثير الملموس قبل وقوعها، كما أشارت إلى إمكانية استخدام العمليات السيبرانية لإضعاف شبكات القيادة والسيطرة التابعة للخصوم، وتعطيل البنية التحتية المرتبطة بالمجالات العسكرية وقدرات الأسلحة؛ مما يعزز الجاهزية الدفاعية لمواجهة التهديدات المتزايدة في الفضاء السيبراني⁽⁶⁾.

وقد حددت استراتيجية الدفاع الوطني الأمريكية لعام 2018 الفضاء السيبراني كمجال رئيسي للنهوض بالمصالح الوطنية وتأمين القيادة العالمية، ووصفت الاستراتيجية الفضاء السيبراني بأنه مجال معقد بشكل متزايد، وأن البيئة الأمنية العالمية تتميز بعودة المنافسة الاستراتيجية طويلة المدى، إلى جانب التغيير التكنولوجي

السريع ومفاهيم الحرب الجديدة. وقد فرض هذا الواقع تحديًا كبيرًا على صناع القرار في الولايات المتحدة الذين أدركوا أن الولايات المتحدة معرضة لخطر فقدان ميزتها في الفضاء السيبراني، وتقويض حرية العمل في الفضاء السيبراني؛ مما قد يضر بازدهار البلاد، ويحد من قدرتها على ردع العدوان والدفاع عن الوطن واستعراض القوة في الخارج⁽⁷⁾.

وفي 19 فبراير 2020، وقع "ترامب" توجيهًا يهدف إلى تشكيل "قوة فضائية"، وكلف وزارة الدفاع بإعداد اقتراح تشريعي لإنشاء هذا الفرع السادس ضمن القوات المسلحة الأمريكية، وأوضح التوجيه أن قوة الفضاء ستركز على تحقيق ثلاث مهام رئيسية: تعزيز فتك وفاعلية القوة المشتركة، ضمان حرية العمل في المجالين الفضائي والسيبراني، وتوفير عمليات عسكرية مستقلة تدعم القيادة الوطنية في الفضاء السيبراني. يمثل هذا التوجيه خطوة استراتيجية لتعزيز القدرات الأمريكية في مواجهة التحديات المتزايدة في الفضاء السيبراني⁽⁸⁾.

كما بدأت وزارة الدفاع التخطيط التفصيلي لإنشاء القوة الفضائية من خلال تشكيل فرقة عمل متخصصة. ففي 22 فبراير 2019، قدمت الإدارة اقتراحًا تشريعيًا للكونجرس لإنشاء القوة الفضائية كجزء من القوات المسلحة. وقد شارك في عملية الإعداد خبراء من القوات الجوية والجيش والبحرية، إلى جانب جنرالات الأركان المشتركة ومكتب وزير الدفاع (OSD) ومجتمع الاستخبارات، ووضعت خطة عمل أولية لإنشاء القوة الفضائية⁽⁹⁾. وفي 17 ديسمبر 2019، أقر الكونجرس قانونًا للسنة المالية 2020 ليمنح وزارة الدفاع الأمريكية الصلاحية لتأسيس "القوة الفضائية" كفرع جديد ضمن القوات المسلحة. وبعد يومين، أقر الكونجرس قانون مخصصات وزارة الدفاع لعام 2020؛ مما أتاح التمويل اللازم لإنشاء الجيش السادس الأمريكي. هذا وتهدف القوة الفضائية إلى تحقيق ثلاث مهام رئيسية، هي: (1) حماية مصالح الولايات المتحدة في الفضاء (2) ردع أي عدوان يستهدف الفضاء أو ينطلق منه (3) تنفيذ العمليات الفضائية بشكل مستقل. كما حددت وزارة الدفاع مسؤوليات القوة الفضائية، والتي تتضمن تحقيق التفوق في الفضاء السيبراني وتعزيز الوعي بمجالات الفضاء المختلفة، بما في ذلك: المجالات العسكرية، والمدنية، والتجارية. وتشمل

المسئوليات التحكم بقدرات القوة السيبرانية الهجومية والدفاعية، وقيادة القوات الفضائية وعملياتها السيبرانية، وتوفير الدعم للعمليات الفضائية مثل الاتصالات الساتلية والقيادة النووية. وبالإضافة إلى ذلك، تركز القوة الفضائية على تقديم التحذيرات المبكرة بشأن الصواريخ ودعم أنظمة الدفاع الصاروخي؛ مما يعزز دورها في حماية الأمن القومي للولايات المتحدة ضمن المجالين الفضائي والسيبراني⁽¹⁰⁾.

وإلى جانب ذلك، بموجب قانون حماية أمريكا (Protect America Act) الصادر في عام 2007، تم إنشاء برنامج سري يحمل الاسم الكودي (US-984XN)، والمعروف إعلاميًا باسم (PRISM)، وهو معني بمراقبة المعلومات في الفضاء السيبراني، بما في ذلك الاتصالات الحية والمعلومات المخزنة التي تخص أشخاصًا محددين داخل الولايات المتحدة وخارجها. ويستطيع البرنامج جمع معلومات مثل رسائل البريد الإلكتروني، ومحادثات الفيديو والصوت، والصور، والاتصالات الصوتية عبر بروتوكول الإنترنت، وعمليات نقل الملفات، وإخطارات الولوج، وتفاصيل الشبكات الاجتماعية⁽¹¹⁾. وبموجب هذا القانون، يحق لوكالة الأمن القومي الأمريكي (NSA)، بعد موافقة أحد القضاة السريين في محكمة مراقبة الاستخبارات الخارجية، طلب بيانات من الشركات العاملة في مجال الإنترنت، مثل "ياهو" و"فيسبوك". ويهدف ذلك إلى الحد من التهديدات السيبرانية مع السعي لتحقيق التوازن بين حماية أمن الأفراد وضمان حريتهم وخصوصيتهم⁽¹²⁾.

كما يمكن القول إن الولايات المتحدة كانت واحدة من الدول التي وضعت إطارًا قانونيًا محكمًا لمراقبة التطبيقات الاجتماعية، حيث تخضع هذه المراقبة لجملة من القوانين التي تُنظم جمع وتحليل البيانات الإلكترونية. ومن أبرز هذه القوانين المادة 207 من قانون مراقبة الاستخبارات الخارجية (FISA) التي تمنح وكالة الأمن القومي الصلاحية لجمع معلومات التواصل الإلكتروني من خلال برامج متطورة مثل برنامج "بريزم" السابق الإشارة له⁽¹³⁾. كما يبرز القانون الوطني (Patriot Act)، وتحديثًا المادة 215 منه، كإطار قانوني آخر يتيح لوكالة الأمن القومي جمع البيانات الهائلة من المكالمات الهاتفية عبر شركات الاتصالات. ويهدف هذا الإجراء إلى تعزيز قدرات الاستخبارات الأمريكية في تحليل المعلومات الضخمة واستباق التهديدات الأمنية.

هذا، وتتعدد الوسائل التي تعتمد عليها وكالة الأمن القومي لجمع البيانات، منها خطوط (Upstream) التي تُستخدم لسحب البيانات مباشرة من الكابلات البحرية التي تُعد العمود الفقري للاتصالات العالمية، بالإضافة إلى الخوادم التي تحتفظ بها شركات أمريكية؛ مما يوفر مخزوناً هائلاً من البيانات التي يمكن الاستفادة منها في التحليل والمتابعة⁽¹⁴⁾. كما كشفت صحيفة "الجارديان" البريطانية -في تقرير لها- أن وكالة الأمن القومي الأمريكية طورت تقنيات لاستغلال تطبيقات الهواتف الذكية لجمع معلومات خاصة بالمستخدمين، وتضمنت الوثائق المسربة أن وكالة الاستخبارات المركزية (CIA) استخدمت هذه البرامج لاستهداف بيانات الهواتف الذكية، لجمع معلومات عن الإرهابيين وأهداف استخباراتية أخرى، وأنفقت الوكالة أكثر من مليار دولار على برامج التجسس التي تستهدف الهواتف الذكية⁽¹⁵⁾.

وفي سياق تحسين الدفاعات السيبرانية، عملت وكالة الأمن القومي الأمريكي على تأسيس فريق يُعرف باسم "الفريق الأحمر" الذي تلقى تدريباً خاصاً تحت اسم "المتلقي المؤهل"، ويتألف هذا الفريق من مجموعة مستقلة تُعرف باسم "قراصنة القبعات البيضاء". ويهدف إلى تحسين فاعلية الدفاعات الإلكترونية من خلال محاولة اختراق شبكات الحواسيب التابعة للنتاجون باستخدام معدات وبرمجيات متوفرة في الأسواق التجارية. ويتيح عمل الفرق الحمراء السيبرانية محاكاة هجمات حقيقية تهدف إلى تقييم وتقوية برامج أمن المعلومات بالكامل⁽¹⁶⁾.

كما امتلكت وكالة الأمن القومي الأمريكي وحدتين رئيسيتين هما استخبارات الإشارة (SIGINT) وأمن المعلومات (INFOSEC). وتضطلع هاتان الوحدتان بأدوار أساسية في إدارة القوة السيبرانية الأمريكية. وتشمل هذه الأدوار التصدي للهجمات السيبرانية المضادة واعتراضها وتدميرها، كما تقوم بأعمال القرصنة الحاسوبية الأخلاقية⁽¹⁷⁾ وعمليات التحري السيبراني لفحص الأنظمة والبرامج الحاسوبية الخاصة بالبنية التحتية السيبرانية الأمريكية، إلى جانب إعداد اختبارات الدفاع السيبراني لضمان حماية البيانات الخاصة بالوكالات والمؤسسات والشركات الأمريكية⁽¹⁸⁾.

وفي هذا السياق، أصدرت وزارة الأمن الداخلي في عام 2012 تقريرًا بعنوان "مراجعة الالتزام بالخصوصية" (Privacy Compliance Review)، والذي أكدت فيه أن مركز العمليات التابع للوزارة يتولى منذ عام 2010 متابعة مواقع التواصل الاجتماعي والمواقع العامة على الإنترنت، ويتضمن ذلك الاطلاع المستمر على المنتديات والمدونات العامة، بهدف تعزيز قدرة الحكومة الأمريكية على التعامل مع الأزمات والكوارث بشكل سريع وفعال. كما أشار التقرير إلى أن هذه الإجراءات تسهم في تحسين استجابة أجهزة المخابرات ووكالة الأمن القومي لحالات الطوارئ وإنشاء قنوات اتصال فورية للتعامل مع الكوارث.

ثانيًا: الأمن السيبراني في السياسات والاستراتيجيات الصينية

تستند الاستراتيجية الصينية للأمن السيبراني إلى أفكار المفكر الاستراتيجي "صن تزو"، الذي على الرغم من وفاته عام 496 ق.م، قدم رؤية استراتيجية تركز على الانتصار دون الحاجة لخوض الحروب التقليدية. وقد أدركت الصين منذ تسعينيات القرن الماضي أهمية تكنولوجيا المعلومات في تعزيز القدرات الوطنية، وخاصة في المجال العسكري، حيث يعد الفضاء السيبراني فرصة لتطوير قدراتها الهجومية دون الحاجة إلى إنفاق ضخم على البنية العسكرية التقليدية⁽¹⁹⁾. وتأسيسًا على ذلك، استثمرت الصين في تطوير بنية سيبرانية قوية لتعزيز قوتها في هذا المجال، مع التركيز على التعاون المدني مع القراصنة لتعظيم قدراتها. ومع ذلك، تنكر الصين رسميًا تورطها في أي هجمات سيبرانية، ولا تتخذ إجراءات ضد عمليات القرصنة؛ مما يؤدي إلى اتهامها دوليًا بشكل مباشر أو غير مباشر⁽²⁰⁾.

كما طور جيش التحرير الشعبي الصيني عقيدة عسكرية سيبرانية، شملت تدريب القوات على آليات الهجوم السيبراني باستخدام برامج محاكاة متقدمة. وقد شملت وحدات تدريبية مثل: أكاديمية قيادة الاتصالات، وجامعة هندسة المعلومات، ومؤسسة الدفاع الوطني والتكنولوجيا. كما لعبت الأبحاث الصادرة عن المؤسسات الأكاديمية والعسكرية الصينية دورًا مهمًا في تحسين القدرات السيبرانية. هذا، وتركز الاستراتيجية الصينية على مهاجمة المعلومات والبيانات العسكرية

والاستيلاء عليها أو تعديلها، مع تنسيق السياسات السيبرانية بين الأجهزة المختلفة، لكن انعدام الشفافية في هذه العمليات يزيد من تعقيد المشهد السيبراني⁽²¹⁾.

ففي عام 2006، نشرت الصين خطة استراتيجية للتنمية المعلوماتية في الفترة بين 2006 و2020، دعت فيها إلى توفير بنية تحتية وطنية عبر الإنترنت، وتعزيز الابتكار التكنولوجي، وتحسين بنية الصناعة السيبرانية، وإحراز تقدم في بناء الاقتصاد والمجتمع الموجه عبر الإنترنت. كما تضمنت الاستراتيجية تعزيز السيطرة على الاقتصاد الوطني، وتعميم الحكومة الإلكترونية، وبناء ثقافة إنترنت متقدمة.

وفي إطار جهودها لتعزيز الأمن السيبراني، أنشأت الصين مجموعة قيادة للأمن السيبراني برئاسة الرئيس "شي جين بينغ"، وقد ركزت هذه المجموعة على تعزيز الانضباط والاستجابة للتهديدات السيبرانية الأجنبية. كما أصدرت الصين في عام 2015 مشروع قانون جديد حول أمن الشبكات، يضع قيودًا على التقنيات الأجنبية، ويعزز إدارة البيانات. وفي العام نفسه، أنشأت القوات المسلحة الصينية قوة دعم استراتيجية جديدة لتحقيق تقدم في تطبيقات القوة السيبرانية العسكرية⁽²²⁾.

وقد ركزت السياسات التوجيهية للحكومة الصينية على تطوير التكنولوجيات الأساسية، وتعزيز دور المعلومات في الاقتصاد والسياسة والثقافة، مع ضمان الأمن السيبراني الوطني. إذ تسعى الصين إلى تعزيز نفوذها على المسرح السيبراني العالمي من خلال إبراز دور المعلومات في الشؤون الدولية، والعمل على تنسيق الجهود بين الحكومة المركزية والمحلية وبين الحزب والجيش⁽²³⁾.

وفي مواجهة التحديات السيبرانية، تبنت الصين تدابير تقنية أطلقت عليها "استراتيجية الوخز بالإبر"، والتي تهدف لحماية مصالحها من الهجمات التي تسعى إلى إلحاق الأذى بالمعلومات القيمة أو القرصنة أو تدمير الأنظمة الحيوية. هذه الجهود تُظهر عزم الصين على تحقيق تفوق في المجال السيبراني، رغم التحديات القانونية والتقنية التي تواجهها.

إذ تتبنى الاستراتيجية الصينية للأمن السيبراني مبدأً أساسيًا يتمثل في أن تحقيق الأمن السيبراني يتطلب بناء قوة سيبرانية تستند إلى الاستقلالية التكنولوجية بعيدًا عن

الاعتماد على منتجات تكنولوجيا المعلومات الغربية. وقد نجحت الحكومة الصينية في تعزيز صناعة تكنولوجيا المعلومات من خلال عدد من الشركات الخاصة التي تسيطر على هذا القطاع، ولكنها لا تنفصل عن الإشراف الحكومي. كما تدير الحكومة الصينية شركات الاتصالات السلكية واللاسلكية الرئيسية، مثل: (China Telecom) و (China Mobile)، التي تهيمن على السوق والاستثمارات. هذا وتخضع القرارات المتعلقة بتطوير التكنولوجيا والصناعة التكنولوجية عمومًا لموافقة الحكومة، بما في ذلك تحديد نوع التكنولوجيا المستخدمة وطرق تطويرها⁽²⁴⁾. ويتسم التعاون بين الحكومة الصينية وشركات التكنولوجيا المحلية بالقوة، حيث تشمل الشركات الرائدة في هذا المجال شركات مثل (Lenovo) و (Dating Mobile). وقد أظهرت هذه العلاقة نجاحًا ملحوظًا، حيث أسهمت صناعة التكنولوجيا في تعزيز الاقتصاد الصيني بشكل كبير. ويُعد سوق تكنولوجيا المعلومات والاتصالات في الصين أحد أكثر القطاعات ديناميكية في الاقتصاد، حيث بلغ حجمه في عام 2021 حوالي 8,1 تريليونات دولار، وهو ما يمثل حوالي 55٪ من الناتج المحلي الإجمالي⁽²⁵⁾.

وفي عام 2017، بلغت صادرات الصين من تكنولوجيا المعلومات والاتصالات حوالي 781 مليار دولار مقارنة ب وارداتها التي بلغت 528 مليار دولار، وفقًا لتقارير شركة استشارات تكنولوجيا المعلومات الصينية. كما تسهم هذه الأرقام في تعزيز مكانة الصين كمنافس قوي في مواجهة الشركات الغربية، وخاصة الأمريكية⁽²⁶⁾.

وتُظهر الشركات الصينية براعة في تطوير التقنيات ومنافسة الأسواق الغربية من خلال تقديم منتجات بأسعار منخفضة وجودة متزايدة. مع نضج سوق تكنولوجيا المعلومات والاتصالات، أصبح التحدي الأساسي يتمثل في دمج التقنيات في الصناعات التقليدية وتحويلها. ومع ذلك، لم تعد الشركات الأجنبية تمتلك حصة سوقية مهيمنة في العديد من القطاعات الفرعية لتكنولوجيا المعلومات والاتصالات؛ مما يعكس قوة التنافس المحلي في الصين⁽²⁷⁾.

كما أن إصرار الصين على ضمان استقلاليتها التكنولوجية يظهر جليًا في المخطط الصناعي الصادر في عام 2019، حيث تعهدت الحكومة ببناء مجمع صناعي للأمن السيبراني في بكين. وفي عام 2020، حقق هذا المشروع عائدات بلغت حوالي 14,8 مليار دولار، مع

توقعات بأن يسهم بمبلغ 330 مليار يوان في نمو الناتج المحلي الإجمالي، وتأسيس ثلاث شركات كبرى تحقق إيرادات سنوية تتجاوز 10 مليارات يوان⁽²⁸⁾. هذا المشروع الصناعي يُدار بالتعاون بين وزارة الصناعة وتكنولوجيا المعلومات (MIIT) وحكومة بلدية بكين، ويهدف إلى تطوير الأبحاث المتعلقة بالتقنيات الرئيسية للأمن السيبراني، وبناء قاعدة بحث وتطوير رائدة عالميًا. ويعكس هذا الجهد المشترك التزام الصين بتلبية احتياجات الأمن القومي، وضمان استقلالية البلاد التكنولوجية في مواجهة التحديات السيبرانية. وبهذا النهج، تؤكد أن بناء قوتها السيبرانية يتطلب تحقيق استقلالية تكنولوجية شاملة؛ مما يعزز قدرتها على مواجهة التحديات العالمية وضمان أمنها القومي⁽²⁹⁾.

ثالثًا: الهجمات السيبرانية المتبادلة بين الصين والولايات المتحدة

ترى الولايات المتحدة الأمريكية أن أكبر وأكثر التهديدات التي يواجهها الأمن القومي الأمريكي في القرن الحادي والعشرين هي قضية الأمن السيبراني، وأن هذه التهديدات 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⁽³⁰⁾. فيما تسعى الصين إلى تحقيق تفوق نسبي على خصومها في المجال التكنولوجي والمعلوماتي. وفي ظل المتغيرات السريعة في بيئة الفضاء السيبراني، بوصفه مجالاً رئيسياً للحرب، ظهرت الحاجة إلى إعادة النظر في مفهوم السيادة السيبرانية وفق استراتيجية الأمن السيبراني الصينية، والاستفادة من أدوات الثورة الرقمية بطرق متطورة وحديثة. إذ تعد الصين من أولى وأهم الدول التي لجأت إلى إرساء مبدأ سيادة الإنترنت على أراضيها، سعيًا منها لحماية فضاءها السيبراني وبنيتها التحتية المعلوماتية، وتجلبت القوة السيبرانية للصين في قدرتها على السيطرة والتأثير عبر الفضاء السيبراني، وتعتمد في ذلك على امتلاك موارد وأدوات فاعلة تمكنها من تحقيق مكانة مرموقة في هذا المجال⁽³¹⁾.

وإلى جانب تعدد الرؤى والأهداف بين الجانبين، تعددت أيضًا الهجمات السيبرانية المتبادلة بين الدولتين، ففي عام 2010، كشفت شركة «جوجل» عبر

مدونتها أنها كانت ضحية هجوم سيبراني وقع في منتصف شهر أكتوبر ومصدره الصين، وذكرت الشركة أن أكثر من 20 شركة أخرى تعرضت للهجوم الذي أسفر عن استهداف أكثر من 34 منظمة. ونتيجة للهجوم، أعلنت «جوجل» عن مراجعة أعمالها في الصين⁽³²⁾. وفي اليوم نفسه، أصدرت وزيرة الخارجية الأمريكية آنذاك «هيلاري كلينتون» بياناً موجزاً أدانت فيه تلك الهجمات، وطلبت ردّاً من الصين. كما أكد الكونجرس الأمريكي أنه يخطط للتحقيق في مزاعم شركة «جوجل» بأن الحكومة الصينية استخدمت خدمات الشركة للتجسس على نشطاء حقوق الإنسان. والجدير بالذكر أن الهجوم استهدف عشرات المنظمات الأخرى، ومنها شركات: «أدوبي»، و«أكاماي»، و«جونيبر للشبكات»، و«راكسبيس»، التي أكدت علناً أنها تعرضت للاستهداف، هذا إلى جانب استهداف شركات مثل: «ياهو»، و«سيمانتك»، و«نورثروب غرومان»، و«مورغان ستانلي»، و«داو كميكال»، و«بلاك بيري»⁽³³⁾.

وقد أطلق على هذا الهجوم اسم «عملية أورورا» من قبل «دميتري أليروفيتش» (نائب رئيس أبحاث التهديدات في شركة الأمن السيبراني «إنتل سيكيوريتي»). وقد اكتشف بحث أجرته الشركة أن «أورورا» كان جزءاً من مسار الملف على جهاز المهاجم الذي تم تضمينه في اثنين من ثنائيات البرامج الضارة التي قالت الشركة إنها مرتبطة بالهجوم، وقد دفع «جورج كورتز» (كبير مسؤولي التكنولوجيا في شركة «إنتل»)، في منشور على إحدى المدونات، بأن هذا هو الاسم الداخلي الذي أعطاه المهاجمون لهذه العملية⁽³⁴⁾.

وبهذا، تعد عملية «أورورا» سلسلة من الهجمات السيبرانية التي تضمنت تهديدات مستمرة متقدمة من مجموعة «إلدروود» (Elderwood) ومقرها في الصين، والتي كانت على علاقات مع جيش التحرير الشعبي، وبدأت الهجمات في منتصف عام 2009، واستمرت حتى نهاية العام نفسه، إذ تعتبر هذه العملية واحدة من أكثر العمليات فاعلية على صعيد الهجوم السيبراني للصين على الولايات المتحدة⁽³⁵⁾.

وردّاً على الهجوم، ذكرت شركة «جوجل» في مدونتها أنها تخطط لتشغيل نسخة غير خاضعة للرقابة تماماً من محرك البحث الخاص بها في الصين، وأشارت إلى أنه

إذا لم يكن ذلك ممكناً، فقد تغادر الصين وتغلق مكاتبها هناك، ومن جهتها، أكدت الصين أن هذا جزء من استراتيجية وضعتها الحكومة الأمريكية⁽³⁶⁾.

أما بالنسبة لأهمية الهجوم، فقد أكدت شركة "إنتل" أن الهدف الأساسي له كان الوصول إلى مستودعات رمز المصدر وربما تعديلها في شركات المقاولات عالية التقنية والأمن والدفاع. وقد ذكر "دميتري ألبيروفيتش" أن إدارة تكوين البرمجيات كانت مفتوحة على مصراعها، حيث لم يفكر أحد في تأمينها من قبل. ومع ذلك، كانت هذه الإدارة تُعتبر "تاج المجوهرات" في معظم هذه الشركات المستهدفة، وهي أكثر قيمة بكثير من أي بيانات مالية أو بيانات شخصية⁽³⁷⁾.

وفي عام 2011، تمكنت الصين من الحصول على التصاميم الخاصة بنظام الأسلحة التكنولوجية الفائقة لمقاتلات F-35 الأمريكية، التي تعد أحدث مقاتلات الجيل الخامس في العالم، عن طريق عمليات اختراق ناجحة لشبكات الكمبيوتر الخاصة بشركة لوكهيد مارتن الأمريكية المسؤولة عن إنتاج هذه الطائرات⁽³⁸⁾.

وفي عام 2013، اتهمت الولايات المتحدة الصين بتنفيذ أعمال تجسس لسرقة معلومات عسكرية وتجارية سرية، وقدمت شركة "مانديانت" الأمريكية للأمن الإلكتروني تقريراً اتهمت فيه وحدات إلكترونية تابعة للجيش الصيني بشن هجمات سيبرانية تمثل تهديدات واسعة النطاق على مؤسسات أمريكية⁽³⁹⁾. هذا، وتعكس الاتهامات المتبادلة بين الصين والولايات المتحدة وجود تنافس دولي على الذكاء الاصطناعي والقوة الإلكترونية، وفي تحليل "ريفا جوجون" (كبير المحللين في معهد ستراتفورد Stratford Institute) الأمريكي للدراسات الأمنية والاستراتيجية)، فإن التنافس بين أقطاب العالم ودوله الصغيرة على امتلاك أحدث برمجيات الذكاء الاصطناعي سيؤدي إلى صراعات جديدة، بسبب خوف الأطراف الدولية من بعضها، وبالتالي، أصبحت تقنية الذكاء الاصطناعي والحصول عليها تحدياً للدول الكبرى⁽⁴⁰⁾.

وعليه، يمكن الدفع بتصاعد وتيرة التهديدات السيبرانية بين الولايات المتحدة والصين والتي ازدادت حدتها في السنوات الأخيرة، فقد تبين أن أكثر من نصف الهجمات السيبرانية (53.5%) التي تعرضت لها الصين في عام 2019 كانت من مصادر أمريكية.

وفي الوقت نفسه، يعتقد البيت الأبيض أن أغلب التهديدات السيبرانية مصدرها الصين، وهي مسؤولة عن معظم الهجمات التي يعاني منها العالم⁽⁴¹⁾. وقد ذكر فريق الأمن السيبراني التابع للحكومة الصينية، والمعروف باسم (CNCERT) أن العدد الإجمالي لهجمات البرامج الضارة على أجهزة الكمبيوتر الصينية بلغ رقمًا كبيرًا⁽⁴²⁾.

وفي عام 2020، استهدف المتسللون الوكالات الصينية والبعثات الدبلوماسية عبر خوادم الشبكة الخاصة الافتراضية (VPN)، في حملة تجسس سيبراني منسقة. وقد أتى ذلك في وقت أصبحت فيه الحكومات والمنظمات العالمية أكثر عرضة من أي وقت مضى للانتهاكات الأمنية، وفقًا لتقرير صادر عن شركة الأمن السيبراني الصينية (Qihoo-360) في أبريل 2020⁽⁴³⁾.

علاوة على ما سبق، اتخذت إدارة "ترامب" إجراءات ضد تطبيقات التواصل الاجتماعي الصينية مثل "تيك توك"، و"وي تشات"، بزعم أنها تشكل تهديدًا للأمن القومي. كما اتهمت وزارة العدل الأمريكية متسللين صينيين في يوليو 2020، باستهداف تطوير لقاح نيابة عن جهاز المخابرات الصيني، كجزء من حملة أوسع امتدت لسنوات من السرقة الإلكترونية العالمية⁽⁴⁴⁾.

إذ تقوم الحكومة الصينية عن طريق: الوحدات الإلكترونية في الجيش الصيني، والشركات الخاصة، والقراصنة السيبرانيين، بتنفيذ عمليات اقتحام تستهدف القوى الغربية الكبرى، وفي مقدمتها الولايات المتحدة. كما تستهدف المؤسسات الأكاديمية والصناعات والمرافق الحكومية لهذه الدول، والغرض الأساسي من هذه الأنشطة هو الحصول على ميزات تنافسية في مختلف المجالات الاقتصادية والسياسية والعسكرية، مثل: التجسس السيبراني، وإتلاف أو تدمير البيانات، وإلحاق الضرر بالخصوم⁽⁴⁵⁾.

رابعًا: تقييم عام

هناك غموض حول حدود قدرات الولايات المتحدة السيبرانية، ويعود هذا الغموض جزئيًا إلى صعوبة وضع مقياس دقيق لتحديد إمكانيات الولايات المتحدة

في هذا المجال. وإلى جانب هذا الغموض، لا يخفى القلق المستمر الذي ينتاب الولايات المتحدة تجاه قوى أخرى ذات قدرات فاعلة في الفضاء السيبراني مثل روسيا والصين⁽⁴⁶⁾. إن البعد السيبراني بين الصين والولايات المتحدة ليس مجرد سباق تقني، بل هو منافسة استراتيجية تهدف إلى الهيمنة على الفضاء السيبراني بوصفه مجالاً جديداً للتنافس العالمي⁽⁴⁷⁾.

فقد تبنت أجزاء كبيرة من العالم رؤية الولايات المتحدة حول الفضاء السيبراني المشترك والمفتوح من أجل المنفعة المتبادلة للجميع. ومع ذلك، فإن منافسي الولايات المتحدة وخصومها قد اتخذوا مقاربة معاكسة، حيث يستفيدون من الإنترنت المفتوح، بينما يقومون في الوقت نفسه بتقييد ومراقبة وصول شعوبهم إليه. كما أنهم يعملون بنشاط على تقويض مبادئ الإنترنت المفتوح في المنتديات الدولية، ويتخفون وراء مفاهيم السيادة، بينما ينتهكون قوانين الدول الأخرى من خلال الانخراط في أنشطة تجسس اقتصادية ضارة وأنشطة سيبرانية عدائية⁽⁴⁸⁾. إذ تسبب هذه الأنشطة في اضطراب اقتصادي كبير، وتلحق الأذى بالأفراد والمصالح التجارية وغير التجارية والحكومات حول العالم، حيث ينظر هؤلاء المنافسون إلى الفضاء السيبراني باعتباره ساحة يمكن فيها تحييد القوة العسكرية والاقتصادية والسياسية الساحقة للولايات المتحدة؛ مما يجعل الولايات المتحدة وحلفاءها وشركاءها عرضة للخطر. وقد قامت روسيا وإيران وكوريا الشمالية بشن هجمات سيبرانية أضرت بالولايات المتحدة؛ مما يجعل من الضروري ردع العدوان السيبراني في المستقبل.

علاوةً على ذلك، انخرطت الصين في عمليات تجسس سيبراني اقتصادي؛ مما أدى إلى سرقة مليارات الدولارات وانتهاك حقوق الملكية الفكرية، كما استغلت جهات غير حكومية، بما في ذلك الإرهابيون والمجرمون، الفضاء السيبراني لجني الأرباح من الولايات المتحدة وحلفائها وشركائها، إضافة إلى استخدامه لتجنيد الأفراد وشن هجمات عدائية، مما زاد من تعقيد الوضع. وفي ظل هذا التصعيد، كافحت الكيانات العامة والخاصة في الولايات المتحدة لتأمين أنظمتها، حيث تزايدت وتيرة الأنشطة السيبرانية الضارة التي يشنها الخصوم؛ مما يفاقم تحديات حماية وتعزيز مرونة شبكاتها وأنظمتها ووظائفها وبياناتها، فضلاً عن اكتشاف الحوادث السيبرانية

والاستجابة لها والتعافي منها⁽⁴⁹⁾. وقد أعطت كل من الصين والولايات المتحدة الأولوية لبرنامج الحد من تهديدات الفضاء السيبراني.

إن الحرب السيبرانية بين الولايات المتحدة والصين تتسم بتعقيداتها المتزايدة وتوسعها لتشمل مجالات متعددة تتجاوز التجسس التقليدي أو الهجمات التقنية. فقد أصبحت هذه الحرب ميداناً استراتيجياً للصراع على النفوذ العالمي والتحكم في الفضاء السيبراني الذي يمثل أحد أهم مجالات القوة في القرن الحادي والعشرين. 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. في المقابل، تعمل الولايات المتحدة على تطوير أدوات هجومية تمكنها من اختراق الأنظمة الصينية وتعطيل عملياتها، مع التركيز على تقنيات الذكاء الاصطناعي لتحسين قدراتها في التصدي للهجمات السيبرانية، كما تسعى واشنطن إلى تعزيز التعاون مع حلفائها لبناء منظومة دفاع سيبرانية مشتركة، وهو ما تعتبره الصين تهديداً مباشراً لاستقلاليتها السيبرانية وسياساتها القائمة على السيادة الرقمية.

ومن جانب آخر، يبرز الدور المتزايد للشركات التكنولوجية الكبرى في الحرب السيبرانية، حيث تتعرض شركات مثل (Google) و (Microsoft) لضغوط من الحكومتين الأمريكية والصينية على حد سواء؛ إذ تستخدم الصين أدواتها السيبرانية لتعزيز سيطرتها الداخلية ودعم صناعاتها التكنولوجية، بينما تدعو الولايات المتحدة هذه الشركات إلى تحسين دفاعاتها والعمل كحليف في مواجهة التهديدات السيبرانية العالمية.

ورغم التوترات المتصاعدة، يبقى هناك مجال للتعاون المحتمل بين البلدين في مجالات مثل مكافحة الجريمة السيبرانية العابرة للحدود، حيث يمكن للطرفين تبادل المعلومات والخبرات للحد من الأنشطة التخريبية التي تهدد الاقتصاد العالمي. إلا أن هذا التعاون يظل محدودًا بسبب تضارب المصالح وانعدام الثقة المتبادل بين الجانبين⁽⁵⁰⁾.

أما على الصعيد القانوني، فقد أثارت الولايات المتحدة والصين خلافات حول قواعد السلوك في الفضاء السيبراني، حيث تدعو واشنطن إلى تبني معايير دولية قائمة على الانفتاح والشفافية، بينما تفضل بكين سياسات أكثر صرامة تركز على السيادة الوطنية، وهذا التباين يزيد من تعقيد المشهد السيبراني، ويجعل من الصعب التوصل إلى توافق عالمي حول تنظيم الفضاء السيبراني⁽⁵¹⁾.

وفي ظل هذه التحديات، تسعى الولايات المتحدة إلى تعزيز استراتيجيتها السيبرانية من خلال مبادرات مثل «الاستراتيجية الوطنية لحماية الفضاء السيبراني»، التي تركز على تعزيز القدرات الوطنية والدفاعية ضد الهجمات، فضلاً عن تطوير شراكات دولية لتنسيق الجهود المشتركة في التصدي للتهديدات السيبرانية. ومن جهتها، تعمل الصين على تعزيز موقعها كقوة سيبرانية عالمية من خلال تطوير تقنيات مستقلة وإطلاق مبادرات مثل «الغطاء الذهبي» لتعزيز سيطرتها على الإنترنت. وقد أسهمت هذه الجهود في تقوية بنيتها التحتية السيبرانية وزيادة اعتمادها على حلول تكنولوجية محلية؛ مما يضعها في موقف أقوى للتنافس مع الولايات المتحدة⁽⁵²⁾.

وتبقى حدود الحرب السيبرانية بين البلدين غير واضحة، حيث يتشابك فيها الجانب التقني مع الجوانب الاقتصادية والسياسية، ومع تصاعد التوترات، يبدو أن الحرب السيبرانية ستظل ساحة مواجهة طويلة الأمد، تتطلب حلولاً مبتكرة وإطاراً دولياً ينظم هذا النوع من الصراعات بما يضمن الأمن والاستقرار العالمي⁽⁵³⁾.

المصادر:

1. شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 1، 2022.
2. إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شئونها في عصر الإنترنت «الولايات المتحدة نموذجاً» (القاهرة: دار العربي للنشر، الطبعة الأولى، 2017) ص. 135.
3. زينب شتوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، المجلة الجزائرية للأمن والتنمية، المجلد 9، العدد 2، 2020.
4. كريم أوراغ، الاختراق الإلكتروني في الفضاء السيبراني وأفضل الطرق للحماية منه، مجلة التطوير العلمي للدراسات والبحوث، المجلد 2، العدد 4، 2021، ص. 71.
5. بهاء الصابري، الحروب الإلكترونية: اللاتماثل في التهديد، مجلة الأزمات والبحوث السياسية، العدد 2، 2017، ص. 63.
6. غريب حكيم، الإرهاب السيبراني الأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، المجلد 5، العدد 2، 2018.
7. Comprehensive Plan for the Organizational Structure of the U.S. Space Force, **Report to Congressional Committee**, 2020.
8. The criticism concerns inadequate resources: A focus on procedure and reporting rather than operational security, and insufficient means to enforce compliance both within and across agencies, 2019, p. 44.
9. فاع حارك، الدولة والهيمنة وتحقيق الأمن في الفضاء السيبراني، المجلة الجزائرية للأمن الإنساني، المجلد 2، العدد 1، 2021.
10. The White House, Cybersecurity: The progress report of the action items is available at The White House, **National Security Council**, Cybersecurity Progress after, 2020, p. 18.
11. إيهاب خليفة، حروب مواقع التواصل الاجتماعي (القاهرة: دار العربي للنشر والطباعة، الطبعة الأولى، 2016) ص. 133.
12. سامي بونيف، دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية: الردع السيبراني أنموذجاً، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 4، العدد 7، 2019.
13. شادي منصور، حروب الجيل الخامس: أساليب «التفجير من الداخل» على الساحة الدولية (الإمارات: مركز المستقبل للأبحاث والدراسات المتقدمة، 2019).
14. سيد محمد، صراع الأمم وحروب الجيل الخامس، وكالة الصحافة العربية، 2019.
15. سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي: الولايات المتحدة الأمريكية أنموذجاً، رسالة ماجستير، جامعة محمد بوضياف - المسيلة، الجزائر، 2018.
16. رياض بن عربية، التهديدات اللاتماثلية في الفضاء السيبراني: حروب الجيل الرابع أنموذجاً، مجلة دفاتر البحوث العلمية، المجلد 10، العدد 1، 2022، ص. 36.
17. القرصنة الحاسوبية الأخلاقية تُعرف أحياناً باسم اختبار الاختراق (Penetration Testing)، وهي عملية منظمة يقوم بها خبراء في أمن المعلومات نيابة عن مالكي الأنظمة وبإذن منهم. وتهدف إلى اكتشاف التهديدات أو نقاط الضعف في الأنظمة أو الشبكات التي قد يستغلها مهاجمون خبيثون، مما قد يتسبب في فقدان البيانات أو خسائر مالية أو أضرار أخرى. تسعى هذه العملية إلى تحسين أمان الأنظمة من خلال تحديد الثغرات وإصلاحها أثناء الاختبار. ويستخدم القراصنة الأخلاقيون الأدوات والأساليب نفسها التي يعتمد عليها قراصنة الحاسوب الخبيثون، ولكن بهدف تعزيز الأمان وحماية الأنظمة بدلاً من الإضرار بها.
18. حازم منيخر، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى: الولايات المتحدة الأمريكية وروسيا الاتحادية أنموذجاً، رسالة ماجستير، كلية العلوم السياسية، جامعة النهرين، العراق، 2020، ص. 85.
19. Charles G. Billo & Welton Chang, **Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States**, Dartmouth College, Institute for Security Technology Studies, 2004, p. 30.
20. Amy Chang, **Warring State: China's Cyber Security Strategy** (Washington: Center for a New American Security, 2014) p. 9.
21. مايكل إس تشايس & آرثر تشان، نهج الصين المتطور إزاء الردع الإستراتيجي المتكامل (كاليفورنيا: مؤسسة راند، 2016) ص. 32.
22. Charles G. Billo, and Welton Chang, Op.cit, 2004, p. 25, p. 40.
23. خالد ساسوي، الحروب السيبرانية والأمن العالمي: التحديات والمواجهة، رسالة ماجستير، جامعة زيان عاشور - الجلفة، الجزائر، 2020.
24. Hanan Abbas Salman & Ibtisam Kazem Jassim, Cyber Power and Its Impact on Economic Power: China as an Example, **Journal of the Kufa Studies Center**, Vol. 1, 2023, p. 12.
25. Hauke Johannes Gierow, **Cyber Security in China: Internet Security, New Challenges to Western Businesses** (Mercator Institute for China Studies, 2015) pp. 1-10.

26. Nigel Inkster, **China's Cyber Power** (Taylor & Francis, 2018) p. 156.
27. فريدة طاجين & فاطمة عوامر، تأثير القوة السيبرانية على الإستراتيجيات الأمنية للدول الكبرى: دراسة حالة الصين، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرياح ورقلة، 2018.
28. Min Jiang, Cybersecurity Policies in China, In Cyber BRICS, 2021.
29. China Securities Regulatory Commission, **Cybersecurity Law of the People's Republic of China**, 2017.
30. علي موسى الكنتاني، الأمن السيبراني في العلاقات الأمريكية - الصينية، صحيفة الزمان اليومية، 2020، ص. 1.
31. فراس جمال شاكر، السيبرانية وتحولات القوة في النظام الدولي، رسالة دكتوراه، معهد العلمين للدراسات العليا، العراق، 2021، ص. 143.
32. مرعي الرمحي، الحرب السيبرانية ومتطلبات الأمن القومي الجديدة (ألمانيا: المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، 2022) ص. 45.
33. Tom Ramstack, Congress to Investigate Google Charges of Chinese Internet Spying, 2010, pp. 1-2.
34. Kim Zetter, **Operation "Aurora" Hit Google**, Others by George Kurtz, 2010, pp. 1-2.
35. سوران بنديان، دور القوة الذكية في إدارة الأزمات الدولية (عمان: الأكاديميون للنشر والتوزيع، 2020) ص. 123.
36. إيهاب خليفة، الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس (القاهرة: العربي للنشر والتوزيع، 2020) ص. 43.
37. عبد القادر دندن، العلاقات الدولية في عصر التكنولوجيات الرقمية تحولات عميقة، مسارات جديدة (الأردن: مركز الكتاب الأكاديمي، 2021).
38. أحمد يوسف كيطان، استراتيجية الأمن الوطني السيبراني للصين: قراءة في قانون الأمن السيبراني الصيني (مركز النهرين للدراسات الاستراتيجية، 2019) ص. 2.
39. بيتر سيل، الكون الرقمي الثورة العالمية في الاتصالات (مؤسسة هندواي سي أي سي، 2021) ص. 141.
40. طارق الطائي، الأمن الدولي في القرن الواحد والعشرون (ماهيته، مقترباته الفكرية العالمية، تحدياته غير التقليدية، وأفاقه المستقبلية) (دار الأكاديميون للنشر والتوزيع، 2021)
41. مركز الحضارة للدراسات والبحوث، السيبرانية: واقع وتحولات (القاهرة: مركز الحضارة للدراسات والبحوث، 2022) ص. 540.
42. علي زياد العلي & علي حسين حميد، تكتيكات الحروب الحديثة: الأمن السيبراني والحروب المعززة والهجنة (القاهرة: العربي للنشر والتوزيع، 2022) ص. 304.
43. إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 1، 2021.
44. إناس ممدوح، دور الأمن السيبراني في مواجهة الإرهاب الإلكتروني، مجلة العلوم القانونية والاقتصادية، المجلد 64، العدد 1، 2022.
45. منال البلقاسي، تأمين التهديدات السيبرانية تحت المجهر الرقمي (البيكان للنشر، 2024) ص. 264.
46. Ellen Nakashima, U.S. Cyberwarfare Force To Grow Significantly, Defense Secretary Says, **The Washington Post**, 2014.
47. صفاء التميمي، توظيف القوة السيبرانية في الأداء الاستراتيجي الأمريكي، كلية العلوم السياسية، جامعة النهرين، العراق، 2021.
48. زياد العتيبي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها، خصائصها، أركانها والدوافع من ارتكابها، المجلة الأكاديمية العالمية للدراسات القانونية، المجلد 3، العدد 1، 2020.
49. Anastasios Arampatzis, Cybersecurity | Information Security Content Writer, **Air Force Academy**, Engineering Faculty, 2019.
50. فاطمة بيرم، مرجع سبق ذكره.
51. نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الإنساني. مجلة النقدية للقانون والعلوم السياسية، المجلد 16، العدد 4، 2021، ص. 2.
52. فاطمة بيرم، مرجع سبق ذكره.
53. وفاء عبد الواحد، الإرهاب الإلكتروني والأمن القومي في ظل جائحة كورونا (كوفيد-19)، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، المجلد 7، العدد 13، 2022.

"حروب التجسس": أبعاد وتداعيات التجسس السيبراني الصيني على الدول الأوروبية

الشيمااء عرفات*

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.

