2023

المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية بجامعة الإسكندرية
https://esalexu.journals.ekb.eg
دورية علمية محكمة
المجلد الثامن (العدد الخامس عشر، يناير 2023)

استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني

حازم محمد خليل

باحث دكتوراه العلوم السياسية

كلية الاقتصاد والعلوم السياسية

جامعة القاهرة

المخلص

كانت ثورة المعلومات وظهور الإنترنت إيذاناً ببزوغ العصر السيبراني وخلق بيئة جديدة هي الفضاء السيبراني، إضافة إلى الأرض والبحر والجو والفضاء، الذي أصبح يُستغل فى النظام الدولي، خاصة مع بروز شكل جديد من القوة هي القوة السيبرانية، التي توزعت بين الفاعلين الدوليين (دولاً وغير دول)، ما أصبح الفضاء السيبراني ساحة جديدة للصراع بين الدول.

تعد الحروب السيبرانية حربًا غير معلنة يخوضها الفاعلون الدوليون (دولًا وغير دول) بعضهم ضد بعض؛ لإلحاق الضرر أو لتدمير دولة أو مؤسسة، من دون عناء أو تكلفة عالية، في الإطار التحضيري الذي يستهدف تدمير البنية الحيوية والمعلوماتية للدولة بما يهدد الأمن القومي، أو أنها وسيلة؛ لكي تحول الدولة المستهدفة إلى دولة فاشلة أو رخوة، مقارنة بالهجمات المسلحة التي تتطلب تكلفة مالية عالية وتدريبًا وتسليحًا.

وتُدار هذه الحرب داخل الفضاء السيبراني الذي أعطته أفضلية عن مسارح العمليات الأخرى في الحروب غير التقليدية. فالفضاء السيبراني ساحة معارك، مثله مثل ساحات المعارك، تدار فيها جميع فعاليات الحروب التقليدية من هجوم ودفاع وردع. كما أن الحرب على الإرهاب والوكالة لم يُستثنَيا من الفضاء السيبراني.

Abstract

Purpose – This paper aims to study the new domain of conflict which is, cyber space and its impact on the concept of power. It brought a new concept with new tools. The concept of cyber power led to the diffusion of power and affected the levels of analysis in international relations. Cyber wars are undeclared wars launched by states and non-states actors, to undermine or destroy the infrastructure of the targeted institution with the minimum preparations and the least cost.

Design/methodology/approach-The paper explores the effectiveness of offensive, defensive and deterrence means of cyberwarfare by using Power Transition Theory. The theory explains the

changes in international relations levels of analysis and the change of power among states and non-state actors. The paper illustrates the case of cyber terrorism and cyber proxy as an example of diffusion of power.

Findings- cyberspace became an open arena for all actors Nation States as the legal and the only actors who monopolize the use of power is no longer a fact. Cyberspace led to the diffusion of power and created new actors with the capability of undermining and causing a lot of harm to other actors as an easy and cheap means.

Originality/value –This paper is able to prove that there is no longer a defining line between what is military and what is civilian. Power now belongs to private individuals. Everyone is being targeted

Keywords: cyberspace- cyber power- cyber proxy- cyber terrorism- power transition theory.

مقدمة

كتب جولين جراى، أستاذ العلاقات الدولية والدراسات الاستراتيجية بالمملكة المتحدة، يقول: "إننا نعلم كل ما تنبغي معرفته عن الحرب، وهذا ليس بالأمر المستغرب؛ لأن لدينا مصادر متنوعة حول 2500 عام من التاريخ الدامي، لكننا لا نعرف شيئًا عن حروب المستقبل، حيث يتم الخلط بين طبيعة الحرب وصفتها".

فالحرب "ذات طبيعة كونية شاملة ودائمة، ولا تتغير. أما صفة الحرب، فهي في تغير دائـم".

فمع ظهور أنماط جديدة من الحروب؛ كحرب المعلومات، وحرب المناخ، وحروب الفضاء، والحرب السيبرانية، والحروب غير المتماثلة، من الممكن أن تتلاشى الحرب التقليدية؛ بفعل التقدم الهائل في التكنولوجيا العسكرية، أو التقليدية، بمعنى النظامية التي تعكس مواجهة عسكرية مباشرة بين جيشين أو أكثر، لا تزال ممكنة، أم أنها توارت بفعل انتشار نمط الحروب غير النظامية بين فاعلين دوليين ودون مستوى الدولة.

فالحرب غير التقليدية عدلت مفهوم الحرب، فهي تعرّف بأنها العمليات ذات الطبيعة

العسكرية، أي التي قد تستخدم في القوة العسكرية بشكل محدود، أو التي تستخدم فيها الوسائط العسكرية المختلفة، التي يتم القيام بها بواسطة عناصر غير نظامية بالأساس، بغض النظر عن هدف أو مشروعية هذه العمليات. بهذا المعنى، تكتسب هذه الحروب خصائص عدة تميزها عن الحرب التقليدية، أبرزها:

1- عدم وضوح أطراف الحرب.

2- عدم الوضوح النسبي للهدف في العمل العسكري، سواء كان زمنيًا أو سياسيًا.

3- اتساع مسرح العمليات والقطاع المدني جزء أساسي في هذه الحرب، سواء كمستهدف من أعمال الحروب غير التقليدية، أو كمشارك فيها، أو كعنصر تأثيري في صناعة القرار السياسي.

4- تعدد وتنوع الأسلحة المستخدمة في هذه الحروب. فالقوة التكنولوجية العسكرية، والمعلومات والاتصالات، والحرب النفسية، والفضاء الإلكتروني، كل ذلك غيّر من طبيعة الأسلحة المستخدمة.

5- غياب القواعد القانونية التي تنظم هذه الحروب؛ فليست لها حدود جغرافية معينة، فهذه الحروب بدون قواعد، فهي وسط الشعب، وتستهدف كل عناصر القوة الشاملة.(دلال, 2018, 5:6)

ومع كل هذه التفاعلات والخصائص التي أظهرتها الحروب غير التقليدية، لم يكن أحد يتوقع أن تكون مشاهد الرئيس الأمريكي "ريجان" في فيلم "ألعاب الحرب" عام 1983 نقطة فاصلة في تطور ترسانة الولايات المتحدة الأمريكية الإلكترونية التي استخدمتها في حرب الخليج الثانية عام 1991 ثم في صربيا، وفي أثناء الحرب الباردة ضد الاتحاد السوفيتي سابقًا.

من هنا، ظهرت الحاجة إلى تطوير مفاهيم واستراتيجيات جديدة، تتلاءم مع العصر السيبراني Cyber Age؛ ذلك العصر الذي يعدّ الإنترنت فيه هو الإطار العام الحاكم لتفاعلاته كافة، سواء كانت شخصية أو عامة، عسكرية، أو سياسية، أو اقتصادية، أو اجتماعية. (إيهاب, 2019 :4)

فقد جاءت جذور كلمة "سيبر" Cyber من " السيبر تطبيقًا Cybernetics". ويعود هذا المصطلح إلى منتصف القرن التاسع عشر، ويصف الحلقات المغلقة لأنظمة المعلومات، لكن في السياق الراهن لشبكات الحاسب.

تداول هذا المصطلح أكثر عن رواية "نيورومانسر Neuromancer" رواية الخيال

العلمي التي كتبها ويليام جيسون William Gibson عام 1984، التي تناولت أعمال التخريب في عالم "الفضاء السيبرانى" الافتراضي.

لقد ازدادت التوقعات بأن تكون حروب المستقبل حتمًا سيبرانية، ولو في جزء منها. وترجح هذه التوقعات بأن يكون الفضاء السيبراني ميدانًا للحرب. كما أن المقاتلين في هذا الفضاء ليسوا هم الجنود أو البحارة أو الطيارين فقط، وإنما كل من يستخدم هذا الفضاء. (كابلات,2019: 14-65)

فمع بروز الفضاء السيبراني كساحة للحروب واجهت المفاهيم التقليدية من الحرب والقوة والدفاع والردع تحديات جوهرية لمدي ملاءمتها، أو حتى تكيفها مع الحروب غير التقليدية، لذا برزت الحاجة الى تفسير هذه التحولات، وبتطبيقها على الإرهاب والوكالة السيبرانية.

المشكلة البحثية

أصبح الفضاء السيبراني اليوم العمود الفقري لمعظم التفاعلات الدولية، لسلاسة الاستخدام ورخص التكلفة وسهولة الاتصال وهشاشة القدرات والتنظيمات الرقابية، مع تزايد اعتماد الدول والحكومات لتبني الحكومة الذكية، الأمر الذي أدى إلى توفير بيئة مناسبة للفاعلين الدوليين من استغلال هذا الفضاء

من هنا، يمكن صياغة المشكلة البحثية في سؤال رئيسي مفاده: ما مستوى وطبيعة استغلال للفاعلين الدوليين (دولاً وغير دول) للفضاء السيبراني فى إطار الحروب غير التقليدية؟ وينبثق منه تساؤلات فرعية محل الدراسة من التحول فى مفاهيم القوة وظهور القوة السيبرانية، وما يحدث من تفاعلات سيبرانية من هجوم ودفاع وردع، ولماذا يفضل الفاعلون الدوليون الفضاء السيبرانى عن غيره من ساحات الحروب؟ مع عرض نموذجين من استغلال الفضاء السيبراني، هما الإرهاب السيبراني والوكلاء السيبرانيون.

للإجابة عن هذه التساؤلات، سوف تقسم الدراسة إلى عدد من المحاور كالآتي:

المحور الأول: الفضاء السيبراني.

المحور الثاني: التحول في مضامين القوة وظهور القوة السيبرانية.

المحور الثالث: الحرب السيبرانية (الهجوم والدفاع والردع السيبراني).

المحور الرابع: الإرهاب السيبراني.

المحور الخامس: الوكالة السيبرانية.

المحور الأول

الفضاء السيبراني

عادة ما تتشكل الجيوش الحربية الحديثة من ثلاث أذرع عسكرية، هي القوات الجوية والبرية والبحرية، تستخدمها للهجوم على أعدائها والدفاع عن أرضها. ولكن في العصر السيبراني، بدأنا نسمع عن معارك تدور رحاها في الفضاء السيبراني، وبين خصوم معظمهم مجهولو الهوية، يهاجمون البنية التحتية الرقمية للدول التي يضعونها في خانة العدو، حيث تهدف الهجمات الرقمية إلى الحصول على معلومات مخابراتية حساسة، أو تدمير بنية الاقتصاد الذي بدأ يعتمد على المعلومات بشكل كبير، أو لمجرد إشعار العدو بأنهم موجودون على الجبهة الرقمية، وبإمكانهم إزعاجه. (يحيى، 237:2014)

لم تعد المجالات الأربعة التي عُرفت في المواجهة المسلحة التقليدية بين الدول (البر والبحر والجو والفضاء) وحدها على الساحة الدولية للصراع، بل دخل مجال خامس للمواجهة، هو (الفضاء السيبراني)، حيث (Cyberspace). (المجال الخامس). فالفضاء السيبراني مجال افتراضي من صنع الإنسان، يعتمد على نظم الكمبيوتر وشبكات الإنترنت، وعدد هائل من البيانات والمعلومات والأجهزة.

مفهوم الفضاء السيبراني

يمكننا القول إن: "الفضاء السيبراني هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، ومكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين، سواء كانوا مشغلين أو مستعملين". وتجدر الإشارة إلى أن مسألة تحديد مفهوم "الفضاء السيبراني" هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل من الدول والهيئات، كل بحسب رؤيته واستراتيجيته وقدرته على استغلال المزايا المتاحة، ومواجهة المخاطر الكاملة في هذا الفضاء. (إسماعيل،2019 :1016-1018)

كما عُرف أيضًا بأنه "مجال عالمي داخل بيئة المعلومات، يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك: الإنترنت، وشبكات الاتصالات، وأنظمة الكمبيوتر، والمعالجات المدمجة، ووحدات التحكم." وبموجب هذا التعريف، ينتشر الفضاء السيبراني في كل

مكان بوصفه مشتركًا عالميًا، لا يخضع لسيادة دولة واحدة أو مجموعة من الدول. غير أنه في المقابل، تؤكد الممارسات الدولية أن الفضاء السيبرانى ليس محصنًا من السيادة الإقليمية أو الولاية القضائية للدول (Wolff :125-126).