* باحث أول بوحدة الدراسات الأوروبية، بالمركز المصري للفكر والدراسات الاستراتيجية

بالرغم من أن الولايات المتحدة هي الهدف الأكثر أهمية للصين، فإن هذا لم يمنعها من التجسس على القوى الأوروبية وبخاصة الأكثر تقدمًا منها، حتى أصبحت هي العنصر الأكثر نشاطًا بجانب روسيا في التجسس على الدول الأوروبية. ولكن ما يفسر تراجع الاهتمام بهذا الأمر جملة من الأسباب التي انعكست أيضًا على قلة الدراسات الرصينة الساعية للتعاطي مع التجسس الصيني على الدول الأوروبية، وهي: قلة التصريحات الأوروبية عن عمليات التجسس الصينية مقارنة بالولايات المتحدة، حيث تفضل القوى الأوروبية وبخاصة ألمانيا خفض التصعيد مع الصين بسبب الترابط التجاري بينهما. هذا إلى جانب تراجع الاهتمام الأوروبي بالأمن السيبراني نسبيًا وبالمقارنة بالاهتمام الأمريكي بهذا المجال، ولا سيما في ظل ريادتها؛ مما يجعل الجانب الأمريكي أكثر قدرة على مواجهة واحتواء وتتبع مصادر التجسس السيبراني مقارنة بغيره من القوى. ناهيك بالتراجع النسبي في مستوى الوعي السيبراني على مستوى الجهات الرسمية سواء الحكومية أو البرلمانية الأوروبية نسبيًا، وبالمقارنة بالولايات المتحدة، وهو ما أسفر عن التراجع النسبي في الاهتمام بتداعيات التجسس السيبراني وبخاصة الصيني بالمقارنة بالجانب الأمريكي.

وعليه، فإن هذا الفصل يسعى لتغطية هذا الجانب الذي لم يلق الكثير من الاهتمام البحثي، وهذا من خلال تتبع أبرز عمليات التجسس السيبراني التي تم الكشف عنها، والتي كان أغلبها في العام الجاري، ومحاولة توضيح الأهداف وراء التجسس السيبراني الصيني على الدول الأوروبية، وما سيؤول له هذا التصعيد المتنامي في توجيه الاتهامات للصين مؤخرًا من قبل الدول الأوروبية على العلاقات بينهم.

أولاً: التجسس السيبراني

يشير التجسس السيبراني إلى الوصول غير المصرح به إلى الأنظمة أو الأجهزة للحصول على المعلومات، وكذلك الهندسة الاجتماعية للأشخاص الذين لديهم حق الوصول المصرح به إلى الأنظمة أو الأجهزة للحصول على المعلومات⁽¹⁾. وبالرغم من تشابه أهداف كل من التجسس التقليدي والسيبراني، فإن الأخير يتميز بسهولة، واستغلاله للفضاء الواسع للإنترنت عالميًا، بما يمكن من ممارسونه من نكران مسئوليتهم.

ويستخدم التجسس السبراني - في المقام الأول - كوسيلة لجمع البيانات الحساسة أو السرية أو الأسرار التجارية أو أشكال أخرى من الملكية الفكرية التي يمكن للمعتدي استخدامها لخلق ميزة تنافسية أو بيعها لتحقيق مكاسب مالية. في بعض الحالات، يهدف الاختراق إلى إلحاق ضرر بسمعة الضحية من خلال الكشف عن معلومات خاصة أو ممارسات تجارية مشكوك فيها. وقد تكون هجمات التجسس السبراني مدفوعة بالمكاسب المالية، كما يمكن توظيفها بالتزامن مع العمليات العسكرية أو كعمل من أعمال الإرهاب السبراني أو الحرب السبرانية. هذا، ويمكن أن يؤدي تأثير التجسس السبراني، وخاصة عندما يكون جزءاً من حملة عسكرية أو سياسية أوسع نطاقاً إلى تعطيل الخدمات العامة والبنية الأساسية، فضلاً عن خسارة الأرواح.

والجدير بالذكر أن تقرير التهديدات العالمية لعام 2024 يكشف عن ارتفاع مثير للقلق في الأنشطة السرية ومشهد التهديدات السبرانية الذي يهيمن عليه التخفي. إذ تزداد سرقة البيانات واختراقات السحابة والهجمات الخالية من البرامج الضارة، ولا سيما في ظل تعدد الأهداف المحتملة للتجسس السبراني لتشمل الشركات الكبرى والوكالات الحكومية والمؤسسات الأكاديمية ومراكز الفكر والمنظمات الأخرى التي تمتلك بيانات تقنية قيمة يمكن أن تخلق ميزة تنافسية لمنظمة أو حكومة أخرى. كما يمكن أيضاً شن حملات مستهدفة ضد الأفراد، مثل القادة السياسيين البارزين والمسؤولين الحكوميين والمديرين التنفيذيين للشركات وحتى المشاهير.

هذا، ويحاول جواسيس الإنترنت في أغلب الأحيان الوصول إلى الأصول التالية: بيانات وأنشطة البحث والتطوير، وبيانات البحث الأكاديمي، والمعلومات الحساسة المتعلقة بتمويل المنظمة ونفقاتها، وقوائم العملاء أو الزبائن وهياكل الدفع، وأهداف العمل والخطط الاستراتيجية وتكتيكات التسويق، والاستراتيجيات السياسية والاتصالات، والاستخبارات العسكرية. ولذا، تُصنف معظم أنشطة التجسس السبراني بأنها تهديد مستمر متقدم ومستدام؛ حيث يخلق المتسلل شكلاً من أشكال الوجود غير المكتشف في شبكة ما، من أجل سرقة بيانات حساسة على مدى فترة طويلة من الزمن. ويتم التخطيط لتلك الهجمات بعناية للتسلل إلى منظمة معينة

والتهرب من تدابير الأمن الحالية لفترات طويلة من الزمن. لذا، يتطلب تنفيذ ذلك درجة أعلى من التخصيص والتعقيد مقارنة بالهجوم التقليدي.

تتضمن معظم هجمات التجسس السيبراني أيضًا شكلاً من أشكال الهندسة الاجتماعية لتحفيز النشاط أو جمع المعلومات اللازمة من الهدف من أجل المضي قدماً في الهجوم. غالباً ما تستغل هذه الأساليب المشاعر البشرية مثل الإثارة أو الفضول أو التعاطف أو الخوف للتصرف بسرعة أو بتهور. وبذلك، يخدع مجرمو الإنترنت ضحاياهم لإقناعهم بالتخلي عن معلومات شخصية أو النقر فوق روابط ضارة أو تنزيل برامج ضارة أو دفع فدية⁽²⁾.

ثانياً: أبرز حالات التجسس السيبراني الصينية المعلنة على أوروبا

في هذا القسم، سيتم استعراض حالات التجسس السيبرانية الصينية الأبرز على الدول الأوروبية، وقد كان من الملاحظ أن السنة الأخيرة شهدت مزيداً من التصريحات الأوروبية المتعلقة بتلك الحالات بشكل أكثر تواتراً عن ذي قبل.

وبشكل عام، يمكن توضيح أبرز تلك الحالات المعلنة والتي تتبعها مركز الدراسات الاستراتيجية والدولية (CSIS)⁽³⁾ على النحو التالي:

- نوفمبر 2024: وجد المركز الوطني للأمن السيبراني في المملكة المتحدة زيادة قدرها ثلاثة أضعاف في الهجمات السيبرانية الأكثر أهمية مقارنة بالعام الماضي. وقد أدرج الصين وروسيا وإيران وكوريا الشمالية على أنها «تهديدات حقيقية ودائمة».
- يوليو 2024: اتهمت ألمانيا الصين بتوجيه هجوم سيبراني «خطير» ضد المكتب الفيدرالي الألماني للرسم الخرائطي والمساحة (BKG)، الذي يُجري رسم خرائط دقيقة للبلاد بأكملها في عام 2021. وقد أتت النتائج في نهاية تحقيق استمر ثلاث سنوات حول الحادث، وإن جاء الاتهام في الوقت التي تخطط فيه ألمانيا لمشروع يُسهّل استبدال البنية التحتية للاتصالات الصينية في ألمانيا بسبب المخاوف الأمنية.

- يوليو 2024: أصدرت المملكة المتحدة وألمانيا إلى جانب أستراليا والولايات المتحدة وكندا واليابان وكوريا الجنوبية ونيوزيلندا تحذيرًا بشأن النشاط السيبراني الخبيث الذي ترعاه الدولة الصينية.
- مايو 2024: هاجم قراصنة صينيون وزارة الدفاع البريطانية بهجوم سيبراني كشف عن معلومات مصرفية عن كل القوات باستثناء القوات الخاصة البريطانية. ولم يقوم وزير الدفاع البريطاني علنًا بتسمية الصين باعتبارها الجاني، إلا أنه تتردد على لسان عدد من السياسيين البريطانيين إشارات تتهم الصين التي سارعت لنفي تلك الاتهامات. وإن وجهت في 25 مارس 2024 حكومة المملكة المتحدة لومًا إلى الصين بسبب سلسلة من الهجمات السيبرانية على مؤسساتها. وقد قال نائب رئيس الوزراء حينها «أوليفر دودن» إن «جهات تابعة للدولة الصينية كانت وراء هجومين خبيثين منفصلين على هيئة مراقبة الانتخابات البريطانية ومشرعين بريطانيين»⁽⁴⁾. وبعد أيام، من هذا التصريح، اتهمت وزارة العدل الأمريكية الصين باستهداف عشرات المشرعين الأوروبيين في هجمات سيبرانية منذ عام 2021. وقالت الولايات المتحدة إن قراصنة صينيين مرتبطين بوزارة أمن الدولة (وهي الوزارة المعنية بالنشاط الاستخباراتي في الصين) هاجموا كل عضو في التحالف البرلماني الدولي بشأن الصين (IPAC)، وهو تحالف من المشرعين الأوروبيين المنتقدين لبكين. ومن بين الأهداف كان وزير الخارجية التشيكي ورئيس الوزراء البلجيكي السابقين ومجموعة من سبعة مشرعين فرنسيين.
- فبراير 2024: تم الكشف عن قيام جواسيس صينيين بوضع برامج ضارة في شبكة عسكرية هولندية في عام 2023. وكانت هذه هي المرة الأولى التي تتهم فيها هولندا الصين علنًا بالتجسس السيبراني. وقد سبق هذا الإعلان تحذير الوكالات المعنية بالاستخبارات الهولندية من الهجمات السيبرانية الصينية. فقد وصفت دائرة المخابرات والأمن الهولندية العامة الصين بأنها «أكبر تهديد للأمن الاقتصادي الهولندي»⁽⁵⁾.
- أكتوبر 2023: حذر جهاز المخابرات البريطاني (MI5) من أن أكثر من 20 ألف شخص في المملكة المتحدة قد تلقوا اتصالات من قبل جواسيس صينيين سرًا عبر الإنترنت. وحذرت الوكالة كذلك من أن عشرات الآلاف من الشركات البريطانية معرضة لخطر سرقة ابتكاراتها.

- مارس 2023: حظرت الحكومة البريطانية تطبيق «تيك توك» الصيني من الأجهزة والهواتف الحكومية لأسباب أمنية، وتبعها البرلمان البريطاني، حيث حرم نوابه من الوصول للتطبيق عبر شبكة الإنترنت الخاصة به. وقد أرجعت بريطانيا هذه الخطوة إلى أن الأمن السيبراني بات مهددًا بسبب الاختراقات من بعض الدول والشركات التي تعمل لحساب الصين. تلك الخطوة التي اتخذتها عدد من الدول الأوروبية الأخرى كبلجيكا والدانمارك وهولندا وفرنسا والنرويج بالإضافة لمؤسسات الاتحاد الأوروبي التي فرضت على موظفيها وأعضاء البرلمان الأوروبي حظرًا على استخدامه في أثناء عملهم، وأصدرت تعميمًا بتفضيل حذف البرنامج من الأساس⁽⁶⁾.
- في فبراير 2023: نبّهت وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) وفريق الاستجابة لحالات الطوارئ الحاسوبية التابع للاتحاد الأوروبي (CERT-EU) المجتمع الدولي من أن العديد من مجموعات القرصنة العسكرية الصينية قد كثفت استهداف الشركات والمنظمات في الاتحاد الأوروبي⁽⁷⁾.

ثالثًا: دلالات التجسس السيبراني الصيني على أوروبا

يُعد التجسس السيبراني شكلًا من أشكال التجسس الذي أصبح معروفًا ومعتمدًا لدى العديد من الدول؛ لتحقيقه عددًا من الأهداف المهمة التي أوضحها الباحث (Magnus Hjortdal) في دراسته⁽⁸⁾، حيث يبيّن دوافع الدول لامتلاك قدرات سيبرانية عدوانية، وهي:

1. العمل على ردع الدول الأخرى من خلال التسلل إلى بنيتها الأساسية الحيوية وشملها، وبهذا يكون الهجوم هو طريق الردع الرئيس.
2. محاولة تلك الدول اكتساب المزيد من المعرفة التكنولوجية، وبخاصة فيما يتصل بالمعلومات الحيوية المتصلة بالتطوير العسكري، بغرض امتلاك معرفة مضادة للقدرات العسكرية التي تملكها الدول الأخرى أو التجسس لامتلاك مختلف المعارف التي تساعد على دفع وتيرة تنميتها الاقتصادية.

3. القدرة على مهاجمة وشل القدرات العسكرية للخصم في أثناء المواجهة معه، إلا أن هذا السبب لا يتضح إلا في أثناء الصراع.

وقد جادل الكاتب بأن الصين التي تطمح لأن تكون القوة الأكبر في العالم بحلول 2049 في كل المجالات، في ضوء تلك الأسباب، قد تلجأ إلى تطوير قدراتها السيبرانية لأغراض التجسس وبقوة؛ بسبب سعيها للتعرف على التطور الغربي وبخاصة في المجال العسكري؛ بغرض تقليص الفجوة الكبيرة بينها وبين الغرب في هذا المضمار، وكذلك من أجل تحقيق ميزات اقتصادية من خلال التعرف على التطورات الصناعية التي تضمن للغرب تفوقه والاستفادة منها.

ونجد أن تلك الأهداف تتواءم مع ما أوضحه تحليل بيانات المستودع الأوروبي لحوادث الإنترنت (EuRepoC) الذي كشف أنه في الفترة ما بين عامي 2005 و2021 كان أكثر من 78٪ من الهجمات السيبرانية منسوبة إلى إحدى الجهات الصينية التي تهدف إلى سرقة البيانات (مقارنة بنسبة 60٪ لروسيا). وقد كانت المؤسسات الحكومية هي الأهداف الأكثر أهمية (بنسبة 32٪). وقد أوضح كذلك أن البنية التحتية الحيوية والمؤسسات التجارية والمؤسسات العلمية وصناعات الدفاع والطاقة والاتصالات وكذلك المؤسسات العسكرية هي العناصر المعرضة للجانب الأكبر من التهديدات الصينية بشكل متكرر. بالإضافة إلى ذلك، أوضح أن الهجمات الصينية كانت أكثر تواتراً وكثافة وقت الزيارات وأنشطة الاندماج والاستحواذ المخطط له للشركات الصينية؛ مما يبرر بشكل أكبر نسبها إلى الحكومة الصينية⁽⁹⁾.

ويجمع الخبراء على أن نشاطات التجسس الصيني تدور حول ثلاث أولويات رئيسية؛ وهي: تشكيل الاتجاهات السياسية والاقتصادية في البلدان المستهدفة بما يتماشى مع مصالحها، وجمع المعلومات عن الصناعات الحساسة، ومراقبة سكان الشتات، وبخاصة الأقليات مثل التبتيين والأويغور ومواطني هونغ كونغ⁽¹⁰⁾.

وفيما يتصل بجمع المعلومات عن الصناعات الحيوية والحساسة، تشير التقديرات إلى أن الصين مسؤولة عما يتراوح بين 50 - 80٪ من عمليات سرقة الملكية الفكرية في جميع أنحاء العالم⁽¹¹⁾. كما سبق وأن أصدر رئيس مكتب التحقيقات

الفيدرالي الأمريكي ورئيس جهاز الاستخبارات الداخلية البريطانية تحذيرات شديدة اللهجة لقادة الأعمال بشأن التهديدات التي يشكلها التجسس الصيني، وخاصة التجسس الذي يهدف إلى سرقة الملكية الفكرية لشركات التكنولوجيا الغربية من أجل تعزيز مصالحها والسيطرة على الصناعات الرئيسية⁽¹²⁾.

وفي هذا السياق، أوضحت وكالات الأمن الألمانية أن قرصنة الإنترنت الصينيين يأتون على قدم المساواة من حيث التهديد مع نظرائهم الروس، إلا أنها لاحظت أنهم لا يسعون للتخريب، خشية أن يجتذبوا انتباهًا غير مبرر. ولهذا فإن الهاكرز الصينيين يدخلون الأنظمة خلسة، ويبقون هناك لعدة سنوات، ويجمعون معلومات حساسة. وهو يتوافق مع أوردته مجلة «شبيجل» من أن العديد من الشركات المدرجة في مؤشر الأسهم القيادية الألماني «داكس» كانت هدفًا لهجمات سببرانية صينية. ووفقًا أيضًا لاستطلاع أجراه «معهد ميركاتور لدراسات الصين» (MERICS)، وهو مؤسسة بحثية ألمانية، صرحت 730 منظمة من بين أكثر من 1000 منظمة أوروبية بأنها كانت هدفًا لهجمات سببرانية في العام السابق. وقد أكد 42٪ منهم أن هجومًا واحدًا على الأقل كان صينياً. ووجد التقرير أن العديد من الجهات التي تم استهدافها تتوافق مع «الأهداف الاستراتيجية للحكومة الصينية»، وخلصت مؤسسة الأبحاث إلى وجود «خطر على ازدهار أوروبا على المدى الطويل» من عمليات الاختراق الصينية⁽¹³⁾.

أما فيما يتعلق بالهدفين الآخرين، فقد بينت «تريزا فالون»، وهي محللة وكاتبة وعضو في مجلس التعاون الأمني في منطقة آسيا والمحيط الهادئ، ومديرة مركز دراسات روسيا وأوروبا وآسيا في بروكسل، في تقرير نشرته مجلة «ناشيونال إنترست» (The National Interest) الأمريكية⁽¹⁴⁾، أن أحد الأهداف الرئيسية لعمليات النفوذ الصينية في أوروبا هو الاستقطاب الاستبدادي، الذي يتمثل في إقناع الشخصيات العامة الأوروبية بأن يكون لديها تقدير إيجابي للحزب الشيوعي الصيني والتحدث بشكل إيجابي عن سياساته الداخلية والخارجية. ويتبع ذلك دعوة هؤلاء البدلاء - أصحاب التفكير المماثل للتحدث كوكلاء لتعزيز مواقف الحزب الشيوعي الصيني.

وفي هذا السياق، يمكن الإشارة إلى آخر تلك القائمة من الأطراف المستهدفة، ففي إبريل 2024، أعلنت النيابة العامة في برلين عن توقيف المتهم «جيان غو»، المقيم في مدينة دريسدن في شرق ألمانيا، وهو أحد مساعدي النائب في البرلمان الأوروبي «ماكسيميليان كراه» منذ عام 2019، للاشتباه في قيامه بتبادل معلومات من داخل البرلمان الأوروبي مع الاستخبارات الصينية، إضافةً إلى التجسس على معارضين صينيين مقيمين في ألمانيا. واتهم الادعاء الألماني «غو» بأنه «عنصر في الاستخبارات الصينية»، كان قد أسهم في نقل معلومات في مناسبات عدة خلال يناير 2024 بشأن مفاوضات وقرارات البرلمان الأوروبي إلى موكله في جهاز الاستخبارات، كما قام بالتجسس على معارضين صينيين في ألمانيا لصالح جهاز الاستخبارات الصيني. كما بدأ المدعون العموم تحقيقات أولية مع «كراه» بشأن مدفوعات مزعومة من مصادر موالية لروسيا والصين، وإن نفى ارتكابه أي مخالفات بالرغم من مواقفه الداعمة المتكررة للمصالح الصينية في جلسات البرلمان الأوروبي. وقد علق المستشار الألماني آنذاك «أولاف شولتس» على تلك الحالات بأنها مقلقة للغاية، وتتطلب إجراءات للتصدي لها، مشددًا على رفضه لمحاولات التجسس على بلاده.

أما الهدف الرئيسي الآخر للحزب الشيوعي الصيني، فهو السيطرة على الأشخاص من أصول صينية داخل جمهورية الصين الشعبية وخارجها. وقد قالت «فالون»: إن الحزب الشيوعي الصيني - للسيطرة على الصينيين في الخارج - أنشأ شبكة عالمية من مراكز الشرطة السرية في 53 دولة في جميع أنحاء العالم. ويتم استخدام هذه المراكز أيضًا لمراقبة سلوك الصينيين في الشتات، وبصفة خاصة مجموعات الأقليات، مثل الإويغور الذين ينتمون إلى إقليم التبت ومنطقة هونج كونج، بهدف منع النشاط المعادي.

وما يزيد من تعقيدات التجسس الصيني على الدول الأخرى هو تقنين هذا التجسس⁽¹⁵⁾؛ فوفقًا للتشريعات الصينية المتعلقة بالأمن القومي، يفرض قانون الأمن القومي لعام 2015 لجمهورية الصين الشعبية على المواطنين والمنظمات تقديم الدعم والمساعدة لأجهزة الأمن العام أو أمن الدولة أو العسكرية في جمهورية الصين الشعبية. كما أقرت بكين في 2017 قانونًا أساسيًا للخدمة السرية⁽¹⁶⁾ يتضمن

إلزام أي منظمة أو مواطن صيني بالتعاون مع الاستخبارات بموجب هذا القانون؛ مما يجعل أي تعاون صيني في أي شكل سواء رسمي أو حتى على مستوى الأفراد تهديدًا محتملاً للأطراف المتعاملة معه.

وعليه، فإن التجسس السيبراني الصيني سيظل قائمًا، ومن الصعب توقع تراجع، نظرًا لأن الأسباب الدافعة له والتي تم استعراضها لا تزال قائمة. ولكن سيظل واقع الإعلان عنها محكومًا بحجم التقارب والتباعد في العلاقات بين الجانبين الصيني والأوروبي.

رابعًا: تداعيات التجسس الصيني على العلاقات الأوروبية-الصينية

بعد استعراض دوافع وأشكال التجسس السيبراني الصيني على أوروبا، سنناقش المآلات المحتملة للتجسس الصيني على العلاقات الأوروبية-الصينية. فقد بدا المشهد وكأن الاتحاد الأوروبي قد بدأ في تبني نهج أكثر تشددًا تجاه الصين. فبنهاية أكتوبر 2024، فرضت المفوضية الأوروبية على الصين تعريفات جمركية على السيارات الكهربائية الصينية على غرار كندا والولايات المتحدة اللتين فرضتا تعريفات تصل إلى 100٪، إلا أن الاتحاد الأوروبي فرض رسومًا تتراوح بين 7,8٪ إلى 35,3٪، بالإضافة إلى رسوم استيراد السيارات التي يفرضها الاتحاد الأوروبي والتي تصل إلى 10٪، إلا ألمانيا التي تُعد أكثر الدول تضررًا وإعلانًا عن حالات التجسس الصينية في الآونة الأخيرة كما سبق القول، كانت واحدة من الدول الخمس من أصل 27 دولة التي اعترضت على القرار، وهو ما يرجع لتخوفها من رد فعل انتقامي من الصين على استيراد السيارات الألمانية؛ حيث يعد السوق الصيني أكبر سوق لها⁽¹⁷⁾. وفي السياق ذاته، صوتت الدول الأخرى صاحبة المصلحة في التهدة مع الصين بالرفض. فاعتبارًا من أكتوبر 2024، كان هناك ثلاثة مصانع بطاريات صينية في ألمانيا، ومصنع للسيارات الكهربائية في بولندا، ومصنعان للسيارات الكهربائية واثنان آخران للبطاريات في المجر، ومصنع للسيارات الكهربائية في إسبانيا. ومن المقرر أن تضخ الصين المزيد من الاستثمارات في تلك البلدان⁽¹⁸⁾، وهو ما انعكس على تصويتها.

ويُعَدُّ الموقف الألماني محوريًا في تحديد اتجاه العلاقات الخارجية الأوروبية، فهي القوة الاقتصادية الأكبر بالاتحاد الأوروبي، وصاحبة النفوذ الأكبر به. فقد اعتمدت ألمانيا استراتيجية تجاه الصين هي تلك التي أطلقتها في يوليو 2023، موضحة فيها كيف ستجنح في تقليل اعتمادها على الصين وبخاصة في القطاعات الحرجة مبررة ذلك بتغير سلوك الصين دوليًا⁽¹⁹⁾. وقبل ذلك، صدر تقرير عن وكالة المخابرات الألمانية أوضح أن الصين تعتبر «أكبر تهديد فيما يتعلق بالتجسس الاقتصادي والعلمي والاستثمارات الأجنبية المباشرة في ألمانيا». وفي الشهر نفسه الذي صدرت فيه الاستراتيجية الألمانية تجاه الصين، حذرت وكالة التجسس العسكرية الألمانية من أن روسيا والصين تعززان أنشطة التجسس في البلاد معتبراً أن الصين وروسيا هما اللاعبان الأكثر نشاطًا في مجال التجسس في البلاد⁽²⁰⁾. إلا أن هذا لم ينعكس على سلوكها وعلاقاتها مع الصين؛ فقد تداول الجانبان سلعة بقيمة 254,2 مليار يورو في عام 2023 وفق المكتب الإحصائي الفيدرالي (Destatis) الألماني، الذي أفاد كذلك بأن جمهورية الصين الشعبية كانت هي الشريك التجاري الأكثر أهمية لألمانيا في عام 2023 للعام الثامن على التوالي، تليها الولايات المتحدة، بحجم تجارة بلغ 252,5 مليار يورو، ثم هولندا في المركز الثالث بحجم تجارة خارجية بلغ 214,8 مليار يورو⁽²¹⁾.

ويتسق المشهد في ألمانيا مع مجمل أوضاع التبادل التجاري بين الصين والاتحاد الأوروبي. ففي عام 2023، تداول الاتحاد الأوروبي والصين سلعة بقيمة 739 مليار يورو (واردات وصادرات). ويمثل هذا 15٪ من إجمالي تجارة الاتحاد الأوروبي من السلع. وبالرغم من حصة الولايات المتحدة التي بلغت حوالي 17٪، فإنه وبالمقارنة بعام 2000، قد انخفضت نسبة التجارة مع الولايات المتحدة بشكل كبير، في حين تضاعفت حصة الصين من تجارة الاتحاد الأوروبي ثلاث مرات تقريباً من 5٪ إلى 15٪⁽²²⁾. إلا أنه بالمقارنة بعام 2022، فإن هذا التبادل بين الجانبين الأوروبي والصيني مثل انخفاضاً بنسبة 14٪⁽²³⁾. ولكن في ظل إدارة أمريكية مرتقبة متشددة تجاه الصين والاتحاد الأوروبي، والتي سبق أن اتخذت من التعريفات الجمركية وسيلة أساسية لتعزيز اقتصادها، فقد يؤدي ذلك إلى تعميق التعاون بين الجانبين الأوروبي والصيني لتعويض الخسائر المحتملة، ما لم يتدخل الجانب الأمريكي بتهديد أمني للقارة الأوروبية يفوق تأثيره تداعيات الخسائر الاقتصادية المحتملة.

في المقابل، فإن الموقف البريطاني الأكثر تشددًا وتصريحًا بالعداء مع الصين قد انعكس على حجم التبادل التجاري بين البلدين، بما قد يؤدي إلى استمرار التدهور في العلاقات بين البلدين. ففي العام الحالي فقط، انخفض التبادل التجاري لما يصل إلى 20٪، ولكن يظل التبادل التجاري بينهما كبيرًا، حيث وصل لما يقرب من 88 مليار جنيه استرليني بنهاية الربع الثاني لعام 2024، وهو ما جعل الصين خامس أكبر شريك تجاري للمملكة المتحدة بنسبة تصل إلى 5٪ من إجمالي تجارتها الدولية⁽²⁴⁾، ولكن حجم التراجع ينذر بقدرة البلدين على تعميق هذا التراجع والقدرة على الاستمرار به.

ختامًا، 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؛ مما 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.

المصادر:

1. Cyber Risk GmbH, From Espionage to **Cyber Espionage**, Cyber-espionage, Available at: <https://www.cyber-espionage.ch/>
2. Kurt Baker, What is Cyber Espionage?, **Crowdstrike**, February 28, 2023, Available at: <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/>
3. **Significant Cyber Incidents, CSIS**, Available at: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>
4. Timeline: Europe under cyber siege in 2024, **Politico**, 8-5-2024, Available at: <https://www.politico.eu/article/europe-cyberattacks-russia-china-uk-ministry-of-defence-hacks/>
5. Stu Sjouwerma, Dutch Intelligence Agencies Warn About Chinese and Russian **Cyber Espionage**, 21-11-2023, Available at: <https://blog.knowbe4.com/dutch-intelligence-agencies-warn-about-chinese-and-russian-digital-cyber-espionage>
6. Kelvin Chan, These countries have already banned TikTok, **PBS News**, 26-4-2024, Available at: <https://www.pbs.org/newshour/world/these-countries-have-already-banned-tiktok>
7. Svenja Meike Kirsch and Bethan Saunders, Addressing Russian and Chinese Cyber Threats: A Transatlantic Perspective on Threats to Ukraine and Beyond, **Belfer Center for Science and International Affairs**, Harvard Kennedy School, May 2023, pp. 37- 47.
8. Magnus Hjortdal, China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence, University of South Florida, **Journal of Strategic Security**, Vol. 4, No. 2, Summer 2011, pp. 3-4.
9. Antonia Hmaid, Here to stay: Chinese state-affiliated hacking for strategic goals, **Mercator Institute for China Studies**, 22-11- 2023, Available at: <https://merics.org/en/report/here-stay-chinese-state-affiliated-hacking-strategic-goals>
10. Amy Hawkins, 'Countries are now forced to confront it': Rise in Chinese espionage arrests alarms Europe, **The Guardian**, May 2024, Available at: <https://www.theguardian.com/world/article/2024/may/08/court-chinese-espionage-europe>
11. **Ibid**, p. 45.
12. الرابطة الدولية للخبراء والمحللين السياسيين، أبعاد الاتهامات الغربية للصين بممارسة أنشطة تجسس، 2022-11-8، متاح على: <https://apa-inter.com/post.php?id=5204#>
13. Ritu Sharma, China's 'Army Of Spies' Horrifies Germany; Report Cautions Against Massive Influx Of Chinese Students, **Eurasian Times**, 3-1-2024, Available at: https://www.eurasiantimes.com/china-cranking-up-espionage-activities-in-germany/#google_vignette
14. Theresa Fallon, Smokeless War: Europe is Getting "Boursicoted" by Beijing, **The National Interest**, Available at: 31-8- 2024, Available at: <https://nationalinterest.org/feature/smokeless-war-europe-getting-%E2%80%9Cboursicoted%E2%80%9D-beijing-212553>
15. Klemen Grošelj, REPORT on the security and defence implications of China's influence on critical infrastructure in the European Union, **Europarl**, 11-12-2023, Available at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0401_EN.html
16. المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، تجسس. واقع ومخاطر تجسس الصين على الأراضي الألمانية، 2024. متاح على: <https://shorturl.at/oU5ZL>
17. China decries new EU tariffs on its electric vehicles, **DW**, 30-10-2024, Available at: <https://www.dw.com/en/china-decries-new-eu-tariffs-on-its-electric-vehicles/a-70637630>
18. The EU's approach to tariffs on Chinese electric vehicles, **IISS**, Volume 30, Available at: https://www.iiss.org/globalassets/media-library---content-migration/files/publications/strategic-comments-delta/2024/sc-30-27-the-eus-approach-to-tariffs-on-chinese-electric-vehicles_corrected.pdf
19. ألمانيا تعتمد استراتيجية «أكثر حزمًا» في التعامل مع الصين، الشرق نيوز، 13-7-2032، متاح على: <https://shorturl.at/pliyc>
20. جاسم محمد، ألمانيا تكشف عن استراتيجية جديدة للتعامل مع الصين، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، 14-7-2032، متاح على: <https://shorturl.at/Jrijb>
21. The People's Republic of China is again Germany's main trading partner, **Statistisches Bundesamt (Destatis)**, Available at: <https://www.destatis.de/EN/Themes/Economy/Foreign-Trade/trading-partners.html>
22. Trade with China increasingly important, **Statistisches Bundesamt (Destatis)**, Available at: https://www.destatis.de/Europa/EN/Topic/Foreign-trade/EU_tradingPartner

23. European Commission, EU trade relations with China. Facts, figures and latest developments, **Policy Trade**, Available at: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/china_en.
24. Department for Business and Trade, Factsheet trade and investment between the UK and China, 22-11- 2024, p. 2, Available at: <https://assets.publishing.service.gov.uk/media/673e4dabb3f0df6d2ebaefaf/china-trade-and-investment-factsheet-2024-11-22.pdf>

”حروب الظل“ : حدود التصعيد الإيراني - الإسرائيلي في الفضاء السيبراني

د. رغدة البهي*

لا يخفى أن لعدد كبير من الصراعات التقليدية في منطقة الشرق الأوسط بعداً سيبرانياً في ظل صعوبة حسم كثير منها على المستوى العسكري، ومن ثمّ 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 أسهمت في تشكيل مشهد التهديدات السيبرانية المحتدمة في المنطقة من ناحية، وأوجدت مزيداً من الأسباب الهيكلية التي أفضت إلى استمرار الصراعات العسكرية من ناحية أخرى. ومن ثمّ، تأثرت بنية الأمن السيبراني في المنطقة بعدة صراعات سياسية وعسكرية اقترنت بالعصر الرقمي الجديد؛ مما منح أطرافها أسباباً إضافية لاستغلال الثغرات عبر الإنترنت؛ مما حول المشهد الافتراضي إلى جبهة جديدة للصراع.

* رئيس وحدة الأمن السيبراني، بالمركز المصري للفكر والدراسات الاستراتيجية

وفي هذا الإطار، تبرز 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 حرباً خفية بين الطرفين تدار في رحي الفضاء السيبراني. فلم يرتفع معدل الهجمات السيبرانية ضد إسرائيل ثلاثة أضعاف بعد 7 أكتوبر 2023 وحسب، بل أصبحت أيضاً الهجمات السيبرانية الإيرانية أكثر تطوراً؛ لتصبح البنية التحتية هي الخاسر الأكبر، وتزداد عمليات خرق بيانات المستخدمين، وتتوقف عشرات المواقع الإلكترونية عن العمل، وتُستهدف الأنظمة الإلكترونية العسكرية. فقد طوّرت إيران استراتيجية سيبرانية فعالة وعززت مهاراتها في هذا المجال، وأصبحت من أكثر الدول نشاطاً في هذا الميدان؛ حيث تهدف هجماتها إلى تقويض المنشآت وتدميرها، وجمع بيانات للاستخبارات، وتداول معلومات خاطئة من أجل أغراض دعائية.

أولاً: الهجمات السيبرانية على إيران

في أعقاب الحرب الإسرائيلية على غزة، تعرضت إيران إلى عدة هجمات سيبرانية كان أخطرها على الإطلاق الهجوم السيبراني الذي قوض استقرار نظامها المصرفي، ودفع السلطات الإيرانية لدفع فدية قدرها 3 ملايين دولار لوقف مجموعة مجهولة من القراصنة من نشر بيانات حسابات فردية لنحو 20 بنكاً محلياً؛ منها (بنك الصناعة والتعدين، وبنك البريد الإيراني، والبنك المركزي)، وهي المجموعة التي تعرف باسم «أي آر ليكس»، والتي هددت في البداية ببيع البيانات التي جمعوها، والتي تضمنت بيانات الحسابات الشخصية وبطاقات الائتمان لملايين الإيرانيين، على شبكة الإنترنت المظلمة ما لم يتلقوا 10 ملايين دولار من العملات الرقمية، لكنهم وافقوا لاحقاً على مبلغ أقل. وقد وافق المسؤولون الإيرانيون على إبرام صفقة؛ خوفاً من أن يؤدي كشف سرقة البيانات إلى زعزعة استقرار النظام المالي في البلاد، والذي يتعرض لضغوط شديدة بسبب العقوبات الدولية. ويذكر أن شركة «توسن» الإيرانية التي تقدم خدمات بيانات للقطاع المالي هي التي دفعت الفدية نيابة عن النظام الإيراني الذي اتهم الولايات المتحدة وإسرائيل بنشر الخوف بين

الشعب، ولكنه لم يعترف مطلقًا بالخرق الذي حدث في منتصف أغسطس 2024 والذي أجبر البنوك على إغلاق ماكينات الصرف الآلي في جميع أنحاء البلاد⁽¹⁾.

كما تعرضت شبكة محطات الوقود في إيران لهجوم سيبراني في ديسمبر 2023، وقد اتهمت إيران قراصنة على صلة بإسرائيل والولايات المتحدة بعد هجوم سيبراني استهدف مستشفى في شمال إسرائيل. وفي أعقاب الهجوم السيبراني على إيران، كشفت «منظمة الدفاع السليبي الإيراني» عن تعطل 3800 من أصل 4396 محطة وقود في أنحاء البلاد (60٪ من محطات الوقود الإيرانية). وقد أعلنت مجموعة قرصنة تُسمى «بريداتوري سبارو» أو «العصفور المفترس» مسئوليتها عن الهجوم مع تأكيدها على أنه نُفذ بطريقة محكمة لتجنب إلحاق أي ضرر محتمل بخدمات الطوارئ. وقد تسبب الهجوم في إرباك عملية توزيع النفط، خصوصًا الحصص التي توزعها الحكومة على السائقين في إطار بطاقة رقمية تصدرها السلطات، وتسمح لهم بحصة شهرية من الوقود بسعر مدعوم. ورغم عودة المحطات إلى العمل بعد 48 ساعة، فإن تقارير نشرتها صحف ومواقع إيرانية، أشارت إلى مشكلات استمرت أيامًا في عملية توزيع الوقود. في الوقت نفسه، اخترق القراصنة إعلانات إلكترونية عملاقة في أنحاء طهران، وكتبوا «أين البنزين يا خامنئي؟»⁽²⁾.

وعلى ضوء المثالين السابقين وغيرهما من أمثلة، أكدت وزارة الاتصالات الإيرانية أن الهجمات السيبرانية ضد بنائها التحتية تكثفت مؤخرًا انطلاقًا من 174 دولة، وأنها تواصل التصدي لهذه الهجمات التي تأتي ردًا على دعمها لحركات المقاومة نصرة للحق وتصديًا لعدوان الاحتلال المتواصل على الشعبين الفلسطيني واللبناني. كما أنها تأتي فيما نفذت إيران عمليتي "الوعد الصادق 1 و2"، واللذان استهدفتا قواعد إسرائيلية في عمق الأراضي الفلسطينية المحتلة، ردًا على العدوان الإسرائيلي واستهدافه عددًا من القادة في محور المقاومة⁽³⁾.

وفي الوقت الذي تتعرض فيه إيران لعدة هجمات سيبرانية، فإن بعض جماعات القرصنة الإيرانية نفذت بنفسها عدة هجمات سيبرانية بدقة متناهية. وقد شنت بالفعل عدة هجمات سيبرانية استهدفت السعودية والإمارات وإسرائيل من بين أهداف أخرى. إذ تمول إيران عددًا من جماعات القرصنة التي تحظى بدعم

حكومي واسع. وتشمل أبرز جماعات القرصنة الإيرانية ، (APT 33 (Refined Kitten) ، APT 34 (OilRig) ، APT 35 (Charming Kitten) ، APT39 (Remix Kitten) ، Fox Kitten ، Static Kitten. وهي الجماعات التي تختلف عن جماعات القرصنة التقليدية التي قد تجعل من المكاسب المادية أولوية لها؛ فوفقًا للتقرير الصادر عن شركة (Verizon) الأمريكية في عام 2024، فإن 94٪ من الهجمات السيبرانية في الشرق الأوسط وأوروبا وشمال أفريقيا إنما تحدث لأسباب مادية⁽⁴⁾.

يبدو أن جماعات القرصنة الإيرانية إنما تهدف إلى الحصول على معلومات داخلية في أحيان، وتدمير وتعطيل البنية التحتية الحيوية في الدول المستهدفة في أحيان ثانية، وتكثيف أنشطة التجسس السبراني للحصول على تقنيات أجنبية ومعلومات استراتيجية تعظم مكاسبها السياسية والعسكرية والاقتصادية في أحيان ثالثة، وتعزيز الهيمنة الإيرانية على المنطقة والتي تتحقق في المقام الأول من خلال الوكلاء في أحيان رابعة. وعلى الرغم من أن محدودية قدرات تلك الجماعات مقارنة بجماعات القرصنة الروسية والصينية على سبيل المثال، فإن قدراتها ومعاييرها آخذة في التزايد تدريجيًا بمرور الوقت، ولا سيما في ظل تطور البرمجيات المخصصة غير المنتشرة من ناحية، وقوة تقنيات الهندسة الاجتماعية المستخدمة من ناحية أخرى⁽⁵⁾.

وتأسيسًا على ذلك، كشف التقرير السنوي الصادر عن شركة «مايكروسوفت» تحت عنوان «الدفاع الرقمي» عن تحول إسرائيل إلى الهدف الأول للهجمات السيبرانية الإيرانية منذ «طوفان الأقصى»، حتى استهدفت نصف العمليات الإيرانية المرصودة من قبل شركة «مايكروسوفت» شركات إسرائيلية منذ السابع من أكتوبر 2023 حتى يوليو 2024. كما دفع التقرير بأن الجماعات الإيرانية وسعت أيضًا عمليات نفوذها عبر الإنترنت إلى ما هو أبعد من إسرائيل، مع التركيز على تقويض الدعم السياسي والعسكري والاقتصادي الدولي للعمليات العسكرية الإسرائيلية. وتحدث التقرير عن حملات رقمية أطلقتها إيران على منصات التواصل الاجتماعي بعد السابع من أكتوبر، بما في ذلك إنشاء حساب يدعى «دموع الحرب» وآخر يدعى «كارما»، وحساب ثالث على تطبيق «تلجرام». وقد هدفت هذه

الحسابات إلى التأثير في الأوساط الإسرائيلية، ففي حين انتحل أحدها شخصيات ناشطين إسرائيليين ينتقدون رئيس الوزراء الإسرائيلي «بنيامين نتنياهو»، قام جزء آخر منها باستعمال شعار حركة «حماس» للتأثير في الإسرائيليين بمنشوراته⁽⁶⁾.

ثانيًا: الهجمات السيبرانية على إسرائيل

تعرضت إسرائيل هي الأخرى إلى عدد كبير من الهجمات السيبرانية التي طالت المواقع الإلكترونية لكل من: شركتي الاتصالات «سيلكوم» و«بارتير»، وشركة «مكوروت»، وصحيفة «جيزوالم بوست»، إلى جانب هيئة البث الرسمية «كان»، وشركة المواصلات العامة «إيجد»، و«بنك ديسكونت»، وشركة «تشيك بوينت» الرائدة، وموقع إذاعة «تن ثري إف إم»، وشركة «إن إس أو»، وغير ذلك. وترجع الغالبية العظمى من تلك الهجمات إلى جماعة القرصنة التي تُطلق على نفسها اسم «أنونيموس سودان» التي تعددت بياناتها المنشورة على تطبيق «تليجرام» والتي أعلنت فيها عن مسئوليتها عن مهاجمة عدد كبير من تلك المواقع، وإن تعرضت أخرى تابعة لميناء حيفا، ووزارة الصحة، وجهاز الأمن العام «الشاباك»، وسلطة الموانئ، ومنشآت المياه، والبنوك التجارية، والمستشفيات، وغير ذلك لهجمات أخرى.

وقد أتى الموقع الإلكتروني لجهاز «الموساد» في مقدمة المواقع الإلكترونية التي استهدفتها «أنونيموس سودان» إلى جانب الموقع الإلكتروني للتأمين الوطني. كما طالت الهجمات السيبرانية على إسرائيل حسابات عدد من المسؤولين في الجيش الإسرائيلي وأجهزة الأمن؛ ويذكر في هذا الإطار اختراق حساب «نتنياهو» على موقع التواصل الاجتماعي «فيسبوك» وكذا على تطبيق «انستغرام»، ليعرض الحسابان نصوًّا ومقاطع فيديو باللغة الفارسية⁽⁷⁾.