المخاطر من الفضاء السيبراني

أحدث الفضاء السيبراني تغييرات في مفاهيم العلاقات الدولية، كمفهوم القوة والصراع والحرب، حيث انتشرت القوة بين الفاعلين الدوليين، وتحول الصراع من المادي إلى الافتراضي؛ ما نتج عنه ظهور تهديدات جديدة تتزايد في الحجم والشدة. فكلما زاد التشابك والاعتماد، زادت التهديدات السيبرانية.

ويلاحظ أيضًا أن التهديدات السيبرانية لا تستهدف الإضرار بالبشر بصورة مباشرة، فهي تؤثر في الأنظمة والشبكات والأجهزة التي يستخدمها الأفراد، وتعتمد عليها الدول، ومن ثم تؤثر في أسلوب الحياة ذاتها بشكل يهدد أمن الدولة ككل (نوران).

فيمكن القول إن المخاطر الناشئة من الفضاء السيبراني تتسم بثلاث سمات رئيسية، هي:

- اتساع نطاق وتعدد مستوياتها.
- عدم إمكان إيقاف مخاطر تلك التهديدات كليًا.
- تنوع المخاطر السيبرانية، سواء من حيث طبيعتها، أو مصادرها، فقد تشنها دول، أو منظمات إجرامية، أو أفراد، أو إرهابيون وغيرهم.

فطبيعة الفضاء السيبراني جعلت المخاطر الأمنية الناتجة عن التفاعل فيه مختلفة كليًا عن التهديدات الأمنية التقليدية. ويعزز من هذا الاختلاف امتناع نطاق الفضاء السيبراني، حيث إنه يتخطى الحواجز الجغرافية والمكانية، ومن ثم يجمع مختلف الفواعل الدولية، التي تمتلك مصالح ورؤى استراتيجية متنوعة. كما أن العولمة أصبحت من الأمور الحتمية. واعتماد الدول المتزايد على الأنظمة الإلكترونية لم يعد أيضًا ممكنًا التراجع عنه، ما يزيد من المخاطر التي قد تتعرض لها الفواعل نتيجة لهذا الاعتماد المتزايد.

كما أن معدلات التطور في الفضاء السيبراني مرتفعة، ومن ثم يترتب على كل تطور ظهور نقاط ضعف جديدة تهدد أمن الدولة؛ أي أن الفضاء السيبراني يتسم بديناميكية متشابكة.

كما أن عدم القدرة على التأكد من هوية الفاعل الدولي القائم بالهجوم هو أحد أهم العوائق

التي تواجه الدولة في التعامل مع التهديدات السيبرانية، وهو ما يختلف عن التهديدات التقليدية. ويتمثل التحدي الأكبر في الفضاء السيبراني في صعوبة إسناد الهجوم لفاعل بعينه، ما يمثل مصدر قوة للفواعل الدولية، حيث تتسم عملياتهم بالسرية وعدم قدرة التعرف على هويتهم، ومن ثم معاقبتهم أو رد الهجمات، خاصة إذا كان مصدرها أكثر من جهاز إلكتروني ومقدم للخدمة في أكثر من دولة (أهمية.2020 :17-30).

بصفة عامة، تنقسم مخاطر الفضاء السيبرانية التي تواجهها الدول إلى أنماط رئيسية، هي:

1. هجمات الحرمان من الخدمة

حيث يتم إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والاستجابة لها؛ ما يؤدي إلى توقفه بصورة جزئية أو كلية، أو إبطاء عمله؛ ما يسبب ضررًا للمستخدم النهائي. وهي تستعمل كثيرًا ضد مواقع الإنترنت أو البنوك أو المؤسسات؛ من أجل التأثير فيها، أو لدفع فدية مالية.

2. إتلاف المعلومات أو تعديلها

ويقصد به الوصول إلى معلومات الضحية عبر شبكة الإنترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات المهمة دون أن يكتشف الضحية ذلك. فالبيانات تبقى موجودة، لكنها مضللة، ما قد يؤدي إلى نتائج كارثية، خاصة إذا كانت خططًا عسكرية، أو مواعيد، أو خرائط سرية.

3. التجسس على الشبكات

ويقصد به الدخول غير المصرح، والتجسس على شبكات الخصم، دون تدمير أو تغيير في البيانات، يكون الهدف منه الحصول على معلومات قد تكون خططًا عسكرية، أو أسرارًا حربية، أو اقتصادية، أو مالية، أو سياسية؛ ما يؤثر سلبًا في مهام الخصم.

4. تدمير المعلومات

ويتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، يصطلح عليه "تهديد لسلامة المحتوى"، ويُعنى به إحداث تغيير في البيانات، سواء بالحذف أو التدمير من قِبل أشخاص غير مخولين (إسماعيل، 2019 :1023-1024) .

وعليه، فلم يقتصر اهتمام الدول بالأمن السيبراني على البعد التقني فحسب، بل تجاوزه إلى أبعاد أخرى، مثل الأبعاد الثقافية والاجتماعية والاقتصادية والعسكرية وغيرها، وهو ما عمل على دعم حقيقة أن الاستخدام غير السلمي للفضاء السيبراني يؤثر في الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية للمعلومات.

إضافة إلى أن تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد أثر بدوره في سيادة الدول، خاصة مع بروز دور الشركات التكنولوجية العابرة للحدود الدولية، وبروز أخطار القرصنة والجريمة السيبرانية والجماعات الإرهابية.

لقد أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، حيث جعل الفضاء السيبراني تلك المصالح مرتبطة ببعضها بعضًا في بيئة عمل واحدة. ومن ثم، فإن أي هجوم على إحدى تلك المصالح يكون سببًا في حدوث عدم توازن استراتيجي، وتهديدٍ خطيرٍ للأمن القومي؛ ما دفع العديد من الدول إلى إدخال الأمن السيبراني ضمن استراتيجياتها للأمن القومي.

إن "ترسيم الخطوط الفاصلة بين الحرب والسلام يمكن أن يتآكل بسهولة في الفضاء السيبراني، فيمكن أن يتم إلحاق أضرار مهما تكن طبيعتها بالخصم، وذلك دون تجاوز الخط الفاصل بين الحرب والسلام بشكل رسمي" (Paulo & Janu.2013 :2).

أفضلية الفضاء السيبراني

كانت ثورة المعلومات وظهور الإنترنت إيذانًا ببزوغ العصر السيبراني، وخلق بيئة جديدة من صنع الإنسان، هي الفضاء السيبرانى (Cyber space)، إضافة إلى الأرض والبحر والجو والفضاء ، الذي أصبح يؤثر في النظام الدولي، خاصة بروز شكل جديد من القوة، هي القوة السيبرانية (Cyber power) التي توزعت وانتشرت بين عدد أكبر من الفاعلين على المستويين الدولي والمحلي؛ ما جعل الفضاء السيبراني مجالًا جديدًا للصراع بين الدول.

فلقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة؛ إذ تزداد المخاطر السيبرانية في أغلب الأحيان كلما زادت هيمنة تكنولوجيا المعلومات والخدمات والاتصالات على النسق العام للحياة، فأصبحنا أمام جرائم حقيقية ومتكاملة الأركان تتم عن طريق شبكات الإنترنت؛ كسرقة الأموال، والنصب والاحتيال، والتخطيط لعمليات إرهابية، وترويج الأخبار الكاذبة، وكذلك القرصنة بعدّها الجريمة الأكثر شيوعًا في العالم الرقمي.

فهناك صراع سيبراني تحركه دوافع سياسية، ويأخذ شكلًا عسكريًا، ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء السيبراني. ويوجد صراع سيبراني ذو طبيعة ناعمة، يدور حول الحصول على المعلومات والتأثير في المشاعر والأفكار، وشن حرب نفسية وإعلامية. كما يأخذ الصراع السيبراني طابعًا تنافسيًا حول الاستحواذ على سبق التقدم التكنولوجي، وسرقة الأسرار الاقتصادية والعلمية، والتحكم بالمعلومات، والعمل على اختراق الأمن القومي للدول؛ كهجمات قراصنة الكمبيوتر. كما يمكن أن يستخدم الفضاء السيبراني كوسيلة من وسائل الصراع داخل الدولة، وبين مكوناتها، على أساس طائفي أو اقتصادي أو ديني (إسماعيل ،2019 :1020-1021).

ففي الحروب التقليدية، كانت البندقية، والمدفع، والطائرة، والصاروخ، والعبوة الناسفة أدوات قتال. واليوم، دخلت أدوات جديدة إلى قوائم التسليح؛ مثل الحاسوب، ومواقع التواصل الاجتماعي، والحرب النفسية، والقوة الذكية، والقوة الناعمة. كما تغيرت طبيعة المحارب الفرد والقوة المقاتلة؛ فلم يعد المقاتل ذلك الجندي النظامي، أو رجل الميليشيا المدرب، ولكن بات أيضًا الطبيب، والمهندس في تقنية المعلومات، وعالم المختبر، ومدوِّن الإنترنت. كما أن الفئات المستهدفة تغيرت لتشمل البيوت، والمدارس، والفرق الرياضية، والعقل الجماعي، والذاكرة الوطنية، وماء الشرب، والهواء والغذاء، والمعاملات المصرفية، والطاقة.

إن تلك الحرب الجديدة أصبحت تتسم بشبكية غير مركزية، وليس لها ثقل مركزي واضح "غياب القيادة وتشتيت الفكر". وهذه التهديدات غير مفهومة الأبعاد، فهي لا تعترف بسيادة الدول، ولا تخضع لمبادئ القانون الدولي أو الإنساني، ولا تحكمها أي أخلاقيات. (ظهر هذا واضحًا في مبادئ الفوضى الخلاقة التي كان هدفها التدمير الذاتي) (Denise.2020:143-147).

وفيما يأتي العناصر الرئيسية لهذه الأفضلية:

1. صعوبة معرفة مصدر الهجمات (الطرف المعتدي)

على الرغم مما وصلت إليه التكنولوجيا من تقدم في عملية التتبع، فإنها تتقدم أيضًا في عمليات التمويه والإخفاء، بصورة تجعل معرفة مصدر الهجمة شبه مستحيلة، إلا في حالة الهجمات الصغيرة البسيطة التي يرتكب أصحابها أخطاء، وليس في حالة الهجمات المعقدة التي تقوم بها دول. فمثلًا، الهجمات الروسية على إستونيا عام 2007، والهجمات الأمريكية-الإسرائيلية على المفاعل النووي الإيراني عام 2010، والهجمات الكورية الشمالية على شركة

"سوني" عام 2015، والرد الأمريكي بقطع الإنترنت عن كوريا الشمالية لمدة 10 ساعات، والاتهامات الأمريكية بالتدخل الروسي في الانتخابات الرئاسية عام 2016، والهجمات الصينية المستمرة على الولايات المتحدة الأمريكية– جميع هذه الهجمات لم يتم تبنّيها صراحة من قِبل الدول المعتدية، بل إن بعضها أنكر القيام بذلك من الأساس. فهذه الاتهامات مبنية على الظروف السياسية المرتبطة على الصراعات القائمة بينها.

2. صعوبة وضع الخصم في تهديد حقيقي

إن الدول التي تتعرض لهجمات سيبرانية هي التي تستطيع أن تقدّر مدى فداحة هذه الهجمات والخسائر المترتبة عليها، ومن ثم فقد تشنّ دولة هجومًا إلكترونيًا انتقاميًا على دولة أخرى؛ بهدف تحقيق الردع بالانتقام، أو إصابة أهداف معينة داخل الدولة. لكن هذا الهجوم في تقدير الدولة المعتدَى عليها غير مؤثر. وفي هذه الحالة، يفشل تحقيق الردع.

وللتوضيح، فعندما شنّت كوريا الشمالية هجمات إلكترونية ضد شركة "سوني" للإنتاج السينمائي في الولايات المتحدة الأمريكية، على خلفية فيلم سينمائي أنتجته الشركة يسيء لرئيس كوريا الشمالية، وترتب عليها تسريب العديد من رسائل البريد الإلكتروني والأفلام الجديدة على الإنترنت، كان رد الولايات المتحدة الأمريكية أنها شنت هجمات إلكترونية على كوريا الشمالية، ترتب عليها قطع الإنترنت لمدة 10 ساعات تقريبًا.