كما استهدفت أنظمة الري الزراعية الإسرائيلية في المناطق الشمالية وتحديدًا في وادي الحولة وغور الأردن مما أدى إلى تعطّلها عن العمل؛ فعند تشغيل أجهزة التحكم في الري - على سبيل التحديد - ظهرت رسالة مفادها «لقد تم اختراقك، لتسقط إسرائيل». وتبرز أهمية تلك الأنظمة لدورها في رصد الحقول وحالة الطقس للذين على إثرهما تُحدد كميات المياه اللازمة للري وتوقيت ضخها. وعلى صعيد آخر، أكد

موقع «إسرائيل ديفينس» استهداف شبكة حواسيب شركة البريد الإسرائيلية عشية عيد الفصح؛ مما اضطر شركة البريد إلى إصدار بيان أكدت فيه تعرضها لهجوم سيبراني استهدف بنيتها التحتية، وإن أشارت إلى إمكانية اكتشافه بواسطة نظام أمن المعلومات الخاص بها، بيد أن ذلك لم يغير حقيقة توقف خدماتها عدة أيام لحين اتخاذ الخطوات اللازمة لزيادة أمن المعلومات في مجالات الخدمة المختلفة. وقد طالت الهجمات السيبرانية خدمات تجارية عدة ذات الصلة بعمليات الجمارك، وسلطة الضرائب، وشركة المياه الإسرائيلية «مكوروت»، وشركة «مواف» إسرائيل، وميناء حيفا.

وقد تم إسقاط الموقع الإلكتروني لصحيفة «جيروزاليم بوست» في الوقت الذي أكدت فيه صحيفة «يديعوت أحرونوت» تعرضها لهجوم وقف الخدمة الموزعة الذي تسبب في تعطل خوادمها بالتزامن مع احتفال إسرائيل بذكرى «يوم الاستقلال» الذي وافق 26 إبريل 2023 والذي يُطلق عليه الفلسطينيون «يوم النكبة». كما أكدت «أنونيموس سودان» أنها أسقطت أيضًا المواقع الإلكترونية لهيئة البث «كان»، وإن تعرض موقع (0404) الإخباري الإسرائيلي هو الآخر لهجوم سيبراني جنبًا إلى جنب مع موقع (12News)، وموقع (Mako)، وموقع (Wint Premium)، وموقع (Hotnet)، وغير ذلك. وهو ما يعني استهداف المواقع الإلكترونية لعدد واسع من شركات الاتصالات وشركات الإنترنت في إسرائيل.

وقد طالت الهجمات السيبرانية الإسرائيلية المواقع الإلكترونية لكل من: جامعة تل أبيب، والجامعة العبرية في القدس، وجامعة بن غوريون في النقب، ومعهد الأبحاث التطبيقية في مدينة حيفا، ومعهد وايزمان للعلوم، والجامعة المفتوحة، وجامعة رايشمان». وقد ورد في البيان الذي نشرته «أنونيموس سودان» في حسابها على «تلغرام» أنه «تم التخلي عن قطاع التعليم في إسرائيل بسبب ما فعلوه في فلسطين». بيد أن اللافت للأنظار في الهجوم الذي استهدف معهد الأبحاث التطبيقية - على سبيل التحديد - هو طبيعته؛ فهو لم يكن هجوم وقف الخدمة الموزعة، وإنما هجوم فدية مقابل 70 قطعة بتكوين⁽⁸⁾.

ووفقًا لصحيفة الشرق الأوسط، كشفت قائدة وحدة الأمن السيبراني في الجيش الإسرائيلي العقيد «راحيلى دمبينسكي» في يوليو 2024 أن عدد الهجمات التي تعرض لها الجيش والدوائر الحكومية والشركات الكبرى والمؤسسات الاقتصادية والأمنية والصحية والتعليمية في إسرائيل بلغت أوجها، بعد أن تخطت 3 مليارات هجوم منذ بداية الحرب على غزة. وهي الهجمات الفردية والجماعية التي استهدفت الفضاء التنفيذي لعمليات الجيش الإسرائيلي وليس فقط الأهداف المدنية، وحاولت بذلك التخريب على عمليات الجيش في قطاع غزة والجنوب اللبناني وبقية العمليات في المنطقة. ووفقًا لها، فإن الحرب السيبرانية بين إسرائيل وخصومها تعد جزءًا حيويًا من حرب حماس وبقية الأذرع الإيرانية، لذا كرس لها الجيش الإسرائيلي كل مقدراته للتخفيف من أضرارها⁽⁹⁾.

ثالثًا: الهجمات السيبرانية بالوكالة

عملت مجموعات القرصنة من إيران والعراق ولبنان والسودان معًا في صورة حملة عرفت باسم (OpIsrael)، والتي هدفت إلى تجميع مواردها وخبراتها لشن هجمات أكثر تعقيدًا وتدميرًا، وهي الهجمات التي هدف بعضها إلى تعطيل البنية التحتية في أحيان، وجمع المعلومات الاستخباراتية في أحيان ثانية، ونشر الدعاية لتقويض جهود الحرب الإسرائيلية في أحيان ثالثة. وفي هذا الإطار، تعقبت شركة الأمن السيبراني الإسرائيلية (Check Point Software) أكثر من 40 جماعة قرصنة شنت بالفعل هجمات على مواقع حكومية وإعلامية في أعقاب الحرب الإسرائيلية على غزة. واعتبارًا من يوليو 2024، أفادت إسرائيل بأن إيران والجماعات المدعومة منها كانت مسؤولة عما يقرب من ثلاثة مليارات هجوم سيبراني، حيث نجحت دفاعات إسرائيل السيبرانية في منع كل هجوم تقريبًا. ومع ذلك، أفادت التقارير أن بعض الهجمات كانت قادرة على التحايل على دفاعات إسرائيل السيبرانية.

كما تتعاون مجموعة القرصنة المؤيدة لروسيا، والمعروفة باسم (Anonymous Sudan)، مع مجموعات القرصنة المؤيدة لفلسطين لتنفيذ هجمات واسعة النطاق لرفض الخدمة الموزعة (DDoS) على مواقع إسرائيلية مهمة. ففي نوفمبر 2023،

أعلنت مجموعة القرصنة المؤيدة لفلسطين، والمرتبطة بإيران والمعروفة باسم (Cyber Toufan)، مسؤوليتها عن استهداف مواقع حكومية إسرائيلية متعددة بما في ذلك أرشيف دولة إسرائيل، وسرقة المعلومات الشخصية التي يمكن التعرف عليها لآلاف من مستخدمي الأرشفة. وقد أدى هذا الهجوم إلى إيقاف أرشفة الدولة عن العمل لعدة أشهر؛ مما يسلط الضوء على فاعلية الحملة الإلكترونية المنسقة.

كما أعلنت مجموعة (Cyber Toufan) مسؤوليتها عن اختراقات سيبرانية استهدفت شركات مقرها إسرائيل أو شركات دولية لها أفرع إسرائيلية. وفي 16 نوفمبر 2023، اخترقت تلك المجموعة شركة (Signature-IT)، وهي شركة إسرائيلية تستضيف مواقع ويب للشركات العاملة في إسرائيل، وقد تمكنت المجموعة من الوصول إلى وتسريب بيانات العديد من الشركات متعددة الجنسيات والمنظمات التي تدير أعمالاً مع شركات إسرائيلية مثل (SpaceX) وفرع لشركة (Berkshire Hathaway)، بالإضافة إلى تعطيل وظائف الموقع وتسريب البيانات الحساسة. فقد استفادت مجموعة (Cyber Toufan) من الوصول إلى رسائل البريد الإلكتروني الخاصة بالشركة لإرسال دعاية مُوجهة. وفي حين استهدفت هذه الهجمات في المقام الأول الفروع الإسرائيلية للمنظمات الدولية، فإن التعقيد المتزايد للعمليات السيبرانية يُعرض الشركات العالمية لمخاطر متزايدة.

وتأسيساً على ذلك، واصلت إيران تمويل وكلائها الذين شنوا هجمات سيبرانية ناجحة، استهدفت إسرائيل وبعض المنظمات والشركات الإسرائيلية. هذا، وتتنحصر مجموعة القرصنة المدعومة من إيران (Moses Staff) في اختراق وتسريب معلومات حساسة لتقويض الثقة في الأمن السيبراني الإسرائيلي وكشف الخطط العسكرية لإضعاف الموقف الاستراتيجي لإسرائيل. واستهدفت المجموعة أيضاً الوكالات الحكومية والمؤسسات المالية وشركات الطاقة وقطاعي التصنيع والمرافق. وعلى نحو مماثل، استهدفت المجموعات التي ترعاها إيران (APT33) و (APT34) البنية التحتية الحيوية، بما في ذلك المستشفيات، من خلال هجمات التصيد واستغلال الثغرات الأمنية في خوادم (Microsoft Exchange)⁽¹⁰⁾.

هذا ويعكس توظيف إيران لجماعات القرصنة والفاعلين بالوكالة أحد ملامح استراتيجية "الدفاع الأمامي" التي تنتهجها إيران في سياساتها الخارجية، والتي تقضي بالحفاظ على الذات من خلال معالجة التهديدات قبل أن تتسلل إلى حدودها. وفي السنوات الأخيرة، توسعت هذه الاستراتيجية لإجراء عمليات سيبرانية هجومية ودفاعية لتحقيق الأهداف الإيرانية. وفي سياق متصل، تبنى الحرس الثوري الإسلامي (IRGC) استراتيجية أمن قومي مرنة متعددة الطبقات للحرب الهجينة تُعرف باسم (Mosaic Defense)، والتي تستفيد من عقود من عدم الثقة الإيرانية في القوى الأجنبية، وتستخدم تكتيكات الحرب غير المتكافئة لتقويض الخصوم. أما الوكلاء السيبرانيون التابعون لإيران، إما أنهم يخضعون لتوجيهات جهاز الأمن القومي الإيراني، وإما أنهم مرتبطون بروابط تجمعهم دون أن تتضح طبيعة تلك الروابط وماهيتها.

وقد كان مقتل اللواء "قاسم سليماني" بمثابة نقطة تحول مهمة في استراتيجية إيران السيبرانية؛ مما دفع طهران إلى تأكيد قوتها ونفوذها من خلال زيادة الأنشطة السيبرانية التي تستهدف الولايات المتحدة وحلفائها، على نحو يظهر براعة إيران التكنولوجية وقدرتها على ردع خصومها في الفضاء السيبراني. كما يوفر الغموض المحيط بالوكلاء وطبيعتهم المساحة اللازمة لإيران لإنكار صلتها بهم، وبالتالي التنصل من أي مسؤولية قد تنجم عن أفعالهم.

وإلى جانب الوكلاء، وظفت إيران الذكاء الاصطناعي والبرامج الضارة المخصصة والثغرات على نحو يعكس درجة التقدم في قدراتها السيبرانية. ففي يونيو 2024، استخدمت إيران والحرس الثوري الإسلامي الذكاء الاصطناعي لإنشاء مواقع إخبارية تنقل المحتوى المنشور على مواقع إخبارية لاستهداف النخبين الأمريكيين. بالإضافة إلى ذلك، في ديسمبر 2023، استخدم المتسللون برعاية إيرانية عمليات تزييف عميقة تم إنشاؤها بواسطة الذكاء الاصطناعي لتعطيل البث الإخباري بغرض التأثير في الرأي العام لصالحهم. وتتمثل الأهداف الأساسية للوكلاء السيبرانيين الإيرانيين في التجسس الاستراتيجي والاستطلاع لدعم الأولويات القومية. كما تستهدف التهديدات السيبرانية الإيرانية الصحفيين الذين يعارضونها بشكل مباشر. فقد نفذ القراصنة الإيرانيون حملة هندسة اجتماعية انتحلوا فيها

هوية الصحفيين ونشطاء حقوق الإنسان لإرسال رسائل بريد إلكتروني إلى الأهداف المرغوبة (تصيد احتيالي). بالإضافة إلى ذلك، نشرت شركة (MuddyWater) التابعة لإيران برنامج (BugSleep) الضار، واستخدمت مزيجًا من تقنيات التصيد المختلفة والهندسة الاجتماعية منخفضة التكلفة عالية العائد لإحداث تأثير نفسي في الجماهير المستهدفة في إسرائيل والولايات المتحدة وحلفائهما⁽¹¹⁾.

وتأسيسًا على ما سبق، مرت العمليات السيبرانية التي نفذتها إيران منذ طوفان الأقصى بثلاث مراحل؛ أولها: هي مرحلة رد الفعل والتضليل، وقد شهدت ادعاءات مضللة من وسائل الإعلام الحكومية الإيرانية كوكالة أنباء تسنيم التابعة للحرس الثوري الإيراني التي ادعت أن مجموعة تسمى "المنتقمون الإلكترونيون" نفذت هجمات سيبرانية ضد قاعدة إسرائيلية. وفي الثامن من أكتوبر 2023، قامت مجموعة أخرى تعرف باسم "فريق مالك" (التي تديرها وزارة الاستخبارات والأمن الإيرانية وفقًا لأرجح التقديرات) بتسريب بيانات شخصية من جامعة إسرائيلية. ولم يكن هناك أي صلة بالصراع الدائر في غزة بخلاف بعض الوسوم المستخدمة على (X) أو تويتر سابقًا) لدعم حماس.

أما ثانيها: فقد بدأت بحلول منتصف أكتوبر 2023 حتى آخر هذا الشهر، وقد شهدت ارتفاع عدد المجموعات التابعة لإيران التي استهدفت إسرائيل، والتي زاد عددها من 9 مجموعات إلى 14 مجموعة. وفي تلك الفترة، وتحديدًا في 18 أكتوبر 2023، استخدمت مجموعة (IRGC's Shahid Kaveh Group) التابعة للحرس الثوري الإيراني برامج فدية مخصصة لتنفيذ هجمات سيبرانية ضد كاميرات أمنية في إسرائيل، ثم استخدمت إحدى شخصياتها الإلكترونية المعروفة باسم (Soldiers of Solomon) لتزعم كذبًا أنها حصلت على فدية مقابل كاميرات أمنية وبيانات تتصل بقاعدة نيفاتيم الجوية، وقد تبين لاحقًا أنها كانت من بلدة تقع شمال تل أبيب بها شارع نيفاتيم، وليس القاعدة الجوية التي تحمل الاسم نفسه.

أما ثالثها: فهي مرحلة اتساع النطاق الجغرافي. ففي أواخر نوفمبر 2023، بدأت الجماعات الإيرانية في توسيع نفوذها خارج إسرائيل مستهدفة الدول التي ترى إيران أنها تدعم إسرائيل. وقد تماشى هذا مع بدء الحوثيين هجماتهم على سفن

البحر الأحمر. وفي 20 نوفمبر 2023، حذرت الشخصية الإلكترونية (Homeland Justice) المتحالفة مع وزارة الاستخبارات والأمن الداخلي من هجمات إلكترونية قادمة على ألبانيا. وأعلنوا لاحقاً مسئوليتهم عن الهجمات على مجموعة من المنظمات والمؤسسات الألبانية في يوم عيد الميلاد. وفي 21 نوفمبر، استهدفت الشخصية الإلكترونية (AI-Toufan) الحكومة البحرينية والمنظمات المالية المنوطة بتطبيع العلاقات مع إسرائيل⁽¹²⁾.

رابعاً: دلالات الهجمات المتبادلة

تبرز خصوصية الصراع بين إسرائيل وإيران في الفضاء السيبراني كونه مثلاً بارزاً على حدود أدوار وتأثيرات الحروب السيبرانية خلال أوقات الصراع العسكري. وبشكل عام، يمكن الوقوف على أبرز دلائل ذلك الصراع من خلال النقاط التالية:

1. **تزايد معدل الهجمات:** لقد ازداد معدل الهجمات السيبرانية ضد إسرائيل في أعقاب الحرب الإسرائيلية على غزة. ففي أعقاب 7 أكتوبر 2024، تحول التركيز الإيراني من الولايات المتحدة إلى الشركات الإسرائيلية، حتى أصبحت إسرائيل هي الهدف الأول للهجمات السيبرانية الإيرانية. وهو ما يمكن الاستدلال عليه من التقرير السنوي لشركة ”مايكروسوفت“، والمعروف باسم تقرير الدفاع الرقمي، والذي أكد كيف صعدت إيران من عملياتها السيبرانية ضد إسرائيل بعد اندلاع الحرب بين إسرائيل وحماس. ففي الفترة بين 7 أكتوبر 2023 إلى يوليو 2024، استهدفت نصف العمليات الإيرانية التي رصدتها شركة ”مايكروسوفت“ شركات إسرائيلية. أما في الفترة بين يوليو وأكتوبر 2023، استهدفت 10٪ فقط من الهجمات السيبرانية الإيرانية إسرائيل، بينما استهدفت 35٪ كيانات أمريكية و20٪ الإمارات العربية المتحدة.

2. **توظيف وسائل التواصل الاجتماعي:** لقد تعددت الأدوات الإيرانية لتحقيق أهدافها حتى شملت وسائل التواصل الاجتماعي؛ فمنذ بدء الحرب الإسرائيلية على غزة، أطلقت إيران العديد من العمليات على وسائل التواصل الاجتماعي بهدف زعزعة استقرار إسرائيل. فقد انتحل حساب يسمى ”دموع الحرب“ صفة

ناشطين إسرائيليين ينتقدون تعامل رئيس الوزراء "بنيامين نتنياهو" مع أزمة احتجاز حماس لعشرات الرهائن. كما ادعى حساب يسمى "كارما"، أنشأته وحدة استخبارات إيرانية، أنه يمثل الإسرائيليين الذين يطالبون باستقالة "نتنياهو". كما أن الخدمات الإيرانية أنشأت حسابًا على تطبيق "تلجرام" باستخدام شعار الجناح العسكري لحماس لنشر رسائل كاذبة حول الرهائن في غزة وتهديد الإسرائيليين، وأضافت أنه لم يتضح ما إذا كانت إيران قد تصرفت بموافقة حماس.

3. حشد الدعم الدولي: وسعت الجماعات الإيرانية عمليات نفوذها السيبرانية إلى ما هو أبعد من إسرائيل، مع التركيز على تقويض الدعم السياسي والعسكري والاقتصادي الدولي للعمليات العسكرية الإسرائيلية. ففي يونيو 2024، حذر رئيس الدفاع السيبراني الإسرائيلي "جاي بورتنوي" من أن العدوان السيبراني الإيراني يمثل مشكلة دولية، وليس فقط إسرائيلية، وبالتالي فإن الحل يجب أن يكون دوليًا. ودعى "بورتنوي" إلى جبهة دولية مشتركة ليس فقط في الدفاع، ولكن أيضًا لبناء الردع، وتحصيل ثمن إيراني مقابل الضرر العالمي الذي سببته. وفي الشهر التالي، ذكرت قوات الدفاع الإسرائيلية أن شبكة الحوسبة السحابية الخاصة بها واجهت أكثر من ثلاثة مليارات هجوم منذ بدء الحرب⁽¹³⁾.

4. تزايد انخراط جماعات القرصنة: تزايد أهمية الدور الذي تلعبه استخبارات التهديد لفهم طبيعة التهديد الذي تفرضه جماعات القرصنة الدولية، بما في ذلك الأهداف التي يسعون إلى استغلالها ودوافعهم وانتماءاتهم وتقنياتهم وأساليبهم. وفي حالة إسرائيل وإيران، تبرز ثلاث جماعات شاركت في التصعيد المتبادل؛ وهي:

أ. (Handala Hack): ففي 3 مارس 2024، زعمت مجموعة القرصنة تلك أنها وصلت عن بعد إلى أنظمة الرادار الإسرائيلية. ثم في 13 أبريل 2024، ادعت المجموعة مرة أخرى أنها اخترقت أنظمة الرادار. إن تلك المجموعة نشطة منذ 18 ديسمبر 2023 على الأقل، وقد نفذت عدة عمليات لتشويه مواقع إلكترونية منخفضة المستوى ضد مؤسسات عامة وخاصة إسرائيلية مرتبطة بالبنية التحتية الحيوية، وهي

مدفوعة بدوافع أيديولوجية، وترغب في ذياع صيتهم رغم نجاح عدد قليل جدًا من هذه الهجمات في الوصول إلى أهدافه.

ب. **مجموعة (Nethunt3r):** وهي مجموعة قرصنة ناطقة باللغة الإنجليزية مؤيدة للفلسطينيين، وهي نشطة منذ 2 أبريل 2024 على الأقل، وهي ذات دوافع أيديولوجية، وتتعاون مع العديد من مجموعات القرصنة المؤيدة للفلسطينيين بما في ذلك: (True Promise)، و(Anonymous South Africa)، و(Makhlab Alnasr)، و(AI Tahrea Team) من خلال مجموعة تسمى (Cyber Court). وفي 4 أبريل 2024، ادعت مجموعة (Nethunt3r) أنها اخترقت وزارة الدفاع الإسرائيلية (MOD)، وسربت العديد من المستندات التي يُزعم أنها أوامر شراء تجمعها بمقاوئي الدفاع الأمريكيين.

ج. **مجموعة (Cyber Aveng3rs):** وهي مجموعة قرصنة ناطقة باللغة الإنجليزية معادية لإسرائيل ومؤيدة لإيران، وهي نشطة منذ عام 2020 على الأقل، وهي ذات دوافع أيديولوجية، وتزعم أنها متخصصة في الهجمات المدمرة لأنظمة التحكم الصناعي. وقد أعلنت عن شن عدة هجمات سيبرانية رفيعة المستوى منذ صيف عام 2020، بما في ذلك هجوم غير مؤكد استهدف أنظمة السكك الحديدية في إسرائيل. في 12 أبريل 2024، شاركت المجموعة عدة مقالات إخبارية إسرائيلية عن انقطاع التيار الكهربائي الإسرائيلي الذي يرجع تاريخه إلى أواخر فبراير، وزعمت أنها شاركت مقطع فيديو يصور العديد من حالات الطوارئ الكهربائية وانقطاعات التيار الكهربائي الإسرائيلية منذ عام 2022؛ مما يشير إلى تورطها المزعوم في تلك الحوادث⁽¹⁴⁾.

5. **تسليح البيانات العامة:** في الآونة الأخيرة، تصاعدت الحرب السيبرانية بين إسرائيل وإيران والتي اتخذت في أحد مظاهرها خروقات البيانات. فلم تعكس تلك الحرب التوترات الجيوسياسية المتزايدة فحسب، بل كشفت أيضًا عن اتجاه مقلق لتسليح البيانات الحساسة. إن تلك الخروقات لم تؤثر فقط في المؤسسات الحكومية والمنظمات الرئيسية، بل أثرت أيضًا في ملايين المواطنين؛ مما يدل على تعدد العواقب بعيدة المدى للحرب السيبرانية.

ففي الثالث من أبريل 2024، ادعت إحدى الجماعات التي شنت هجمات باسم (MakhlalNasr) أنها تمكنت من الوصول إلى بيانات 8 ملايين إسرائيلي مؤمن عليهم لدى "معهد التأمين الوطني الإسرائيلي". وقد تضمنت المعلومات تفاصيل الحسابات المصرفية والمواقع السكنية وغير ذلك من بيانات شخصية. وقد تمت مشاركة تلك البيانات الحساسة على مجموعة "تليجرام" المرتبطة بمجموعة القرصنة (Makhlal_Nasr). وفي 7 إبريل 2024، ادعت إحدى الجماعات عبر منتهى الاختراق نفسه قدرتها على الوصول إلى معلومات حساسة تتبع وزارة الدفاع الإسرائيلية؛ فتعرضت للكشف والتسريب آلاف السجلات الإضافية التي تحتوى معلومات عن: الهوية الوطنية، والاسم الأول، والاسم الأخير، والمشروع، والمجموعة، ورقم الهاتف، وعنوان البريد الإلكتروني، وتاريخ الميلاد، والعمر، وتاريخ الميلاد باللغة العبرية، والمدينة، والعنوان، والجنس، والحالة، واسم الأب، وبلد المنشأ، وغير ذلك.

وفي حادث منفصل، أدى خرق آخر لأحد التطبيقات الانتخابية - التي استخدمها حزب الليكود وغيره - إلى الكشف عن أكثر من 6,5 ملايين سجل ضم كل منها: بيانات تسجيل الناخبين، والتفاصيل الشخصية للمواطنين الإسرائيليين. كما تضمنت المعلومات المخترقة: الأسماء الكاملة، وأرقام الهواتف، وأرقام بطاقات الهوية، والعناوين السكنية، والجنس، والعمر، والتفضيلات السياسية، والبريد الإلكتروني.

وبشكل عام، ارتفع العدد الإجمالي للخروقات التي استهدفت إسرائيل بنسبة 80٪ في الأشهر الأخيرة من عام 2024؛ مما يعكس تصاعد الحرب السيبرانية. وبالمثل، لم تكن إيران محصنة ضد مخاطر الحرب السيبرانية. فقد كشفت الجهود التعاونية بين روسيا وإيران، كما يتضح من تسريب (Crescent of Anon) عن تحالف مثير للقلق في الفضاء السيبراني. وهو التسريب الذي كشف ليس فقط عن عناوين البريد الإلكتروني وعناوين بروتوكولات الإنترنت وأسماء النطاقات، ولكن أيضاً عن وثائق واتفاقيات بين روسيا وإيران. تسلط هذه الوثائق الضوء على عمق التعاون بين البلدين في مجال الحرب السيبرانية؛ مما يثير تساؤلات حول أهدافهما الجماعية والمحتملة. بالإضافة إلى ذلك، يتضمن التسريب إشارات إلى قضايا تتعلق بالطائرات بدون طيار؛ مما يشير إلى مناقشات أو خطط لعمليات تتجاوز مجالات الصراع التقليدية⁽¹⁵⁾.

6. تعدد الأهداف وفداحة التداعيات: تهدف الأنشطة المتبادلة في إطار الحرب السيبرانية إلى جمع المعلومات الاستخباراتية وتقويض نشاط البنية التحتية الحيوية والكيانات الحكومية وغير الحكومية، من خلال: التسلل إلى الشبكات باستخدام حملات التصيد بالرمح المتطورة، ونشر برامج ضارة، وسرقة المعلومات الحساسة، وإلحاق الضرر بالأنظمة، وشل العمليات المالية. وتأسيساً على ذلك، تعد المنظمات والشركات الحكومية والعسكرية الإسرائيلية، بجانب الصناعات التجارية المتكاملة مثل التمويل والطاقة والاتصالات والتكنولوجيا، أهدافاً محتملة يؤدي تعطيلها إلى تقويض الاستقرار الاقتصادي لإسرائيل ومكانتها الدولية. ومع ذلك، فإن التهديدات الإيرانية امتدت إلى أبعد من ذلك لتشمل الشركات الأجنبية التي تدير أعمالها مع شركات مقرها إسرائيل أو تعمل داخلها. وهو ما أدى إلى اضطرابات تشغيلية شديدة وخسائر مالية ضخمة، ولا سيما أن تداعيات ذلك تطل المعلومات الحساسة، وقد تسفر عن توقف عمليات التشغيل، وقد تقوض سمعة الشركات الدولية.

أما بالنسبة للشركات التي يقع مقرها خارج إسرائيل، والتي تستخدم الموردين المقيمين في إسرائيل، فإن تعرضها لهجمات سيبرانية قد يؤدي إلى اضطرابات كبيرة في سلسلة التوريد. وقد تشمل التأثيرات المباشرة كلاً من: تأخر تسليم المنتجات، وزيادة التكاليف التشغيلية، وربما توقف الإنتاج؛ مما يؤثر ليس فقط في الشركات المستهدفة بشكل مباشر، ولكن أيضاً على العملاء الذين يعتمدون على منتجاتها أو خدماتها. وهو ما يفرض مخاطر مستقبلية على الشركات والمنظمات التي تستخدم التكنولوجيا التشغيلية (OT) لتشغيل البنية التحتية الحيوية، مثل: محطات معالجة المياه، والكهرباء، وشبكات الطاقة، وخدمات الرعاية الصحية⁽¹⁶⁾.

خاتماً

قد لا يتصدر الصراع السيبراني 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 دارت سرّاً 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. ومن بين هذه المجموعات "فريق بنغلاديش الغامض" المعروف بهجماته السيبرانية المتكررة ضد فرنسا، وقد أعلنت المجموعة استعدادها لشن هجمات سيبرانية ضد أهداف إسرائيلية، كما شنت هجومًا لحجب الخدمة على موقع منظمة التعاون الإسلامي للمطالبة من خلال قناة المجموعة على تطبيق "تليجرام" باتخاذ تدابير صارمة ضد إسرائيل. ومنذ منتصف نوفمبر 2023، نشرت مجموعة أخرى من نشطاء القرصنة كميات هائلة من البيانات السرية التي تخص شركات ومؤسسات حكومية إسرائيلية؛ بما في ذلك: وزارة الصحة، وهيئة الطبيعة والمتنزهات، ووزارة الرعاية والخدمات الاجتماعية، وهيئة الأوراق المالية، وبوابة الدفع الحكومية، والأرشيف الوطني.

المصادر:

1. إيران تدفع ملايين الدولارات لإنهاء هجوم سيبراني على نظامها المصرفي، الشرق الأوسط، 5 سبتمبر 2024، متاح على: <https://bitly.cx/b7kc>
2. نائب الرئيس الإيراني ينتقد هشاشة محطات الوقود ضد الهجمات السيبرانية، ميدل إيست نيوز، 8 سبتمبر 2024، متاح على: <https://bitly.cx/XH4Ho>
3. وزارة الاتصالات الإيرانية: الهجمات السيبرانية ضد بنانا التحتية تكثفت مؤخراً من 174 دولة، الميادين، نت، 13 أكتوبر 2024، متاح على: <https://bitly.cx/LRmu>
4. Cathrin Schaer, Why is the Middle East losing so much money to cybercrime?, **DW**, September 3, 2024, Available at: <https://www.dw.com/en/why-is-the-middle-east-losing-so-much-money-to-cybercrime/a-70123520>
5. Patrick McAteer, Rising Cyber Threats in the Middle East – A Virtual Battleground, **SecurityHQ**, Nov 2023, Available at: <https://www.securityhq.com/blog/rising-cyber-threats-in-the-middle-east-a-virtual-battleground/>
6. تقرير يؤكد تصاعد الهجمات الإلكترونية الإيرانية ضد الاحتلال بعد 7 أكتوبر، عربي 21، 17 أكتوبر 2024، متاح على: <https://bitly.cx/o5HZ>
7. رغدة البهي، أنماط تصاعد الهجمات السيبرانية ضد إسرائيل، تقديرات مصرية، السنة الرابعة، العدد 50، 2023، ص ص. 49-51.
8. المرجع السابق، ص ص. 49-51.
9. إسرائيل تعرضت لـ3 مليارات هجوم سيبراني منذ حرب 7 أكتوبر، الشرق الأوسط، متاح على: <https://bitly.cx/270UK>
10. Lauren Menzie, The Role of Cyber Operations in Middle East Conflict, **Teneo**, October 21, 2024, Available at: <https://www.teneo.com/insights/articles/the-role-of-cyber-operations-in-middle-east-conflict/>
11. Michael Mieses, Noelle Kerr, Nakissa Jahanbani, Artificial Intelligence Is Accelerating Iranian Cyber Operations, **Lawfare Media**, October 9, 2024, Available at: <https://www.lawfaremedia.org/article/artificial-intelligence-is-accelerating-iranian-cyber-operations>
12. Clint Watts, Iran accelerates cyber ops against Israel from chaotic start, **Microsoft**, Feb 6, 2024, Available at: <https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/>
13. Iran cyber attacks against Israel surged after Gaza war started, Microsoft reports, **Times of Israel**, 15 October 2024, Available at: <https://www.timesofisrael.com/iran-cyber-attacks-against-israel-surged-after-gaza-war-started-microsoft-reports/>
14. Amid Escalating Iran-Israel Conflict, Understanding the Hybrid Nature of Cyber Threats, **Flashpoint**, April 15, 2024, Available at: <https://flashpoint.io/blog/iran-israel-conflict-cyber-threats/>
15. Alberto Casares, Recent Breaches in Israel and Iran: A Closer Look at Cybersecurity Vulnerabilities, **Constella**, May 9, 2024, Available at: <https://constella.ai/recent-breaches-in-israel-and-iran-a-closer-look-at-cybersecurity-vulnerabilities/>
16. Cyber Threats Linked to Iran-Israel Conflict, **ReliaQuest Threat Research Team**, 25 April 2024, Available at: <https://www.reliaquest.com/blog/cyber-threats-linked-to-iran-israel-conflict/>

التصعيد السيبراني بين إسرائيل وحزب الله

لواء أ.ح.م / محمد مجدي رشاد علام*

يسلط هذا الفصل 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 قديماً أو حديثاً. فقد دلت 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 يقتضي 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.

* ملحق الدفاع بالملكة المغربية سابقاً، ورئيس كرسي الحرب الإلكترونية بكلية الحرب العليا سابقاً

أولاً: حزب الله.. التأسيس والصراع مع إسرائيل

تأسس حزب الله بدعم مباشر من إيران ومساعدة سوريا، ليكون حركة مقاومة إسلامية تهدف إلى تحرير الجنوب اللبناني من الاحتلال الإسرائيلي. وتمثل علاقة حزب الله وإيران رمزاً لتعقيد ديناميكيات القوة في الشرق الأوسط؛ حيث يشارك حزب الله إيران في الفكر الشيعي، ويعتبر المرشد الأعلى في إيران «آية الله علي خامنئي» مرشده السياسي ومصدر إلهامه الروحي. وبالتالي، يتمتع حزب الله بقاعدة أيديولوجية قوية ترتبط بالثورة الإسلامية في إيران. وقد استخدمت إيران حزب الله ببراعة في امتداد لمصالحها الاستراتيجية. وقد مكن الدعم المالي والعسكري لحزب الله إيران من توسيع نفوذها في المنطقة دون الحاجة لاشتباكات عسكرية مباشرة. كما حصل حزب الله على دعم من إيران، بما في ذلك الصواريخ والتدريب واللوجستيات. ويعتبر حزب الله هو جزء من مخطط جيواستراتيجي إيراني يهدف إلى تأسيس «قوس نفوذ شيعي» يمتد من إيران عبر العراق وسوريا ولبنان، وهي العلاقة التي تعزز موقف إيران في المنطقة، وتمنحها نفوذاً إقليمياً أوسع.

هذا ويعرف حزب الله أيضاً باسم المقاومة الإسلامية في لبنان. وفي أعقاب الغزو الإسرائيلي للبنان في عام 1982، أصبح حزب الله جزءاً من التوجه الإيراني لتجميع مجموعة متنوعة من الجماعات الشيعية المسلحة تحت سقف واحد. والجدير بالذكر أن حزب الله يستند إلى الأيديولوجية الخمينية ومبدأ ولاية الفقيه، ويتمتع بقوة عسكرية تقدر بحوالي 100 ألف مقاتل، كما يمتلك كميات محدودة من الصواريخ المضادة للطائرات والقذائف المضادة للسفن، فضلاً عن آلاف من القذائف المضادة للدبابات، ولا يمتلك أي طائرات أو دبابات أو مركبات مدرعة في لبنان، لأنها لا تستطيع مواجهة التفوق الجوي الإسرائيلي. ومع ذلك، يحتفظ حزب الله بمدرعات في سوريا المجاورة، بما في ذلك دبابات تي-55- و تي-72. وقد بنى مقاتلوه عددًا كبيراً من مخبئي الأسلحة والأنفاق والملاجئ المحصنة في جنوب لبنان. ويشكل حزب الله جزءاً من محور المقاومة الذي تقوده إيران في أجزاء كثيرة من الوطن العربي.

وبشكل عام، يهتم حزب الله بمصير ومستقبل لبنان، ويسهم مع بقية القوى السياسية اللبنانية في إقامة مجتمع أكثر عدالة وحرية. كما يرفع الحزب شعارات

الالتزام بالوحدة الوطنية في لبنان والدعوة إلى رفض الوجود الأجنبي فيه. ويهتم بالقضايا العربية والإسلامية وبخاصة القضية الفلسطينية. ولا يخفى الصراع بينه وبين إسرائيل، فعلى مدى أربعة عقود، ظل حزب الله وإسرائيل في مواجهة بلا هوادة، يراقب كل منهما الآخر، ويتجسس عليه، ويقصفه، ويغتال أعضائه إن لزم الأمر. فقد علم كل منهما طبيعة خصمه معرفة جيدة.

وقد مر الصراع بين حزب الله وإسرائيل بعدة محطات أساسية، كان أبرزها الغزو الإسرائيلي للبنان في عام 1982، حين شنت إسرائيل حملة عسكرية واسعة النطاق في لبنان بهدف طرد منظمة التحرير الفلسطينية وتحقيق أهداف أمنية؛ مما أدى إلى تشكيل "حزب الله" ككيان شيعي لمقاومة للقوات الإسرائيلية في جنوب لبنان. وبعد انسحاب إسرائيل من الجنوب عام 2000 -بعد ثمانية عشر عامًا من الاحتلال- اعتبر حزب الله أن ذلك يعد انتصارًا استراتيجيًا على إسرائيل ونقطة تحول في الصراع.

ومن المحطات البارزة أيضًا في علاقة إسرائيل وحزب الله تفجير السفارة الإسرائيلية في الأرجنتين عام 1992، حيث تعرضت السفارة الإسرائيلية في بوينس آيرس للتفجير، وقُتل 29 شخصًا وأصيب أكثر من 200 آخرين. هذا بالإضافة إلى تفجير حافلة في برغمان في عام 1994 في لندن، حيث تعرضت حافلة تقل ركابًا إسرائيليين لتفجير في منطقة برغمان نتج عنه مقتل 22 شخصًا وإصابة أكثر من 40 آخرين. هذا إلى جانب تفجير مركز "أميا" في عام 1994، والمعروف باسم "مركز الملك داوود"؛ حيث استهدف الهجوم مبنى الجمعية التضامنية اليهودية الأرجنتينية (أميا) في بوينس. هذا وتعتبر الأرجنتين موطنًا لمجتمع يهودي كبير يبلغ تعدادة حوالي 200 ألف شخص، وهو الأكبر في أمريكا اللاتينية والسادس في العالم خارج إسرائيل. وقد وجه اتهام رسمي للحكومة الإيرانية وحزب الله اللبناني بالتورط في هذا.

وبحلول أواخر عام 1990، توسع دور حزب الله سياسيًا وعسكريًا، وبدأ بشن حرب عصابات ضد الجيش الإسرائيلي في منطقة الشريط الأمني العازل. وفي عام 2000، اتخذت إسرائيل قرارًا بسحب قواتها من جنوب لبنان، لتنتهي بذلك سيطرتها التي دامت هناك ثمانية عشر عامًا. ولا شك أن عام 2006 كان عامًا فارقًا في علاقتهما،

وصولاً لحرب «تموز» التي استمرت طيلة 34 يوماً، ولم تنتهِ إلا بالقرار الأممي رقم 1701. وقد شهدت تلك الحرب حملات جوية وبحرية وبرية من قبل القوات الإسرائيلية على أجزاء كبيرة من لبنان. وفي ذلك الوقت، قُتل أكثر من 1100 لبناني في الضربات الإسرائيلية، بما في ذلك حوالي 250 من مقاتلي حزب الله، بينما قُتل 121 جندياً و43 مدنياً على الجانب الإسرائيلي بهجمات صاروخية شنها حزب الله.

وإلى جانب التوترات والحروب العسكرية، تجدر الإشارة إلى القدرات السيبرانية لحزب الله وكيف وظفها في مواجهة إسرائيل، أخذاً في الاعتبار أن إيران وفرت تدريباً إلكترونياً لعناصر حزب الله، وساعدتها على بناء وحدة إلكترونية استخباراتية في إطار برنامج طهران السيبراني الذي يُركز على توسيع عملياتها السيبرانية وقدراتها على المراقبة الرقمية. ووفقاً لمجلة «ناشيونال إنترست» الأمريكية، فإن طهران تشارك البنية التحتية السيبرانية مع وكلائها وحلفائها في منطقة الشرق الأوسط، بهدف تعزيز مصالحها الاستراتيجية. وقد كُلفت الوحدة الإلكترونية التابعة لحزب الله بشكل أساسي بجمع معلومات استخباراتية عن مؤسسات الدولة اللبنانية، وتعزيز الدفاعات السيبرانية لجهاز الأمن الإيراني. ويرجح امتلاك تلك الوحدة لمعدات حاسوبية مشابهة لتلك الموجودة في «جامعة شريف للتكنولوجيا» بالعاصمة طهران. وقد تمكن حزب الله من تحقيق اختراق هائل في ساحة المعركة الإلكترونية في عام 2006، حتى دفعت بعض التحليلات بأن المواجهة بين إسرائيل وحزب الله كانت مثلاً صارخاً على الحرب النفسية غير المتكافئة بعد أن انتصرت المليشيات الموالية لإيران إلى حد كبير في «حرب الصور» خلال التركيز على تقنيات الاتصال وأساليب نشر الرسائل.

ولطالما كانت هجمات حزب الله السيبرانية مصدر قلق لحكومات الشرق الأوسط والغرب. ففي يناير 2021، اكتشف أن وحدة إلكترونية تابعة لجماعة له تُعرف باسم «سيدار إيه بي تي اللبنانية» (Lebanese Cedar APT) قد شنت هجمات لفترة تزيد عن عام على شركات الاتصالات ومزودي خدمات الإنترنت في الولايات المتحدة والمملكة المتحدة وإسرائيل والسعودية ولبنان والأردن وفلسطين والإمارات. كما اخترق عناصر وحدة «سيدار» الشبكات الداخلية للشركات مثل شركة «فرونتيروميونيكيشنز»، ومقرها

الولايات المتحدة، لجمع بيانات حساسة. وفي عام 2010، وصفت إدارة الرئيس الأمريكي الأسبق "باراك أوباما" حزب الله بأنها "الجماعة الإرهابية الأكثر قدرة تقنيًا في العالم".

ثانيًا: إسرائيل وحزب الله في أعقاب طوفان الأقصى وحادثة البيجر

في اتجاه مضاد للقدرات السبيرانية لحزب الله، مر الأخير بمرحلة حرجة في أعقاب اندلاع الحرب الإسرائيلية على غزة في أعقاب "طوفان الأقصى"؛ حيث هدفت إسرائيل لإعادة حوالي ثمانين ألفًا من سكانها المستوطنين بالأجزاء الشمالية من إسرائيل إلى أماكنهم في الشمال. كما هدفت إسرائيل إلى إضعاف قدرات حزب الله من خلال تجنيد عملاء داخله، ومراقبة وتتبع نشاط قياداته إلكترونياً تمهيداً لتصفيتهم جسدياً، وال ضربات الجوية لمقرات الحزب وخاصة في الضاحية الجنوبية لبيروت، والحرب النفسية والتلفزيونية وكذا بالمنشورات. وتأسيساً على ذلك، تمكنت إسرائيل من اختراق أسرار حزب الله عبر أدوات التجسس المتطورة وتجنيد العملاء؛ مما مكنها من تنفيذ ضربات دقيقة ضد قياداته ومنشآته. وفي اتجاه مضاد للإجراءات الأمنية المشددة التي يتخذها حزب الله، فإن التجسس الإسرائيلي اتسم بالفاعلية، ولا سيما في ظل تنامي الاعتقاد في قدرة إسرائيل على تجنيد عملاء من داخل حزب الله على نحو عزز دقة معلوماتها.

وبين التطور التكنولوجي وتكتيكات التجنيد، باتت الحرب الاستخباراتية تتفوق على النزاعات العسكرية التقليدية في الصراع بين إسرائيل وحزب الله، فعلى الرغم من التقدم العسكري لحزب الله، فإن اختراقات الاستخبارات الإسرائيلية لأسراره وأمنه أسفرت عن ضربات موجعة، سواء على مستوى قياداته أو مراكزه ومنشآته العسكرية المموهة. وعلى الرغم من تدابير الأمنة الاستثنائية تجنباً للرصد الجوي الإسرائيلي ومنها؛ (تجنب استخدام الهواتف، وتعطيل كاميرات المراقبة، وتقليل الظهور العلني لعناصره، ونقل القادة إلى أماكن إقامة جديدة، وتغيير وسائل التنقل)، فإن فاعلية الاستهدافات الإسرائيلية بقيت على وتيرتها؛ مما يعكس فاعلية أدوات التجسس في هذا الصراع الاستخباراتي الذي يزداد تعقيداً مع مرور الوقت وتطور

وسائل المراقبة وجمع المعلومات؛ مما يجعل من التهديدات السيبرانية تحديًا حقيقيًا يضاف إلى الصراع الممتد في المنطقة.

وفي هذا الإطار، تفاجأ العالم يوم الثلاثاء 17 سبتمبر 2024 بانفجار مئات أجهزة الاستدعاء «البيجر» في الجنوب اللبناني، مُسببًا مقتل نحو 12 شخصًا، من بينهم طفلان، إضافة إلى إصابة ما يقرب من 3 آلاف شخص معظمهم من قيادات حزب الله.

بعد سلسلة انفجارات متزامنة لأجهزة الاتصال المحمولة في أنحاء لبنان، قتل وأصيب مئات في عدد من المدن اللبنانية. والجدير بالذكر أن هناك تفاصيل عدة لم تتكشف بعد حول سبب استخدام حزب الله لهذه الأجهزة التي انتهى عمرها، ولم يعد أحد يستخدمها في الاتصالات بعد ظهور الهواتف الخلوية.