3. صعوبة منع الهجمات الصفرية

يتميز الفضاء السيبراني بالتحديث التكنولوجي المستمر. فبصورة يومية، يتم اختراع وتطوير فيروسات في معامل خاصة، لم يتم الكشف عنها، ولم ترصدها شركات الأمن السيبراني، فبعضها يصيب المكون المادي، مثل "ستاكنت"، وبعضها – وهو كثير– يصيب الجانب البرامجي، وبعضها –وهو أيضا غير محدود– يركز على المعلومات؛ بهدف السرقة أو التضليل أو التدمير.

كما أن هذه الفيروسات تستغل الثغرات الحديثة التي تظهر في الأنظمة قبل أن يتم تحديثها ومعالجتها، فيما يعرف بالهجمات الصفرية. ومن ثم، قد تظهر الثغرة اليوم وتستغلها بعض الفواعل لشن هجمة إلكترونية، قبل أن يتم اكتشافها ومعالجتها من قِبل الأجهزة المختصة، ومن ثم يفشل تحقيق الردع بالمنع؛ بسبب ثغرات أمنية في أنظمة الدفاع أو فيروس

جديد تم تطويره (Tabansky,.2016: 107-114) .

4. حروب الإنترنت حروب لا تناظرية (Asymmetric)

إن التكلفة المتدنية نسبيًا للأجهزة اللازمة لشن حروب كهذه لا تماثل تكلفة تصنيع ترسانة أسلحة؛ مثل حاملات الطائرات ذات التكلفة العالية، لتنفذ تهديدًا خطيرًا ومؤثرًا على دول، حتى ولو كانت الولايات المتحدة.

5. تمتع المهاجم بأفضلية واضحة

تمتع المهاجم في حروب الإنترنت بأفضلية واضحة وكبيرة عن المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة.

6. فشل نماذج "الردع" المعروفة

يعد مفهوم الردع، الذي تم تطبيقه بشكل أساسي في الحرب الباردة، غير مُجدٍ في حرب الإنترنت. فالردع بالانتقام أو العقاب لا ينطبق على هذه الحروب بخلاف الحروب التقليدية؛ حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليه. ومن الصعوبة بمكان، بل من المستحيل، في كثير من الأحيان، تحديد الهجمات الإلكترونية ذات الزخم العالي. بعض الحالات قد تتطلب أشهرًا لرصدها، ما يلغي مفعول الردع بالانتقام. وكثير من الحالات لا يمكن تتبع مصدرها، وتبين أنها تعود إلى فاعلين غير حكوميين. في هذه الحالة، لم يكن لديهم أصول القواعد؛ حتى يتم الرد عليها.

7. المخاطر تتعدى استهداف المواقع العسكرية

لا ينحصر إطار الحرب السيبرانية في استهداف المواقع العسكرية، فهناك جهود متزايدة لاستهداف البنى التحتية المدنية والحساسة في البلدان المستهدفة، وهو أمرٌ أصبح واقعيًا في ظل القدرة على استهداف شبكات الكهرباء والطاقة، وشبكات النقل والنظام المالي، والمنشآت الحساسة النفطية، أو المائية، أو الصناعية، بواسطة فيروس يمكنه إحداث أضرار مادية واقعية تؤدي إلى انفجارات أو دمار هائل (المجال الخامس).

في هذا السياق، يستهدف الفضاء السيبراني ثلاثة مستويات مختلفة، هي:

1- المستوى الأول: يستهدف الفرد. وفق هذا المستوى، فإن أي فرد مذنب؛ حتى تثبت براءته (أنت جيش عدوك). في هذا المستوى، تكون أسرار الأشخاص غير محمية، وكذلك الأسماء والرموز التي تمارس بشكل اعتيادي، تصبح مجال متاجرة. بهذا الشكل وعند نشوب نزاع، لا

شيء يمنع الخصم من تهديد، عبر استهداف عائلاتهم، مستخدمًا محتويات الحواسب والمعلومات التي توفرها لتنفيذ اعتداءات.

2- المستوى الثاني: يشمل حرب المعلومات من خلال التجسس الصناعي والاقتصادي على الدول والمنظمات غير الحكومية، ملكية الفكرة وسباق التسلح. ووفقًا لمعلومات مكتب التحقيقات الفيدرالية الأمريكية، هناك (122) بلدًا تمارس تجسسًا مستمرًا على الولايات المتحدة في المجالين الصناعي والاقتصادي، وتقدر الخسائر الناجمة عن هذا الموضوع بـ(300) مليار دولار سنويًا.

3- المستوى الثالث والأخير: حرب معلومات موجهة من أمة ضد أمة، ويمكن أن يتضمن التجسس على المجموعات المنظمة في إطار الحكومات، أو التشكيلات "الإرهابية" التي تمتلك أدوات الحكومة نفسها. (مفاهيم عسكرية)

المحور الثاني

التحولات في مضامين القوة وظهور القوة السيبرانية

أصبح الفضاء السيبراني أحد العناصر الأساسية التي تؤثر في النظام الدولي، بما يتيحه من أدوات تكنولوجية مهمة لعمليات الحشد والتعبئة في العالم، فضلًا عن التأثير في القيم السياسية. فسهولة الاستخدام ورخص التكلفة زادا من قدرته على التأثير في مختلف مجالات الحياة، سواء السياسية، أو الاقتصادية، أو العسكرية، أو الاجتماعية، وحتى الأيديولوجية. وبات جليًا أن من يمتلك آليات توظيف البيئة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه، والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

ومن الأمور المتعارف عليها في العلاقات الدولية أن مصادر قدرة الدولة وأشكالها تتغير. فإلى جانب القوة الصلبة، ممثلة في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع. ومع ثورة المعلومات، ظهر شكل جديد من أشكال القوة، هو القوة السيبرانية (Cyber power)، التي لها تأثير كبير على المستويين الدولي والمحلي، من ناحية، بما أدى إلى توزيع وانتشار القوة بين تمدد أكبر من الفاعلين؛ ما جعل قدرة الدولة على السيطرة موضع شك. من ناحية أخرى، منحت هذه

القوة الفاعلين الدوليين من غير الدول قدرة أكبر على ممارسة كل من القوتين الصلبة والناعمة عبر الفضاء السيبراني، ما يعني تغيرًا في علاقات القوى في السياسة الدولية.