البيجر هو جهاز اتصال لا سلكي صغير كان يستخدم قديمًا قبل ظهور الهواتف الذكية، وقد تم تطويره في الستينيات للاستخدام في حالات الطوارئ، ويعتمد على إرسال إشارات رقمية عبر موجات الراديو لإخطار المستخدم بأن شخصًا ما حاول الاتصال به كما يمكن إرسال رسائل نصية قصيرة عبر هذا الجهاز. كانت أجهزة البيجر وسيلة شائعة للتواصل قبل انتشار الهواتف الذكية، وبخاصة بين الأطباء العاملين في المناوبات الليلية، وموظفي خدمات الطوارئ. كما استُخدم أيضًا في المجالات العسكرية والأمنية.

تدور أسباب اعتماد عناصر حزب الله على البيجر رغم تقادمه كوسيلة اتصال حول الأمان الذي يقدمه؛ إذ تعتبر أجهزة البيجر واحدة من التقنيات القديمة نسبيًا التي لا يمكنها الاتصال بالإنترنت، ولذلك تعتبر آمنة نوعًا ما من الاختراقات السيبرانية ومحاولات التجسس والتتبع الشائعة عند استخدام الهواتف المحمولة أو الذكية. ولهذا، لا تزال تُستخدم في المجالات العسكرية والأمنية، وهذا على الأرجح السبب الذي يدفع عناصر حزب الله لامتلاكها واستخدامها. ولا يزال من المبكر معرفة كيف انفجرت هذه الأجهزة بالتحديد؛ حيث تتعدد التفسيرات حول أسباب ذلك، وأبرزها زرع شريحة ما في أجهزة البيجر كافة قبل استيرادها واستخدامها من

قبل عناصر حزب الله، مع تفعيل تلك الشريحة من خلال موجات الراديو المرسلة عبر طائرات مُسيرة تم إطلاقها في مختلف أرجاء لبنان، بحيث تعمل تلك الموجهات على تفجير الشريحة أو رفع درجة حرارة بطارية الجهاز على نحو يؤدي إلى انفجارها من خلال برمجيات خبيثة تسببت في رفع حرارة البطاريات.

ويمكن تصنيف تلك الحادثة على أنها حادثة إرهابية عادية ولكن بفكر جديد ومتقدم؛ حيث استُخدمت فيها القدرات السبيرانية لوحدة الحرب الإلكترونية الإسرائيلية (8200) مع القدرات الاستخباراتية للموساد والشاباك، بهدف تتبع توريد إحدى شحنات أجهزة البيجر موديل (Apollo Rugged Pager AR-924 pagers) والأجهزة اللاسلكية (ICOM IC-V82)، وذلك لاستخدامها في الاتصالات بين قيادات حزب الله؛ حيث إنها توفر قدرًا كبيرًا من سرية المحادثات، لكونها تستخدم تكنولوجيا قديمة جدًا لم تعد تستخدم في الوقت الحالي، وبالتالي لا تتوافق مع نظم الاستطلاع الإلكتروني الحديثة؛ مما يصعب اكتشافها أو تحديد أماكنها. ومن ثم، قررت إسرائيل أن تضرب عصفورين بحجر واحد، فتدمر شبكة اتصالات حزب الله وتدمر أعضاء وقياداته في آن واحد.

وكان الموساد قد بدأ في التخطيط لهذه العملية قبل هجوم السابع من أكتوبر، حينما كان الهدوء يعم الجبهة الشمالية لإسرائيل، وتصادف قيام حزب الله بالبحث عن أجهزة اتصال لاسلكية لقواته بشرط عدم قابليتها للاختراق من قبل وسائل التصنت الإسرائيلية. ولسوء الحظ، راقب الموساد تلك الاتصالات التي قام بها حزب الله، وهنا بدأ الموساد -من خلال عملائه- الإيعاز لحزب الله بالتعاقد على شراء هذه الأجهزة التايوانية من خلال امرأة تايوانية لديها توكيل من الشركة الأصلية. ومع التعاقد، طلب حزب الله إجراء بعض التعديلات على الأجهزة، بحيث تتضمن بطارية قوية يمكنها العمل لمدة أشهر قبل الحاجة لإعادة شحنها.

وقد اتهم حزب الله إسرائيل بالوقوف وراء هذا الهجوم السبيرانى، الذي يُعد الأول من نوعه منذ بداية الحرب في غزة في أكتوبر 2023. فقد تسبب هذا الهجوم في آلاف الانفجارات بين أعضاء حزب الله، حيث أصاب أجهزة البيجر الخاصة بهم، ثم أجهزة الاتصال اللاسلكية في اليوم التالي. وإجمالاً، أسفرت الانفجارات عن مقتل 37 شخصًا على الأقل، بما في ذلك بعض الأطفال، وإصابة ما يقرب من 3000 شخص،

وفقاً للسلطات الصحية اللبنانية، وكثير منهم من المارة المدنيين. ولقد فاجأ الهجوم حزب الله الذي اختار تقنيات تناظرية (Analogu) بعد التخلي عن الهواتف المحمولة الرقمية (Digital) لتفادي الاختراق الإسرائيلي. وقد اعترف وزير الدفاع الإسرائيلي السابق "يوآف غالانت" ضمناً بدور بلاده في اليوم التالي لهجوم أجهزة البيجر، مشيداً بالإنجازات الممتازة لجهاز الأمن الداخلي (الشاباك) بجانب الموساد.

وفي اعتقادي، فإن الطريقة تم بها التفجير هي مجرد عملية إرهابية تم فيها تفجير عبوة ناسفة من بعد، أما الجديد فيكمين في كيفية وصول الأجهزة لإسرائيل وكيفية إخفاء العبوة الناسفة داخل البطاريات بطريقة متطورة لدرجة أنه لم يتم اكتشافها خلال رحلة توريد الأجهزة.

وبصفة عامة، تحتوي العبوة المتفجرة على عدة مكونات رئيسية؛ هي: شحنة شديدة الانفجار، ومفجر كهربائي أو حراري، ومصدر للطاقة لتفجير المفجر، وشريحة إلكترونية لتلقي إشارة التفجير. وهذا ليس جديداً أو ابتكاراً، فقد وظفت عمليات إرهابية عدة الأسلوب نفسه بتفجير عبوات ناسفة باستخدام أجهزة التليفونات المحمولة والتي يتم توصيلها كهربائياً بمفجر العبوة الناسفة لتنفجر بمجرد تلقيها اتصالاً عن بعد.

ويتوافق ذلك مع التقييمات الأولية التي أجرتها السلطات اللبنانية، كما خلصت بعثة لبنان لدى الأمم المتحدة في رسالة بعثتها إلى مجلس الأمن الدولي إلى أن التحقيق الأولي توصل إلى أنه تم زرع متفجرات بأجهزة الاتصالات قبل وصولها إلى البلاد، وتم العبث بها "بطريقة احترافية" من قبل كيانات أجنبية وسلاسل توريد (Supply Chain) غامضة تمتد من تايوان إلى المجر، حيث تم فك الأجهزة واستبدال بطارياتها بأخرى بها مواد شديدة الانفجار مع مفجر تم توصيله بشريحة استقبال لإشارة البدء. كما أثبتت التحقيقات أن هذه النوعية من الأجهزة قد تكون مزيفة، ولا سيما في ظل توفر عدة نسخ منها يمكن شراؤها (ON Line) من مواقع مثل "علي بابا" و "أمازون" بسهولة.

وفي ضوء ما سبق، يمكن الدفع بأن قدرات الموساد في تلك العملية تتلخص في: معرفة احتياج حزب الله لأجهزة اتصالات نصية بدلاً من الهواتف التقليدية،

وتحديد نوعية الأجهزة المطلوبة وموديلاتها، وتحديد مصادر استيراد أجهزة البيجر، وتتبع رحلة الشحنة من المصدر حتى وصولها إلى بيروت، واعتراض مسار الشحنة قبل وصولها لحزب الله، وفك الأجهزة واستبدال البطاريات بأخرى متفجرة مع زرع الشريحة الإلكترونية في سرية تامة، وإعادة الشحنة إلى مسارها الطبيعي في سلسلة التوريد، وزرع مفجر كهربائي، وزرع شريحة أو مستقبل إلكتروني لتفجير البطارية عند استقبال إشارة أو كود محدد، وتعديل نظام التشغيل بحيث يُجبر المستخدم على القبض على الجهاز بكلا اليدين لفك شفرة الرسائل الواردة لضمان إصابة اليدين معًا عند تفجير الجهاز، وهذا ما تحقق بالفعل.

وقد فتح حزب الله تحقيقًا بشأن سلسلة توريد الأجهزة لتحديد ملابسات هذا الحادث ومعرفة الثغرات الأمنية التي أدت إليها. كما دأبت وزارة الصحة اللبنانية على تحديد عدد المصابين والجرحى. والجدير بالذكر أنه منذ أكتوبر 2023 وحتى 24 نوفمبر 2024، قُتل 3768 وجُرح 15699 شخصًا على الأقل في لبنان. ولا تميز الأرقام بين مقاتلي حزب الله والمدنيين أو عدد القتلى في صفوف حزب الله فحسب، وإن أعلن الأخير عن مقتل نحو 500 من مقاتليه في المعارك حتى اللحظة التي شنت فيها إسرائيل هجومها على جنوب لبنان في سبتمبر 2024. ووفقًا لمعهد دراسات الأمن القومي التابع لجامعة تل أبيب -الذي تربطه علاقات وثيقة بالمؤسسة العسكرية- فإن حزب الله خسر إجمالاً 2450 فردًا، في الوقت الذي قتلت فيه غارات حزب الله 45 مدنيًا في شمال إسرائيل وهضبة الجولان المحتلة. ووفقًا للسلطات الإسرائيلية، قُتل 73 جنديًا إسرائيليًا على الأقل في شمال إسرائيل وهضبة الجولان ومعارك جنوب لبنان.

يجمع معظم المحللين الاستراتيجيين والأمنيين على 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، إضافة إلى أن تكنولوجيا التعرف على الوجه شهدت تقدمًا كبيرًا مكن القوات الإسرائيلية من التعرف على الأشخاص من خلال كاميرات عالية الدقة على متن المُسيّرات أو الأقمار الاصطناعية.

ثالثاً: التصعيد الإسرائيلي-اللبناني وصولاً لوقف إطلاق النار

في أعقاب تفجيرات البيجر، وخلال سبتمبر 2024، تصاعد الصراع بين حزب الله وإسرائيل بشكل كبير، وبنهاية سبتمبر 2024 كانت إسرائيل قد قضت على ما يقرب من 52 من قيادات الحزب بما فيهم أمين عام الحزب السابق "حسن نصر الله". وقد بدأت الأحداث في 17 سبتمبر عندما قررت إسرائيل تصعيد الصراع مع حزب الله ونقل جهدها العسكري من قطاع غزة إلى الجبهة الشمالية لمواجهة لحزب الله على الحدود الجنوبية اللبنانية؛ حيث شنت إسرائيل سلسلة من الهجمات الجوية الشاملة على لبنان، مستهدفة معازل حزب الله في الجنوب والبقاع؛ مما أدى إلى مقتل وإصابة العديد من الأشخاص. وفي 23 سبتمبر 2024، قامت إسرائيل بشن هجوم جوي شامل على لبنان، تضمن أكثر من 600 طلعة جوية ومهاجمة أكثر من 1300 هدف، حيث مثلت هذه الهجمات نقلة نوعية في الصراع بين الجانبين، إذ تحولت إلى حرب استنزاف مستمرة. والجدير بالذكر أنه في 25 سبتمبر 2024، استهدفت إسرائيل مبنى في الضاحية الجنوبية لبيروت، حيث كان كبار قادة قوة الرضوان (قوات النخبة في الحزب) يجتمعون؛ مما أدى إلى مقتل عدد كبير منهم، وصولاً إلى مقتل "حسن نصر الله" في 27 سبتمبر 2024 على خلفية غارة جوية إسرائيلية استهدفت مقر قيادة حزب الله في الضاحية الجنوبية لبيروت. ويمكن القول تعقيباً على ذلك إن تلك العملية كانت نتيجة متابعة وتخطيط استمر لسنوات من قبل إسرائيل، حيث تم استخدام مادة غامضة لتعقب مكانه.

ونتيجة لذلك، تصاعدت الخروقات الإسرائيلية لقرار مجلس الأمن رقم 1701، المتخذ بالإجماع في 11 أغسطس 2006، والذي تمثل الهدف منه في حل النزاع اللبناني-الإسرائيلي، والذي وافقت عليه الحكومة اللبنانية بالإجماع، وأعلن "حسن نصر الله" أن قواته سوف تحترم وقف إطلاق النار، وستتوقف هجمات حزب الله الصاروخية على إسرائيل. فاعتباراً من عام 2024، لم يتم تنفيذ القرار بالكامل، فلم ينسحب حزب الله والجماعات المسلحة الأخرى في جنوب لبنان على الإطلاق، بل وزاد حزب الله منذ ذلك الحين من قدراته التسليحية بشكل كبير، حيث جمع ما يقرب من 120-200 ألف صاروخ باليستي موجه قصير المدى وأخرى غير موجهة

قصيرة ومتوسطة المدى، وزاد من نشر قواته المسلحة جنوب نهر الليطاني، وطوّر الأنفاق ومخابئ الأسلحة ومهابط الطائرات والمنشآت العسكرية. كما اتهمت لبنان إسرائيل بعدم الانسحاب الكامل من الأراضي اللبنانية (الجزء الشمالي ومزارع شبعا وتلال كفرشوبا)، وانتهاك حدودها الجوية والبحرية.

والجدير بالذكر أن القرار 1701 سبق وأن دعى حينها إلى إيجاد منطقة بين الخط الأزرق (الفصل بين لبنان وإسرائيل) ونهر الليطاني جنوب لبنان، بحيث تكون خالية من أي مسلّحين ومعدات حربية وأسلحة، ما عدا تلك التابعة للقوات المسلحة اللبنانية وقوات حفظ السلام (اليونيفيل). وقد وافق حزب الله على ذلك القرار قبل أن يخرقه بإعادة انتشاره في جنوب الليطاني بشكل كامل، كما خرّقه إسرائيل مرارًا على مدى السنوات الماضية، فهي لم تنسحب من الأراضي اللبنانية المحتلة (مزارع شبعا وتلال كفرشوبا)، إضافة إلى تنفيذها خروقات جوية على مدى السنوات، وأخيرًا القصف العنيف على قرى الجنوب، وتهجير أكثر من مليون لبناني من بيوتهم. كما نص الاتفاق على: نزع سلاح جميع الجماعات المسلحة في لبنان، وإجلاء قوات حزب الله والقوات الإسرائيلية جنوب نهر الليطاني، وحظر وجود قوات أجنبية في لبنان دون موافقة حكومته، مع تزويد الأمم المتحدة بجميع خرائط الألغام الأرضية في لبنان التي بحوزة إسرائيل. وقد أكد القرار في الوقت نفسه على أهمية السيطرة الكاملة للحكومة اللبنانية على جميع أراضيه، وعلى دعم مجلس الأمن القوي، والاحترام الكامل للخط الأزرق والسلامة الإقليمية والسيادة والاستقلال السياسي للبنان داخل حدوده المعترف بها دوليًا.

وقد توصل حزب الله وإسرائيل إلى اتفاق تهدئة لوقف إطلاق النار في 26 نوفمبر 2024 بعد عام من الهجمات المتبادلة، والتي تصاعدت إلى حرب على الحدود اللبنانية-الإسرائيلية. وقد تضمن الاتفاق: إنشاء آلية مراقبة بالتنسيق بين الولايات المتحدة، وفرنسا لمتابعة ومراقبة تنفيذ وقف إطلاق النار لمدة 60 يومًا، وانسحاب القوات الإسرائيلية من الجنوب اللبناني، مع حق إسرائيل في التحرك ضد حزب الله في حال تهديده لها، وكذلك سحب حزب الله لمقاتليه وأسلحته من منطقة الحدود الواقعة جنوب نهر الليطاني إلى حوالي 20 ميلًا إلى الشمال من نهر

الليطاني، وتفكيك البنية التحتية العسكرية التي تعد خارج سيطرة الدولة اللبنانية، مع انتشار الجيش اللبناني في المناطق الحدودية، وكذلك قوات الأمم المتحدة المؤقتة في لبنان «اليونيفيل»، فضلاً عن التفاوض على ملف ترسيم الحدود البرية بين لبنان وإسرائيل.

وبالرغم من ذلك، شهدت الساحة اللبنانية بعض الخروقات لاتفاق الهدنة، ما بين عمليات تفجير تقوم بها إسرائيل في جنوب لبنان، فضلاً عن القصف الإسرائيلي المستمر بعد الاتفاق على القرى القريبة من الحدود في جنوب لبنان في بلدة مرجعيون، وبلدة بيت ليف، وقصف معبر «جوسية» في محيط القصير، واستهداف قوافل حزب الله العائدة من سوريا. وقد بلغ عدد الخروقات الإسرائيلية أكثر من 60 مرة بحسب التصريحات الرسمية لرئيس حكومة تصريف الأعمال في لبنان «نجيب ميقاتي»، وفي تقديرات أخرى وصل عدد الخروقات نحو 155 منذ بدء سريان الاتفاق. وقد تنوعت أساليب خرق الاتفاق ما بين إطلاق الصواريخ، واستخدام قذائف الهاون من قبل حزب الله، بقصف موقع «رويسات العلم» في تلّال كفر شوبا في 2 ديسمبر 2024.

إذ تواصل إسرائيل انتهاك الهدنة باستخدام المدفعية والطائرات المسيّرة في وقت فرضت فيه حظراً على التنقل في المناطق الواقعة جنوب نهر الليطاني، بدءاً من الساعة الخامسة مساءً وحتى الساعة صباحاً، حتى أكد رئيس مجلس النواب اللبناني «نبيه بري» أن الخروقات لا تعدو كونها انتهاكاً فاضحاً للاتفاق ومن غير المسموح استمرارها، مشيراً إلى وجود اتصالات مع الجهات الدولية المعنية لمعالجة تلك الانتهاكات الإسرائيلية أملاً في أن يؤدي اكتمال عقد لجنة الإشراف على مراقبة تطبيق الاتفاق إلى وقفها.

ونتيجة لنجاح إسرائيل في إضعاف قوات حزب الله، فقد تسارعت الأحداث اعتباراً من السادس من ديسمبر 2024 بسبب انسحاب حزب الله من مدينة حلب السورية، وذلك لتعزيز دفاعاته أمام الجبهة الإسرائيلية بجنوب لبنان؛ مما أعطى الفرصة لأحزاب المعارضة السورية التي تمثلها جبهة النصرة لتقوم بهجوم مباغت على شمال سوريا والاستيلاء على مدينتي حلب وحماه والتقدم نحو العاصمة

دمشق والسيطرة عليها بعد سقوط سريع للجيش السوري ومغادرة الرئيس السوري "بشار الأسد" للبلاد.

الخاتمة:

تعد القضية الفلسطينية واحدة من القضايا المركزية في الصراع العربي-الإسرائيلي، وهي جزء أساسي من التوترات في منطقة الشرق الأوسط. هذا النزاع يعود إلى تأسيس الصهيونية والهجرة اليهودية إلى فلسطين والاستيطان فيها، بالإضافة إلى دور الدول الكبرى في تلك الأحداث. كما تعد إيران وأهدافها السياسية والعقائدية بالمنطقة من أهم أسباب تأجيج الصراعات بالعالم العربي واستقطابها للمليشيات العسكرية بلبنان واليمن وسوريا وغزة. بيد أن حل تلك الصراعات يكمن في الحوار السلمي بين شعوب المنطقة، وتخلي كل من إيران وإسرائيل عن أهدافهما السياسية التوسعية، وهذا أمر مستبعد، لذا فإن الحل الواقعي يكمن في تضامن العرب وإحياء القومية العربية وتوحيد سياساتهم واقتصاداتهم، وتخلي القادة العرب عن النظرة المحلية والمصالح الشخصية من أجل إقامة الدولة الفلسطينية وتحرير جميع الأراضي العربية من القوى الأجنبية والمليشيات العسكرية.

الاستراتيجيات والأدوات الذكية في الحروب الافتراضية: دراسة في الحالة الإسرائيلية

د. رانيا فوزي*

يمثل الذكاء الاصطناعي بالنسبة لإسرائيل مجاًلاً تكنولوجياً 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 القوة العسكرية اعتمادًا على الحروب الذكية. إضافة إلى ذلك، تُسخر إسرائيل تقنيات الذكاء الاصطناعي في عملياتها النفسية وحروبها الإعلامية على شبكات

* خبيرة في الشؤون الإسرائيلية، ومتخصصة في تحليل الخطاب الإعلامي

التواصل الاجتماعي؛ مما يمنحها تأثيراً يتجاوز المجال العسكري التقليدي ليصل إلى الرأي العام العالمي وصناع القرار السياسي في المجتمع الدولي.

من هنا تأتي أهمية هذا الفصل الذي يحاول تقديم فهم شامل لديناميكيات الحروب الافتراضية الإسرائيلية، مع التركيز على الأدوات والاستراتيجيات الذكية المستخدمة، ورصد تأثيرها في مستقبل الصراعات في المنطقة. وعليه، هدف هذا الفصل إلى تحليل الاستراتيجيات التي تعتمدها إسرائيل في الحروب الافتراضية، وتبسيط الضوء على الأدوات الذكية التي توظفها لتحقيق أهدافها. كما سيستعرض أبرز الحالات العملية التي أظهرت فيها إسرائيل تفوقها في هذا المجال في عملياتها العسكرية، خاصة في حريها الأخيرة على غزة كدراسة حالة، وذلك من خلال ثلاثة محاور؛ دار أولها حول استراتيجيات الحروب الذكية الإسرائيلية وأدواتها، فيما ناقش ثانيها الأبعاد الاستراتيجية للحروب الافتراضية في السياق الإسرائيلي، وإن تطرق ثالثها إلى توظيف الحروب الافتراضية الإسرائيلية في حرب السابع من أكتوبر.

أولاً: استراتيجيات الحروب الذكية الإسرائيلية وأدواتها

أدركت إسرائيل أن التطور التكنولوجي الحديث يخلق ساحة جديدة للحرب؛ مما جعل استخدام الأسلحة الذكية إحدى أهم الأدوات في إدارة حروبها الحالية والمستقبلية، بعدما أصبحت جزءاً أساسياً من استراتيجيات أقوى الجيوش في العالم. من هنا، أتت الرغبة الإسرائيلية في زيادة توظيف الذكاء الاصطناعي في الاستراتيجية العسكرية للجيش الإسرائيلي، لتشمل تطوير هذه التكنولوجيا داخل وزارة الدفاع، وإدارة تطوير الأسلحة والبنية التحتية التكنولوجية، وكذلك الوحدات الاستخباراتية والتكنولوجية المختلفة في الجيش إضافةً إلى الصناعات الدفاعية. وقد بدأت إسرائيل بالفعل في السنوات الأخيرة، تكييف تقنيات الذكاء الاصطناعي الموجودة في السوق المدنية مع المؤسسة الأمنية بشكل تدريجي حتى باتت تتطور أكثر بفضل استخدام هذه التقنية المتطورة في عملياتها العسكرية. وقد اتخذ الجيش الإسرائيلي خطوات عملية لتطوير واستيعاب تقنيات الذكاء الاصطناعي بالاعتماد على قوة بشرية فريدة ومدرّبة، من بينهم مهندسو المعلومات، وكذلك المتخصصون في تحليل واسترداد البيانات، وذلك لخلق بيئة واعدة لتنمية مسارات التميز لجنود وضباط الاحتياط المتفردين في هذا المجال⁽¹⁾.

1. الاستراتيجيات الإسرائيلية للحروب الذكية:

تلعب إسرائيل دوراً محورياً في المجال التكنولوجي؛ مما جعل الاستراتيجية العسكرية للجيش الإسرائيلي تعتمد بشكل كبير على البيانات والذكاء الاصطناعي، لما لهما من دور حاسم في حسم الصراعات المستقبلية. وتهدف هذه الاستراتيجية إلى معالجة الكميات الهائلة من البيانات التي تُنتجها أجهزة الاستشعار المختلفة، وتحويلها إلى معلومات دقيقة وقابلة للتنفيذ. كما تضع استراتيجية الجيش الإسرائيلي سيناريوهات متعددة تشمل استخدام أجهزة استشعار متقدمة عبر منصات متنوعة، لجمع البيانات حول التهديدات المحتملة وإرسالها إلى الأنظمة القادرة على اتخاذ إجراءات سريعة وفعالة. يتيح هذا النهج للجيش جمع البيانات الواردة من الجو والأرض والبحر ودمجها باستخدام تقنيات الذكاء الاصطناعي؛ مما يُنتج صورة موحدة تُعتمد عليها القوات الإسرائيلية في ميدان القتال. وتعمل القوات من غرفة حرب واحدة على مجموعة البيانات نفسها، بهدف صياغة صورة دقيقة قدر الإمكان لدعم القرارات العملية وتقليل الأضرار الجانبية.

وقد سعى الجيش إلى تعزيز فاعليته وكفاءته لمواجهة التحديات والتهديدات الجديدة، خاصة في أعقاب حرب السابع من أكتوبر 2023، التي شهدت هجوماً متعدد الجبهات، وتطلبت استجابة مرنة في ساحات قتال متعددة. وقد تم تنفيذ الاستراتيجية العسكرية الجديدة من خلال قسم ذكاء اصطناعي مركزي تم إنشاؤه كجزء من التحول الرقمي الشامل للجيش الإسرائيلي الذي دفعه رئيس الأركان الأسبق «أفييف كوخافي» على مدى السنوات الماضية⁽²⁾. هذا القسم يمثل الهدف الرئيسي له في تقديم حلول تعتمد على الذكاء الاصطناعي للتحديات التي يواجهها العنصر البشري في ساحة المعركة دون استبداله. ومن بين مهامه، تطوير تقنيات تهدف إلى الحد من ظاهرة الرماية الثنائية. وقد قام هذا القسم بتطوير العديد من البرمجيات التي تستخدمها قواته، ومن أبرز هذه البرمجيات تلك المعنية بمراقبة وصيانة قدرات القوات والدبابات خلال التدريبات. إن قدرات تلك البرمجيات لا تقتصر فقط على تقييم حالة كفاءة القوات، بل تشمل أيضاً التحذير في الوقت الفعلي من التهديدات التي تقترب من القوات في أراضي العدو.

في سياق آخر، وبالتعاون مع قسم الذكاء الاصطناعي، تم تطوير قدرة جديدة للكوادر الطبية في كتيبة الاتصالات التابعة للقيادة الجنوبية. هذه القدرة تتضمن لوحة تحكم شاملة لعملية الإخلاء الطبي للجرحى من ساحة المعركة تحت مسمى «الساعة الذهبية»، وهو مصطلح يشير إلى الوقت الحاسم الذي يجب فيه إخلاء الجرحى الذين يعانون من إصابات خطيرة إلى المستشفى لإنقاذ حياتهم. كما يوفر هذا التطوير حسابات دقيقة وصحيحة لاتخاذ القرارات الحاسمة في إخلاء الجرحى، من خلال تحديد المستشفى الأنسب بناءً على العوامل المختلفة مثل الأحمال الموجودة في المستشفى أو نوع الإصابة، وتحديد أولويات الإخلاء استناداً إلى: خبرة المستشفى، ووقت وطبيعة الإخلاء، وإمكانية وصول الفرق الطبية إلى المنطقة، والموقع الجغرافي للإصابة.

أما فيما يخص التطورات الأخرى، كتلك التي تشمل مجالات العمليات الحساسة، تم تطوير برمجيات خلال حرب إسرائيل على غزة للمساعدة في تحديد واكتشاف أنفاق حركة «حماس» لتدميرها، بالإضافة إلى العثور على الرهائن واستهداف كبار المسؤولين في حركة حماس. كما أدخلت شعبة الاتصالات مفاهيم جديدة للدفاع عن الحدود من خلال استخدام الذكاء الاصطناعي لتحليل البيانات والمتغيرات؛ مما يتيح التعرف المبكر على التهديدات، واستهداف أسرع وأكثر دقة وحماية أكثر فاعلية. تكمن المهمة هنا في جمع البيانات من مصادر متعددة ودمجها، وتحليل الاتجاهات والأحداث، لتوفير رؤى تدعم اتخاذ القرارات من قبل القادة⁽³⁾. فنتيجة لتنوع القدرات التكنولوجية، ظهرت الحاجة إلى مهن جديدة في الجيش الإسرائيلي، مثل المساعدين التكنولوجيين للقادة والمحللين المسؤولين عن المعلومات في جميع أنحاء الجيش. هذا يأتي في إطار التحضير للحروب التكنولوجية المستقبلية متعددة الجبهات التي تعتمد بشكل أساسي على الوسائل الرقمية⁽⁴⁾.

1. الأدوات الإسرائيلية في إدارة الحروب الذكية:

بدأ الجيش الإسرائيلي في توظيف الذكاء الاصطناعي في أنشطته ضمن مجالات رئيسية؛ يتعلق أولها بتحليل المعلومات الاستخباراتية وتحديد الأهداف العسكرية، بينما يتعلق ثانيها بأنظمة التنبيه والتنبؤ بالتهديدات، بالإضافة إلى الحماية والسيطرة عليها. ففي المجال الأول، تم تطبيق نظام (The Gospel) في عام

2021، الذي يمر عبر طبقات متعددة من المعلومات الاستخباراتية. إذ يوفر هذا النظام للمحللين الاستخباراتيين توصيات حول الأهداف المحتملة التي قد تكون أهدافاً عسكرية؛ مما يساعد في تقليص الوقت اللازم لجمع وتحليل البيانات مقارنة بالعملية اليدوية التقليدية التي قام بها سلفاً المحققون بأنفسهم. أما في المجال الثاني، فقد تم الكشف عن نظام آخر يعتمد على الذكاء الاصطناعي في عام 2023 وهو (Fire Factory)، الذي يهدف إلى تحديد الأهداف العسكرية للغارات الجوية وتعزيز التنسيق الاستراتيجي للعمليات العسكرية. ويقوم هذا النظام بتحليل البيانات الناتجة عن الهجمات السابقة، ويحسب الذخيرة المطلوبة لكل هجوم، ويقدم جداول زمنية مثالية، بالإضافة إلى تحديد الأولويات للأهداف المختلفة.

من الأنظمة الأخرى التي اعتمدها الجيش الإسرائيلي هو نظام (Fire Weaver) الذي طورته شركة «رافائيل». هذا النظام يعزز الاتصال بين الجنود المنتشرين في ساحة المعركة والمعلومات الاستخباراتية المجمعة؛ مما يتيح خيارات عمل مبنية على عوامل مثل: الموقع، وخط الرؤية، والكفاءة، والذخيرة المتاحة، بهدف زيادة الدقة وتقليل الأضرار الجانبية. وإلى جانب هذا، وفي الآونة الأخيرة، تم استخدام نظام جديد يعتمد على الذكاء الاصطناعي يسمى «لافندر»، والذي تم تطبيقه بشكل أساسي في المراحل الأولى من القتال في قطاع غزة. إذ يهدف هذا النظام إلى تحديد المواقع المشتبه في انتمائها إلى المنظمات الإرهابية في القطاع كأهداف محتملة⁽⁵⁾. وفي ضوء تجلي توظيف إسرائيلي لتقنيات الذكاء الاصطناعي في عملياتها العسكرية، نرد عددًا من الأنظمة والاستخدامات على النحو التالي:

أ. الروبوتات المقاتلة والأسلحة ذاتية التشغيل: شهدت السنوات الأخيرة تزايداً ملحوظاً في اعتماد إسرائيل على أنظمة الأسلحة ذاتية التشغيل، بما في ذلك الطائرات دون طيار التي تعتمد على التكنولوجيا الحديثة لأغراض استطلاعية وعملياتية. وفي إطار سعي إسرائيل لتطوير استراتيجيات جديدة قائمة على الذكاء الاصطناعي، قامت بإطلاق الجيل الثاني من الروبوت المقاتل «رووك 6×6» الذي صُمم لأداء مهام الجنود في المعارك. يشمل ذلك: أنشطة المراقبة، والإدارة عن بُعد، والدفاع، والمناورة، والهجوم، بالإضافة إلى مهام إنقاذ الجثث ونقل الإمدادات وتنفيذ العمليات بتنسيق آلي دقيق⁽⁶⁾.

تتميز هذه الروبوتات بقدرتها على التعامل مع المهام «الخطرة» أو «القدرة» مثل تفكيك الذخائر المتفجرة والتعامل مع المواد الإشعاعية، متجاوزة بذلك القيود البشرية الفسيولوجية. كما تم توظيف هذه الروبوتات من قبل إسرائيل في عمليات ميدانية، تشمل: إطلاق الغاز المسيل للدموع، والقنابل الصوتية، والرصاص المطاطي ضد المتظاهرين الفلسطينيين، وخاصة في الضفة الغربية. وقد شهدت مدينة الخليل توظيف هذه الروبوتات كجزء من الجهود الإسرائيلية للتعامل مع الاشتباكات والمواجهات مع الفلسطينيين⁽⁷⁾.

ب. أنظمة المراقبة: شهدت السنوات الأخيرة تصاعداً في استخدام إسرائيل لتقنيات المراقبة الجماعية في إطار استراتيجياتها الأمنية. ومن أبرز هذه التقنيات، تركيب كاميرات مراقبة في نقاط التفتيش والحواجز بهدف تتبع الأهداف البشرية خلال المواجهات مع الفصائل الفلسطينية تحت ذريعة «مكافحة العمليات الإرهابية». وقد تجاوز عدد الكاميرات المثبتة في الضفة الغربية 1700 كاميرا. ولم تكن هذه الاستراتيجية جديدة، حيث اعتمدت إسرائيل سابقاً على تقنيات متقدمة لمراقبة الفلسطينيين، بما في ذلك استخدام أجهزة المخابرات لتطبيقات إلكترونية تتيح تتبع كلمات وعبارات محددة يتم تداولها داخل الأراضي المحتلة. تسهم هذه التقنيات في تعزيز قدرة إسرائيل على جمع المعلومات ومتابعة التحركات؛ مما يعكس تطور أساليب المراقبة ضمن سياق الحروب الذكية⁽⁸⁾. قبل اندلاع حرب السابع من أكتوبر، كثفت الآلة الإعلامية الإسرائيلية جهودها لتسليط الضوء على ما اعتبرته إنجازات في مجال توظيف الذكاء الاصطناعي. وركزت هذه الجهود على بناء قاعدة بيانات رقمية متكاملة على مدار سنوات بهدف تعزيز آليات المراقبة على الفلسطينيين. وقد شملت هذه العمليات استخدام كاميرات مراقبة متطورة وتطبيقات برمجية متخصصة لالتقاط صور دقيقة لوجوه الفلسطينيين، ضمن استراتيجية شاملة للملاحقة والمراقبة الجماعية والتجسس⁽⁹⁾.

توقع اندلاع الحروب المستقبلية: تشهد الأبحاث العلمية تصاعداً في تطوير استخدامات الذكاء الاصطناعي للتنبؤ بالحروب المستقبلية من خلال إنشاء قواعد

بيانات شاملة تحتوي على معلومات دقيقة حول الدول، مثل تاريخها ومستوى تسليحها وبيانات أخرى ذات صلة. وفي هذا الإطار، تعمل إسرائيل على توظيف الذكاء الاصطناعي في المجال العسكري لإنشاء سيناريوهات متقدمة تُحدد وفقًا لعوامل زمنية وجغرافية محددة. تعتمد هذه السيناريوهات على خوارزميات مدروسة يتم برمجتها استنادًا إلى معطيات دقيقة؛ مما يتيح تقييم فرضيات معينة إما بتأكيداها وإما بنفيها. يهدف هذا النهج إلى تحسين القدرة على التنبؤ بالحروب قبل وقوعها؛ مما يمكن إسرائيل من تخطيط استراتيجيات عسكرية استباقية ومواجهة التهديدات المحتملة بفاعلية أكبر، مع ضمان اتخاذ قرارات مستنيرة ومدروسة تدعم عملياتها العسكرية المستقبلية.

ج. توظيف تقنية التزييف العميق: أدركت إسرائيل حجم التأثير الذي يمكن أن يحدثه التضليل البصري عبر وسائل التواصل الاجتماعي والمنصات الرقمية الأخرى؛ مما دفعها إلى تطوير تقنيات متقدمة تعتمد على الذكاء الاصطناعي لاكتشاف وتوظيف التزييف العميق. وقد برزت حرب السابع من أكتوبر كواحدة من أبرز الأمثلة على الحروب الافتراضية، حيث اعتمدت كل من إسرائيل والمقاومة الفلسطينية بشكل كبير على هذه التقنية، حيث تم بث عشرات من مقاطع الفيديو عبر منصات مثل «تيك توك»، و«فيسبوك»، و«تليجرام». وقد كان جزء كبير منها مزيّفًا باستخدام خوارزميات الذكاء الاصطناعي. وقد تم توظيف هذه الفيديوهات كأداة في الحروب الافتراضية، بهدف التأثير في الطرف الآخر وتعزيز استراتيجيات الحرب النفسية⁽¹⁰⁾.

ثانيًا: الأبعاد الاستراتيجية للحروب الافتراضية في السياق الإسرائيلي

شهدت تقنيات الذكاء الاصطناعي تطورات كبرى في السنوات الأخيرة؛ مما أتاح إنتاج النصوص والصور ومقاطع الفيديو بشكل متقدم. وبعد إخفاق الجيش الإسرائيلي في تحقيق صورة نصر واضحة خلال حرب لبنان الثانية عام 2006، لجأت إسرائيل إلى توظيف تقنيات الذكاء الاصطناعي لتعزيز الحروب الافتراضية. كان الهدف الأساسي لهذه الاستراتيجية هو التأثير في العقول بطرق غير مباشرة، وتحسين صورة إسرائيل عالميًا، بالإضافة إلى مواجهة الدعاية السلبية الموجهة ضدها. وفي هذا

السياق، استعانت أجهزة الاستخبارات الإسرائيلية والوحدات الإعلامية التابعة لها بمنصات التواصل الاجتماعي كساحة جديدة للحروب الافتراضية، حيث تم توظيف هذه المنصات من جانب للتنبؤ بثورات محتملة في العالم العربي، ومن جانب آخر لاختراق الرأي العام العربي والتلاعب بتوجهات الشباب في منطقة الشرق الأوسط. كما هدفت هذه الأنشطة إلى التأثير في الأفكار والسيطرة على التوجهات بما يخدم المصالح الإسرائيلية في إطار حرب ناعمة متعددة الأبعاد.

1. الدوافع الإسرائيلية من الحروب الافتراضية:

تستخدم إسرائيل الحروب الافتراضية لتعزيز قدراتها المعلوماتية والاستخباراتية مستفيدة من تقنيات الذكاء الاصطناعي التي تمكنها من شن عمليات متقدمة في الحرب على العقول. تعتمد هذه الحروب على استراتيجيات التخفي وعدم الكشف عن الهوية؛ مما يجعلها أداة فعالة لتغيير القناعات وتحقيق أهداف أمنية واستراتيجية دون أن تظهر الجهة الحقيقية التي تقف وراءها. يمكن تلخيص الدوافع الإسرائيلية في عدد من النقاط التالية:

- أ. شن حروب معلوماتية سرية: تُعنى باستهداف الأعداء من خلال جمع المعلومات الاستخباراتية وتنفيذ هجمات رقمية تسهم في إحباط مخططاتهم.
- ب. إحباط أعمال المقاومة: تقوض الجهود التي تبذلها جهات المقاومة ضد إسرائيل من خلال الكشف عن خططها وإفشالها في المراحل المبكرة.
- ج. تعزيز القدرات الدفاعية والهجومية: تطور أدوات وتقنيات لتمكين وحدات الحروب الافتراضية من العمل بكفاءة في فضاء المعلومات الذي أصبح ساحة قتال حديثة.
- د. إمداد الجيش الإسرائيلي بالمعلومات الدقيقة: تجمع وتحلل كميات كبيرة من البيانات لدعم القرارات الاستراتيجية وتعزيز قدرة الجيش على تنفيذ العمليات بكفاءة.
- هـ. تحقيق أهداف الأمن القومي: تستخدم الحروب الافتراضية كوسيلة للردع وكشف نوايا الأعداء، مما يساهم في حماية المصالح الإسرائيلية وإحباط مشاريع معادية.

و. شن حروب ناعمة: تصعيد استخدام الحروب النفسية والشائعات لزعزعة استقرار المجتمعات المستهدفة. يتم ذلك عبر التأثير في الفئات المستهدفة باستخدام أساليب تعتمد على تقنيات الذكاء الاصطناعي.

ز. استهداف المواقع الحساسة: جمع معلومات استخباراتية عن المواقع العسكرية والمنشآت الأمنية في الدول التي ترى إسرائيل أنها تمثل تهديداً مستقبلياً.

ح. تعقب المعلومات الاقتصادية: توظيف الذكاء الاصطناعي لجمع بيانات عن المشروعات الاستثمارية والقطاعات الاقتصادية؛ مما يسمح باختراق تلك الدول عبر عناصر الموساد.

ط. إحداث تفكك اجتماعي وثقافي: تنفيذ عمليات تهدف إلى تخريب القيم الأخلاقية والثقافية باستخدام تقنيات الهندسة الاجتماعية لإثارة الخلافات داخل المجتمعات المستهدفة.

ي. تعزيز الإعلام الإسرائيلي: توظيف الذكاء الاصطناعي لدعم الحملات الإعلامية التي تهدف إلى تحسين صورة إسرائيل، عبر التركيز على:

- تلطيف صورة العنف الذي تمارسه آلة الحرب الإسرائيلية.
- استخدام الدبلوماسية العامة ومنصات الرقمية للرد على أي نشر سلبي ضد إسرائيل.
- جذب التعاطف العربي عبر الاستقطاب الإلكتروني وإنشاء قنوات تواصل بين النخب العربية والإسرائيلية.

ك. الوحدات المسؤولة عن التنفيذ: تتولى الوحدات التكنولوجية العسكرية في الجيش الإسرائيلي تنفيذ هذه المهام، حيث يتم تقسيمها إلى أقسام متخصصة تتعامل مع العمليات المعلوماتية المختلفة؛ مما يضمن تحقيق الأهداف الاستراتيجية بكفاءة وسرعة⁽¹¹⁾.

2. دور الحروب الافتراضية في الاستراتيجية الإسرائيلية:

لم تكن في الحروب الماضية هناك مشكلة خاصة في تعريف الحسم والنصر، حيث كان الحسم واضحاً على أرض الواقع في ميدان المعركة، وبعدها انتقل الحسم في المعارك إلى شبكات التواصل الاجتماعي التي نجحت في العقد الماضي في تشكيل الوعي الجمعي والسلوكي لرواد الشبكة العنكبوتية، أصبح هناك إشكالية معقدة

في تحديد الحسم والنصرومن هو المعتدي ومن هو المدافع. وهو ما دفع الجيش الإسرائيلي لتطوير استراتيجيته الإعلامية واستحداث وحدات جديدة تواكب العصر بعد انتهاء عصر الحروب التقليدية إلى الحروب الافتراضية، وفيما يلي استعراض لأبرز تلك الوحدات والمهام الاستراتيجية المكلفة بها⁽¹²⁾:

أ. غرفة الحرب الرقمية والمهام المكلفة بها: في السنوات الأخيرة، ركز الجيش الإسرائيلي بشكل متزايد على توظيف شبكات التواصل الاجتماعي كأداة مركزية في الحروب الافتراضية، خاصة مع تراجع فرص تحقيق انتصارات حاسمة في المعارك التقليدية. أصبحت منصات مثل «يوتيوب»، «تويتر»، «فيسبوك»، و«تيك توك» جزءاً أساسياً من استراتيجيات الحرب الرقمية، حيث جرى تجهيز «غرفة الحروب الرقمية» للتعامل مع أي سيناريو محتمل. وبشكل عام، اعتمد الجيش على تقنيات الذكاء الاصطناعي، مثل التزيف العميق، لإنتاج محتوى مرئي موجه يعرض صوراً إيجابية له بهدف تحسين صورته والتخفيف من الانتقادات الموجهة إليه بسبب القوة المفرطة خلال فترات الحرب. وعليه، تسعى غرفة الحروب الافتراضية إلى التحكم في السردية الرقمية وقيادتها على الإنترنت، خصوصاً في أثناء الأزمات. بدلاً من التفاعل مع ما يتحدث عنه الجميع، تعمل على تقديم محتوى يتماشى مع لغة الشبكات الاجتماعية، معتمدة على دراسة دقيقة للحالة المزاجية للمستخدمين للتأثير في آرائهم وتوجهاتهم⁽¹³⁾.

ب. مكتب (I Monitor) والمهام المكلف بها: تعمل المخابرات الإسرائيلية على جمع وتحليل المعلومات من وسائل الإعلام التقليدية والشبكات الاجتماعية لمواجهة التهديدات الأمنية المحتملة. ومن خلال مكتب (I Monitor)، يتم مراقبة النشاط والشخصيات المؤثرة في العالم العربي، حيث تُفحص ملايين المكالمات والرسائل يومياً لاكتشاف ما يعتبره الاحتلال تهديدات أمنية، مثل تسريب الأسرار العسكرية أو الكشف عن أنشطة سرية. إذ يقوم المكتب بتحليل البيانات الرقمية، بما في ذلك الصور ومقاطع الفيديو، بهدف تقديم استنتاجات وتحليلات استراتيجية لصناع القرار العسكريين والسياسيين. تعتمد هذه التحليلات على أدوات متقدمة لتقييم الأوضاع في المناطق المستهدفة وفهم أنماط المقاومة والاحتجاجات. وتركز المخابرات الإسرائيلية على تتبع قادة

المقاومة الفلسطينية والشخصيات المؤثرة في الدول المعادية، كما تراقب التحولات السياسية الإقليمية، بما في ذلك الاحتجاجات في العالم العربي. ويوفر المكتب معلومات استراتيجية تُستخدم لرصد ديناميكيات الصراع وتوجيه السياسات الإسرائيلية، فيتفرد باستخدام تقنيات متطورة مثل خوارزميات التعرف على الوجوه واستخراج البيانات من المصادر المفتوحة. كما يولي أهمية خاصة لمتابعة الشخصيات المؤثرة، مثل الصحفيين وصناع الرأي، بهدف التأثير في المشهد الإعلامي والسياسي، بل وحتى تأجيج الخلافات بين الدول الإقليمية مثل قطر والسعودية، لتعزيز الأهداف الإسرائيلية في المنطقة⁽¹⁴⁾.

ج. وحدة 3060 والمهام المكلفة بها: تم إنشاء الوحدة 3060 في عام 2014 عقب عملية «الجرف الصامد» في قطاع غزة، وظلت طي الكتمان حتى أعلن الجيش الإسرائيلي عن وجودها في يناير 2018. تعتبر هذه الوحدة جزءاً محورياً من ثورة علوم البيانات التي يعتمد عليها الجيش الإسرائيلي لمواجهة التحديات الاستخباراتية في العصر الرقمي. إذ يواجه الجيش الإسرائيلي تحديات متزايدة ناجمة عن التدفق الهائل للمعلومات من مصادر متنوعة، مثل: النصوص المكتوبة، والتسجيلات الصوتية، والصور، ومقاطع الفيديو، والجداول، والخرائط، فضلاً عن التفسيرات المشتقة من هذه البيانات. هذا الكم الضخم من البيانات، إلى جانب الحاجة لاتخاذ قرارات فورية في أثناء العمليات، دفع شعبة الاستخبارات إلى استخدام تقنيات الذكاء الاصطناعي والخوارزميات لتسهيل معالجة البيانات وتحويلها إلى رؤى قابلة للتنفيذ. وعليه، تتولى الوحدة 3060 تطوير أنظمة وتطبيقات تلبي احتياجات ضباط الاستخبارات في مختلف القطاعات. في أثناء العمليات القتالية، تتطلب عملية تحديد الأهداف سلسلة معقدة ومتكاملة من المهام الاستخباراتية، تشمل جمع المعلومات وتحليلها ومعالجتها في ظل ضغوط زمنية كبيرة. وللتعامل مع هذه المتطلبات، تعتمد الوحدة على أنظمة ذكاء اصطناعي متطورة يتم تدريبها باستخدام بيانات سابقة عن أهداف محددة. تساعد هذه الأنظمة في تمييز الأهداف المحتملة، ترتيب أولوياتها، وتقديم اقتراحات دقيقة؛ مما يسرّع عمليات اتخاذ القرار ويحسن كفاءة الاستهداف خلال العمليات العسكرية⁽¹⁵⁾.

د. القسم التكنولوجي واللوجستي للدعم والإمداد: يقدم هذا القسم مجموعة متنوعة من الخدمات التقنية للجيش الإسرائيلي؛ أبرزها: صيانة وتأهيل الوسائل القتالية التقليدية وغير التقليدية، وضمان الجاهزية التقنية الشاملة للجيش، وتوفير حلول لوجستية رقمية ومعلوماتية متطورة. بالإضافة إلى ذلك، يختص بتقديم الأبحاث الاستخباراتية والمعلوماتية للجهات المعنية.

هـ. قسم تكنولوجيا الاتصالات والدفاع السيبراني: يتولى هذا القسم الرقمي العسكري وضع سياسات تكنولوجيا المعلومات والاتصالات المطبقة في الوحدات التقنية التابعة للجيش الإسرائيلي، إلى جانب توفير الحلول التشغيلية والإلكترونية لتلبية احتياجات الجيش بالكامل في هذا المجال، إضافة إلى تنفيذ مهام رقمية ومعلوماتية أخرى. ويركز القسم بشكل كبير على تطوير أساليب الحرب الإلكترونية التي يستهدف بها الجيش الإسرائيلي الجهات المعادية، من خلال ابتكار أنظمة إلكترونية وبرامج تطبيقات حاسوبية متقدمة. كما يعمل على تشغيل أجهزة لبث المعلومات المضللة عبر وسائل الإعلام ومنصات التواصل الاجتماعي والإنترنت⁽¹⁶⁾.

وعليه، يمكن إجمال استخدامات الذكاء الاصطناعي في الأبعاد الرئيسية للأمن الإسرائيلي على النحو الآتي:

أ. الأمن الخارجي والداخلي: يستخدم نظام الأمن تطبيقات الذكاء الاصطناعي في مجالات الاستخبارات، وأنظمة الأسلحة، والأنظمة العسكرية الأخرى.

ب. علاقات إسرائيل الخارجية ومكانتها الدولية: يوظف الذكاء الاصطناعي في ضوء الحفاظ على مكانة إسرائيل وتحسين صورتها الذهنية.

ج. الحوكمة: يتم استخدام الذكاء الاصطناعي في الإشراف على اتخاذ القرار والتنفيذ، ودعم اتخاذ القرار والمحاكاة.

وفي ضوء ذلك، نستنتج أن العناصر الأساسية لمفهوم الأمن الإسرائيلي، القائم في مجمله على الردع والتنبية والتصميم والحماية، تؤكد بما لا يدع مجالاً للشك أن الذكاء الاصطناعي بات بعداً رئيسياً لدى إسرائيل لما له من قدرة على إحداث تأثير إيجابي من خلال تطوير ذلك التعاون مع الوحدات العسكرية الإسرائيلية المختلفة، وخاصة الوحدات التكنولوجية العامة في حروب الميديا⁽¹⁷⁾.

3. الأبعاد الاستراتيجية للحروب الافتراضية الإسرائيلية:

بدأت إسرائيل بالفعل توظيف الذكاء الاصطناعي في حربيها الإعلامية، معتبرةً أن الإعلام هو «فن النصر دون حرب». وعندما لا يتحقق النصر العسكري، تصبح هذه التقنيات أداة لتمهيد الظروف للحرب، كما شهدته العمليات العسكرية في قطاع غزة⁽¹⁸⁾. ولذلك، أصبح توظيف الذكاء الاصطناعي أداة حيوية لوحدة الحروب الافتراضية في الجيش الإسرائيلي. فمع انتشار الأجهزة الإلكترونية بين جمهور منصات التواصل في الشرق الأوسط، وتصفح الإنترنت عبر الهواتف المحمولة، وإنتاج كميات هائلة من المعلومات، كان لدى إسرائيل الدافع لتطوير أدوات وأساليب لجمع وتحليل هذه البيانات. وللتكيف مع هذه التطورات، تم توظيف الذكاء الاصطناعي عبر حسابات مزيفة، خاصة بالعالم العربي، لتسهيل استهداف الجمهور دون إثارة الشكوك. في هذا السياق، تعد المعلومات والأخبار عنصراً أساسياً للأمن والاستقرار، ولا يمكن لأي دولة تجاهل دورها الحاسم في إشعال الحروب⁽¹⁹⁾.

ومن أبرز نماذج استخدامات إسرائيل للذكاء الاصطناعي في الحروب الافتراضية استخدام التزييف العميق في التضليل المعلوماتي؛ فمع تطور تقنيات الذكاء الاصطناعي، أصبحت عملية تزييف الوعي والحقائق ونشر المعلومات المضللة أكثر تعقيداً وشيوعاً في العالم من خلال نشر صورة أو مقطع فيديو أو نص أو خبر أو إعلان على وسائل التواصل الاجتماعي، لينقل فكرة أو شعوراً معيناً للتأثير في الرأي العام. إذ يعتمد التزييف العميق على تطبيقات الذكاء الاصطناعي، حيث يمكن إنشاء محتوى مزيف يبدو حقيقياً من خلال الجمع بين الصور ومقاطع الفيديو الموجودة على الصور ومقاطع الفيديو الأصلية. بسبب هذه القدرات، ومن خلال هذه التقنية يمكن إنتاج مقاطع فيديو لاغتيال معنوي لساورة ومشاهير لإشاعة أخبار كاذبة للتأثير في الرأي العام. فيما تكمن خطورة توظيف تقنية التزييف العميق في حروب الوعي بأنها تبدو قريبة جداً من الشيء الحقيقي، في عالم يمكنك فيه نشر المعلومات للعالم بسرعة كبيرة وجعل صدق لها، البعض قد يعتقد أن بعض الشخصيات السياسية قالت شيئاً وهو لم يُقال في الواقع، حيث يتيح إنتاج مقاطع فيديوهات وصور اصطناعية مزيفة، تظهر لأول وهلة وكأنها حقيقية بشكل كبير. وهو ما يجعل

من الصعب اكتشاف التزييف عند إطلاق المحتوى الاصطناعي على شبكة الإنترنت وعبر وسائل الإعلام ومواقع التواصل الاجتماعي المختلفة، ويستمر هذا المحتوى بحصد نسب كبيرة من المشاهدات والمشاركات بالملايين حتى بعد اكتشاف التزييف من قبل المتخصصين المحترفين.

وفيما يلي استعراض لتقنيات واستخدامات الذكاء الاصطناعي في نشر المعلومات المضللة، والتي من أبرزها ما يلي:

أ. تقنية الفيديوها المبركة «Deep fakes Videos»: تحتاج الفيديوها المبركة لدرجة عالية من الدقة واستخدام متقن للوسائل التكنولوجية، بالإضافة إلى توفر الوقت اللازم والإمدادات المالية وأيضاً المهارة الفردية.

ب. تقنية نسخ الصوت «Voice Cloning»: طريقة يتم من خلالها التلاعب بالحقائق، حيث تسمح العديد من التطبيقات عبر الإنترنت والهواتف المحمولة للمستخدمين القيام بمحاكاة أصوات المشاهير.

ج. تقنية الصور المزيفة Deep fakes Images: إذ تأتي هذه الصور على شكل لقطة مصورة لوجه شخص تبدو حية للغاية على الرغم من كونها غير حقيقية.

د. تقنية النصوص المفتعلة Generative Text: إذ يتم استخدام نماذج اللغة الموجودة بأجهزة الكمبيوتر لإنشاء النصوص المختلفة، وهي التي يمكن أن يستغلها الخصوم الأجانب.

وفي ضوء ذلك نستعرض عددًا من الأسباب لاستخدام إسرائيل لتقنيات الذكاء الاصطناعي في نشر المحتوى المزيف من أبرزها:

أ. زرع الانقسامات الاجتماعية، بهدف نشر الدعاية الموجهة لتقسيم الجمهور ومهاجمة وتشويه سمعة الأطراف السياسية المعارضة.

ب. نزع الثقة في المؤسسات والسلطات، وذلك من خلال نشر فيديوها تدعي على سبيل المثال ممارسة بعض الأفراد من قوى إنفاذ القانون بشكل خاص طرق التحايل على النظام.

ج. تقويض الصحافة والمؤسسات الإخبارية البارزة ومصادر المعلومات الجديرة بالثقة، بالإضافة لزرع الفتنة حتى في القنوات الشرعية والمسئولة عن الأخبار والمعلومات⁽²⁰⁾.

ثالثاً: توظيف الحروب الافتراضية الإسرائيلية في حرب السابع من أكتوبر

مع التحول الجذري نحو الإعلام الرقمي وتزايد الاعتماد على تقنيات الذكاء الاصطناعي، أصبحت الحروب الافتراضية أحد العناصر الحاسمة في النزاعات الحديثة. وقد أثبتت هذه الحروب، التي تستند إلى تكنولوجيا المعلومات والذكاء الاصطناعي، أنها تُحدث تأثيراً كبيراً في الرأي العام؛ مما يجعلها سلاحاً فعالاً في تشكيل الوعي المجتمعي والتأثير في الخصوم. وفي عصر ما بعد الحقيقة، يشهد العالم تصاعداً غير مسبوق في انتشار المعلومات المضللة، حيث تلعب تقنيات التزييف العميق دوراً رئيسياً في تضليل الرأي العام وتشويه الواقع. يتمثل الخطر الأكبر لهذه التقنيات في قدرتها على إنشاء محتوى بصري وصوتي يبدو واقعياً للغاية ولكنه في الحقيقة زائف؛ مما يؤدي إلى تشويش الحقائق وزعزعة الثقة في قدرة الأفراد والمجتمعات على التمييز بين الحقيقة والخداع⁽²¹⁾.

وخلال حرب السابع من أكتوبر، استغلت إسرائيل هذه القدرات الرقمية لتوظيف الحروب الافتراضية كأداة استراتيجية في صراعها ضد حماس وأطراف أخرى مثل حزب الله وإيران. فاستخدمت إسرائيل خوارزميات الذكاء الاصطناعي وتقنيات التزييف العميق في إطار حملات تستهدف: التلاعب بالحقائق، وتشويش الوعي لدى الرأي العام المحلي والدولي لصالح تحقيق أهدافها الاستراتيجية، وكذلك تعزيز الهيمنة الإعلامية من خلال السيطرة على السرديات المطروحة في الفضاء الرقمي. وفي هذا السياق، يمكن القول إن الحروب الافتراضية التي قادتها إسرائيل في السابع من أكتوبر تمثل نموذجاً معاصراً للحروب الرقمية التي تجمع بين الأبعاد النفسية والإعلامية والعسكرية؛ مما يعزز من أهمية دراسة هذه التجارب لفهم الدور المتنامي للذكاء الاصطناعي في النزاعات المستقبلية⁽²²⁾.

وفيما يلي استعراض للأبعاد الاستراتيجية لتوظيف تقنيات الذكاء الاصطناعي في حرب السابع من أكتوبر، وذلك على النحو التالي:

1. استخدامات تقنيات الذكاء الاصطناعي في حرب السابع من أكتوبر:

أحدثت تقنيات الذكاء الاصطناعي تحولاً جذرياً في إدارة النزاعات العسكرية بين إسرائيل والتنظيمات، حيث أصبحت أداة استراتيجية تُسهم في تعزيز الكفاءة وتحسين فاعلية القرارات العسكرية. وفي سياق حرب السابع من أكتوبر، لعبت هذه التقنيات دوراً محورياً في دعم العمليات العسكرية الإسرائيلية من خلال المحاور التالية:

أ. تحليل تحركات العدو وإدارة القتال: فقد أسهمت تقنيات الذكاء الاصطناعي في تحليل كميات هائلة من البيانات والاستخبارات الميدانية بسرعة ودقة؛ مما قلل من احتمالية الأخطاء البشرية. ساعدت هذه الأدوات المتقدمة في تقييم التحركات العسكرية، التنبؤ بالتهديدات، وتقديم توصيات استراتيجية تعتمد على التحليل الفوري للبيانات، وذلك من خلال:

- التخطيط الاستراتيجي: تمكن الذكاء الاصطناعي من تقديم تصور شامل عن تحضيرات العدو واستراتيجياته؛ مما سمح بتنفيذ حرب نفسية فعالة واستغلال نقاط الضعف.
- إدارة المعركة: ساعدت هذه التقنيات في التكيف السريع مع المتغيرات الميدانية؛ مما عزز من قدرة الجيش على اتخاذ قرارات أكثر فاعلية في اللحظات الحرجة.

ب. دعم القيادات العسكرية في عملية اتخاذ القرار: أسهم الذكاء الاصطناعي في تعزيز عملية اتخاذ القرار من خلال توفير تحليل معمق للبيانات وإنتاج سيناريوهات متعددة لمواجهة مختلف التحديات، وذلك من خلال:

- دقة التقييم: قدمت الأنظمة الذكية رؤى غير تقليدية قد لا تكون ظاهرة للضباط؛ مما ساعد على تعديل الخطط لتناسب مع الأوضاع المتغيرة.

- تعزيز المرونة: مكنّ الذكاء الاصطناعي القيادات من اتخاذ قرارات استراتيجية تعتمد على أسس علمية وتنبؤية؛ مما أتاح لهم ميزة تنافسية في إدارة العمليات العسكرية.
- ج. الأسلحة الذكية والمستقلة: شهدت الأسلحة تطوراً كبيراً بفضل الذكاء الاصطناعي، الذي رفع كفاءتها ودقتها، على سبيل المثال:
 - الصواريخ الموجهة: أصبحت بفضل تقنيات الذكاء الاصطناعي قادرة على المناورة وتحديد الأهداف بدقة عالية، مع مراعاة وسائل الحماية المستخدمة من قبل العدو.
 - إدارة المركبات القتالية: أتاحت خوارزميات الذكاء الاصطناعي إمكانية تشغيل المركبات باستخدام بيانات الخرائط والتضاريس؛ مما زاد من دقة تنفيذ المهام وتعزيز كفاءة الأداء الميداني.
- د. إدارة وصيانة المعدات العسكرية: واجهت الجيوش تحديات متزايدة في صيانة المعدات وإدارة الموارد، وهو ما ساعدت تقنيات الذكاء الاصطناعي في تحسينه بشكل كبير.
 - الصيانة الوقائية: ساعدت هذه التقنيات في التنبؤ بمواعيد الصيانة المثلى للأسلحة والذخيرة؛ مما قلل من التكاليف وهدر الموارد.
 - الكفاءة التشغيلية: وفرت أدوات الذكاء الاصطناعي آليات دقيقة لتحديد المعدات غير الصالحة وإصلاحها في الوقت المناسب؛ مما أسهم في تحسين الجاهزية العسكرية بشكل كبير.
- هـ. تحليل أنماط القرار لرجال المقاومة: تم في إحدى الدراسات الحديثة تحليل القرارات الاستراتيجية التي يتخذها قادة التنظيمات باستخدام تقنيات متقدمة في تحليل صنع القرار المحوسب، حيث تم تطبيق برنامج (Huddle AI Decision)، للتنبؤ بسلوك التنظيمات المسلحة وسيناريوهات استجابتها في مواقف استراتيجية مختلفة. وقد خلص تحليل القرارات للقيادي الحمساوي «يحيى السنوار» قبل تصفيته أنه يعتمد في اتخاذ قراراته على منهج عقلائي يتمشى

مع أهداف التنظيم، حيث يركز على تحليل الخيارات المتاحة وتوقع النتائج المستقبلية بناءً على أهدافهم الاستراتيجية⁽²³⁾. وفي ضوء ذلك، نستنتج أن تقنيات الذكاء الاصطناعي تمثل عنصراً أساسياً في حرب السابع من أكتوبر، حيث لعبت هذه التقنيات دوراً حاسماً في تعزيز القدرات الإسرائيلية؛ مما يعكس التأثير العميق لهذه الأدوات الرقمية في إعادة تعريف طبيعة النزاعات المسلحة⁽²⁴⁾.

2. الذكاء الاصطناعي والدعاية الإسرائيلية: نماذج للتأثير في الرأي العام الدولي

شهدت حرب السابع من أكتوبر على غزة تحولاً نوعياً، حيث يمكن وصفها بأنها أول «حرب ذكاء اصطناعي» بين حماس وإسرائيل. اعتمدت الأطراف المتصارعة بشكل كبير على تقنيات الذكاء الاصطناعي، لا سيما تقنيات التزييف العميق، للتأثير في الرأي العام الدولي ونقل رواياتهم الخاصة. فقد برزت خلال الحرب مقاطع فيديو وصور مزيفة تم إنتاجها باستخدام الذكاء الاصطناعي، انتشرت بسرعة عبر القنوات الإعلامية والمنصات الرقمية حول العالم. هذه المواد المصطنعة لم تكتفِ بنقل صورة مغلوطة عن الحرب فحسب، بل أسهمت أيضاً في تشويه الواقع؛ مما زاد من صعوبة التحقق من صحة المعلومات المتداولة.

ومنذ اليوم الأول لعملية «طوفان الأقصى» التي شنتها حماس على مستوطنات غلاف غزة، وجدت إسرائيل نفسها أمام تحدٍ جديد يتمثل في التعامل مع التهديدات التكنولوجية المتقدمة التي فرضتها هذه الحرب الرقمية. وللتصدي لهذا، اعتمدت إسرائيل على أدوات الذكاء الاصطناعي الخاصة بها لاحتواء التأثيرات النفسية لهذه الحملات الإعلامية، مع السعي إلى إعادة صياغة الخطاب الإعلامي بما يخدم مصالحها. هذا المشهد يعكس بوضوح كيف أصبحت تقنيات الذكاء الاصطناعي أداة مركزية في الحروب الحديثة، حيث لم تعد المواجهات تقتصر على العمليات العسكرية التقليدية، بل امتدت إلى ساحات افتراضية قادرة على تغيير موازين الصراع عبر التأثير المباشر في الرأي العام للعالم⁽²⁵⁾. ولذلك أصبح الذكاء الاصطناعي أداة أساسية في الحرب الدعائية بين إسرائيل وحماس، حيث لعب دوراً محورياً في تشكيل الرأي العام الدولي. خلال

الحرب الإسرائيلية على غزة، حققت الحملات المؤيدة للفلسطينيين تأثيراً غير مسبوق في منصات التواصل الاجتماعي؛ مما أدى إلى إحداث صدى عالمي واسع.

ومع تصاعد الأحداث، وتحديداً خلال الهجوم الإسرائيلي على رفح الذي أسفر عن مقتل عشرات المدنيين، برزت حملة إعلامية مؤثرة تحت شعار «كل العيون متجهة إلى رفح»، انطلقت من حسابات فلسطينية على «إنستجرام». حظيت إحدى الصور في هذه الحملة بأكثر من 47 مليون مشاركة خلال أربعة أيام فقط. في المقابل، ردت إسرائيل بحملة على المنصة ذاتها تحت شعار «أين كانت عيونكم في 7 أكتوبر؟»، حيث تضمنت صوراً تم إنشاؤها باستخدام الذكاء الاصطناعي، من بينها صورة مؤثرة لطفل ذي شعر أحمر جالس على أرض ملطخة بالدماء، وخلفه أنقاض ومقاتل من حماس وراية إسرائيل المشتعلة. حققت هذه الصورة وحدها 300 ألف مشاركة خلال أربعة أيام.

فقد أصبح الذكاء الاصطناعي أداة أساسية في الحرب الدعائية بين إسرائيل وحماس، حيث لعب دوراً محورياً في تشكيل الرأي العام الدولي. خلال الصراع الإسرائيلي على غزة، حققت الحملات المؤيدة للفلسطينيين تأثيراً غير مسبوق في منصات التواصل الاجتماعي، مما أدى إلى إحداث صدى عالمي واسع. ومع تصاعد الأحداث، وتحديداً خلال الهجوم الإسرائيلي على رفح الذي أسفر عن مقتل عشرات المدنيين، برزت حملة إعلامية مؤثرة تحت شعار «كل العيون متجهة إلى رفح»، انطلقت من حسابات فلسطينية على «إنستجرام». حظيت إحدى الصور في هذه الحملة بأكثر من 47 مليون مشاركة خلال أربعة أيام فقط. في المقابل، ردت إسرائيل بحملة على المنصة ذاتها تحت شعار «أين كانت عيونكم في 7 أكتوبر؟»، حيث تضمنت صوراً تم إنشاؤها باستخدام الذكاء الاصطناعي، من بينها صورة مؤثرة لطفل ذي شعر أحمر جالس على أرض ملطخة بالدماء، وخلفه أنقاض ومقاتل من حماس وراية إسرائيل المشتعلة. حققت هذه الصورة وحدها 300,000 مشاركة خلال أربعة أيام⁽²⁶⁾.

في إطار الحروب الافتراضية، قامت شركة الذكاء الاصطناعي (AI21 Labs) بإطلاق موقع إلكتروني مستقل لتوثيق الأدلة المتعلقة بحرب «السيوف الحديدية» وترجمتها إلى اللغة الإنجليزية. يهدف هذا الموقع إلى إنشاء قاعدة بيانات متكاملة للأدلة يمكن الوصول إليها من قبل الكيانات التي تعمل على تعزيز الدبلوماسية العامة الإسرائيلية،

وكذلك جمهور الإنترنت حول العالم. كما تم تصميم المنصة لتقديم محتوى موجه يوضح الأحداث المتعلقة بالحرب للرأي العام داخل إسرائيل وخارجها. تضمنت العملية إدخال الاستشهادات بالأحداث باللغة العبرية أو الإنجليزية، ليقوم النظام بتحويلها إلى نصوص باللغة الإنجليزية مصحوبة بسلسلة من الصور المصممة بصيغة «ستوري- قصة»؛ مما يسهل مشاركتها على منصات التواصل الاجتماعي.

إلى جانب ذلك، تم ترجمة هذه الشهادات إلى لغات متعددة، بما في ذلك الإسبانية والفرنسية؛ مما أتاح استخدامها عالمياً. كان أحد الأهداف الأساسية من هذا التوثيق هو تمكين عائلات المختطفين الإسرائيليين من الاستفادة من هذه البيانات في تقديم دعاوى قانونية أمام محكمة العدل الدولية في لاهاي. يعكس هذا المشروع كيفية توظيف الذكاء الاصطناعي لتعزيز الحرب الإعلامية والتأثير في الرأي العام الدولي، من خلال تقديم محتوى رقمي موجه مصمم خصيصاً للتفاعل مع الجماهير العالمية وإعادة تشكيل الإدراك العام للأحداث⁽²⁷⁾.

وفي سياق حرب السابع من أكتوبر، أصبحت أدوات الذكاء الاصطناعي، وسيلة محورية في معركة التأثير في الوعي والإعلام الدولي، خاصة مع تصاعد الشكوك والمخاوف تجاه إسرائيل. استُخدمت هذه التقنيات بشكل مكثف لتحقيق أهداف متعددة، أبرزها التأثير الإيجابي في الجمهور المستهدف من جهة، وردع محاولات استغلالها لنشر الأخبار الكاذبة والتضليل باستخدام تقنيات التزييف العميق من جهة أخرى.

وقد اعتمد الجيش الإسرائيلي على الذكاء الاصطناعي التوليدي في جهوده القتالية والدعائية. أحد التطبيقات البارزة تمثل في منصات التعرف على الوجه، التي ساعدت في تحديد هوية الضحايا والمفقودين والمختطفين. تعمل هذه المنصة عبر مقارنة صورتين للشخص المستهدف، وتقديم تقييم يعتمد على مدى التشابه بينهما. كما تم تطوير منصة أخرى تحت اسم «السيوف الحديدية» (الاسم الذي أطلقته إسرائيل على حرب السابع من أكتوبر)، تتيح البحث عن أسماء المفقودين وتحديث حالاتهم، مع إمكانية مشاركة التفاصيل الجديدة مع الأصدقاء والمتابعين عبر شبكات التواصل الاجتماعي.

من المزايا المهمة لاستخدام الذكاء الاصطناعي في هذه الحرب القدرة على إنشاء مقاطع فيديو متعددة اللغات؛ مما أتاح الوصول إلى جمهور عالمي. شملت هذه المقاطع ميزات مثل الدبلجة، الرسوم المتحركة، الترجمة الصوتية، والترجمة النصية؛ مما جعل عملية نشر المعلومات أكثر سهولة وسرعة. فعلى سبيل المثال، تم استخدام صوت وصورة الممثلة الإسرائيلية «نوعا تاشفي» لشرح مسار الحرب بعدة لغات. استخدمت منصة (HeyGen) لتكرار مقاطع الفيديو الخاصة بها، مع الحفاظ على الصوت والصورة الأصلية، لكن بلغات مختلفة. هذه التقنيات ساعدت في تعزيز جهود الإعلام الإسرائيلي عالمياً من خلال إيصال الرسائل الموجهة إلى جمهور دولي بفاعلية كبيرة. إضافةً إلى ذلك، تم تطوير برنامج دردشة آلي خاص بحرب «السيوف الحديدية»، يتيح للمستخدمين من جميع أنحاء العالم إجراء «محادثة» افتراضية لفهم الحرب وأحداثها بأي لغة؛ مما يعزز من قدراتهم على استيعاب الوضع الحالي ودعم الجهود الإعلامية.

كما لجأت إسرائيل إلى توظيف الذكاء الاصطناعي في إنتاج صور ومقاطع تحمل رسائل إعلامية موجهة، مثل الصور التي تربط بين حركة حماس وتنظيم داعش، حيث تم تصميمها بشكل احترافي باستخدام تقنيات الذكاء الاصطناعي. حتى في الجوانب النفسية، استخدمت هذه التقنيات لتطوير محتوى خاص للأطفال، مثل إنشاء مقاطع فيديو للاسترخاء للأطفال عبر مجموعات واتساب، بهدف تقديم دعم نفسي للأطفال في ظل الأوضاع الصعبة. وعليه، تعكس هذه الجهود كيف أصبح الذكاء الاصطناعي أداة استراتيجية لا غنى عنها في الحروب الحديثة، ليس فقط على المستوى العسكري، بل أيضاً في التأثير في الرأي العام الدولي⁽²⁸⁾.

الخاتمة:

من خلال تحليل الحروب الافتراضية التي تعتمد عليها إسرائيل باستخدام تقنيات الذكاء الاصطناعي، يمكننا أن نلاحظ تطوراً ملحوظاً في استخدام هذه التقنيات في الصراعات الحديثة. وعلى صعيد الحالة الإسرائيلية، فقد 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، أسهمت في تشكيل استراتيجية دفاعية وهجومية فعالة تركز على التأثير في الرأي العام الدولي، بالإضافة إلى تحسين القدرات العسكرية التقليدية.

كما أظهرت دراسة الحالة في حرب السابع من أكتوبر كيف يمكن للذكاء الاصطناعي أن يكون أداة فعالة في التأثير في مسارات الحرب وتوجيهها لصالح إسرائيل، سواء من خلال عمليات المعلومات أو من خلال تعزيز قدرات اتخاذ القرارات العسكرية الاستراتيجية. في هذا السياق، يمثل الذكاء الاصطناعي تطوراً مهماً في مسار الحروب المستقبلية؛ مما يفرض على الدول العربية تبني استراتيجيات جديدة لمواكبة هذا التحول التكنولوجي، وفيما يلي عدد من التوصيات لصانع القرار العربي:

1. تطوير استراتيجيات حرب ذكية عربية، بما يتوجب على الدول العربية أن تعمل على تطوير استراتيجيات حروب ذكية تعتمد على تقنيات الذكاء الاصطناعي، بهدف التفاعل مع الحروب الافتراضية والذكية التي قد تشنها إسرائيل أو أي دول أخرى.

2. وجوب دمج تقنيات الذكاء الاصطناعي في التدريبات العسكرية والعمليات الحربية لتقليل الفجوة التكنولوجية.

3. تعزيز قدرات الدول العربية في مجال الأمن السيبراني وتحليل البيانات، حيث إن الهجمات الإلكترونية واستهداف البنية التحتية الرقمية تشكل جزءاً كبيراً من الحروب الافتراضية. الاستثمار في البحث والتطوير في هذه المجالات يعد أولوية استراتيجية.

4. تكثيف الدول العربية جهودها في مواجهة الحرب النفسية والإعلامية الإسرائيلية عبر الإنترنت، باستخدام تقنيات مكافحة التضليل المعلوماتي. يجب تطوير أدوات تكنولوجية للكشف عن التزييف العميق والمحتوى المضلل الذي يمكن أن يشوه الحقائق.
5. تدريب الكوادر العربية العسكرية والسياسية على الحروب الافتراضية؛ نظراً لتعقيد الأبعاد النفسية والإعلامية للحروب الحديثة، ينبغي تأهيل القيادات العسكرية والسياسية في الدول العربية على فنون الحروب الرقمية وكيفية التعامل مع وسائل الإعلام الرقمية والشبكات الاجتماعية لتعزيز موقفهم في الساحة الدولية.
6. نسج تعاون إقليمي بين الدول العربية لتبادل الخبرات والموارد في مجالات الذكاء الاصطناعي، الأمن السيبراني، والحروب الرقمية. هذا التعاون يمكن أن يؤدي إلى تشكيل قوة إقليمية قادرة على التصدي للتحديات المستقبلية التي تفرضها الحروب الذكية.
7. تشجيع البحث العلمي في مجالات الذكاء الاصطناعي والتقنيات الحديثة هو أمر حيوي لتعزيز قدرة الدول العربية على الابتكار في هذا المجال. توفير التمويل والدعم اللازم للمؤسسات التعليمية والبحثية سيمكنها من إنتاج حلول تكنولوجية محلية.
8. بلورة استراتيجية موحدة لمواجهة تهديدات الأمن السيبراني، فيجب وضع استراتيجية عربية موحدة لمواجهة تهديدات الأمن السيبراني بما يشمل بناء أنظمة متقدمة لمكافحة الهجمات الإلكترونية وحماية البنية التحتية الرقمية.
9. مواكبة التطورات التكنولوجية، بشكل استباقي من خلال بناء قدرات وطنية وإقليمية متكاملة في مجالات الذكاء الاصطناعي والأمن السيبراني، بالإضافة إلى تعزيز الجهود الإعلامية والسياسية لمكافحة الحروب النفسية والإعلامية الإسرائيلية.

المصادر:

1. نوريث كوهين-إنجروجال أ. كامينكا، بعد كل التوقعات: الجيش الإسرائيلي في طريقه إلى جيش ذكي - خارطة الطريق لتبني تقنيات الذكاء الاصطناعي في الجيش الإسرائيلي، ديجتل 2.0، الجيش والتكنولوجيا في عصر المعلومات، العدد 18، ديسمبر 2018، ص 90-103 - متاح على: <https://2u.pw/N03ToQE>
2. استراتيجية إسرائيلية لدمج الذكاء الاصطناعي في الجيش، 13 فبراير 2022، متاح على: <https://2u.pw/5JxbjGL>
3. يواف زيتون، النظام الذي سيحدد مكان السنوار؟ هكذا يستخدم الجيش الإسرائيلي الذكاء الاصطناعي في الحرب ضد حماس، يديعوت أحرونوت، 16 مارس 2024، متاح على: <https://www.ynet.co.il/news/article/hkxie1bc6>
4. داني زاكين، مناقصات مع الأجهزة اللوحية، الاستخبارات مع الذكاء الاصطناعي: الثورة الرقمية في الجيش الإسرائيلي، جلوبس، 14 إبريل 2021، متاح على: <https://www.globes.co.il/news/article.aspx?did=100136684514.04.2021>
5. تل ميمرون، جال داهان، المستقبل بالفعل هنا: الذكاء الاصطناعي في خدمة الجيش الإسرائيلي في ساحة المعركة، مشروع الكتابة الموضوعية لمنتدى الدراسات القانونية، جامعة تل أبيب، إبريل 2024، متاح على: https://www.taulawreview.sites.tau.ac.il/post/mimran_dahan
6. إسرائيل تكشف عن الجيل الثاني من «المقاتل الآلي»، 17 نوفمبر 2021، متاح على: <https://2u.pw/8xdO5u>
7. إسرائيل، تنشر بنادق آلية يتم التحكم بها عن بعد في الضفة الغربية، نوفمبر 2021، متاح على: <https://2u.pw/ooqPJKV16>
8. كيف تستخدم إسرائيل الذكاء الاصطناعي، بالتعاون مع مايكروسوفت لمراقبة الفلسطينيين؟، 1 نوفمبر 2019، متاح على: <https://arabic.euronews.com/2019/11/01/how-israel-uses-artificial-intelligence-to-surveil-palestinians-in-the-west-bank>
9. ريهام المقادمة، كيف أصبحت التكنولوجيا لعنة على الفلسطينيين؟، 21 نوفمبر 2021، متاح على: <https://2u.pw/JaRJSIG>
10. الثورة الثالثة: الاتجاهات العشر لتوظيف الذكاء الاصطناعي في الحروب، إترريجونال للتحليلات الاستراتيجية، 1 فبراير 2023، متاح على: <https://2u.pw/Blv78Rk>
11. وليد غسان سعيد، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير، جامعة النجاح الوطنية، كلية الدراسات العليا، 2013، ص ص 148-156.
12. فيليكس فريش، الإعلام في الجيش الإسرائيلي: دراسة جديدة تبحث في مفهوم «الحسم الإدراكي»، 16 ديسمبر 2022، متاح على: <https://www.ynet.co.il/articles/0,7340,L=2318835,00.html>
13. داني زاكين، المناقصات مع الأجهزة اللوحية، والاستخبارات مع الذكاء الاصطناعي: الثورة الرقمية في الجيش الإسرائيلي، جلوبس، 14 إبريل 2021، متاح على: <https://www.globes.co.il/news/article.aspx?did=1001366845>
14. أمير بوجبوط، «قوة الاستخبارات التي تقضي على نشاط الإرهاب عبر الشبكات الاجتماعية»، موقع «واللا» العبري، 16 إبريل 2022، متاح على: <https://news.walla.co.il/item/3500932>
15. هيجر بوجبوط، نظرة خاطفة: الوحدة 3060 في الجيش الإسرائيلي تقود ثورة في المعلومات الاستخباراتية، يديعوت أحرونوت، 30 سبتمبر 2018، متاح على: <https://www.ynet.co.il/articles/0,7340,L=5361168,00.html>
16. وليد غسان سعيد، مرجع سبق ذكره، ص ص 148-156.
17. ليران عناتي، الذكاء الاصطناعي والأمن القومي في إسرائيل، الفصل العاشر: الذكاء الاصطناعي، الأمن القومي في إسرائيل واستراتيجية الجيش الإسرائيلي، معهد دراسات الأمن القومي، ص 92.
18. ياس خضير البياتي، برمجة الحروب برمجة الإعلام، 12 نوفمبر 2020، متاح على: <https://www.alhadathcenter.net/index.php/views/66386-2020-11-12-04-45-05>
19. العمود الفقري لتقنيات التجسس حول العالم... ماذا تعرف عن وحدة 18200 الإسرائيلية، 18 مايو 2021، متاح على: <https://2u.pw/ZO6DR1M>
20. منهجيات التحقق: كيف نواجه استخدام الذكاء الاصطناعي في التضليل المعلومات، 03 أكتوبر 2022، متاح على: <https://2u.pw/g2AoxD>
21. نوريث أندرمين «تحذير، محتال رقمي: هل ستؤثر تقنية «الديب فيك» على الانتخابات في إسرائيل؟»، 25/2/2019، متاح على: <https://www.haaretz.co.il/gallery/cinema/2019-02-25/ty-article/.premium/0000017f-f2bc-df98-a5ff-f3bd8c>
22. باحثان عراقيان يصدران كتاباً، عن لغة الذكاء الصناعي في 'حروب السيران' الإعلامية، 10 أغسطس 2021، متاح على: <https://www.nasnews.com/view.php?cat=67120> 2021/8/10
23. بيليد أرفيلي، تحققنا بالذكاء الاصطناعي مما يدور في ذهن السنوار؟ الصورة قائمة للغاية، 27 يونيو 2024، متاح على: www.maariv.co.il/business/tech/article-1110681

24. أساف جولان، تحليل خطوات العدو وإدارة القتال: الذكاء الاصطناعي سيغير ميدان المعركة، 22 أكتوبر 2023، متاح على: <https://www.israelhayom.co.il/tech/tech-news/article/14738865>
25. ميت ليبوفيتش، الإسرائيليون الذين جندوا للحرب ضد التزييف العميق لحماس.. الذكاء الدعائي، 21 أكتوبر 2021، متاح على: <https://www.zman.co.il/430605/popup> פורסם בתאריך
26. عوديد بن يهودا، «بين إسرائيل وحماس تُدار حرب الخوارزميات الأولى»، 4 يونيو 2024، متاح على: <https://www.haaretz.co.il/gallery/art/design/2024-06-04/ty-article-magazine/.premium/0000018f-e378-d821-a7df-f3fce7e0000>
27. بمساعدة الذكاء الاصطناعي: الموقع الذي يترجم الشهادات من الحرب إلى عدة لغات»، 22 أكتوبر 2023، متاح على: <https://www.ice.co.il/digital-140/news/article/985015>
28. شيرين ملبيدوفسكي سومخ، المعركة على الوعي: هكذا تستخدمون الذكاء الاصطناعي لمساعدة إسرائيل في الحرب»، 15 أكتوبر 2023، متاح على: <https://marketing.walla.co.il/item/3616233>

الحروب السيبرانية بالوكالة: الأبعاد والتحديات وفرص المواجهة

د. عادل عبد الصادق*

دفعت تطبيقات الثورة الصناعية الرابعة إلى عملية نشوء وتحويل وانتقال القوة وممارستها في النظام الدولي عبر أدوات وتطبيقات جديدة، مدفوعة بحجم التغييرات البنيوية التي أصابت العلاقة بين الاقتصاد والتقنية والأمن، وذلك مع تصاعد الأهمية الاستراتيجية للمجال السيبراني، والذي تحول إلى شبكة عالمية يمكن الوصول إليها من أي مكان ومن أي شخص دون تمييز. وكان من تأثير ذلك حدوث تداخل بين الأبعاد التقنية اللازمة للتشغيل في ظل إضفاء الطابع السياسي عليها وحيادية الشبكة وخضوعها لتحيز الفاعلين وخاصة في ظل المزج بين الاستخدامات المدنية والعسكرية، وبما عمل على تقويض أمن الفضاء السيبراني مع حالة التطور في تطبيقات الحروب السيبرانية والتي تلجأ لها الدول ذات السيادة في ظل التسارع

* خبير بوحدة الدراسات الأمنية والعسكرية،

ومدير برنامج دراسات المجتمع الرقمي بمركز الأهرام للدراسات السياسية والاستراتيجية

العالمي في التحول الرقمي وزيادة انتشار ونفاذ الخدمات الرقمية، وزيادة التهديدات السيبرانية، وتساعد خسائر الاقتصاد العالمي بسببها.

ومن ثَمَّ، برزت أهمية البحث عن مصادر للحماية من جانب الدولة ذات السيادة سواء عبر تنمية قدراتها الذاتية في مجال القوة السيبرانية أو عبر التعاون والتحالف الإقليمي أو الدولي أو بالاستعانة بفاعلين آخرين دون الدولة، والذين كان منهم مجموعات القرصنة المدعومة من الدولة (State-Sponsored Hackers)؛ وهو الأمر الذي أدى إلى تصاعد نمط الحرب السيبرانية بالوكالة، وظهور نمط جديد غير مباشر لممارسة الدولة لحقها في استخدام القوة وفق القانون الدولي. وكان لها تأثيرات مختلفة في أنماط الصراع السيبراني في السباق نحو الاستحواذ على الثروة والهيمنة والمكانة، وكان لتلك الجهود الأحادية من جانب الدول تأثيرات كبيرة في الأمن السيبراني للدولة القومية من جهة وعلى الأمن الجماعي الدولي من جهة أخرى، وخاصة أنها تأتي في ظل متغيرات حاكمة سيطر عليها غلبة التوتر الجيوستراتيجية بين القوى الإقليمية والدولية وزيادة دور الثورة الصناعية الرابعة في حاضر ومستقبل ترابعية القوة في النظام الدولي، وصعود الذكاء الاصطناعي التوليدي.

ويطرح ذلك العديد من التساؤلات حول ماهية حركات القرصنة الدولية وخصائصهم وأهدافهم وطبيعة هيكلهم التنظيمي؟ وما تأثيرات تصاعد دور القرصنة المدعومين من الدولة على الأمن السيبراني العالمي؟ وما الأبعاد النظرية لظهور نمط الحروب السيبرانية بالوكالة؟ وما محفزات تصاعد عملية توظيف هذا النمط في القوة السيبرانية للدولة؟ وما المؤشرات الكمية لتصاعد هذا الدور مقارنة بغيره من أنماط التهديدات السيبرانية الأخرى؟ وما تحديات وفرص المواجهة على المستوى الوطني والإقليمي والعالمي؟ وما اتجاهات مستقبل الحرب السيبرانية بالوكالة في ظل تطبيقات الذكاء الاصطناعي التوليدي؟

أولاً: ماهية مجموعات القرصنة الدولية وخصائصها وهيكلها التنظيمي

كلمة «القرصنة» كانت تشير تاريخياً إلى قيام مجموعة من الأفراد بقطع الطريق عبر البر أو البحر للحصول على مكاسب مالية من القوافل أو السفن التي تعبر. ولكن في عام 1955، أصبحت تستخدم هذه الكلمة للإشارة لأول مرة إلى الكمبيوتر. وفي فترة الستينيات والسبعينيات، تم تطوير استخدام مصطلح القرصنة⁽¹⁾ بشكل أكبر لوصف الأعمال السلبية التي تؤثر في شبكة حماية المعلومات الحساسة، وتميزت تلك الفترة بكونها كانت مرحلة للتجريب والاستكشاف، وذلك مع غياب الوعي بالأمن أو أي تجريم قانوني.