يُعد جوزيف س ناي (Joseph S. Nye) من أبرز المهتمين بالقوة السيبرانية، حيث يعرفها بأنها "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبرانى لإيجاد مزايا للدولة، والتأثير في الأحداث المتعلقة بالبيئات التشغيلية الأخرى، وذلك عبر أدوات سيبرانية". كما يوضح جوزيف س ناي أن القوة السيبرانية "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات، والشبكات الإلكترونية، والبنية التحتية المعلوماتية، والمهارات البشرية المدربة للتعامل مع هذه الوسائل". ويتناول مفهوم القوة السيبرانية مجمل القضايا التي تتعلق بالتفاعلات الدولية العسكرية، والاقتصادية، والسياسية، والثقافية، والإعلامية، وغيرها (Joseph,.2010 :3-10).

المحور الثالث

الحرب السيبرانية (الهجوم، الردع، الدفاع السيبراني)

برغم أن الحديث عن الحرب السيبرانية يعود لما يقرب من ربع قرن من الزمان، فإن المفهوم لا يزال يشهد حالة من الغموض وعدم الوضوح، بل وعدم اتفاق بين الأكاديميين أيضًا حول ما إذا كانت الحرب السيبرانية حقيقة أم لا، وهي حالة سببها الرئيسي التطور المتسارع في التقنيات الذكية، وتزايد الاعتماد على التكنولوجيا في الحياة اليومية، وضيق الفجوة بين التقنيات الميدانية العسكرية في الفضاء السيبراني؛ ما جعل ظاهرة الحرب السيبرانية يعاد تشكيلها بصورة مستمرة؛ الأمر الذي أدى إلى عدم صقل المفهوم، واتضاح جميع أبعاده بصورة كاملة على الأقل لدى المجتمع الأكاديمي؛ حتى أصبح لدينا مفهومان للحرب السيبرانية Cyber War & Cyber warfare.

حيث كان أول من تنبأ بالحرب السيبرانية J. Arquilla and D. Ronfeldt في مقالهما المنشور عام 1993 بعنوان cyberwar is coming حينما حذرا من أن الحرب السيبرانية قادمة، وعرّفاها بأنها "تنفيذ العمليات العسكرية، والاستعداد لتنفيذها وفقًا للمبادئ المعلوماتية، من

خلال تعطيل– إن لم يكن تدمير– نظم المعلومات والاتصالات على أوسع نطاق". ووسّع الكاتبان مفهوم الحرب السيبرانية ليشمل أيضًا أبعادًا غير مادية، تتمثل في "تدمير العقيدة العسكرية للعدو، التي يعتمد عليها لتحديد هويته وخططه وتصرفاته وأهدافه، والتحديات التي يواجهها" وذلك عبر معرفة كل شيء عن العدو، ومنعه في الوقت نفسه من معرفة أي شيء عن الطرف الآخر، وتحويل ميزان المعرفة ليكون في مصلحة هذا الطرف. ويعرّفها Joseph Nye بأنها "الأعمال العدائية في الفضاء السيبرانى التي لها آثار تعادل أو تفوق عنف الحركات التقليدية". فى حين يعرّفها Kenneth Geers بأنها "القدرة على الدفاع عن والهجوم على المعلومات، من خلال شبكات الحاسب الآلي عبر الفضاء السيبراني، بالإضافة إلى شل قدرة الخصم على القيام بهذه الهجمات نفسها". وتشمل الحرب السيبرانية عند جريس "خمسة عناصر رئيسية، هي التجسس، والدعاية، والحرمات من خدمة الإنترنت، وتعديل البيانات والتلاعب بها، والتلاعب أيضًا بالبنية الحيوية"(إيهاب,2019 :17).

كما يمكن تعريفها بأنها "إجراءات من قِبل الدولة القومية لاختراق أجهزة الكمبيوتر، أو شبكات دولة أخرى لأغراض التسبب في ضرر أو تعطيل". ولكن التعريفات الأخرى تشمل أيضًا الجهات الفاعلة غير الحكومية؛ مثل الجماعات الإرهابية، والشركات والجماعات السياسية، أو الأيديولوجية المتطرفة، والمخترقين الأفراد، والمنظمات الإجرامية العابرة للحدود (يحيى,2014 :228).

تكمن خطورة الحروب السيبرانية في كثرة اعتماد العالم على الفضاء السيبراني، لاسيما في البنى التحتية المعلوماتية. فلا شك في أن ازدياد الهجمات السيبرانية قد يصبح سلاحًا حاسمًا في الصراعات بين الدول في المستقبل.

ولذلك، فإن مظاهر الحرب السيبرانية قائمة ومستمرة، ولكن لها طبيعة خاصة من حيث الفاعلون فيها، وميدان المعركة، ونوعية الخسائر وتوقيت المعركة. كما أنها لا تفرّق بين هدف مدني أو عسكري، ما يهدد الأمن الإنساني للأفراد. أما ميدان المعركة، فهو بيئة مصنوعة، وليست طبيعية، فليس لها من يحكمها.

قد لا يستطيع القانون الدولي أن يحكم التفاعلية التي تجري فيها، ليس فقط لغياب مفهوم السيادة فيها، ولكن لصعوبة معرفة الفاعل الحقيقي الذي شنّ هذه الحرب. والخسائر فيها قد تكون

مباشرة، تتمثل في تدمير البيانات، والبنى التحتية، والمعدات العسكرية. وقد تكون غير مباشرة تتمثل في تراجع التنافسية الاقتصادية للدولة، وفقدان الثقة بالاقتصاد القومي. وقد فرض ذلك العديد من التحديات على المفهوم بصورته التقليدية (Muhamma, 2021 :1-2).

يمكن التمييز بين ثلاث صور رئيسية لعمليات الحرب السيبرانية، هي:

1. هجمات شبكات الحاسب الآلي: عن طريق اختراق الشبكات وتغذيتها بمعلومات محرفة لإرباك مستخدمي الشبكات، أو من خلال نشر الفيروسات بهدف تعطيل الشبكة.
2. الدفاعات عن شبكات الحاسب الآلي: عبر تأمينها من خلال إجراءات معينة، يقوم بها "حراس الشبكات" من خلال برامج وتطبيقات تقوم بأعمال المراقبة للزائرين غير المرغوبين (الهاكرز).
3. استطلاع شبكات الحاسب الآلي: يعني القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، بهدف الحصول على البيانات دون تدميرها، التي قد تشتمل على أسرار عسكرية ومعلومات استخباراتية (أهمية,2020 :17-30).