وفي فترة الثمانينيات، انتشر استخدام الكمبيوتر الشخصي في المنازل، ولتنشأ في تلك الفترة أول مجموعة قرصنة⁽²⁾، وبرز مصطلح «الهacker الأمني» مع «روبرت موريس» (Robert Morris) بنشره أول هجوم لإنكار الخدمة، والذي عُرف باسم «دودة موريس» عام 1986، والتي أدت إلى خسائر كبيرة دام تأثيرها لأيام⁽³⁾. وتميزت تلك الفترة كذلك بالتحول من القرصنة بشكل فردي إلى القرصنة بشكل منظم لارتكاب جرائم سرقة البيانات الشخصية وأرقام بطاقات الائتمان. وفي فترة التسعينيات، ظهر نوع جديد من القرصنة عُرف باسم (Script Kiddie)، والذي اعتمد على إعادة كتابة الأكواد للقرصنة، ولكنها كانت أضعف⁽⁴⁾. وفي فترة الألفيات، ظهرت أنماط جديدة من الجرائم السيبرانية وقرصنة «نشطاء الإنترنت» ذوي الأهداف السياسية، ومجموعات القرصنة المدعومة من الدولة، والتي كانت من أشهرها استخدام فيروس «ستاكسنت» ضد المنشآت النووية في إيران، والذي كشف عن ارتباطه بإسرائيل والولايات المتحدة عام 2010. ومنذ ذلك الحين حتى 2024، حدث تطور هائل في نشاط مجموعات القرصنة وأساليب الجريمة السيبرانية، وذلك مع زيادة الاعتماد على الفضاء السيبراني وضعف قدرات الحماية.

ومن ضمن تعريف «مجموعات القرصنة» أنها مجموعات من الأفراد الذين يستخدمون مهاراتهم التقنية لخرق أنظمة الأمن السيبراني بهدف تحقيق الضرر بها». وتختلف هذه المجموعات من حيث أهدافها وأساليبها وتنظيمها. وأسهم في

ذلك دور شبكة الإنترنت في تعزيز الاتصال والتشبيك والتنظيم وتجاوز عقبات الزمان والمكان عبر الحدود، بما ساعد في تبلور تجمع جديد يعبر عن سلوك لفاعلين جدد في الفضاء السيبراني. وهو ما يجعل من تشكيل جماعة القرصنة عملية مرنة وقابلة للزيادة أو النقصان، في ظل نظام عضوية مفتوحة وأخرى مغلقة وسرية. وخاصة مع الزيادة الهائلة في عدد المتصلين بشبكة الإنترنت عالمياً، وبروز المصادر مفتوحة المصدر للتعليم والمشاركة ونقل الخبرات وإتاحة الفرصة للإبداع والابتكار، بما يقوى الأهمية النسبية لمجموعة دون أخرى وبحسب مدى قدرتهم على قراءة حجم التغير التقني وفهمه، ومن ثمّ كسب الخطى نحو توظيفه لصالح أهداف المجموعة.

ويكشف الهيكل التنظيمي لمجموعات القرصنة الدولية عن تحركها في شكل تجمعات شبكية بقيادة مركزية مباشرة تتضمن العقول المدبرة التي توجه وتمول العمليات السيبرانية من خلال التواصل والتنسيق ونقل الخبرات وإدارة فرق الاحتيال والكشف عن الثغرات الأمنية. وتتحول المجموعة من مجرد تنظيم ضيق إلى مستوى تنظيم مؤسسي ينتقل من رد الفعل الفردي - المعتمد على المهارات الفردية - إلى عمل جماعي يسعى إلى التعبئة والتجنيد للقيام بالأنشطة السيبرانية، وخاصة بين الشباب الملم بالتقنية أو العاطل أو عبر الانضمام إلى شركات وهمية تقوم بتلك الأعمال لإضفاء المشروعية على نشاطها. وتتمر المجموعة برحلة حياة تبدأ بالتشكيل والتفعيل وممارسة أنشطتها المحددة ثم التفكك والانزواء إما لتحقيق هدفها وإما للتهرب من الملاحقة الأمنية وإما الاستمرار بأعضائها تحت مسمى جديد لمجموعة أخرى⁽⁵⁾.

وتسعى مجموعات القرصنة لتحقيق عدة أهداف؛ منها: البحث عن المكاسب المالية من خلال ممارسة الأنشطة السيبرانية الضارة من خلال الاحتيال؛ وهناك مجموعات تعتنق معتقدات سياسية أو أيديولوجية. وغالباً ما تكون مرتبطة بالدولة، ويتم توظيفها ضد الخصوم أو الأعداء لشن هجمات تستهدف سرقة البيانات أو تعطيل الخدمات. وتستهدف مجموعات قرصنة أخرى القيام بأنشطة التجسس ضد الهيئات الحكومية العسكرية أو الشركات التابعة للدولة «الخصم»، وهي أقرب للعمل تحت راية الدولة ذات السيادة، وهناك مجموعات قد تمارس القرصنة

بغرض الانتقام «الداخلي» سواء على المستوى الفردي أو الجماعي عبر تسريب البيانات الداخلية أو تخريب الأنظمة أو تشويه مواقع الإنترنت. وهناك مجموعات أخرى قد تمارس القرصنة خاصة على المستوى الفردي بغرض جذب الانتباه أو الرغبة في التحدي أو إثبات الذات.

ومن حيث نطاق النشاط، هناك جماعات قرصنة تنشط في الإنترنت المعروف والذي يمثل فقط 4٪ من حجم الشبكة، بينما ينشط الباقي في الإنترنت العميق أو المظلم والذي يمثل 96٪ من شبكة الإنترنت، ويمثل مجاًلاً خصباً للأنشطة الإجرامية وغير المشروعة، وتأمين التواصل والتعاون بين القراصنة ونقل الخبرات والتنسيق، ومشاركة التكتيكات لاختراق البيانات⁽⁶⁾. وهو الأمر الذي يؤدي إلى الخسارة المالية للأفراد والشركات والحكومات عبر ارتكاب الجرائم السيبرانية، والإضرار بالبنية التحتية الحرجة، بما يلحق أضراراً اقتصادية وسياسية، مثل اختراق البنوك وسرقة الأموال أو الاحتيال، وسرقة الهوية والبيانات وتسريبها وبيعها إلى أطراف ثالثة، وتعطيل الخدمات عبر المنصات أو الشبكات والتجسس وسرقة الأسرار الصناعية أو التجارية، ونشر البرمجيات الخبيثة مثل الفيروسات أو برامج الفدية⁽⁷⁾. وقد شمل ذلك إصابة أجهزة الكمبيوتر والهواتف الذكية وأجهزة إنترنت الأشياء وأجهزة التوجيه الشبكي وأجهزة الصراف الآلي.

وتنقسم مجموعات القراصنة إلى عدة أنواع، ولكنها قابلة للتداخل أو الانتقال من نمط إلى آخر وفق محفزات التغيير أو توظيف أدوارها، فتعمل مجموعات قراصنة المعروفة باسم «ذوي القبعة البيضاء» (Whitehat Hackers) على كشف الثغرات الأمنية والدفاع ضد المخترقين وحماية الخصوصية، وغالباً ما يعمل القراصنة الأخلاقيون تحت ستار من السرية⁽⁸⁾. وبينما تبحث المجموعات المعروفة باسم «ذوي القبعة السوداء» (BlackHat Hackers) عن الثغرات الأمنية من أجل الحصول على المال، تجمع المجموعات المعروفة باسم «ذوي القبعة الرمادية» (Grayhat Hackers) ما بين أنشطة وأهداف ذوي القبعة البيضاء والسوداء.

ويستخدم نشطاء الإنترنت (Hacktivists) القرصنة كشكل من أشكال الاحتجاج أو التغيير الاجتماعي أو الدفاع عن أجندة سياسية محددة أو الضغط على الحكومات

لتنفيذ مطالب ما. وهناك مجموعة أضعف تُدعى مستخدمي الأكواد البرمجية (Script Kiddies)، حيث تختلف دوافعهم ويستخدمون نصوصًا أو أدوات مكتوبة سابقًا لشن الهجمات، ويفتقرون إلى المهارات المتطورة للقرصنة. وهناك مجموعة يُطلق عليها «الطابور الخامس» أو «المهدد الداخلي» (Insider Threats)، والمتمثل في قيام الموظفين داخل الشركات أو الهيئات باستغلال صلاحياتهم للقيام بشن الهجمات سواء تم بشكل فردي أو مدفوع من قبل آخرين من الخارج. فيما يهدف قرصنة «الإرهاب السيبراني» (Cyberterrorists) إلى نشر الخوف لتحقيق أهداف سياسية أو أيديولوجية. أما أكثر تلك المجموعات تنظيمًا وتمويلًا وتأثيرًا، فهم مجموعة القرصنة التي ترعاها الدولة (State-Sponsored Hackers) عن طريق توظيفهم للقيام بعمليات الحرب السيبرانية لتعزيز المصالح الاستراتيجية للدولة ذات السيادة.

ثانيًا: الأبعاد النظرية لظهور نمط الحروب السيبرانية بالوكالة

كان نمط الحرب بالوكالة (Proxy War) مستعرًا إبان الحرب الباردة بين الاتحاد السوفيتي والولايات المتحدة في ظل إسقاط أنظمة وصعود أخرى موالية، وإدارة الصراع عن بعد عبر وكلاء إقليميين، وتصاعد دور الإعلام في الحرب النفسية، وتكثيف نشاط الأجهزة الاستخباراتية في التجسس وجمع المعلومات والتي أدت إلى سقوط الاتحاد السوفيتي بدون طلقة رصاص أمريكية، بل بتوظيف القوة الناعمة بشكل أكبر. وجاءت العولمة وتطبيقاتها لتعمل على تراجع دور الدولة كفاعل رئيسي في العلاقات الدولية، وبرزت توجهات غربية لإعادة انتشار القوة العسكرية والاقتصادية للدولة، وبرزت ظاهرة شركات الأمن الخاصة، التي تقوم بمهام قتالية خارجية، ويتم تجنيدها على أساس مالي وليس عقائدي بالضرورة. ومن جهة أخرى، تصاعد دور الفاعلين من غير الدول مثل الجماعات الإرهابية، وتصاعدت أدوارها كأدوات لتنفيذ السياسة الخارجية للدول الكبرى.

وجاء انتشار تكنولوجيا الاتصال والمعلومات، ليضيف أبعادًا جديدة مع بروز دور الشركات التقنية العابرة للحدود في مجال الخدمات الرقمية، وتحول دورها

من البعد التجاري إلى الاستراتيجي، وإتاحة فرصة التدخل «الناعم» في الشئون الداخلية للدول الأخرى، وإعادة تشكيل الرؤى والاتجاهات لدى الجمهور عبر التأثير في الرأي العام العالمي. وذلك في تجاوز للمفاهيم التقليدية حول السيادة الوطنية للدولة، وباتت تتعرض عناصر تحققها كالثروة والشعب والإقليم وعمل الحكومة إلى مهددات جديدة، ومن ثمّ تحاول الدول منفردة الدفاع عن مصالحها القومية وما تراه ضمن اعتبارات الأمن القومي لديها من خلال حماية المصالح الجديدة عبر الفضاء السيبراني.

وقد أتاح الفضاء السيبراني الفرصة للاستحواذ على القوة بشقيها الصلب والمرن عبر مصادر مختلفة، وبدأت عملية تطور أنماط الحرب غير التقليدية والحروب الهجينة، وخاصة مع تبني الدول الكبرى والمتوسطة في النظام الدولي استراتيجية دفاعية مرنة تجاه الخصوم، وحرصها على تنوع طبيعة القدرات المستخدمة، والتي قد تتمثل في تشكيل جبهات أو فرق عسكرية خاصة مثل وحدات للحرب السيبرانية، وهي مجموعات من الخبراء التقنيين الذين عينتهم الحكومات والشركات لتحديد نقاط الضعف الأمنية وإصلاحها قبل أن تتمكن الجهات الخبيثة من استغلالها. وهو الأمر الذي دفع إلى إمكانية المواجهة العسكرية بنفس المرونة التنظيمية وسرعة الحركة في مواجهة باقي الفاعلين من الدول أو من غير الدول، وتبني القدرات التقنية والعسكرية المتقدمة، ومن ثمّ كان احتضان مجموعات القرصنة الدولية وجذبها للتعاون مع الدول للقيام بالمهام الخاصة التي تتميز فيها دون غيرها، والتهرب من المسؤولية القانونية المباشرة للدولة وفق القانون الدولي، في ظل محدودية الاتجاه إلى الحرب التقليدية بين القوى الدولية لصالح البحث عن أدوات للقوة الذكية يكون لها نتيجة الحرب المباشرة نفسها، وبتقديم الدعم للقوى المحلية المعارضة وتدريبها عسكرياً وتقنياً وتوفير غطاء سياسي دولي واستخباراتي لها من أجل توجيهها عن بعد لخدمة مصالح خارجية لدول أخرى.

ومن جهة أخرى، فإن إدراك القوة الصاعدة في النظام الدولي لخطورة الانزلاق إلى حرب مباشرة على فرص قوتها المستقبلية يدفعها إلى اللجوء إلى أدوات لإدارة الصراع بعيداً عن المواجهة المباشرة قبل عملية تشكيل النظام الدولي إلى جانب

تزايد التكلفة الاقتصادية للحرب بين القوى الكبرى، وفي ظل تحول الفضاء السيبراني لساحة للتفاعلات العابرة للحدود والتي مكنت من يملك القوة من تعزيز فرصته للوصول إلى المعلومات والاتصال المباشر مع المواطنين الأجانب عبر الحدود، بما يجعل من التأثير فيهم أكثر عمقاً واستدامة بدلاً من التأثير في حكوماتهم.

وعليه، بات تأمين الفضاء السيبراني أحد أهم أهداف عديد من دول العالم، كأحد عوامل استقرار الدولة وتعزيز قدرتها على اللحاق بالتقدم التكنولوجي، ودفع عجلة النشاط والنمو الاقتصادي، والذي يتم تحقيقه عبر تطبيقات مثل التجارة الإلكترونية والمعاملات المالية والحكومة الإلكترونية. ومع تعقد حالات الاختراق وتنوعها، قامت العديد من الحكومات باتخاذ استجابات متعددة على المستوى التقني والتشريعي والتنظيمي والدولي بغية العمل على مواجهة التهديدات السيبرانية والتي تؤدي إلى خسائر مالية وأزمة ثقة في المؤسسات والإجراءات والسياسات المتبعة. ومن ثم، تحاول الدول مواجهة الخسائر الفعلية والمحتملة لها سواء من طرف دولة أو من طرف فاعل من غير الدول، والعمل على توفير ضمانات للحفاظ على أمنها القومي في الفضاء السيبراني، وممارسة سيادتها السيبرانية على موارد الفضاء السيبراني، وتعزيز قدرتها في مجال الصناعات التكنولوجية والبرمجيات والتطبيقات والموارد البشرية.

وفي ظل العصر الرقمي، حدث تغيير جذري في مفهوم الأمن، وقد فرض ذلك على الدولة الانفتاح والتعاون مع الفاعلين من غير الدول في الداخل من جهة، والتعاون مع الخارج لتعزيز القدرات من جهة أخرى. ومن ثم، فقد لجأت الدول إلى زيادة الإنفاق على تنمية القدرات في مجال الدفاع السيبراني. هذا وتنطلق الدول في ذلك من حقيقة أن إمكانية الوصول إلى مستويات أعلى من الأمن السيبراني سيوفر الثقة بين مختلف أطراف البيئة الرقمية.

ومن ثم، كان هناك أنماط للتفاعلات الدولية منها؛ تفاعلات ذات طابع تعاوني، وأخرى ذات طابع صراعي، وثالثة ذات طابع تنافسي بين الدول والشركات حول الاستحواذ على القوة في العصر الرقمي والتي منها تطبيقات الثورة الصناعية الرابعة والأسواق والصناعة والتجارة وما يرتبط بها من إحراز تقدم في البنية

التحتية والصناعات التكنولوجية والعسكرية كأشباه الموصلات وتطبيقات الذكاء الاصطناعي. كما اتجهت الدول كذلك إلى زيادة مصادرها من القوة عبر الاستعانة بالفاعلين من غير الدول ومنها جماعات القرصنة (State-Sponsored Hackers)، لتحقيق أهدافها وذلك عبر تنفيذ هجمات سيبرانية ضد دولة أو حكومة أو منظمة أخرى في بلد أجنبي. وهو ما يعني ظهور نمط جديد غير مباشر لممارسة الدولة لحقها في استخدام القوة أو العنف أو الهجوم للدفاع الشرعي عن النفس عبر الاستعانة بوكلاء ليسوا فقط من الدول بل وأيضًا من غير الدول.

وقد جذب القرصنة اهتمام الدول ذات السيادة للاستفادة من خبراتهم وتجنيدهم لخدمة الأهداف القومية، وبرز اتجاه إلى دمجهم بشكل مباشر في القوات المسلحة الرسمية أو لتوظيفهم كجنود جند للعمل بشكل غير مباشر، لما يمتلكونه من مهارات قتالية سيبرانية، فيقفون خلف الشاشات، ويتمتعون بمهارات رقمية استثنائية. ويأتي ذلك في ظل بيئة محفزة لتوظيف القرصنة من قبل الدول في الحروب السيبرانية والتي تلاءم خصائصهم وحالة التغير في طبيعة الحرب وأهدافها والبعد عن المواجهة الميدانية وعدم وضوح أطراف الحرب، بخلاف الحرب التقليدية التي تدور بين جيوش نظامية واضحة وفي أرض معركة محددة، وذلك لصالح اتساع مسرح العمل الحربي أو العسكري والاتجاه إلى غلبة الأبعاد غير العسكرية على الصراع ووجود محددات لتطبيقات قانون الحرب على الحرب السيبرانية، ومن ثم إمكانية التهرب من المسؤولية الجنائية الدولية.

وجاءت الأنشطة السيبرانية المعادية التي تقودها الدولة بشكل مباشر أو غير مباشر بفعل انتقال مستويات التوتر الدولي بين القوى الكبرى إلى المجال السيبراني، وهو ما يفسر تصاعد عملية توجيه الاتهامات المتبادلة بين الشرق والغرب دون أدلة واضحة أو من خلال تحقيق رقمي مستقل. وهو ما أدى إلى بروز ما يعرف بالعقوبات السيبرانية من أجل القيام بإجراءات أحادية من جانب الدولة لمعاقبة الأفراد أو المجموعات المرتبطة بدول المتورطة في شن هجمات سيبرانية⁽⁹⁾.

وتقوم مجموعات القرصنة المرتبطة بالدولة بالتسلل إلى أنظمة الكمبيوتر والبنية التحتية لتكنولوجيا المعلومات لدى خصوم «الدولة» والابتزاز للهيئات

الحكومية من أجل الحصول على المال أو الأسرار وجمع المعلومات الاستخبارية. وتستهدف تلك المجموعات كذلك حكومة «الخصم» أو الجيش، وإصابة قطاعات أخرى مختلفة، مثل الرعاية الصحية والاتصالات وسرقة الملكية الفكرية، بما يتسبب في خسائر مالية واقتصادية وسياسية. وتكمن خطورة هذا النمط من نشاط مجموعات القرصنة الدولية في قوة الدولة التي تقف ورائها من حيث الدعم التقني أو السياسي أو الأمني أو المالي، والتي تمكنها من القيام بحروب سيبرانية بالوكالة سواء فيما يعرف باسم «الحرب السيبرانية الصلبة» (مثل: القرصنة والاختراق والإضرار بالبنية التحتية الحرجة)، وذلك إلى جانب دورهم في «الحرب السيبرانية الناعمة» (للقيام بالأنشطة السرية والتجسس وجمع المعلومات وشن الحرب النفسية عبر التأثير في الرأي العام المحلي والعالمي).

ومن نتائج تعزيز نشاط مجموعات القرصنة المدعومة من الدولة تعرض الدولة أو الدول المستهدفة إلى عمليات تجسس تستهدف الاستحواذ على الأسرار الصناعية وانتهاك حقوق الملكية الفكرية والتي تعطي لمن يقف وراء تلك الهجمات مزايا تجارية تنافسية، مقابل خسائر مالية كبيرة للدولة المستهدفة. ومن جهة أخرى، تؤدي تلك العمليات إلى أضرار اقتصادية، وبخاصة لو تحولت تلك المعلومات المسربة إلى تطوير أو إنشاء منتجات رقمية أو صناعية، وهو ما يحمل خسارة اقتصادية كبيرة للشركات أو الهيئات البحثية المستهدفة، إلى جانب فقدان الاقتصاد الوطني القدرة على توفير فرص العمل. وتتسبب كذلك مجموعات القرصنة المدعومة من الدولة في مجال التجسس السيبراني في انتهاك سيادة الدولة والتعرض لتهديدات كبيرة للأمن القومي، والتي ينتج عنها سرقة المعلومات السرية المتعلقة بمشروعات أو تطوير نظم التسليح والوضع الفعلي للقدرات العسكرية أو التدخل في نظام عمل الأجهزة الاستخباراتية، وهو ما يوفر فرصاً للتدخل في الشؤون الداخلية والتأثير في الاستقرار السياسي وتقويض النظم الانتخابية أو القضائية أو المالية. ويؤدي نمط التجسس السيبراني من قبل تلك المجموعات إلى حدوث اختراقات للبيانات الحساسة أو المالية أو الشخصية، والتي يمكن أن تستخدم في أنشطة الاحتيال المالي المختلفة، بما يؤثر في سمعة الحكومات أو الشركات، وفقدان فرص النمو الاقتصادي.

ويمكن أن تؤدي الهجمات السيبرانية التي تقوم بها مجموعات لصالح دولة ما إلى المزيد من التوتر في العلاقات الدولية، والتأثير في الجهود الدبلوماسية لحل الخلافات أو الصراعات بالطرق السلمية. إلى جانب تأثيرها المحتمل في سلامة سلاسل التوريد العالمية وانتهاك الخصوصية وحقوق الإنسان الرقمية، ومدى التقدم في مجال التعاون الرقمي لمواجهة التحديات العالمية للأمن السيبراني. ومن شأن تصاعد القرصنة لصالح الدولة في الفضاء السيبراني أن تؤثر كذلك في استدامة الخدمات الرقمية وعمل البنية التحتية الحيوية، وخاصة أن تلك الهجمات لا تقتصر تأثيرها فقط في الفضاء السيبراني، بل يصل إلى الفضاء المادي في ظل حالة الاندماج الوظيفي بين المجالات الدولية كالبر والبحر والجو والفضاء الخارجي.

وعلى الرغم من قيام الولايات المتحدة بأنشطة سيبرانية معادية عبر التعاون مع مجموعات قرصنة دولية أو عبر وكالاتها الأمنية المتخصصة فإن هناك تركيزاً أمريكياً على اتهام الصين بالقيام بأنشطة سيبرانية معادية لتحقيق مصالحها الوطنية، بما في ذلك اختراق شبكات البنية التحتية الحيوية وسرقة الملكية الفكرية. هذا إلى جانب اتهام روسيا في أنشطة سيبرانية مرتكزة على حملات موسعة من التجسس والتدخل في الانتخابات الأمريكية. كما تتهم كوريا الشمالية بارتكاب نشاط سيبراني هجومي لجمع المعلومات الاستخباراتية وسرقة الأموال وتوظيف العملات المشفرة. كما تتهم الولايات المتحدة كذلك إيران بالقيام بشن هجمات للتجسس والتدخل في الشؤون الداخلية وإلحاق الضرر بالخصوم الإقليميين والدوليين.

ثالثاً: محفزات تصاعد نمط توظيف القراصنة في الحروب السيبرانية

تغذي التوترات المتصاعدة بين القوى الدولية فرص الحروب السيبرانية من جهة، وتؤدي إلى تصاعد فرص توظيف القراصنة المدعومين من الدولة للقيام بأنشطتهم من جهة أخرى، وذلك إلى جانب حالة التغير في البيئة الدولية والتي كان من ملامحها تسارع وتيرة التغييرات التقنية التي تحد من القدرة على التنبؤ بالمخاطر، وهو ما يعزز من أهمية الاستجابة للتهديدات وإنشاء نظام للردع السيبراني. كما أن أمن الفضاء

السيبراني يتطلب وجود نظام مرن وآمن للأفراد والشركات والحكومات، وهو ما يعزز من الثقة في البيئة الرقمية ودورها في تحقيق أهداف التنمية المستدامة. هذا إلى جانب تزايد حجم الخسائر الاقتصادية وارتفاع تكلفة التهديدات السيبرانية، ووجود حالة من التبني السريع للرقمة من قبل الحكومات سواء كانت في شكل تطبيقات أو منتجات أو لتقديم الخدمات، ومن ثم إمكانية زيادة التعرض كذلك للمخاطر، مع تصاعد دور المجال السيبراني في عمل وتكامل سلاسل التوريد العالمية ووجود البرمجيات مفتوحة المصدر أو ذات الطابع العابر للحدود، بما يطرح إشكاليات حول ملكية الأنظمة والاختصاص القانوني، ووجود أطراف ثالثة لتقديم وظائف مهمة. هذا إلى جانب تزايد اعتماد الدول على الخدمات الرقمية المتكاملة، مع تبني إنترنت الأشياء (IoT) وتطبيقات الذكاء الاصطناعي، والتي يمكن أن تتم في جزء كبير منها عبر الحدود الدولية ومن قبل شركات أجنبية كبرى. ناهيك بتصاعد أهمية الاقتصاد الرقمي في توسيع الأسواق وفي جني الأرباح وفي الاستثمار في الإبداع والابتكار في ظل حالة التداخل الوظيفي بين المجال السيبراني وغيره من المجالات الدولية الأخرى كالبر والبحر والجو والفضاء الخارجي.

وتشمل محفزات لجوء الدول إلى نمط الحرب السيبرانية ما يلي:

1. صعوبة إسناد المسؤولية للدولة عن سلوكها في الفضاء السيبراني، وعن سلوك الفاعلين من غير الدول بداخلها، وعدم وجود تقدم كبير في تقنين مسؤولية الدولة عن سلوكها في الفضاء السيبراني.
2. التقدم في مجال تطبيقات القرصنة والتجسس، ووجود سوق سوداء لبيعها، إلى جانب وجود مصادر مفتوحة لتعلم أساسيات القرصنة وبرامجها المتطورة أو التطور في مجال تشفير الاتصالات والأمن السيبراني.
3. محاولة الدولة اكتساب المرونة اللازمة لمواجهة التهديدات السيبرانية المتطورة، والمتسارعة ومواجهة البعد البيروقراطي للمؤسسات الرسمية المعنية بالأمن والدفاع داخلها.
4. مواجهة الفجوة داخل الدولة في المهارات التقنية، والخبرات المرتبطة بتطوير القدرات الذاتية في مجال شن الهجمات السيبرانية والكشف عن الثغرات الأمنية وضمان التقدم المستمر في عمليات الدفاع والهجوم والردع السيبراني.

5. استفادة الدولة من حالات التطور في البنية التحتية الرقمية، في دول أخرى لشن هجمات سيبرانية ضد دول أو جماعات أخرى معادية لها.
6. تعزيز القدرة التنافسية للدولة من خلال تعزيز القدرات السيبرانية، ومواجهة تأثير الهجمات السيبرانية في الاقتصاد والأمن، وتوفير بيئة رقمية آمنة للتحويل الرقمي، وتعزيز الثقة في الخدمات الحكومية، وتساعد دور الاقتصاد الرقمي في إيجاد طرق جديدة لتكوين الثروة والنفوذ، ودوره في النمو الاقتصادي والتنمية المستدامة.
7. تصاعد أهمية الإبداع والابتكار في الاقتصاد الرقمي، وهو الأمر الذي يتطلب حماية الملكية الفكرية، ومواجهة التهديد الأكبر بسرقة تلك المنجزات، بما يؤدي إلى أكبر عملية نقل للثروة في التاريخ البشري من مكان إلى مكان ومن فاعل إلى فاعل جديد.
8. ما تتميز به مجموعات القرصنة من قدرات في الاختراق، بما يمكن الأجهزة الاستخبارية التابعة للدولة من توفير مصادر للمعلومات والتجسس غير المسبوق وبطرق غير مكلفة وأكثر فاعلية.
9. مواجهة فارق القوة النسبية بين الدول ذات السيادة وخصومها، فيما يتعلق بالقدرات السيبرانية واللجوء إلى عمليات نوعية سيبرانية تحقق أهدافاً تكتيكية مرشحة للتحويل إلى أهداف استراتيجية مع التقدم التقني الهائل في مجال التطبيقات العسكرية للذكاء الاصطناعي.
10. مواجهة ارتفاع تكلفة الحرب التقليدية، في مقابل توظيف تطبيقات الحروب السيبرانية والتي هي أرخص في التكلفة مقارنة بتكلفة دبابة والتي يمكن أن يسهم ثمنها فقط في شن حرب سيبرانية واسعة النطاق، وخاصة مع انتشار الأسلحة السيبرانية وإتاحة الفرصة لاستخدامها عبر الحدود.
11. إن حالة التضخم العالمي في الاقتصاد تدفع إلى تباطؤ نمو قطاع تكنولوجيا المعلومات، ومن ثمَّ زيادة البطالة بين المبرمجين والمهندسين مع تسريحهم من وظائفهم، ومن ثمَّ يتجهون إلى القيام بأنشطة سيبرانية ضارة للحصول على المال، في ظل إمكانية استقطابهم من دول أو منظمات إرهابية أو إجرامية.

12. الحصول على مزايا استراتيجية في زمن الصراع أو الحرب مع الارتفاع في حجم التهديدات والتوترات الجيوسياسية، وهو ما يدفع العديد من الدول إلى الولوج إلى تلك القدرات لتحصيل التفوق والسبق والهيمنة مقارنة بخصومها التقليديين أو المحتملين على المستويين الإقليمي أو الدولي.

13. إمكانية توظيف البعد الجيلي في التجنيد والتعبئة، لمجموعات القرصنة وخاصة أن الشباب هم الأكثر ارتباطًا بالثورة التقنية والأكثر معاناة من الظروف الاقتصادية والاجتماعية والفقر وعدم المساواة، وذلك مع الانتشار والدخول الكثيف لتكنولوجيا الاتصال والمعلومات عالميًا.

14. تنامي دور الذكاء الاصطناعي في تعزيز قدرات القرصنة وفي شن الهجمات السيبرانية، وتوظيف التزييف العميق والهندسة الاجتماعية في التلاعب بالمستخدمين أو الشركات أو المؤسسات وفي إجراء المعادلات والاحتمالات بسرعة ودقة، بما يساعد في توظيف الخوارزميات في اختراق كلمات المرور وفك التشفير.

15. لجوء الدول -مع تصاعد أخطار التهديدات السيبرانية- إلى تحديث استراتيجيات أمنها القومي، لتأخذ في اعتبارها الأمن السيبراني كرافد مهم له، وقيام عدد كبير من الجيوش الحديثة بإنشاء وحدات للحرب السيبرانية ووحدات للحرب الفضائية أو الجوفضائية، وهو فرع حديث في تاريخ العلوم العسكرية.

رابعًا: المؤشرات الكمية لتساعد دور القرصنة في الحروب السيبرانية

في دراسة مسحية لعدد 2506 هجوم سيبراني، كشف المستودع الأوروبي للحوادث السيبرانية أنه خلال الفترة من عام 2000 حتى نهاية 2023، كانت مسئولية الدول عن الهجمات تمثل 53,2٪. وقد حظيت الصين وروسيا بالنسبة الأكبر من شن تلك الهجمات بما يصل إلى 22,8٪ من الهجمات السيبرانية خلال تلك الفترة. وجاءت روسيا في المركز الأول عالميًا تلتها الصين ثم إيران وكوريا الشمالية وأوكرانيا والولايات المتحدة وباكستان وتركيا⁽¹⁰⁾. في حين بقيت نسبة 46,8٪ من الهجمات

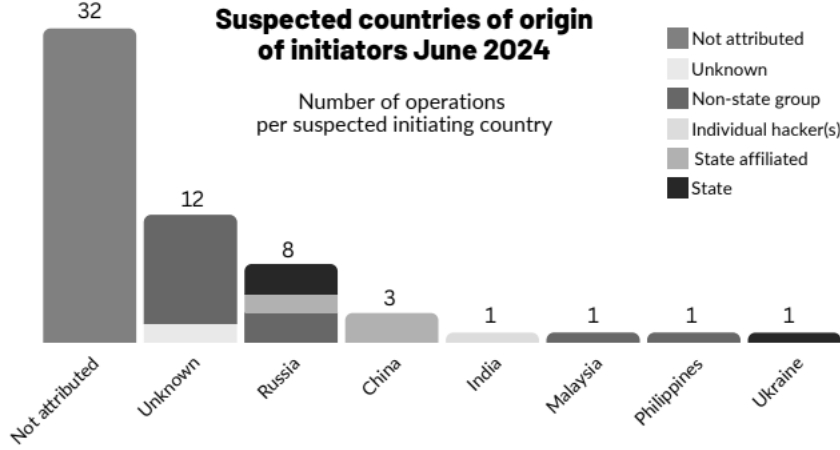
السيبرانية دون معرفة المسئول عنها، وهو ما يكشف الاتجاه الكبير لدى الدول لتبني مجموعات القرصنة المدعومة لشن الهجمات السيبرانية.

وقد قدم كذلك المستودع الأوروبي للحوادث السيبرانية نموذجًا لذلك التصاعد؛ ففي خلال شهر يونيو 2024 تم رصد نحو 32 هجومًا دون إسناده لأي جهة، بينما نُسب إلى الفاعلين دون الدول ما يقارب من 12 هجومًا سيبرانيًا، في حين تم رصد 3 هجمات مرتبطة بالدول منسوبة إلى الصين، بينما نسب إلى روسيا 8 هجمات، توزعت ما بين جهات تابعة لمجموعات دون الدول والجهات الرسمية في الدولة وأخرى مرتبطة بهواة؛ الأمر الذي يكشف عن تصاعد تلك الهجمات غير المسندة لفاعل ما، ونشاط المجموعات دون الدول وتلك المرتبطة بالدولة⁽¹¹⁾.

وخلال العام الماضي، تم رصد ما يزيد على 14 مجموعة قراصنة ترعاها الدول من جميع أنحاء العالم، لتستهدف روسيا وبعض أعضاء الاتحاد السوفيتي السابقين (أذربيجان وبيلاروسيا وقيرغيزستان وكازاخستان) بحملات مدمرة أو تجسس⁽¹²⁾، وقد زادت الهجمات ذات الدوافع السياسية التي تعرضت لها روسيا بنسبة 116٪ في العام الماضي. وكان هناك ما لا يقل عن 28 هجومًا سيبرانيًا كبيرًا ضد المؤسسات الروسية التي نفذتها مجموعات قراصنة تسيطر عليها دول أجنبية⁽¹³⁾.

ويرتبط ذلك بتصاعد الهجمات السيبرانية عالميًا، حيث يقع هجوم سيبراني كل 39 ثانية، ويتم اختراق ما يقدر بنحو 30 ألف موقع إلكتروني كل يوم⁽¹⁴⁾، ويتوقع أن تبلغ خسائر الجريمة السيبرانية أكثر من 23 تريليون دولار بحلول عام 2027، والتي كانت قد وصلت إلى 8,4 تريليونات دولار في عام 2022. ويخسر الاقتصاد ما يقدر بتريليون دولار سنويًا من الجريمة الإلكترونية، وهو ما يعادل 4,1٪ من الناتج المحلي الإجمالي لدول العالم. وأشار صندوق النقد الدولي إلى تضاعف الهجمات السيبرانية منذ جائحة كوفيد-19 - وزيادة الخسائر المرتبة عليها⁽¹⁵⁾. وظهر ذلك في تضاعف تلك الهجمات على مدى العامين الماضيين، بما كلف المنظمات والشركات ما يقدر بنحو 1,6 مليون دولار لكل حادث⁽¹⁶⁾. ومن المتوقع أن ترتفع التكلفة العالمية للجرائم الإلكترونية في السنوات المقبلة، بعد أن ارتفعت من 9,22 تريليونات دولار في عام 2024 إلى 13,82 تريليون دولار في عام 2018⁽¹⁷⁾. وقد أعلن «الإنتربول» في 2 ديسمبر 2024 عن اعتقال

5,500 لاتهمهم بالتورط في نشاط الجريمة الإلكترونية عالميًا والاستيلاء على أكثر من 400 مليون دولار، وتم ذلك بالتعاون مع 40 دولة والتي عرفت بعملية (HAECHI-V) التي جرت ما بين يوليو ونوفمبر 2024⁽¹⁸⁾.

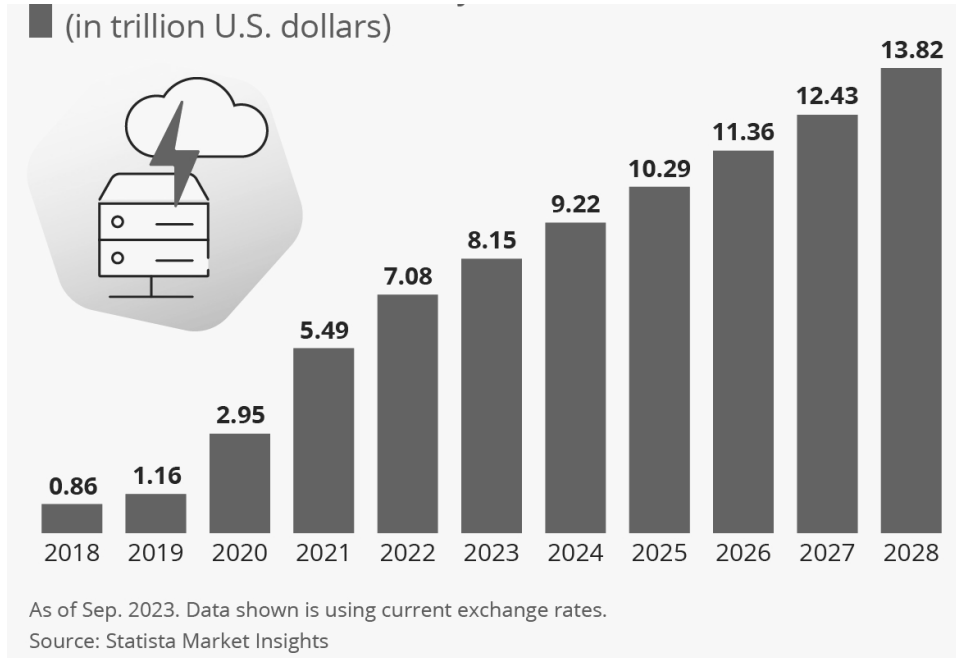


شكل (1): عدد الهجمات السيبرانية منسوبة إلى فاعليها خلال شهر يونيو 2024

المصدر: The European Repository of Cyber Incidents

وقد شهدت السنوات الأخيرة تزايد نمط الهجمات السيبرانية التي ترعاها الدولة القومية للحصول على ميزة على منافسيها الجيوسياسيين، سواء عن طريق سرقة المعلومات الحساسة أو تعطيل البنية التحتية الحيوية⁽¹⁹⁾. وقد أثارت الزيادة الأخيرة في نشاط جماعات القراصنة التي ترعاها الدولة وهجماتها السيبرانية على البنية التحتية الحيوية قلقًا عالميًا، وذلك لتأثيرها المتنامي في الأمن القومي وفي البنية التحتية المعلوماتية⁽²⁰⁾. وهو الأمر الذي يتطلب فهمًا عميقًا للعامل الجيوسياسي ودوافع الدول القومية لتفسير تلك الهجمات المعقدة والتي قد لا يعرف من المسؤول عنها، ولكن يتم إيعازها مبدئيًا إلى من هو صاحب المصلحة. وكشفت الولايات المتحدة عن تصاعد عدد حوادث التجسس الصينية التي تم الإبلاغ عنها، ولكنها شهدت انخفاضًا بعد الاتفاق بين الرئيس الأسبق «باراك أوباما» والرئيس الصيني «شي جين بينج» لتقييد التجسس التجاري من قبل الكيانات الحكومية عام 2015⁽²¹⁾.

وفي 2024، تمت إضافة ستة قرصنة إلى لائحة عقوبات الاتحاد الأوروبي كانوا مرتبطين سابقاً بهجمات سيبرانية ترعاها الدولة الروسية، وتفرض عقوبات الاتحاد الأوروبي على المتورطين تجميد جميع الأموال والموارد الاقتصادية داخل الدول الأعضاء⁽²²⁾. وتفرض العقوبات منع تقديم أي أموال أو موارد اقتصادية للأفراد أو الكيانات الخاضعة للعقوبات. وعلى الرغم من عدم فاعلية تلك العقوبات، فإنها تمثل ضغوطاً دبلوماسية على الأفراد أو المجموعات أو الدول التي تقف وراءها. واتخذت كذلك الولايات المتحدة والمملكة المتحدة في عام 2024 إجراءات ضد 31 مجموعة قرصنة ترعاها الدولة الصينية⁽²³⁾.



شكل (2): التوقعات العالمية لخسائر الجريمة السيبرانية عالمياً

المصدر: Statista

ويتوقع أن تصل خسائر الاقتصاد العالمي من الجرائم السيبرانية عام 2025 إلى 10,29 تريليون دولار بعد أن وصلت إلى 9,22 تريليونات دولار عام 2024، ويتوقع كذلك أن تصل إلى 13,82 تريليون دولار عام 2028⁽²⁴⁾. وما يزيد من خطورة ذلك هو تصاعد الفجوة في حجم العجز العالمي في المتخصصين في الأمن السيبراني والتي وصلت إلى

3,4 ملايين⁽²⁵⁾، ويتوقع أن يصل سوق تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني إلى 135 مليار دولار بحلول عام 2030.

خامسًا: تحديات مواجهة تصاعد دور القرصنة

توجد تحديات في مواجهة تصاعد دور القرصنة المدعومين من الدولة في الحروب السيبرانية منها ذات طبيعة ذاتية تتعلق بخصائص تلك المجموعات وقدراتها، ومنها تحديات ترتبط بإشكالية تحديد العلاقة ما بين الدولة ومجموعات القرصنة، وتحديات أخرى ترتبط بتأثير التطور التقني في وجود مشكلات في التعقب أو المراقبة أو الإثبات، ناهيك بالتحديات القانونية والتقنية والسياسية التي تحد من التعاون الدولي لمواجهة الظاهرة. ومن ضمن ملامح تلك التحديات ما يلي:

1. تعد جريمة القرصنة لصالح الدولة من الأنماط الحديثة للجريمة السيبرانية العابرة للحدود، وبما يمثل صعوبات أمام وكالات إنفاذ القانون لتعقب تلك المجموعات أو محاكمتهم، وخاصة إذا كانت الدولة المستهدفة لا تمتلك القدرات التقنية في الأدلة السيبرانية.
2. إن نجاح بعض الدول في تطوير شبكات إنترنت محلية، عزز من قدرتها على توظيف القراصنة لشن هجمات سيبرانية ضد دول أخرى وحمايتها من تلقي هجمات مضادة بسهولة من أطراف أخرى، بما يُعَلِّي من قوتها النسبية في شن تلك الهجمات السيبرانية عبر القراصنة، ولعل أبرز النماذج هي: كوريا الشمالية، والصين، وروسيا، وإيران.
3. توفر الملاذ الآمن للأموال، مع التطور في عمليات تلقي ونقل وتخزين واستخدام الثروة عبر المجال السيبراني مع الأصول الرقمية والعملات المشفرة التي لا تخضع لرقابة البنوك المركزية العالمية.
4. اتجاه الحركات الإرهابية والحركات المسلحة المعارضة، في دعم قدراتها السيبرانية إلى توظيف القراصنة للجمع ما بين من يبحث عن المال إلى جانب من يبحث عن

السياسة، وذلك إلى جانب بناء قدراتها الذاتية أو إمكانية تلقي دعم غير مباشر من أجهزة استخباراتية خارجية لخدمة أهداف السياسة الخارجية للدول الكبرى.

5. صعود الذكاء الاصطناعي التوليدي، ودوره في تعزيز قوة نشاط جماعات القرصنة الدولية وما يوفره من سهولة الكشف عن الثغرات الأمنية، ووضع تحديات أمام الكشف عن هوية أعضاء مجموعة القرصنة لاعتمادهم على بوتات في نشاطهم الإجرامي.

6. التحديات القانونية التي تحول دون توجيه الاتهام المباشر للدولة عن الوقوف بمجموعات القرصنة أو شن الهجمات السيبرانية، وبما يمكن من تهرب الدولة من أي مسؤولية عن سلوكها عبر الفضاء السيبراني. ناهيك بإشكاليات الاعتراف بالأدلة الجنائية الرقمية والتحقيقات التي تستند عليها أجهزة إنفاذ القانون.

7. غياب توافق دولي حول بناء نظام دولي، للعقوبات السيبرانية يخضع لإشراف الأمم المتحدة. هذا وتكشف عملية فرض العقوبات السيبرانية ضد أنشطة مجموعة القراصنة المرتبطة بالدولة في تطبيقها سواء من قبل الاتحاد الأوروبي أو الولايات المتحدة عن تبني نمط انتقائي ومزدوج المعايير، بجانب غلبة الاعتبارات السياسية على حساب الاعتبارات القانونية، وغلبة الإجراءات الأحادية مقابل اعتبارات الأمن الجماعي الدولي.

8. القدرة الفائقة من قبل تلك المجموعات على التخفي تحت أسماء أغلبها لا يحمل معنى محدداً؛ فقد يكون مزيج من أحرف وأرقام، بما يساعد في مجهوليتها وإمكانية خضوعها إلى حماية خاصة من قبل الدول التي تعمل من خلالها أو تدعمها بما يوفر لها سياجاً أمنياً لملاحقتها والهروب إلى الإنترنت المظلم أو العميق لتأمين نشاطها وإبعاده عن المراقبة.

9. اعتماد القراصنة على الإبداع والابتكار والكر والفر، بما يعزز قدراتهم على مواجهة جهود الملاحقة البشرية إلى جانب تطبيقات الذكاء الاصطناعي.

10. التقدم في مجال التحالفات السيبرانية الاستخبارية، بين الحلفاء والتي تأخذ طابعاً استقطائياً بين القوي الدولية، بما يحد من تبادل الخبرات والتحري السيبراني عن نشاط تلك المجموعات، ويحد من فرص تعزيز التعاون الدولي في مواجهتها.

11. زيادة فرص انتشار المعرفة التقنية بالقرصنة، وتوافر المصادر المفتوحة ناهيك بدور تطبيقات الذكاء الاصطناعي، بما يعزز من ظهور فاعلين جدد وفي تكوين متزايد لمجموعات القرصنة الدولية، ناهيك عن زيادة الاتجاه إلى التعاون ما بين المجموعات بعضها ببعض لشن هجمات منسقة.

خامساً: فرص مواجهة تصاعد دور القرصنة

يعد تحسين الأمن السيبراني للدفاع ضد الهجمات السيبرانية التي ترعاها الدولة من خلال توظيف القرصنة عملية معقدة ولكنها ممكنة للحد من تأثيراتها في الأقل، وذلك من خلال تبني عدد من السياسات والإجراءات على المستويات الوطنية والإقليمية والعالمية، والتي تكون ركيزتها العمل على تخفيف حدة التوتر والصراع في النظام الدولي، فزيادة الأنشطة العدائية المرتبطة بالدولة ما هو إلا انعكاس لحالة الصراع على المصالح المادية. ويأتي هذا إلى جانب أهمية تفعيل الاتفاق الرقمي العالمي الذي تم إقراره في قمة المستقبل للأمم المتحدة عام 2024، وتفعيل اتفاقية الأمم المتحدة للجريمة السيبرانية التي تم الموافقة عليها في عام 2024، وتعزيز التعاون الرقمي من خلال إقامة الشراكات على المستوى الإقليمي والعالمي لمواجهة التهديدات السيبرانية وتبادل المعلومات الاستخبارية حول مجموعات القرصنة التي ترعاها الدولة بشكل جماعي، وذلك على أساس أن الأمن السيبراني العالمي هو رديف للأمن الجماعي العالمي.

كما تزداد أهمية التوافق على تقييم انتهاكات المعايير الدولية في إطار الحوار المفتوح والمتعدد بين كل أصحاب المصلحة في محاولة لإنجاح أي نظام مستقبلي للعقوبات السيبرانية ضد الدول التي يثبت تورطها في دعم مجموعات قرصنة ضد دول أخرى، وذلك وفق إجراء تحقيق دولي مستقل، والحد من الإجراءات الأحادية التي تخرج عن التوافق الدولي، وأن يتم ذلك تحت مظلة الأمم المتحدة بهدف تعزيز دور

المجال السيبراني في السلم والأمن الدوليين، مع التأكيد على أهمية الأطر التشريعية الدولية وتطبيق القانون الدولي على المجال السيبراني، والاستثمار في عملية بناء القدرات والمهارات الرقمية في مجال الأمن السيبراني، ومواجهة النقص في المتخصصين عالمياً في ظل تزايد التهديدات السيبرانية والخسائر المترتبة عليها. هذا إلى جانب إجراء تقييم للمخاطر والتهديدات للبنية التحتية الحيوية بشكل مستمر من أجل معرفة مدى التطور فيها ومدى اتساع الفجوة في الحماية والتقييم لنقاط الضعف وامتلاك مرونة كافية للتعافي من التهديدات السيبرانية، وتطبيق معايير لتطبيقات الأمن السيبراني يلتزم بها كل الفاعلون من الحكومة والقطاع الخاص وتعزيز الشراكة فيما بينهما بما يضمن الالتزام بأفضل الممارسات للحماية من التهديدات السيبرانية، مع التأكيد على أهمية الاستثمار في البحث والتطوير وتشجيع الابتكار في حلول الأمن السيبراني وخاصة في مجال تطبيقات الذكاء الاصطناعي التوليدي، ومن شأن ذلك أن يعمل على تعزيز قدرات الاستجابة للحوادث السيبرانية على المستوى الوطني. ويمثل العنصر البشري الركيزة الأساسية للحماية من خلال الوعي بالمخاطر ورفع قدراتهم في مجال الأمن السيبراني والمهارات الرقمية والتدريب لمواجهة مخاطر تطبيقات الحروب السيبرانية من جهة ومواجهة تصاعد التهديدات الداخلية من جهة أخرى.

كما تزداد أهمية تبني استراتيجية وطنية للأمن السيبراني من أجل تعزيز القدرات في مجال الدفاع والهجوم والردع السيبراني، والتعاون الدولي من أجل تعزيز السلوك المسؤول للدولة في الفضاء السيبراني. وتلعب عملية دمج الذكاء الاصطناعي والتعلم الآلي دوراً محورياً في استراتيجيات الدفاع والهجوم والردع السيبراني، وذلك لدوره في الكشف عن التهديدات والثغرات، وتعزيز الاستجابة لمواجهة التهديدات السيبرانية. وتوفير أدوات جديدة للحماية من الفيروسات وحماية أمن البيانات والكشف عن الاحتيال والتسلل وتعزيز الهوية الرقمية. هذا إلى جانب التأكيد على أهمية دور الذكاء الاصطناعي في إدارة المخاطر بكفاءة، ومحاكاة التعرض لهجمات الهندسة الاجتماعية، وتحليل البيانات الضخمة وتحسين عملية صنع القرار بشأن الأمن السيبراني وتحسين قدرات الردع السيبراني والتنبيه بالمخاطر قبل استغلالها من قبل القراصنة، مع مواجهة اتساع الفجوة بين العديد من الدول في تبني تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني.

خاتمة: مستقبل الحرب السيبرانية بالوكالة

إن عملية تصاعد نمط القرصنة المدعومة بالدولة في الفضاء السيبراني تأتي للتعبير عن محاولة الدولة بإرادتها المنفردة وبدون وجود غطاء دولي ممارسة قوتها غير العسكرية لتحقيق أهدافها القومية. ويأتي هذا في ظل فشل الأطر الدولية للحوكمة العالمية في حفظ السلم والأمن الدوليين، وارتباط ذلك بحالة الصراع على هيكلية النظام الدولي، وتأثير ذلك في ظل تصاعد حالة العسكرة في العلاقات الدولية. ويحرك ذلك ثلاثة متغيرات؛ أولها: أن الأمن السيبراني لا يقتصر فقط على بعده التقني، بل تتعداه إلى أبعاد أخرى في ظل تراجع سيادة الدولة وتزايد العلاقة بين الأمن والتكنولوجيا بصفة عامة؛ خاصة مع إمكانية تعرض المصالح الاستراتيجية للدول إلى أخطار وتهديدات في وقت يعاد فيه تعريف مفهوم «الأمن القومي» للدول. ويتعلق ثانيها: بالدور المتصاعد للفضاء السيبراني في تعظيم القوة والاستحواذ عليها وممارستها ليس فقط في المجال السيبراني، بل في كل المجالات الدولية كالأرض والبحر والجو والفضاء. وارتبط ثالثها: بعلاقة الفضاء السيبراني ببروز أنماط جديدة من الصراع بين الفاعلين من الدول أو من غير الدول حول القيم والأسواق والأرباح.

ويرتبط 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 محوراً مهماً على أجندة الأمن الدولي نتيجة لما يضيفه من عنصر قوة جراء ذلك التحالف، ناهيك بوجود تحالفات دولية سيبرانية صاعدة بين الدول والتي يحركها 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 في المجتمع الدولي، وتخفيف حدة التوتر بين القوى الدولية للحد من الظاهرة وتأثيراتها المختلفة. ومن جهة أخرى، تتزايد أهمية العمل على دعم التنمية المستدامة داخل بلدان العالم النامي من أجل مواجهة الفقر والبطالة بين الشباب الذين قد يكونون ضحية أو فاعلين في أنشطة القرصنة الدولية، وبناء قدراتهم

ومهاراتهم لجعلهم أكثر مواكبة لفرص العمل الجديدة، وخاصة في ظل تصاعد دور الذكاء الاصطناعي التوليدي.

وتدفع طبيعة «التهديد» السيبراني العابر للحدود الدولية لأهمية التعاون الدولي في مواجهة الفجوة القانونية الدولية التي تتيح الفرصة للالتفاف حول أي عقوبات جراء التورط في الهجمات السيبرانية، ومن جهة أخرى دفع الحكومات إلى الانفتاح على التعاون مع القطاع الخاص وغيره من أصحاب المصلحة في الداخل لتحسين وجودة نمط الاستجابة، والتوصل إلى توافق عالمي حول التهديدات السيبرانية، والوصول إلى حلول وسط وتفاهم مشترك بين من يعتبر الهجمات السيبرانية أنشطة تجسسية أو تخريبية أكثر من كونها أعمال حرب، ومن يرى أنها تأتي في إطار التنافس التجاري بمعزل عن اعتبارها تهديدًا للأمن القومي.

من شأن التدابير المضادة خارج نطاق الأمم المتحدة عبر تجنيد الدولة ذات السيادة لمجموعات قرصنة ضد دول أخرى أن تقوض من أهداف ومقاصد ميثاق الأمم المتحدة التي تحض على حل الأزمات عبر الطرق الدبلوماسية، ويمثل خروجًا من جهة أخرى عن آليات النظام الدولي متعدد الأطراف تحت قيادة الأمم المتحدة باعتبارها المنظمة المعنية بالأمن الجماعي الدولي، وهو ما يهدد باتساع التوظيف السياسي والعسكري للبنية التحتية الحرجة للإنترنت والفضاء السيبراني، بما يؤثر في الطابع المدني والسلمي له، ويؤثر في الخدمات المدنية المقدمة للملايين عبر العالم، وعلى عمل المنشآت المدنية، وهو ما يمثل توظيفها في الحروب السيبرانية انتهاكًا للقانون الدولي الإنساني.

هذا، ويرتبط مستقبل ظاهرة الحرب السيبرانية بالوكالة بعدة اتجاهات لعل أهمها ما يلي:

الاتجاه الأول: تبني تطبيقات حديثة ومبتكرة في مجال القرصنة المدعومة من الدولة من خلال توظيف التقنيات البازغة مثل الذكاء الاصطناعي والتعلم الآلي

لتحسين قدراتهم في مجال الرصد والإصابة والتخفي وتوظيف البوتات والروبوتات في تنفيذ الهجمات بما يجعل من التعقب والكشف مسألة صعبة.

الاتجاه الثاني: توسيع أهداف القرصنة لتشمل قطاعات واسعة تشمل استخدامات مدنية أو عسكرية خاصة في ظل زيادة الاعتمادية والتحول الرقمي العالي وتساعد قدرات القرصنة في إصابة الأهداف عبر الحدود بما يزيد من تأثيرها العالمي.

الاتجاه الثالث: اتجاه زيادة توظيف القرصنة المدعمن من الدولة في نمط الحرب السيبرانية الناعمة من خلال زيادة نطاق التأثير ليشمل التأثير المعنوي والنفسي مع اتساع قدرات التجسس والتأثير والانتشار الشامل للأدوات المستخدمة في الهجمات عبر الذكاء الاصطناعي ونشر المعلومات المضللة والتزييف العميق ونشر الانقسامات وبث الكراهية والعنف بما يزيد من تأثير ذلك في الاضطرابات العالمية.

الاتجاه الرابع: تساعد لجوء الدولة إلى توظيف القرصنة لخدمة أهدافها القومية للتهرب من المسؤولية وشن الحرب التقليدية وذلك في مواجهة تزايد الاتجاه العالمي نحو تنظيم المجال السيبراني وتطبيق السيادة السيبرانية على موارد الفضاء السيبراني.

الاتجاه الخامس: اتجاه الدول إلى التعاون فيما بينها على تدشين تحالفات سيبرانية لتعزيز قدراتها في مجال توظيف مجموعات القرصنة لخدمها أهدافها حتى من بين سكان الدول المعادية بما يعكس تأثير التوتر الجيوسياسي في نشاط الحرب السيبرانية بالوكالة.

الاتجاه السادس: زيادة اتجاه دفع تزايد نشاط القرصنة بالوكالة إلى زيادة الأعمال الانتقامية والتدابير المضادة خارج نطاق مقررات الأمن الجماعي الدولي والاتجاه إلى فرض عقوبات تتميز بالأحادية والتسييس.

الاتجاه السابع: انتعاش نشاط القرصنة المدعومين من الدولة استناداً على توافر فرص تشكيل المجموعات والذي يتم تجنيد أعضائها من بين الشباب العاطل

أومن بين مهندسي البرمجيات أو الشبكات أو غيرها مع حالة التضخم في الاقتصاد العالمي والذي أثر في تسريح الموظفين ونقص في فرص العمل.

الاتجاه الثامن: تصاعد دور التهديدات الداخلية والأخطاء البشرية في تعطل الخدمات الرقمية على حساب المصادر الخارجية للهجمات السيبرانية، وتراجع الأنشطة الرسمية من قبل الدول في الحروب السيبرانية لصالح توظيف القراصنة للقيام بها بالوكالة عن الدولة القومية.

الاتجاه التاسع: صعود نمط الحرب السيبرانية بالوكالة كمهدد للأمن السيبراني العالمي نتيجة للقدرات غير المسبوقة لها من جانب دعم الدولة مقارنة بغيرها من أنماط القراصنة الآخرين.

وخلاصة القول، إن كانت الاستراتيجيات الكبرى في الماضي تهدف إلى «كسب السلام» كما في نموذج الحرب الباردة، فإن هذا العصر يمتلئ بالمخاطر التي تستهدف الأمن الجماعي الدولي. ومن ثمّ، نحن بحاجة إلى البحث عن «السلام السيبراني» والانتقال من الفوضى إلى التنظيم، والتوازن ما بين الحقوق والواجبات في الفضاء السيبراني، وذلك من أجل تعزيز دوره في السلم والأمن الدوليين، والذي أصبح بمثابة مرفق دولي وتراث مشترك للإنسانية.

المصادر:

1. تشتق من كلمة «قرصنة» (Hacke) لوصف من يقوم أو يتورط بها إلى «قرصان» أو «هاكر» (Hacker).
2. مثل مجموعة (The Cult of the Dead Cow) ومجموعة (The Chaos Computer Club) في ألمانيا.
3. Catherine Hiley, Brief history of cyber security and hacking, **cyber news**, Cyber News, October 04, 2022, Available at: <https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/>
4. History of Computer Hacking and Cyber security Threats: From the 50s to Today, **Mayhem**, April 21, 2023, Available at: <https://www.mayhem.security/blog/history-of-computer-hacking-and-cybersecurity-threats-from-the-50s-to-today>
5. قام الباحث بدراسة قائمة، من 163 مجموعة من القرصنة المدعومة من الدولة من حيث تنوع الأهداف والخصائص المشتركة والمختلفة وطبيعة النشاط والدول التي ترتبط بها ومسمياتها ويمكن الوصول للقائمة عبر الرابط التالي: <https://attack.mitre.org/groups>
6. Juan H., Dark web statistics & trends for 2024, Prey Project, Feb 12, 2024, Available at: <https://preyproject.com/blog/dark-web-statistics-trends>
7. Yola Verbruggen, Cyber-attacks as war crimes, International Bar Association, **Ibanet**, 10 January 2024, Available at: <https://www.ibanet.org/Cyberattacks-as-war-crimes>
8. The Evolution of Ethical Hacking: From Curiosity to Cyber security, **Stay Safe Online**, August 15, 2024, Available at: <https://www.staysafeonline.org/articles/the-evolution-of-ethical-hacking-from-curiosity-to-cybersecurity>
9. عادل عبد الصادق، العقوبات السيبرانية بين التسييس والمشروعية في ضوء قواعد القانون الدولي، كراسات إستراتيجية، المجلد 31، العدد 339، أغسطس 2022، ص ص. 14-12.
10. لمراقبة ورصد نشاط تلك المجموعات من القرصنة المدعومة من الدولة، يمكن رؤيتها عبر منصة المستودع الأوربي للحوادث السيبرانية، والتي توفر تحديث لحظي بالهجمات، مع تحديد المسؤولية واسم المجموعة المتورطة والبلد التي ربما ترتبط بها، عبر الرابط التالي: <https://eurepoc.eu/cyber-trackers>
11. Jackson Colling, Recapping cyber in war: lessons from the Russia Ukraine conflict, **Lieber Institute**, Jan 8, 2024, Available at: <https://lieber.westpoint.edu/recapping-cyber-war-lessons-russia-ukraine-conflict/>
12. Daryna Antoniuk, Russia and Belarus targeted by at least 14 nation-state hacker groups, researchers say, **The Record**, Available at: <https://therecord.media/>, February 27, 2024, Available at: <https://therecord.media/russia-belarus-cyberthreat-research-factt>
13. Zeba Siddiqui and Christopher Bing, Microsoft says Russian state-sponsored hackers spied on its executives, **Reuters**, January 20, 2024, Available at: <https://www.reuters.com/technology/cybersecurity/microsoft-says-it-was-hacked-by-russian-state-sponsored-group-2024-01-19/>
14. "30 Crucial Cybersecurity Statistics [2023]: Data, Trends and More, **Zippia**, Jun. 15, 2023, Available at: <https://www.zippia.com/advice/cybersecurity-statistics/>
15. Unexpectedly, the cost of big cyber-attacks is falling, **The Economist**, May 17, 2024, Available at: <https://www.economist.com/graphic-detail/2024/05/17/unexpectedly-the-cost-of-big-cyber-attacks-is-falling>
16. Or Kadosh, Analyzing the Rise of State-Sponsored Cyber Attacks, **Findings**, Available at: <https://findings.co/analyzing-the-rise-of-state-sponsored-cyber-attacks/>
17. Anna Fleck, Cybercrime Expected to Skyrocket in Coming Years, **Statista**, Feb 22, 2024, Available at: <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>
18. Interpol Arrests 5,500 in Global Cybercrime Crackdown, Seizes Over \$400 Million, **The Hacker News**, Dec 02, 2024, Available at: <https://thehackernews.com/2024/12/interpol-arrests-5500-in-global.html>
19. Antonia Hmadi, Here to stay" – Chinese state-affiliated hacking for strategic goals, **MERICs**, Nov 22, 2023, Available at: https://merics.org/sites/default/files/2023-11/MERICs%20Report%20medium_Hacking.pdf
20. Anna Ribeiro, Global alarm intensifies as state-sponsored cyberattacks raise risks to critical infrastructure, national security, **Industrial Cyber**, May 12, 2024, Available at: <https://industrialcyber.co/features/global-alarm-intensifies-as-state-sponsored-cyberattacks-raise-risks-to-critical-infrastructure-national-security/>
21. Survey of Chinese Espionage in the United States Since 2000, **Center for Strategic & International Studies**, 2023, Available at: <https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000>
22. Russian hackers sanctioned by European Council for attacks on EU and Ukraine, **The Record**, June 24, 2024, Available at: <https://therecord.media/six-russian-hackers-sanctioned-european-council-eu-ukraine>

23. Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure, **Treasury**, March 25, 2024, Available at: <https://home.treasury.gov/news/press-releases/jy2205>
24. Market insights, Cyber Crime Cost globally, 2024, **Statista**, Available at: <https://www.statista.com/statistics/1417524/worldwide-data-breach-by-main-cost-segments/>
25. 67 Cyber Security Statistics, Facts & Trends: Data on Attacks, Breaches & Threats for 2024, **Cloud Wards**, Available at: <https://www.cloudwards.net/cyber-security-statistics/>

الإرهاب الرقمي: القدرات السيبرانية للتنظيمات الإرهابية «داعش نموذجًا»

تقى النجار*

استخدمت التنظيمات الإرهابية التكنولوجيا 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. من ثَمَّ، 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. ومن ثَمَّ، يسعى هذا الفصل إلى تناول القدرات السيبرانية للتنظيمات الإرهابية بالتركيز على تنظيم «داعش» من خلال خمسة أقسام رئيسية.

* باحث أول ببرنامج الأمن والدفاع، بالمركز المصري للفكر والدراسات الاستراتيجية

يستعرض القسم الأول استغلال تنظيم «داعش» للإعلام الرقمي، وذلك على خلفية تخصيص التنظيم الكثير من الموارد لتدشين شبكة إعلامية لترويج أفكاره المتطرفة، فضلاً عن استخدامه لوسائل التواصل الاجتماعي من أجل تعزيز سمعته الجهادية. وحل القسم الثاني الكيفية التي استغل بها تنظيم «داعش» الطائرات بدون طيار، حيث استخدمها في أغراض الاستخبارات والدعاية من ناحية، ولتنفيذ العمليات الإرهابية من ناحية أخرى. كما اهتم الفصل في القسم الثالث بتوضيح دور العملات الافتراضية في تمويل نشاط تنظيم «داعش»، فيما بحث القسم الرابع استغلال تنظيم «داعش» لألعاب الفيديو في عمليات التجنيد. وفي القسم الخامس استعرض الفصل التهديدات المرتبطة بتوظيف التنظيمات الإرهابية لا سيما «داعش» لتطبيقات الذكاء الاصطناعي.

أولاً: توظيف الإعلام الرقمي والشبكات المظلمة

أدركت التنظيمات الإرهابية قوة وسائل الإعلام، حيث وظفتها في عمليات التجنيد واستخدمتها كسلاح للحرب النفسية. ويعد تنظيم «داعش» من أكثر التنظيمات الإرهابية استغلالاً لوسائل الإعلام، حيث جعلها أداة لنشر أفكاره المتطرفة من ناحية، ولتعزيز صورته الجهادية من ناحية أخرى.

وقد خصص التنظيم الكثير من الموارد المالية والبشرية للوكالات الإعلامية التي مكنت علامته التجارية من أن تصبح واحدة من أكثر الأسماء الإرهابية شهرة، حيث دشّن شبكة ضخمة من المؤسسات الإعلامية في إطار ديوان الإعلام المركزي التابع له، وعدت أبرز هذه المؤسسات مؤسسة «الفرقان للإنتاج الإعلامي» التي تعتبر منصة إعلامية ذات أهمية كبيرة للتنظيم، وذلك في ضوء مسئوليتها عن نشر خطابات وبيانات قادته. كذلك «مؤسسة حياة الإعلامية» التي تعد مؤسسة مركزية له، حيث تنتج مقاطع الفيديو التي تركز على استقطاب المتطرفين في الغرب، فضلاً عن إصدارها مجلتي «رومية» و«دابق» (والتي كانت توزع ورقياً في مناطق سيطرة التنظيم في العراق وسوريا)، لكن توقف إصدارهما في 2016 وفي أواخر 2017 على الترتيب.

كما تعد الوكالات الإخبارية إحدى أبرز مؤسسات التنظيم الإعلامية، وهنا تبرز وكالة «أعماق للأخبار»، وهي وكالة الأنباء الرسمية للتنظيم التي تنشر بيانات حول العمليات الإرهابية التي تبناها أو نفذتها عناصره، وذلك على خلفية تواصلها مع العناصر الميدانية للتنظيم في المناطق الجغرافية المختلفة، والتي تحصل منهم على تقارير محدثة عن العمليات الإرهابية التي يتم تنفيذها.

كذلك تلعب الصحف الإلكترونية دوراً مهماً في شبكة تنظيم «داعش» الإعلامية، ويأتي على رأسها صحيفة «النبأ»، التي تعد المجلة الرئيسية للتنظيم، وتصدر أسبوعياً باللغة العربية. وتحتوي على مقالات تتضمن معلومات عن ساحات معاركه. فضلاً عما تتضمنه من بيانات إحصائية عن عملياته، بجانب نشرها مقالات ذات طابع ديني، ومقابلات مع القيادات التنظيمية.

وعلى صعيد موازٍ، يعد الاستخدام المكثف لوسائل التواصل الاجتماعي من أهم ملامح الآلة الإعلامية لتنظيم «داعش»، حيث وظف التطبيقات المختلفة لنشر رسائله الإعلامية وتشجيع الآخرين، وخاصة الشباب، على تقديم الدعم له سواء بالانضمام إلى صفوفه أو نشر أفكاره المتطرفة⁽¹⁾.

وفي هذا السياق، قدرت الأمم المتحدة في يناير 2019 أن عدد المقاتلين الأجانب الذين انضموا لتنظيم «داعش» في العراق وسوريا يزيد عن 40 ألف مقاتل⁽²⁾ ممن ينتمون إلى جنسيات مختلفة؛ مما يؤكد الدور الذي لعبته وسائل التواصل الاجتماعي في تجنيدهم.

وبصفة عامة، مرت استراتيجية «داعش» الإعلامية بمرحلتين أساسيتين؛ أولاهما هي مرحلة التمدد في الفترة من 2014 إلى 2019. وثانيهما هي مرحلة التراجع التي بدأت في مارس 2019 مع سقوط «الباغوز» التي كانت تعتبر آخر معاقل التنظيم في سوريا. ففي المرحلة الأولى، ركز التنظيم في فترة قوته على جملة من الرسائل الإعلامية الأساسية، يتعلق أولها: بإبراز انتصاراته الميدانية ونجاحه في السيطرة المكانية على مساحات واسعة من الأراضي. وينصرف ثانيها: إلى التأكيد على قوته كدولة خلافة مزعومة لديها مؤسسات حكم مختلفة. ويتصل ثالثها: باستعراض

العنف والوحشية المفرطة بدافع جذب انتباه وسائل الإعلام. أما بالنسبة للمرحلة الثانية فقد شهدت تحولين رئيسيين في رسالته الإعلامية، نتيجة تراجع نشاطه وفقدان سيطرته الميدانية على معظم الأراضي؛ يتعلق أولهما: بتحول فكرة الخلافة من أمر واقع إلى خلافة افتراضية، وينصرف ثانيها: إلى تصاعد التحريض على هجمات الذئاب المنفردة مع التركيز على عمليات الطعن والدهس⁽³⁾.

وفي ضوء التهديدات المتعددة التي فرضها توظيف تنظيم «داعش» لوسائل التواصل الاجتماعي، اتخذت شركات مثل «فيسبوك» و«تويتر» خطوات لمجابهة استغلال التنظيمات الإرهابية لمنصاتها، حيث قامت بحظر الحسابات الخاصة بعناصر تلك التنظيمات من منصاتها. وفي مرحلة ما بعد حظر حساباته، توسع التنظيم في الاعتماد على تطبيق «تليجرام»⁽⁴⁾ الذي يحظى بشعبية كبيرة بين عناصر التنظيم لاحتوائه على مفتاح تشفير يصعب فكّه، بجانب إتاحتها إجراء محادثات سرية يمكن مسح محتواها بعد وقت محدد⁽⁵⁾. وعلى الرغم من حذف مئات الآلاف من الحسابات يوميًا من قبل إدارة التطبيق، فإن التنظيم لا يزال نشطًا عليه، حيث يقوم بفتح حسابات جديدة⁽⁶⁾.

وتجدر الإشارة إلى أن «داعش» أصدر برنامجًا تعليميًا تقنيًا لأتباعه في عام 2015، يرشدهم إلى كيفية حماية أنفسهم من نظام المراقبة الحكومي، وأعطى قائمة لتصنيف تطبيقات الدردشة بناءً على مستوى تشفير؛ إذ صنفت القائمة تطبيقات مثل (SilentCircle) و(Redphone) و(Signal) على أنها «الأكثر أمانًا»؛ وتطبيقات (Telegram) و(Wickr) و(Threema) و(Surespot) على أنها «آمنة»؛ وتطبيقات (WeChat) و(WhatsApp) و(Hike) و(Viber) و(Imo.im) على أنها «غير آمنة»⁽⁷⁾.

هذا، وتجدر الإشارة إلى العلاقة الوثيقة بين «داعش» والشبكة المظلمة، إذ تُشير الأخيرة إلى مواقع إلكترونية مجهولة يصعب رصدها أو تعقبها أو فهرستها بواسطة محركات البحث التقليدية، مثل «جوجل» وغيره. ومن ثَمَّ، يصعب تحديد هويات مستخدميها أو تتبعهم من قبل شركات الإنترنت ووكالات الاستخبارات⁽⁸⁾. وتهيمن المحتويات غير المشروعة على الشبكة المظلمة بنسبة 57٪، بما في ذلك

حسابات العملات المشفرة، والوصول إلى الخدمات المصرفية عبر الإنترنت، والمحافظ الإلكترونية⁽⁹⁾.

وقد تزايد اعتماد «داعش» على الشبكة المظلمة لتجنيد المقاتلين، وتبادل الآراء، والتخطيط للهجمات. وهو ما تدلل عليه هجمات باريس في عام 2015. فعلى إثرها، أعلن التنظيم عن نقل موقع «إصدارات» (الأرشيف الإلكتروني لمؤلفاته الدعائية) إلى شبكة الويب المظلمة بفعل الضغوط المتزايدة عليه⁽¹⁰⁾. كما نشرت «مؤسسة حياة الإعلامية» روابط وتعليمات حول الوصول إلى موقع الويب المظلم الخاص بهم على المنتديات المرتبطة بالتنظيم وعبر قنواتهم على تطبيق «تليجرام»⁽¹¹⁾.

ومن ثمّ، يظل تعقب التنظيمات الإرهابية على وسائل التواصل الاجتماعي للوقوف على تكتيكات عملها وآليات تجنيدها هو الخيار الأفضل لمكافحة دعايتها المتطرفة⁽¹²⁾؛ على أن يأتي ذلك بالتوازي مع تعزيز وعي الأفراد بشأن التهديدات المحتملة التي يمكن أن يتعرضوا لها على وسائل التواصل الاجتماعي أو الشبكة المظلمة، لأن الوعي هو عنصر حاسم في الاستفادة من التكنولوجيا وتجنب أخطارها.

ثانياً: الاستخدام المزدوج للطائرات بدون طيار

اعتمدت التنظيمات الإرهابية على الطائرات بدون طيار في ضوء مميزاتها المتعددة، ومنها توفير المعلومات؛ إذ تتيح الفرصة للحصول على أكبر قدر من المعلومات التي يصعب الوصول إليها عبر الأفراد خوفاً من اكتشافهم. هذا بجانب انخفاض أسعارها؛ فلا تتطلب مبالغ كبيرة للحصول عليها. ناهيك بقدرتها على توفير الوقت جرّاء تنفيذ العمليات بسرعة، وعدم الكشف عن هوية مستخدميها بالضرورة؛ مما يجعلهم في مأمن من الرصد والتعقب⁽¹³⁾.

ويمكن تقسيم استخدام التنظيمات الإرهابية للطائرات بدون طيار إلى فئتين؛ أولهما: استخدامات دفاعية سلبية، بمعنى توظيفها في أغراض الاستخبارات والمراقبة والاستطلاع وتصوير الدعاية. ثانيهما: استخدامات هجومية نشطة مثل

توصيل المتفجرات إلى هدف بعينه⁽¹⁴⁾. وقد استخدم "داعش" إبان فترة تمده في العراق وسوريا الطائرات بدون طيار في كلا الفئتين؛ حيث بدأ منذ عام 2014 في تكييف الطائرات التجارية الرخيصة بدون طيار لأغراض الاستخبارات والمراقبة والدعاية، ثم مع سيطرته على مدينة الموصل قام بتجهيز ورشة كاملة لإنتاج وتصنيع الطائرات بدون طيار. وبحلول أواخر عام 2016، وظف تلك الطائرات في العمليات الهجومية، حيث بدأ في تسليحها لمهاجمة جنود البشمركة في شمال العراق، ثم استخدامها لاحقاً ضد أهداف تابعة للجيش العراقي في أثناء الحملة في الموصل، كما وظفها في المعارك التي دارت في شرق سوريا خلال النصف الثاني من عام 2017⁽¹⁵⁾.

وهنا يتجلى بوضوح حقيقة مفادها أنه في حين بلغ استخدام الطائرات بدون طيار ذروته خلال السنوات التي كان فيها تنظيم «داعش» في أوج قوته، انخفض استخدامه لها عندما صعدت قوات التحالف الدولي من وتيرة القتال ضده. وبمجرد سقوطه وإضعافه، توقف التنظيم عن استخدام الطائرات بدون طيار في معاقلة التقليدية، لأن الحصول عليها أصبح أكثر صعوبة، بل لأنه لم يعد قادراً على مواجهة العقاقب المترتبة على استخدامها⁽¹⁶⁾؛ ذلك أن توظيف التنظيمات الإرهابية للطائرات بدون طيار يعني بالضرورة قيامها بمهام تتشابه مع سلطات وصلاحيات الدول فيما يتعلق بالسيطرة على المجال الجوي؛ مما يحفز الأخيرة على اتخاذ خطوات موسعة لتقويض نفوذ الأولى.

وتجدر الإشارة إلى أن الطائرات بدون طيار التي استخدمها تنظيم «داعش» لم تكن متطورة للغاية. ففي معظم الحالات، استخدم تقنيات بسيطة للجمع بين مكونات عالية ومنخفضة التقنية تم الحصول عليها من آسيا وأوروبا عبر سلسلة من الشركات الوهمية المعقدة، ثم استخدم شركات وهمية أخرى لشراء مكونات مستقلة مثل الكاميرات ووحدات نظام تحديد المواقع العالمي (GPS)، واعتمد على شركات وهمية للمرة الثالثة لشحن تلك الطائرات إلى ولاياته المختلفة⁽¹⁷⁾.

وبالانتقال إلى أفريقيا، نجد أن الولايات التابعة لتنظيم «داعش» اقتصر في استخدامها للطائرات بدون طيار على الاستخدام الدفاعي السلبي (أي الاستطلاع والدعاية). ففي مايو 2020، استخدمت «جماعة أهل السنة والجماعة» التابعة

لتنظيم «داعش» في موزمبيق والتي تعتبر جزءاً من «ولاية وسط أفريقيا»، طائرات بدون طيار لتحديد الأهداف في هجماتها على بلدة «موكيمبوا دي برايا» التي تقع في محافظة «كابو ديلغادو» شمال موزمبيق. وفي العام التالي، استخدمت المجموعة ذاتها طائرات بدون طيار مرة أخرى لأغراض الاستخبارات والمراقبة والتجسس في هجومها على مدينة «بالما».

كما استخدمت «ولاية غرب أفريقيا» التابعة لتنظيم «داعش» طائرات بدون طيار للاستطلاع والدعاية أيضاً، حيث استخدمت في يوليو 2022 طائرة استطلاع بدون طيار لمسح موقع قافلة عسكرية نيجيرية قبل نصب كمين لها في بلدة جويبو بنيجيريا. كما أصدرت الولاية ذاتها مقاطع فيديو دعائية في يناير وأبريل 2022 تعرض لقطات جوية من المحتمل أن تكون قد تم تصويرها باستخدام طائرة بدون طيار رباعية المراوح⁽¹⁸⁾.

ورغم أن التنظيمات الإرهابية في أفريقيا لم تستخدم الطائرات بدون طيار في تنفيذ عمليات هجومية حتى الآن، فإن العديد من المراقبين رأوا أنها مسألة وقت قبل أن تبدأ في القيام بذلك. كما أن هناك مخاوف أخرى مرتبطة باحتمالية توظيف التنظيمات الإرهابية لتلك الطائرات في توزيع المواد الكيميائية والبيولوجية، وخاصة الأمراض المعدية؛ الأمر الذي من شأنه أن يوفر للتنظيمات الإرهابية سبلاً جديدة لتهديد الأمنين الإقليمي والدولي⁽¹⁹⁾.

وفي هذا السياق، حريت الإشارة إلى احتمالية توظيف التنظيمات الإرهابية للسيارات ذاتية القيادة، بالنظر إلى العلاقة الوثيقة التي تربط التنظيمات الإرهابية والسيارات التي تُستخدم في كثير من عمليات الدهس في مناطق جغرافية متعددة. إن زيادة استقلالية تلك السيارات قد تسمح لتلك التنظيمات بتنفيذ العديد من الهجمات عن بعد دون الحاجة إلى التضحية بعناصرها⁽²⁰⁾. وحتى الآن، لم تستطع التنظيمات الإرهابية توظيف السيارات ذاتية القيادة في عملياتها الإرهابية، لكن هناك مخاوف قائمة من احتمالية ذلك في المستقبل⁽²¹⁾.

ثالثاً: العملات الافتراضية والتمويل

تختلف العملات الافتراضية عن مثيلتها الورقية؛ كونها تتميز بعدد من السمات التي يتمثل أبرزها في حماية الهوية، إذ لا يتطلب تنفيذ عمليات الشراء أو البيع الإفصاح عن أي معلومات شخصية لمستخدميها. ناهيك بصعوبة التعقب، حيث يصعب تعقب المعاملات التي تتم بها وبالتبعية هوية مستخدميها⁽²²⁾. وقد حفزت تلك السمات التنظيمات الإرهابية ولا سيما تنظيم «داعش» على استخدام تلك العملات، حيث لجأ بشكل متزايد إليها، وبخاصة في المناطق التي تقوضت فيها الطرق المالية التقليدية بسبب تدابير مكافحة الإرهاب. فقد أدرك أن اعتماده على العملات الورقية سهل استهداف الولايات المتحدة لمخازن احتياطاته النقدية، ومن ثم عمل على توظيف العملات الافتراضية (مثل: «بيتكوين»، و«تيثر» و«إيثريوم»، وغيرها)⁽²³⁾، من أجل: دعم نشاطه، وشراء الأسلحة، وتدريب المقاتلين.

وقد بدأت شواهد توظيف تنظيم «داعش» للعملات الافتراضية تتبلور مع إصدار أحد مؤيديه وثيقة بعنوان «بيتكوين وصدقة الجهاد» ليحدد فيها الأحكام الشرعية لاستعمال «البيتكوين»، مشدداً على ضرورة استعمالها كآلية لتمويل أنشطة تلك التنظيمات، وقد شرحت الوثيقة كيفية استخدام العملات الافتراضية، بجانب كيفية إنشاء الحسابات المالية على الإنترنت. هذا بجانب الأدلة التي كشفتها شركة «إس توتي» -التابعة لجهاز المخابرات السيبرانية في سنغافورة- في يناير 2015 والتي تؤكد طلب خلية تابعة لتنظيم «داعش» من داعميهما جمع تبرعات بالعملات الافتراضية لتعزيز نشاطها، ناهيك بالدور الذي لعبته «البيتكوين» في العملية الإرهابية التي استهدفت سريلانكا في 2019، فقد استخدم التنظيم بوابة الدفع (CoinPayments) لتحويل «البيتكوين» إلى نقود ورقية⁽²⁴⁾.

وفي الوقت الحالي، تتباين استخدام ولايات «داعش» للعملات الافتراضية، حيث هناك ولايات أكثر ميلاً لاستخدامها مثل «ولاية خراسان» التي استخدمت عمله «تيثر» لتلقي الأموال⁽²⁵⁾، في حين أن الولايات التابعة للتنظيم في كل من نيجيريا وموزمبيق وجمهورية الكونغو الديمقراطية لديها حد أدنى، إن وجد، من استخدام العملات الافتراضية. وفي حالة نيجيريا، فإن هذا يتعارض مع سياق الدولة ذاتها،

حيث تحتل المرتبة الثانية في العالم من حيث تبني العملات الافتراضية⁽²⁶⁾. ولهذا السبب، من المحتمل أن نرى مزيداً من استخدام العملات المشفرة من قبل تنظيم «داعش» في غرب أفريقيا. ومع ذلك؛ نظراً لأن التنظيم هناك يتركز إقليمياً ويحقق كثيراً من إيراداته نقداً من خلال الإتاوات والابتزاز، فمن المنطقي تراجع استخدامه للعملات الافتراضية⁽²⁷⁾.

وفي حين كانت «البيتكوين» و«تيثير» من العملات الافتراضية المفضلة لدى تنظيم «داعش» قبل عام 2020، زاد انتشار «مونرو» حالياً داخل شبكات التنظيم، حيث تلاشت جاذبية «البيتكوين» الأولية، بسبب زيادة الشفافية في المعاملات المالية والمحاسبة مع تقنيات «بلوكتشين» محسنة تبنتها وكالات الأمن في جميع أنحاء العالم. إن تحول التنظيم نحو العملات المشفرة التي تركز على الخصوصية مثل «مونرو»، والتي تقدم ميزات خصوصية متقدمة مثل العناوين الخفية والمعاملات السرية، يجعل من المستحيل على آليات إنفاذ القانون تتبع المعاملات المرتبطة بها أو منعها⁽²⁸⁾.

يعود استخدام «مونرو» كعملة مفضلة للتنظيم إلى بوابة «أخبار المسلمين» المؤيدة لتنظيم «داعش» التي أعلنت عن تغيير وسيلة التبرعات من «بيتكوين» إلى «مونرو» حصرياً في يونيو 2020. وفي يوليو 2021، أوصت «مؤسسة آفاق إلكترونية» (وحدة الدفاع السيبراني التابعة لتنظيم «داعش») صراحةً بعملة «مونرو» لميزاتها الفائقة في إخفاء الهوية وصعوبة تتبع المعاملات في قنواتها على تطبيق «تليجرام»⁽²⁹⁾.

كذلك دعت مجلة «صوت خراسان» (المجلة الصادرة باللغة الإنجليزية والتابعة لولاية خراسان) في عددها رقم 32 الصادر في يناير 2024 أتباعها أو المتعاطفين معها إلى «الإنفاق في سبيل الله»، وحثتهم على إرسال الدعم المالي للمسلمين الذين يواجهون الحرب والكوارث، وحذرتهم من إرسال التبرعات باستخدام وسائل غير آمنة؛ حيث نشرت إرشادات مفصلة للتبرع بعملة «مونرو». وارتباطاً بهذا الطرح، تشير بعض المصادر إلى أن «ولاية خراسان» استخدمت العملات الافتراضية لتحويل الأموال إلى المتورطين في الهجوم الذي استهدف موسكو في مارس 2024⁽³⁰⁾.

ومن ثَمَّ، هناك حاجة ملحة إلى تعزيز التعاون الدولي لمواجهة التحديات التي يفرضها توظيف التنظيمات الإرهابية للعمليات الافتراضية. وبالإضافة إلى ذلك، فإن بناء قدرات مسؤولي إنفاذ القانون يمثل عنصرًا مهمًا في التعاطي مع هذا النمط من التهديدات، مما يستلزم إنشاء وحدات متخصصة مجهزة بالإمكانات اللازمة للتحقيق في الجرائم المتعلقة بالعمليات الافتراضية، على أن يكون ذلك بالتوازي مع رفع مستوى الوعي العام بالمخاطر المرتبطة بتلك العمليات من أجل اتخاذ خطوات استباقية للتعاطي مع تلك التهديدات⁽³¹⁾.

رابعًا: ألعاب الفيديو والتجديد

تحتل ألعاب الفيديو بشعبية هائلة؛ إذ تقدر قيمة صناعة تلك الألعاب بنحو 200 مليار دولار أمريكي، ويلعبها ما يقرب من 3 مليارات شخص في جميع أنحاء العالم⁽³²⁾. وقد أظهرت الدراسات أن هناك جاذبية معينة تربط المراهقين الذكور الشباب بألعاب الرماية العنيفة «من منظور الشخص الأول»، وتجربة خيالات القوة ومشاعر السطوة والنفوذ وبيئات ساحة المعركة الحقيقية⁽³³⁾. ومن ثَمَّ دفعت الشعبية التي تحتل بها تلك الألعاب التنظيمات الإرهابية لاستغلالها لدعوة للشباب لمحاكاتها وحمل السلاح.

ففي عام 2014، عندما بدأ تنظيم «داعش» في السيطرة على الأراضي، أصدر لعبة فيديو خاصة به بعنوان «صليل الصوامر» المستوحاة من لعبة الفيديو الأمريكية الشهيرة «جراند ثيفت أوتو». وقد تولى اللاعبون دور مقاتلي «داعش» الذين يقاتلون في مناطق صراع حقيقية مثل العراق وسوريا. إذ كان الهدف الرئيس من إنتاج اللعبة هو لفت الانتباه إلى التنظيم وإغراء الشباب الذين غالبًا ما يفتنون بألعاب الحركة من خلال تزويدهم بنظرة افتراضية على الحياة في الخلافة المزعومة⁽³⁴⁾.