الهجوم السيبراني

تتعدد أهداف الهجمات السيبرانية لتشمل: "التجسس السيبرانى"، وإغلاق النظم المعلوماتية، واستهداف أنظمة معلومات الخصم، سواء المدنية أو العسكرية. ويمكن أن تشمل أيضًا التلاعب بأنظمة توجيه الأسلحة التي قد تتسبب في إطلاق النار بعيدًا عن الأهداف المستهدفة، التي قد تشمل: البنية التحتية الحيوية المدنية؛ كشبكة الكهرباء، وأسواق الأوراق المالية، وقواعد البيانات المالية، وخطوط تنقية المياه، وغيرها.

ويشكل كل ذلك خطرًا شديدًا على الدول القومية، سواء على اقتصاداتها، أو بنيتها التحتية الحيوية، أو أنظمتها السرية التي تعتمد على نظم المعلومات. كما يؤثر ذلك سلبًا في القدرات العسكرية للدول، خاصة أن الهجمات السيبرانية من شأنها أن تقوم بجمع وتحليل معلومات استخبارية موثوق بها عنها. ولذا، فإن ردع تلك الهجمات لا بد أن يكون من أولويات الردع السيبراني (رغدة البهي).

تتطلب دراسة الردع السيبراني التعرض إلى أنواع الهجمات السيبرانية لتحليل طبيعة ما يمكن ردعه منها. فيمكن للهجمات السيبرانية أن تتسبب في دمار هائل يطول الأمن القومي للدول،

ويمكنها أيضًا أن تستهدف القيادة السياسية، والأنظمة العسكرية، والمواطنين العزل (Kenneth,2010 :298-303) خاصة أنها تشمل مجموعات كاملة من الأساليب والأدوات التي يمكنها التأثير في الفضاء السيبراني (Dorothy,2015:8-15).

يمكن تعريف الهجمات السيبرانية بأنها "فعل يُقوّض قدرات وظائف شبكة الكمبيوتر، لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف ما تُمكّن المهاجم من التلاعب بالنظام" . (MAJ..2016 :13-22). فهدف أنظمة المعلومات هو إتاحة المعلومات وضمان سلامتها. ولذا، تهدف الهجمات السيبرانية – على العكس من ذلك – إلى سرقة المعلومات، أو انتهاك سريتها، أو تعديلها، أو منع الوصول إليها. ولعل أبرز أنواع الهجمات ما يأتي:

1. الهجمات السرية

تعد أحد أنواع التجسس التقليدي باستخدام وسائل التكنولوجيا الفائقة. ولعل معظم الهجمات السيبرانية المتطورة، التي أطلقت من قِبل الدول القومية أو الجماعات الإجرامية، تقع ضمن هذه الفئة.

2. هجمات النزاهة على البيانات Integrity Attacks

تصمم بعض الهجمات لتحقيق ميزة تكتيكية أو استراتيجية عن طريق تخريب نظم المعلوماتية للخصم، سواء المدنية أو العسكرية المهمة. فيمكن أن ينطوي التخريب على التلاعب بالبيانات داخل نظم المعلومات، التي يمكن أن تشوّه وعي العدو عن طريق نشر معلومات خاطئة داخل أنظمة ذكائه، أو إخفاء أنشطة محددة قد تكون تحت سيطرة المراقب.

3. الهجمات المتاحة للسيطرة Availability Attacks

هي تلك التي تسعى لإغلاق نظم المعلومـــات To Bring Information System Offline وتكمن خطورة الهجمات الطويلة المدى منها فيما تسببه من أضرار مدمرة على الاقتصاد، بتأثيرها في شبكة الاتصالات أو الكهرباء، على سبيل المثال. أما الهجمات القصيرة المدى التي تستهدف جمع المعلومات الاستخبارية، فيمكن أن تحجب قدرة الدولة على رؤية التهديد السيبراني التقليدي أو الواسع النطاق، من خلال منع المدافعين من الوصول إلى البيانات أو المصادر الاستخباراتية الحيوية. وهكذا، يمكن أن تشكل تلك التهديدات خطرًا على الأمن القومي. (Dmitri,2011:89-90)

4. الهجمات على العمليات الحكومية المدنية والعسكرية

تتعرض الأنظمة الحكومية والعسكرية لهجمات يومية في جزء من عمليات التجسس. وتمارس دول عدة هذه العمليات التي تهدف إلى سرقة تصاميم أنظمة الأسلحة أو الحصول على المعلومات المفيدة بسرقة مخططات المعارك، أو فهم طرق الشبكات، وحرمان جيوش العدو من استخدامها في أثناء الحرب. ويعدّ أي نظام متصل بالإنترنت عرضة للهجوم. لذا، قد تجد الحكومات والجيوش التي تعتمد في القيام بوظائفها الرئيسية على هذه الأنظمة أنها غير متوافرة، أو لا يمكن الاعتماد عليها عندما تكون في أشد الحاجة إليها. وبالتالي، فإن ميزة الشبكة العسكرية المتفوقة التي يتمتع بها جيش يتسلح بالتقنية الحديثة قد تزول تمامًا بفعل الهجمات السيبرانية.

5. الهجمات على البنية التحتية

لا يجوز إطلاقًا الاستهانة بالتدمير والخسائر المحتملة التي يتكبدها البلد، خلال هجمات على المؤسسات الحيوية المدنية والعسكرية، من الشلل الذي قد يصيبه؛ من جراء انقطاع خدمات الإنترنت عنه، في ظل تزايد استخدام أنظمة التحكم الصناعي للإنترنت من بعد. فأصبح بإمكان العابثين الإلكترونيين السيطرة والتحكم عن بعد بوظائف البنية التحتية للدولة؛ ما يسبب ضررًا وإرباكًا ليس للدولة فقط، بل على المستويين الإقليمي والعالمي (Richard .2011).