ويستهدف تنظيم «داعش» الأفراد من سن المراهقة من خلال ألعاب وجهة النظر (POV) مثل (Call of Duty)، وكذلك ألعاب إطلاق النار من منظور الشخص الأول (FPS) مثل (Far Cry) و(Halo) و(ARMA3) و(Grand Theft Auto) لتجنيدهم، إذ تتمتع تلك الألعاب بشعبية كبيرة لدى اللاعبين الذكور الذين تقل أعمارهم عن

35 عامًا⁽³⁵⁾. كذلك يعد الأطفال هدفًا محتملاً أيضًا، لأنهم يقضون وقتًا طويلًا على الإنترنت وهم يلعبون ألعاب الفيديو، وقد يصبحون أهدافًا لتلك التنظيمات⁽³⁶⁾.

وفي هذا السياق، توصلت دراسة بعنوان «كيف انتقلت فكرة ألعاب الفيديو من مقاطع الفيديو الدعائية لتنظيم الدولة الإسلامية إلى المحتوى الدعائي» والصادرة في 2019 إلى أن التنظيمات الإرهابية تغير استراتيجيات التجنيد الخاصة بها لتعكس ألعاب الفيديو العنيفة من أجل إضفاء الطابع الجذاب على مجموعاتها للمجندين المحتملين. وقد وجدت الدراسة أن مقاطع الفيديو الدعائية والتجنيدية الاحترافية لتنظيم داعش «تنسخ ألعاب الفيديو الشعبية، وأبرزها لعب (Call of Duty)».

وغالبًا ما تحاكي مقاطع الفيديو الخاصة بتنظيم «داعش» أو تنسخ اللقطات وتقلد أنماطًا وتسلسلات بطرق مفصلة قد لا يتعرف عليها إلا اللاعبون العاديون تمامًا. يتضمن ذلك أشياء مثل «كيف يظهر السلاح الذي يحمله مطلق النار في اللقطة، والتقدم من الأسلحة الأخف إلى الأسلحة الأثقل، واستخدام مقاطع فيديو الطائرات بدون طيار، والطريقة التي يتم بها استخدام الرسومات والعناوين⁽³⁷⁾».

كما تحتوي منصات الألعاب مثل «روبلكس» على وظائف الدردشة التي توفر منصة للشباب للتواصل مع بعضهم البعض وتشكيل مجتمعات عبر الإنترنت من الأفراد ذوي التفكير المماثل، ثم يتحول هذا إلى غرفة صدى؛ حيث يتم تضخيم المعتقدات الحالية لأعضاء هذه المجموعات الصغيرة؛ مما يسهل مسارهم النفسي نحو التطرف⁽³⁸⁾.

وعلى الرغم من عدم وجود الكثير من الأدلة على أن التنظيمات الإرهابية تستخدم ألعاب الفيديو لجمع الأموال، فإن ثمة مخاوف من احتمالية قيامهم بذلك في المستقبل، وذلك لأن تلك الألعاب تفتقر إلى الرقابة الكافية، ويسهل استغلالها نسبيًا؛ فيمكن للتنظيمات الإرهابية غسل مبالغ كبيرة من الأموال عبر آلاف المعاملات الصغيرة⁽³⁹⁾. وقد اتخذت بعض البلدان تدابيرًا في هذا الصدد. فعلى سبيل المثال، أنشأت الشرطة الدانمركية وحدة دورية عبر الإنترنت، حيث يتم تكليف الضباط بمراقبة شبكات الألعاب في أثناء لعب هذه الألعاب للبحث عن أي نشاط إرهابي وإجرامي⁽⁴⁰⁾.

خامساً: الذكاء الاصطناعي وتطوير الدعاية

يكشف تقرير المخاطر العالمية لعام 2024 - الصادر عن المنتدى الاقتصادي العالمي - عن المخاطر الناجمة عن إساءة استخدام الذكاء الاصطناعي، بما يزعزع استقرار النظام العالمي⁽⁴¹⁾. وقد سعت التنظيمات الإرهابية إلى توظيف الذكاء الاصطناعي في آلياتها وتكتيكاتها؛ حتى وظفت أحد تطبيقاته المتمثلة في الطائرات بدون طيار كما سبق القول. ومع التطورات التي شهدتها الذكاء الاصطناعي، وبرز نماذج أكثر تطوراً كأنظمة الذكاء الاصطناعي التوليدي، اتخذت تلك التنظيمات خطوات متعددة من أجل الاستفادة من هذه الأدوات المتطورة⁽⁴²⁾.

وفي هذا السياق، نشرت تنظيم «داعش» في صيف عام 2023 دليلاً يوضح فيه كيفية استخدام أدوات الذكاء الاصطناعي التوليدي. وفي أغسطس 2023، شاركت مجموعة دعم تقني متحالفة مع التنظيم دليلاً باللغة العربية مقترناً بإرشادات لحماية البيانات والحفاظ على الخصوصية عند استخدام المحتوى الذي تم إنتاجه بالذكاء الاصطناعي⁽⁴³⁾.

كذلك تداول تنظيم «داعش» في 27 مارس 2024، بعد تنفيذه هجوم «كروكوس سيتي هول» في موسكو، مقطع فيديو على إحدى المنصات التابعة له، يظهر خلاله مذيع أخبار يقول فيه: «إن هذا الهجوم كان جزءاً من «السياق الطبيعي للحرب المشتعلة بين التنظيم والدول التي تحارب الإسلام». وقد أفاد موقع (SITE Intelligence Group) أن المذيع كان مزيفاً وقد تم إنشاؤه بواسطة الذكاء الاصطناعي⁽⁴⁴⁾.

كما أطلق التنظيم برنامج «حصاد الأخبار»، وهو أيضاً بث إخباري مُصور تم إنشاؤه بواسطة الذكاء الاصطناعي، حيث يتم تحويل المعلومات المكتوبة إلى صوت بشري. هذا، ويستخدمه التنظيم لوصف عملياته في مناطق جغرافية مختلفة⁽⁴⁵⁾. فضلاً عن قيام التنظيم باستخدام الذكاء الاصطناعي التوليدي لترجمة خطابه إلى لغات متعددة مثل الإنجليزية والاندونيسية؛ حيث ينتج «داعش» دعايته بما يزيد على 12 لغة⁽⁴⁶⁾، مما يساعده على توسيع نطاق انتشاره الجغرافي بالوصول إلى ثقافات مختلفة.

ومن ثَمَّ يمكن القول إن الذكاء الاصطناعي قد يعزز من آليات الدعاية والتجنيد للتنظيمات الإرهابية، إذ يساعد استخدام الصور ومقاطع الفيديو المزيفة التي يتم توليدها بواسطة الذكاء الاصطناعي على زيادة نطاق الدعاية المنتجة والتأثير في مواقف الأفراد وعواطفهم⁽⁴⁷⁾. كما يمكن لروبوتات الدردشة المدعومة بالذكاء الاصطناعي التفاعل مع الفئات المستهدفة من خلال تزويدهم بمعلومات مخصصة بناءً على ميولهم ومعتقداتهم، وبالتالي جعل رسائل تلك التنظيمات تبدو أكثر ارتباطًا باهتمامات الفئات المستهدفة، وبالتالي تسهل عملية الاستقطاب والتجنيد⁽⁴⁸⁾.

كما قد يلعب الذكاء الاصطناعي دورًا أيضًا في نشر المعلومات المضللة عبر توظيف تقنية «التزييف العميق» (Deep Fake) التي أسهمت بشكل كبير في تفشي حالة اللاتيقين في مجتمعاتنا المعاصرة، وكان لها أكبر الأثر في استهداف مصداقية الإعلام التقليدي. ومن المتصور استغلالها من قبل التنظيمات الإرهابية بهدف خلق حالة من الضبابية من أجل تزييف الوعي وتقويض الثقة في مؤسسات الدولة⁽⁴⁹⁾.

ناهيك بأن احتمالية دمج الذكاء الاصطناعي في الهجمات السيبرانية من شأنه أن يعزز من تأثيراتها ويزيد من فاعليتها، وقد أطلق تنظيم «داعش» بين أواخر عام 2016 وأوائل عام 2017 أول سلسلة من هجمات حجب الخدمة باستخدام أداة تسمى «مدفع الخلافة» (Caliphate Cannon) التي استهدف من خلالها البنية التحتية العسكرية والاقتصادية والتعليمية لعدد من الدول⁽⁵⁰⁾؛ مما يشير إلى أنه من الممكن تكرار تلك الهجمات مرة أخرى ولكن بفاعلية أكبر مع التطورات التي تشهدها أنظمة الذكاء الاصطناعي.

وارتباطًا بتلك التهديدات حذرت الوكالات الحكومية في الولايات المتحدة من استخدام التنظيمات الإرهابية للذكاء الاصطناعي التوليدي، إذ كشف «كريستوفر راي» (مدير مكتب التحقيقات الفيدرالي) في أواخر أكتوبر 2023، أن مكتب التحقيقات الفيدرالي لديه من الأدلة ما يدل على توظيف الذكاء الاصطناعي بواسطة التنظيمات الإرهابية لتضخيم دعاياتهم ونشرها بالتوازي مع استخدام أدوات الترجمة لجعل الدعاية «أكثر تماسكًا وزيادة مصداقيتها في عمليات التجنيد المحتملة»⁽⁵¹⁾.

في المقابل، خلص تقرير بعنوان «اعتماد الإرهابيين المبكر للذكاء الاصطناعي التوليدي»، والصادر عن مبادرة «تكنولوجيا مكافحة الإرهاب» في أوائل نوفمبر 2023، إلى وجود أدلة قليلة نسبياً على توظيف الإرهابيين للذكاء الاصطناعي التوليدي بشكل منهجي منظم، لكونه لا يعدو في مرحله التجريبية⁽⁵²⁾. ويظل توسع التنظيمات الإرهابية في استغلال أدوات الذكاء الاصطناعي التوليدي مرتبطاً بجملة من العوامل؛ منها: أيديولوجيتها، وتكلفة الاستخدام، وسياقات نشاطها⁽⁵³⁾. ويشكل فهم هذه العوامل مجتمعة أو منفصلة بعداً رئيسياً في التعاطي مع التنظيمات الإرهابية التي قد تتبنى أدوات الذكاء الاصطناعي التوليدي في المستقبل⁽⁵⁴⁾. ومن ثمّ يتعين على صناع السياسات ووكالات إنفاذ القانون والمجتمع المدني ومختلف الأطراف الفاعلة التعاون بشكل وثيق لتطوير استراتيجيات قوية لمواجهة إساءة استخدام التنظيمات الإرهابية للذكاء الاصطناعي بتطوراتهِ المختلفة⁽⁵⁵⁾.

مجمل القول، تميزت التنظيمات الإرهابية بمرونتها وقدرتها على التكيف؛ مما دفعها 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، بجانب ذلك وظفت العملات الافتراضية في التمويل والألعاب الفيديوية التجنيد، وتتخذ في الوقت الراهن خطوات من شأنها الاستفادة من التطبيقات المختلفة للذكاء الاصطناعي من أجل تطوير قدراتها.

وبالتالي، فإن هناك حاجة ماسة لدراسة وبحث الآليات والتكتيكات التي توظف بها التنظيمات الإرهابية التكنولوجيا، مع العمل على اتخاذ خطوات استباقية لا تقتصر على مكافحة فقط، بل تمتد إلى الوقاية أيضاً، مما يستدعي تقاسم المسؤولية بين الوكالات الحكومية والمؤسسات الأكاديمية وشركات التكنولوجيا، فضلاً عن تعزيز التعاون الدولي والإقليمي من أجل اتخاذ التدابير المناسبة لتقليل المخاطر المرتبطة باستغلال التنظيمات الإرهابية للتكنولوجيا من جهة، والبحث عن السبل المثلى لتوظيف التكنولوجيا في مكافحة الإرهاب والتطرف من جهة أخرى.

المصادر:

1. Lisa Blaker, The Islamic State's Use of Online Social Media, **Military Cyber Affairs**, January 2016, Available at: https://digitalcommons.usf.edu/mca/vol1/iss1/4/?utm_source=digitalcommons.usf.edu%2Fmca%2Fvol1%2Fiss1%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages
2. Twenty-third report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities, **United Nations Security Council**, 15 January 2019.
3. هاجر أيمن، ماذا تغير في الخطاب الإعلامي لداعش؟، المركز المصري للفكر والدراسات الاستراتيجية، 28 يوليو 2023، متاح على: <https://ecss.com.eg/35568>
4. Mia Bloom, Telegram and Online Addiction to Terrorist Propaganda, **Minerva Research Initiative**, 29 May 2019, Available at: https://minerva.defense.gov/Owl-In-the-Olive-Tree/Owl_View/Article/1859857/telegram-and-online-addiction-to-terrorist-propaganda/
5. Mia Bloom and Chelsea Daymon, Assessing the Future Threat: ISIS's Virtual Caliphate, **Orbis**, May 2018, Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0030438718300437>, Bennett Clifford, Trucks, Knives, Bombs, Whatever: Exploring Pro-Islamic State Instructional Material on Telegram, **Combating Terrorism Center**, May 2018, Available at: <https://ctc westpoint.edu/trucks-knives-bombs-whatever-exploring-pro-islamic-state-instructional-material-telegram/>
6. Rita Katz, The Islamic State may have a new propaganda haven, **The Washington Post**, 28 January 2019, Available at: https://www.washingtonpost.com/opinions/the-islamic-state-might-have-found-the-perfect-propaganda-machine/2019/01/28/0d31f7ec-2036-11e9-8e21-59a09ff1e2a1_story.html
7. Margaret Coker, Sam Schechner, and Alexis Flynn, How Islamic State Teaches Tech Savvy to Evade Detection, **The Wall Street Journal**, 16 November 2015, Available at: <https://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824>
8. رغدة البهي - تقى النجار، ساحات بديلة: كيف وظفت التنظيمات الإرهابية التطورات التكنولوجية؟، المركز المصري للفكر والدراسات الاستراتيجية، 8 أغسطس 2019، متاح على: <https://ecss.com.eg/6679>
9. Soumya Awasthi, The Dark Web as Enabler of Terrorist Activities, **Issue Brief**, 1 Jul 2024, Available at: <https://www.orfonline.org/public/uploads/posts/pdf/20240701105925.pdf>
10. رغدة البهي - تقى النجار، مرجع سبق ذكره.
11. Gabriel Weimann, Terrorist Migration to the Dark Web, **Perspectives on Terrorism**, 2016, pp. 4044-, Available at: <http://www.jstor.org/stable/26297596>
12. Lisa Blaker, **Op.cit.**
13. رغدة البهي - تقى النجار، مرجع سبق ذكره.
14. Rueben Dass, The Evolving Threat From Terrorist Drones in Africa, **The Lawfare Institute**, 1 May 2023, Available at: <https://www.lawfaremedia.org/article/the-evolving-threat-from-terrorist-drones-in-africa>
15. Syria: footage shows Islamic State drone blowing up stadium ammo dump, **ABC News**, 25 October 2017, Available at: <https://www.abc.net.au/news/201725-10-/footage-shows-is-drone-attack-on-syrian-government-stadium/9085750>
16. Ali Haxhimustaf, From ISIS to Ukraine: The Evolution of Drones' Use On The Battlefield, **The Defence Horizon Journal**, 31 July 2023, Available at: <https://tdhj.org/blog/post/evolution-drones-ukraine-isis/>
17. Thomas Brau, Miniature Menace: The Threat of Weaponized Drone Use by Violent Non-state Actors, **960th Cyberspace Wing**, 22 Sept 2020, Available at: <https://www.960cyber.afrc.af.mil/News/Article-Display/Article/2353270/miniature-menace-the-threat-of-weaponized-drone-use-by-violent-non-state-actors/>
18. Rueben Dass, The Evolving Threat From Terrorist Drones in Africa, **Op.cit.**
19. Thomas G. Pledger, The Role of Drones in Future Terrorist Attacks, **The association of the United States army**, February 2021, Available at: https://www.ousa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf
20. Jeffrey W. Lewis, A Smart Bomb in Every Garage? Driverless Cars and the Future of Terrorist Attacks, **Smart**, 28 September 2015, Available at: <https://www.start.umd.edu/news/smart-bomb-every-garage-driverless-cars-and-future-terrorist-attacks>
21. Kelly Lin, ISIS Working on Weaponizing Self-Driving Cars, NATO Expert Warns, **Motor Trend**, 2 May 2016, Available at: <https://www.motortrend.com/news/isis-working-on-weaponizing-self-driving-cars-nato-expert-warns/>

22. رغبة البهي - تقى النجار، مرجع سبق ذكره.
23. رغبة البهي، العملات الافتراضية وسيلة جديدة لتمويل الإرهاب.. أفكار مقترحة للمواجهة، المركز المصري للفكر والدراسات الاستراتيجية، 18 يوليو 2019، متاح على: <https://ecss.com.eg/6484/>
24. المرجع السابق.
25. Thirty-First Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2610 (2021) Concerning ISIL (Da'esh), Al-Qaida and Associated Individuals and Entities, **United Nations Security Council**, 13 February 2023.
26. The 2023 Global Crypto Adoption Index, **Chainalysis**, 12 September 2023, Available at: <https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/>
27. Jessica Davis, **Op.cit.**
28. Animesh Roul, The Rise of Monero: ISKP's Preferred Cryptocurrency for Terror Financing, **The Global Network on Extremism and Technology**, 4 October 2024, Available at: <https://gnet-research.org/202404/10//the-rise-of-monero-iskps-preferred-cryptocurrency-for-terror-financing/>
29. **I bid.**
30. Jessica Davis, The Financial Future of the Islamic State, **Combating Terrorism Center**, July/August 2024, Available at: <https://ctc.westpoint.edu/the-financial-future-of-the-islamic-state/>
31. Varun VM LL.M, Prospects and Models of Combating Cryptocurrency Crimes: The India-EU Dialogue as a Perspective?, **Eucrim**, 2023, Available at: https://eucrim.eu/media/issue/pdf/eucrim_issue_202304-.pdf#page=63
32. 32 -Menso Hartgers, Eviane Leidig, Fighting extremism in gaming platforms: a set of design principles to develop comprehensive P/CVE strategies, **The International Centre for Counter-Terrorism**, 1 June 2023, Available at: <https://icct.nl/publication/fighting-extremism-gaming-platforms-set-design-principles-develop-comprehensive-pcve>
33. Ahmed Al-Rawi, Video games, terrorism, and ISIS's Jihad 3.0, **Terrorism and Political Violence**, 5 Aug 2016, Available at: <https://www.tandfonline.com/doi/pdf/10.1080/09546553.2016.1207633#page=9>
34. Rueben Dass, The Link Between Gaming and Violent Extremism, **The Diplomat**, 8 March 2023, <https://thediplomat.com/202303//the-link-between-gaming-and-violent-extremism/>
35. Alexander J. Ham-Kucharski, Respawnng Jihadist: ISIS Recruiting Through Online Gaming Communities, **Portland State University**, 2022, Available at: https://pdxscholar.library.pdx.edu/cgi/viewcontent.cgi?article=1001&context=is_student
36. Tech Trends Position Statement Generative AI, **ESafety Commissioner**, 15 Augusta 2023, Available at: <https://www.esafety.gov.au/sites/default/files/202308-/Generative%20AI%20-%20Position%20Statement%20-%20August%20202320%.pdf?v=1734786801250>
37. Cori E. Dauber, Mark D. Robinson, Jovan J. Baslios, Austin G. Blair, Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos, **Perspectives on Terrorism**, June 2019, pp. 1731-.
38. Rueben Dass, The Link between Gaming and Violent Extremism, **Op.cit.**
39. Moshe Klein, Video Games Might Matter for Terrorist Financing, **Lawfare**, 30 May 2024, Available at: <https://www.lawfaremedia.org/article/video-games-might-matter-for-terrorist-financing>
40. Oleg Danylov, The Danish police created the Police Online Patrol, which plays games with young people, **Mezha**, 19 December 2022, Available at: <https://mezha.media/en/202219/12//the-danish-police-created-the-police-online-patrol-which-plays-games-with-young-people/>
41. These are the 3 biggest emerging risks the world is facing, **World Economic Forum**, 13 Jan 2024, Available at: <https://www.weforum.org/stories/202401//ai-disinformation-global-risks/>
42. تقى النجار، الذكاء الاصطناعي والإرهاب. ازدواجية الأدوار، الديمقراطية، العدد 96، أكتوبر 2024، ص ص. 101-96.
43. رغبة البهي، حدود التوظيف: الإرهاب والذكاء الاصطناعي التوليدي، المركز المصري للفكر والدراسات الاستراتيجية، 5 سبتمبر 2024، متاح على: <https://ecss.com.eg/47950/>
44. Rita Katz, SITE Special Report: Extremist Movements are Thriving as AI Tech Proliferates, **The SITE Intelligence Group**, 17 May 2024, Available at: <https://ent.siteintelgroup.com/Articles-and-Analysis/extremist-movements-are-thriving-as-ai-tech-proliferates.html>
45. Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts, **The Soufan Center**, 30 October 2024, Available at: <https://thesoufancenter.org/intelbrief-2024-october-3/>
46. رغبة البهي، حدود التوظيف: الإرهاب والذكاء الاصطناعي التوليدي، مرجع سبق ذكره.

47. Considerations of the Impacts of Generative AI on Online Terrorism and Extremism, **GIFCT**, 20 September 2023, Available at: <https://gifct.org/wp-content/uploads/202309/GIFCT-23WG-0823-GenerativeAI-1.1.pdf>
 48. Gabriel Weimann, Alexander T. Pack, Rachel Sulciner, Joelle Scheinin, Gal Rapaport, and David Diaz, Generating Terror: The Risks of Generative AI Exploitation, **Combating Terrorism Centre**, January 2024, Available at: <https://ctc.westpoint.edu/january-2024/>
 49. Tokka El naggar, AI-powered terrorism, **Al Ahram**, 2 July 2024, Available at: <https://english.ahram.org.eg/NewsContentP/50526454//AlAhram-Weekly/AIpowered-terrorism.aspx>
 50. Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes, **United Nations Office of Counter-Terrorism**, 2021, Available at: https://unicri.it/sites/default/files/202106/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf
 51. Dan Sabbagh, Terrorists could try to exploit artificial intelligence, MI5 and FBI Chiefs warn, **The Guardian**, 18 October 2023, Available at: <https://www.theguardian.com/technology/2023/oct/18/terrorists-exploit-artificial-intelligence-ai-mi5-fbi-chiefs-warn>
 52. Early terrorist experimentation with generative artificial intelligence services, **Tech Against Terrorism**, November 2023, Available at: <https://techagainstterrorism.org/hubfs/Tech%20Against%20Terrorism%20Briefing%20-%20Early%20terrorist%20experimentation%20with%20generative%20artificial%20intelligence%20services.pdf>
 53. Yannick Veilleux-Lepage, Chelsea Damon & Emil Archambault, Learning from Foes: How Racially and Ethnically Motivated Violent Extremists Embrace and Mimic Islamic State's Use of Emerging Technologies, **Global Network on Extremism and Technology**, 7 June 2022, Available at: <https://gnet-research.org/202207/06/learning-from-foes-how-racially-and-ethnically-motivated-violent-extremists-embrace-and-mimic-isl>
54. تقى النجار، الذكاء الاصطناعي والإرهاب. ازدواجية الأدوار، مرجع سبق ذكره.
55. Chris Vallance, Imran Rahman-Jone, Urgent need for terrorism AI laws, warns think tank, **BBC**, 3 January 2024, Available at: <https://www.bbc.com/news/technology-67872767>

اتجاهات الحروب السيبرانية: نتائج مستخلصة

د. رغدة البهي*

دَلَّت الأعوام القليلة الماضية على تزايد خطورة التهديدات السيبرانية؛ لتطال الوكالات الحكومية، والمفاعلات النووية، والمنظمات العالمية، والمؤسسات الصحية، ويُستهدف الأفراد والشركات والدول الصغرى والمتوسطة والكبرى، وتُطور برمجيات الفدية وسبل الاختراق والقرصنة والمتاجرة بالبيانات وبيعها. وعلى تعدد تلك التهديدات، يبرز - في هذا الإطار - الحروب السيبرانية، ولا سيما مع بروز نمط الحروب اللامتماثلة من ناحية، وتزايد الاعتماد على الفضاء السيبراني في عدد واسع من الاستخدامات المدنية والعسكرية على حد سواء من ناحية ثانية. فمع تزايد الاعتماد على الشبكات الإلكترونية لإدارة الأنظمة المسؤولة عن توجيه وإدارة البنية التحتية الحيوية بجانب الأنظمة العسكرية، ازدادت بالتبعية احتمالات استهدافها

* رئيس وحدة الأمن السيبراني، بالمركز المصري للفكر والدراسات الاستراتيجية

في ضوء صعوبة تأمينها من مختلف التهديدات السيبرانية بشكل مطلق، وذلك على الرغم من إنفاق الدول مليارات الدولارات لتأمين تلك الشبكات.

أولاً: الحروب السيبرانية.. اتجاهات التعريف

يحتدم الجدل بين الخبراء حول تعريف الحرب السيبرانية، بجانب طبيعة الأنشطة التي تدخل في نطاقها وتلك التي تخرج عنها. ويُشار لها -بشكل عام- بالهجوم السيبراني أو سلسلة الهجمات السيبرانية التي تستهدف دولة ما بقصد إحداث وفيات بشرية أو دمار في البنية التحتية الحكومية والمدنية، وتعطيل الأنظمة الحيوية. وقد تأخذ شكل استخدام فيروس أو شن هجمات الحرمان من الخدمة الموزعة (DDoS) لإتلاف شبكة معلومات دولة أخرى أو غير ذلك. إذ تتضمن تلك الحرب عادة قيام دولة قومية بشن هجمات سيبرانية على دولة أخرى، وقد ينخرط فاعلون آخرون في تنفيذ تلك الهجمات، وذلك على شاكلة التنظيمات الإرهابية أو الدول المُعادية⁽¹⁾.

ووفقاً لوكالة الأمن السيبراني وأمن البنية التحتية، فإن هدف الحرب السيبرانية هو إضعاف أو تعطيل أو تدمير دولة أخرى. ولتحقيق أهدافها، تستهدف الحرب السيبرانية مجموعة واسعة من الأهداف التي يمكن أن تضر بالمصالح الوطنية، لذا قد تأخذ صور الدعاية والتجسس وتعطيل البنية التحتية على نطاق واسع من خلال استهداف مقدمي خدمات الإنترنت أو أنظمة الاتصالات أو معدات الشبكات أو الشبكات الكهربائية أو الشبكات المالية لتعطيل أنشطة الدولة القومية⁽²⁾. وانطلاقاً من هذا المعنى، تدور رحى تلك الحرب داخل ومن خلال أجهزة الكمبيوتر والشبكات التي تربطها ضد شبكات أخرى حكومية وعسكرية من أجل تعطيل استخدامهما أو تدميرها أو منع استخدامهما.

ويجد مفهوم الحرب السيبرانية جذوره في مقالة «الحرب السيبرانية قادمة!» للكاتبين «جون أركيلا» و«ديفيد رونفيلدت» بمؤسسة «راند»، والتي نُشرت في عام 1993 في مجلة «الاستراتيجية المقارنة». وقد أشارا فيها إلى أن الحرب السيبرانية قد تستهدف البنية التحتية المادية للفضاء السيبراني باستخدام الأسلحة وأساليب

القتال التقليديّة. إذ يمكن تدمير أجهزة الكمبيوتر، وتفجير الأجهزة المكونة للشبكات الإلكترونية، واستهداف / قتل / خداع المستخدمين البشريين للبنية التحتية المادية من أجل الوصول الفعلي إلى الشبكات المستهدفة أو أجهزة الكمبيوتر. وعادةً ما تتضرر تلك الشبكات في حالات الصراع المسلح أو الحروب التقليديّة. ومن الأمثلة البارزة على ذلك حرب حلف شمال الأطلسي (الناتو) ضد يوغوسلافيا في عام 1999، وحرب الولايات المتحدة ضد العراق في عام 2003، حيث تضررت شبكات الاتصالات ومرافق الكمبيوتر في حالات، وتعرضت للضرر في حالات أخرى.

وبخلاف استهداف البنية المادية، قد تتعرض الأنظمة والبرامج المشغلة لها للضرر باستخدام الأسلحة السيبرانية التي تدمر أو تتداخل أو تفسد أو تراقب أو تلحق الضرر ببرامج التشغيل. وتشمل تلك الأسلحة البرامج الضارة مثل الفيروسات وأحصنة طروادة وبرامج التجسس والديدان التي يمكنها إدخال تعليمات برمجية تالفة إلى البرامج الموجودة، ما يتسبب في قيام الكمبيوتر بتنفيذ إجراءات أو عمليات غير مقصودة من قبل مشغله. كما تشمل الأسلحة السيبرانية الأخرى هجمات رفض الخدمة الموزعة التي يقوم فيها المهاجمون باستخدام البرامج الضارة باختطاف عدد كبير من أجهزة الكمبيوتر لإنشاء ما يُسمى بشبكات الروبوت التي تهاجم بعد ذلك الأجهزة المستهدفة الأخرى. وقد استُخدمت تلك الطريقة في الهجمات السيبرانية ضد إستونيا في إبريل ومايو 2007، وضد جورجيا في أغسطس 2008. وفي كلتا الحالتين، زُعم أن قراصنة الإنترنت الروس، وأغلبهم من المدنيين، قاموا بشن هجمات لحجب الخدمة ضد مؤسسات حكومية ومالية وإعلامية وتجارية رئيسية في كلتا الدولتين. وقد منعت تلك الهجمات مؤقتًا وصول حكومات ومواطني تلك البلدان إلى المصادر الرئيسية للمعلومات والاتصالات الداخلية والخارجية.

كما تتلاعب الهجمات السيبرانية الدلالية (المعروفة أيضًا بالهندسة الاجتماعية) بتصورات المستخدمين وتفسيراتهم للبيانات من أجل الحصول على معلومات قيّمة من المستخدمين (مثل: كلمات المرور، والتفاصيل المالية، والمعلومات الحكومية السرية) من خلال وسائل احتيالية. وتشمل تقنيات الهندسة

الاجتماعية التصيد الاحتيالي، حيث يرسل المهاجمون رسائل بريد إلكتروني تبدو غير ضارة للمستخدمين المستهدفين، ويدعونهم إلى الكشف عن معلومات محمية⁽³⁾.

وهناك من يُوسّع الحرب السيبرانية لتشمل أنشطة عدة تشمل: التجسس على دولة أخرى لسرقة الأسرار باستخدام شبكة الروبوتات، أو هجومات التصيد بالرمح للحصول على موطئ قدم في الكمبيوتر قبل استخراج المعلومات الحساسة، والتخريب بعد تحديد مواطن الضعف المحتملة، وهجومات الحرمان من الخدمة لتعطيل مواقع إلكترونية مهمة يستخدمها المواطنون أو العسكريون أو العلماء أو غيرهم لتعطيل العمليات أو الأنظمة المهمة، واختراق شبكات الطاقة الكهربائية لتعطيل الأنظمة الحيوية، وشل البنية التحتية. علاوة على ذلك، قد يؤدي الهجوم على شبكات الطاقة الكهربائية إلى تعطيل الاتصالات، ما يجعل من المستحيل استخدام خدمات مثل الرسائل النصية أو الاتصالات السلكية/اللاسلكية. وقد يمتد الأمر ليشمل هجمات دعائية للسيطرة على عقول أو قلوب الأشخاص الذين يعيشون في البلد المستهدف أو يقاتلون من أجله أو لكشف حقائق محرجة أو لنشر الأكاذيب التي تجعل المواطنين يفقدون الثقة في بلدانهم أو يتعاطفون مع العدو. هذا وتعتمد معظم الأنظمة الاقتصادية الحديثة على أجهزة الكمبيوتر لتعمل، لذا قد تؤدي مهاجمة شبكات الكمبيوتر الخاصة بالمنشآت الاقتصادية مثل أسواق الأوراق المالية أو أنظمة الدفع أو البنوك إلى منح المتسللين إمكانية الوصول إلى الأموال أو منع أهدافهم من الحصول على الأموال التي يحتاجونها⁽⁴⁾.

وعليه، يمكن الدفع بأن هناك ثلاثة مستويات رئيسية للحروب السيبرانية: يتمثل أولها في العمليات المصاحبة للحروب التقليدية لتحقيق التفوق المعرفي كمهاجمة نظام الدفاع الجوي، والذي قد يؤدي إلى خسائر استراتيجية واسعة النطاق. ويتمثل ثانيها في الحرب السيبرانية المحدودة التي تتعرض فيها البنى التحتية والأهداف المدنية للهجمات السيبرانية. ويتصل ثالثها بالحرب السيبرانية غير المحدودة التي يسعى من خلالها المهاجم إلى تعظيم الآثار التدميرية للبنى التحتية، بحيث يؤثر سلباً في البناء الاجتماعي للدولة كمهاجمة أسواق رأس المال، وخدمات الطوارئ، والأنظمة الإلكترونية الخاصة بمولدات الطاقة، وغير ذلك من

أهداف قد تترتب عليها آثار تدميرية واسعة النطاق بهدف توسيع نطاق الخسائر المادية قدر الإمكان⁽⁵⁾.

واستعداداً لذلك النوع من الحروب، اتجهت العديد من الدول إلى تأسيس ما يُسمى «الجيش السيبرانية». واللافت للنظر أن القراصنة المحترفين أضحووا عنصرًا مهمًا باعتبارهم «جنود ظل» في صفوف القوات المسلحة التقليدية بما لديهم من إمكانيات وتقنيات برمجية وإلكترونية تمكنهم من تغيير قواعد اللعبة في أوقات الأزمات والحروب. فقد لجأ كثير من الدول إلى الاستثمار في الطاقات البشرية لشن / صد الهجمات السيبرانية، كخيار بديل تتضاءل تكلفته نسبيًا من خلال «المليشيات السيبرانية» التي يتأسس جوهرها على الدوافع الوطنية لأعضائها، والاستثمار في المواهب النادرة التي تمتلك تقنيات تكنولوجيا المعلومات لتحفيز الابتكار، وتحقيق النمو الاقتصادي، وحماية الأمن القومي. فإلى جانب الجيوش السيبرانية، قد تحظى بعض المليشيات السيبرانية باعتراف رسمي من الدول، بل وقد يتم توظيفها وتمويلها بواسطتها، ما يُمكنها من التعاون مع مختلف أجهزة إنفاذ القانون والاستخبارات، وهو ما يُسفر عن التطوير المضطرد لمهاراتها وقدراتها⁽⁶⁾.

وعموماً، يمكن تصنيف الهجمات التي يمكن أن تقوم بها الجيوش السيبرانية إلى ثلاثة أنواع رئيسية هي: مهاجمة شبكات الخصم، واستطلاعها والتجسس عليها، والدفاع عن شبكات الدولة. فعلى صعيد النوع الأول، فإنه يشمل اختراق الشبكات لحقن الحاسبات بكم هائل من البيانات أو وضع بيانات ومعلومات مُحرفة لإرباك المستخدمين، ونشر الفيروسات وما شابهها من البرامج الصغيرة المؤذية مثل الديدان، وتلغيمها بالقنابل المنطقية (Logic Bombs) التي تُتلف ما تحتويه الحاسبات من بيانات وبرمجيات، أو القيام بهجمات سيبرانية لقطع خدمات الإنترنت عن الخصم، وتدمير قواعد البيانات التي يمتلكها، وتعطيل قدرته على النشر السريع لقدراته وإمكانياته وقواته، أو قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها وتعطيل شبكات الكمبيوتر، أو شل أنظمة الدفاع الجوي أو التوجيه الإلكتروني للخصم أو السيطرة على وحدات القيادة والتوجيه أو إفقاد العدو قدرته على التحكم أو الاتصال بالأقمار الصناعية. وقد يصل الأمر إلى التدمير المادي

من خلال تدمير: الخوادم، والأسلاك، والكابلات، والأجهزة التي تحتوي على معلومات يصعب التأثير عليها عن بعد.

أما النوع الثاني، فيشمل الدفاع عن الشبكات بما يشمل ذلك من حماية الشبكات وأجهزة الكمبيوتر من أي عملية اختراق خارجي. ويجب أن يكون التأمين على مستوى البرمجيات (Software) والمكون المادي للشبكات (Hardware). بحيث يتم تأمين الشبكة من أي اختراق خارجي بأي من الأسلحة السيبرانية السابق ذكرها. وكذلك تأمين المكون المادي للشبكات مثل الخوادم أو الشرائح الإلكترونية. والتي قد تكون مُبرمجة من قبل المصمم لكي تعمل في ظروف غير عادية لصالحه.

أما النوع الثالث، فيشير إلى القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، دون أن يُصاحب ذلك تدمير أو تخريب البيانات والمعلومات التي قد تشمل خطط الدفاع /الهجوم العسكري أو أسرارًا عسكرية /حربية أو معلومات سياسية واستخباراتية. ولا تتوقف وظيفتها عند ذلك الحد فحسب، بل يمكن من خلالها رسم خرائط لشبكات الحاسب الآلي واستخدامها مستقبلاً في عمليات الهجوم السيبراني. كما يمكن ترك بعض الثغرات من خلال الأبواب الخلفية (Backdoors) لحقن الشبكة بفيروسات للقيام بمهام معينة مثل نقل البيانات إلى أجهزة المُتجسس. كما يمكن أيضًا استخدامها في التأثير على أفكار وسلوكيات الخصم من خلال شن حرب نفسية، وذلك بنشر مثل تلك الخطط العسكرية والبيانات أو إرسالها إليه مرة أخرى، كي يدرك أنه مُخترق ولن يستطيع المواجهة⁽⁷⁾.

ثانيًا: اتجاهات محتملة

على الرغم من أن الحرب السيبرانية تقتصر حاليًا 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 تحدد كيفية تدريب القوات الجوية والقواعد الحاكمة لانتشارها في ساحات المعارك المستقبلية.

ومن ثم من المتوقع أن تدور اتجاهات الحرب السيبرانية في المستقبل حول جملة من الاتجاهات التي يمكن توصيفها بأنها أهم النتائج المستخلصة من هذا الكتاب، والتي يمكن استعراضها من خلال النقاط التالية:

- بالتواكب مع التطورات التكنولوجية المتسارعة، من المتوقع أن تشهد الحروب السيبرانية تطورات أكبر، ما يطرح تحديات جديدة تطال الأنظمة الرقمية والبنى التحتية. ومع تزايد الاعتماد على الشبكات الرقمية والاتصالات اللا سلكية في العمليات العسكرية، سيزداد الضغط على الجيوش لحماية أنظمتها من الهجمات السيبرانية.
- لم تعد الحروب تعتمد كلية على الجيوش الاعتيادية بعد أن أصبحت التكنولوجيا أداة في حروب أكثر ضراوة وأقل دماءً وأقل ضجيجًا. ومن ثم باتت الحروب السيبرانية إحدى أدوات إدارة الصراعات التقليدية وساحة موازية لها.
- أصبحت الحرب السيبرانية متعددة الساحات تسيطر على العقلية العسكرية للعديد من الدول التي أسست جيوشًا سيبرانية خلف الحواشيب بحثًا عن ثغرات قد تمكنها من إلحاق أكبر ضرر ممكن بالخصم.
- دفع «صن تزو» في كتابه «فن الحرب» بأن أعظم انتصار هو ذلك الذي لا يحتاج إلى معركة، وهو ما ينطبق على الحرب السيبرانية التي يتمثل أكبر مخاطرها في طبيعتها؛ فهي ليست حربًا مادية تُدار في ساحات المعارك، بل هي حرب صامتة تندلع دون ضجيج في الفضاء السيبراني، وقد تدور رحاها لسنوات قبل أن تحسم نتائجها.
- تدار الحروب السيبرانية بطرق متعددة، ففي حالة الصين تُدار بالتجسس، وفي حالة الولايات المتحدة تُدار بالتوازي مع قدرات عسكرية متقدمة، وفي حالة روسيا تُدار من خلال شل البنية التحتية والسيطرة على وسائل التواصل الاجتماعي.
- إن الحروب السيبرانية قادرة على شل البنوك والمطارات والبورصات، في ظل تنامي اعتمادها على الأنظمة الإلكترونية والبرمجيات لتسيير عملياتها في ظل العالم الرقمي وإنترنت الأشياء والذكاء الاصطناعي. ومن شأن استهداف تلك الأنظمة أن يؤدي إلى تعطيل الأنظمة، وفقدان البيانات، واختراق الشبكات، أو حتى تعطيل العمليات المالية واللوجستية بشكل عام.

- تصاعدت الحروب السيبرانية في منطقة الشرق الأوسط، والتي اتخذت في أحد مظاهرها خروقات البيانات. فلم تعكس تلك الحروب التوترات الجيوسياسية المتزايدة فحسب، بل كشفت أيضًا عن اتجاه مقلق لتسليح البيانات الحساسة. إن تلك الخروقات لم تؤثر فقط على المؤسسات الحكومية والمنظمات الرئيسية، بل أثرت أيضًا على ملايين المواطنين، مما يدل على تعدد العواقب بعيدة المدى للحرب السيبرانية.
 - تهدف الأنشطة المتبادلة في إطار الحرب السيبرانية إلى جمع المعلومات الاستخباراتية، وتقويض نشاط البنية التحتية الحيوية والكيانات الحكومية وغير الحكومية، من خلال: التسلل إلى الشبكات باستخدام حملات التصيد بالرمح المتطورة، ونشر برامج ضارة، وسرقة المعلومات الحساسة، وإلحاق الضرر بالأنظمة، وشل العمليات المالية.
 - إن فاعلية الوسائل التجسسية لن تكون حاسمة لولا وجود اختراق بشري كبير، ليتكامل العنصر البشري مع الوسائل التكنولوجية، ومنها تقنيات مراقبة الهواتف المحمولة وتكنولوجيا التعرف على الوجه، ما يمكن القوات العسكرية من التعرف على الأشخاص من خلال كاميرات عالية الدقة على متن المُسيّرات أو الأقمار الاصطناعية.
 - إن البعد السيبراني سيكون حاضرًا وذا تأثير ممتد في الحروب العسكرية المستقبلية، وربما يحضر بقوة حتى مع تسوية بعض الحروب الدائرة في منطقة الشرق الأوسط أو في العالم.
 - في المستقبل، سيتصاعد نمط الحروب السيبرانية بالوكالة، وبالتبعية القرصنة المدعومة بالدولة في تحركات دولية أحادية بصرف النظر عن الشرعية الدولية.
- قصارى القول، من المتوقع أن تمتد الحرب السيبرانية مستقبلًا لتشمل: شبكات الاتصالات، وأنظمة الكمبيوتر، والمعالجات المدمجة. والتي تشمل أيضًا الشبكات غير المتصلة بالإنترنت مثل: روابط البيانات التكتيكية، وشبكات التحكم بالأقمار الصناعية، وشبكات التحكم في الإطلاق، والشبكات الأخرى التي لا تعتمد تقليديًا على بروتوكولات وتقنيات نقل البيانات عبر الإنترنت؛ لتتسع بذلك عمليات استهداف الشبكات غير التقليدية وما يتصل بها من أنظمة، مثل: الأقمار الصناعية،

والكترونيات الطيران، وكبسولات الاستهداف، وأجهزة الراديو الرقمية، والطائرات الموجهة عن بعد. وستشمل التأثيرات الناتجة عن ذلك: الاضطراب، والتشتيت، والتشويه، وانعدام الثقة، والارتباك، والفوضى.

المصادر:

1. Imperva, Cyber Warfare, **Imperva**, Available online: <https://www.imperva.com/learn/application-security/cyber-warfare/>, Accessible at: November 24, 2023.
2. Alexander S. Gillis, Definition Cyberwarfare, **Tech Target**, March 2023, Available online: <https://www.techtarget.com/searchsecurity/definition/cyberwarfare>, Accessed on November 24, 2023.
3. John B. Sheldon, Cyberwar, **Britannica**, Nov 21, 2023, Available online: <https://www.britannica.com/topic/cyberwar>, Accessed on November 24, 2023.
4. Cyber Readiness Center and Breaking Threat Intelligence, What Is Cyberwarfare?, **Fortinet, Inc.**, Available online: <https://www.fortinet.com/resources/cyberglossary/cyber-warfare>, Accessed on November 24, 2023.
5. نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الإلكتروني (القاهرة: المكتب العربي للمعارف، 2015) ص. 30.
6. رغدة البهي، المليشيات السيبرانية.. كيف توظف الدول الطاقات البشرية في الدفاع السيبراني؟، المركز المصري للفكر والدراسات الاستراتيجية، 17 إبريل 2019، متاح على: <https://ecss.com.eg/4434>، تاريخ الاطلاع 25 نوفمبر 2023.
7. إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي (القاهرة: مركز المستقبل للأبحاث والدراسات المتقدمة بأبوظبي بالتعاون مع دار العربي للنشر، 2019)، ص. 32-30.



ECSS

المركز المصري
للفكر والدراسات الاستراتيجية
EGYPTIAN CENTER FOR STRATEGIC STUDIES