6. الحرمان من الخدمة

هو الهجوم الذي يرمي إلى إيقاف قدرة الهدف على تقديم الخدمات المعتادة، عن طريق إغراق جهاز الحاسب الآلي بأعداد كبيرة من الأوامر، تؤدى إلى توقفه عن العمل لتقديم الخدمة لمستخدمها. وقد ينتج عن هذه الهجمات أيضًا إيقاف الاتصال بين الأجهزة الأخرى أو نظام معين، مثلما شهدته دولة إستونيا عام 2007 عندما تعرضت لعدد كبير من هجمات الحرمان من الخدمة، التي استهدفت البنية التحتية، والمواقع الإلكترونية الخاصة برئيس الوزراء، والبرلمان والبنوك. وجاءت هذه الهجمة في ظل الاضطرابات مع روسيا. وفي أغسطس عام 2008، اندلع نزاع مصالح بين جورجيا وروسيا. وتعرضت جورجيا، بالتزامن مع الهجمات العسكرية، إلى هجمات الحرمان من الخدمة، التي استهدفت الموقع الخاص بالرئيس الجورجي، وطالت عددًا كبيرًا من الوزارات والمواقع الإخبارية. وفي أبريل عام 2001، حدث توتر في العلاقات الأمريكية– الصينية؛ نتيجة إرسال الولايات المتحدة طائرة تجسس على الساحل الجنوبي للصين، ردت عليه بكين بإرسال طائرة

حربية اصطدمت بالطائرة الأمريكية؛ ما أدى لهبوط الأخيرة. في ظل هذه الأحداث، تعرضت المواقع الإلكترونية الخاصة بالجيش الأمريكي لهجمات الحرمان من الخدمة من قِبل جماعات صينية عدة، كان من بينها جماعة أطلق عليها Honker Union (أهمية، 2020 :25-30).

مزايا الهجمات السيبرانية

يتزايد يومًا بعد يوم شكل الهجمات السيبرانية بصورة سريعة متطورة، فقد تكون مرة عبر أجهزة الحاسب، ومرة أخرى عبر إنترنت الأشياء، ومرة ثالثة عبر أجهزة الهواتف المحمولة. ومستقبلًا، قد يكون عبر نظم الذكاء الاصطناعي والروبوت، بحيث يستهدف في إحداها الأموال، وفى مرة أخرى الاعتراض السياسي أو الإرهاب. وبسبب هذا التنوع والانتشار بين المستهدفين من الهجمات، أفرادًا كانوا أو مؤسسات، أصبحت الهجمات ذات ميزة تفوقية لهذه الأسباب:

1- ضيق الفجوة الزمنية بين الهجمات الكبرى

يكون الفارق الزمني بين هجمة سيبرانية، وغيرها، قصيرًا جدًا، فيمكن أن نشهد هجمات كبرى عدة خلال عام واحد. فما يكاد العالم يخرج من تداعيات هجمة، حتى تظهر له غيرها، مختلفة في الآلية والنطاق والأهداف.

2- الاعتماد على العملات الافتراضية

في هذا الجيل، تصبح "العملات الافتراضية؛ مثل "البيتكوين"، أساس الهجمات، وذلك لأنها صعبة التعقب، وليست لها إدارة مركزية. ومع ذلك، يمكن البيع والشراء من خلالها، أو حتى تحويلها إلى عملات تقليدية من خلال ماكينات الصراف الآلي المنتشرة في دول متعددة، فتصبح العملة الرسمية للهجمات السيبرانية.

3- زيادة درجة تعقيد الهجمة وتداعياتها

تكون الهجمات معقدة في طريقة تنفيذها، ويصعب تعقبها أو معرفة مصدرها. فقد يشارك فيها عدد كبير من الفاعلين الدوليين، وتُستخدم أجهزة غير متوقعة في عملية الهجوم؛ مثل الطائرات بدون طيار (المسيّرات) من أجل التضليل، وتكون تداعياتها لا تتحمل مستوى الأفراد أو الدول.

4- مشاركة غير الفنيين

تم تطوير عدد من برامج القرصنة الإلكترونية التي لا تحتاج إلى مطورين ومختصين

لاستخدامها، بل يمكن شراؤها واستخدامها بصورة سهلة؛ ما يفتح الباب لقطاع كبير من غير المختصين للمشاركة في هذا النوع من الهجمات (إيهاب.2019 :126-127) .

ويعني ذلك تعدد أشكال الهجمات السيبرانية، ومصادرها، وآلياتها، فلا يمكن الوقوف على مرتكبيها على نحوٍ دقيق. وقد تشمل الأفراد، والقراصنة، والجماعات، والتنظيمات الإرهابية، والدول، وغيرها، الأمر الذي يتعذر معه حصر الهجمات السيبرانية كافة بشكل كامل، ومنها يصعب معالجتها أو ردعها (رغدة البهي).

آثار الهجمات السيبرانية وخطورتها

تختلف تهديدات الهجمات السيبرانية من حيث أشكالها، ومصادرها، ودرجة خطورتها، وتتراوح بين تهديدات بسيطة ومتوسطة ومعقدة.

فالتهديدات البسيطة تتمثل في تلك الهجمات التي يستطيع أي فرد يمتلك قدرات تحليلية وتقنية بدائية القيام بها عن طريق تحديد نقاط الضعف التي يمكن مهاجمتها، حيث يستطيع أي فرد أن يقوم بتحميل البرامج الخاصة بالقرصنة من الإنترنت دون الحاجة إلى وجود موارد خاصة، أو هياكل مؤسسية للقيام بالهجوم.

والتهديدات المتوسطة هي تهديدات أكثر تقدمًا، حيث يمتلك المهاجم معرفة واسعة بالهدف وأنظمة الأمان التي يطبقها، والأنظمة المشغلة للأجهزة الإلكترونية الخاصة به.

أما التهديدات المعقدة، فلا يقوم بها فرد أو مجموعة صغيرة من الخبراء، وإنما يتطلب الأمر مجموعات كبيرة، تمتلك قدرات معرفة بمختلف الجوانب التقنية بجميع الشبكات وأنظمة التشغيل والتحكم، وكيفية جمع المعلومات الاستخباراتية وتحليلها؛ ما يمثل الخطر الأكبر على الأمن القومي للدولة.

الردع السيبراني

يُعرّف الردع السيبراني بأنه "قدرة الدولة علي تطوير قدرات عسكرية موثوق بها ومتبادلة ومتماثلة في الفضاء السيبراني، وتكون قادرة على التأثير في قرارات الخصم ومنعه من شن هجمات عسكرية عبر الفضاء السيبراني". إن هناك صعوبات عديدة تعترض إمكانية تحقيق الردع الكامل في المجال السيبراني؛ نظرًا لصعوبة معرفة مصدر الهجمات بدقة، وصعوبة وضع الخصم في تهديد

حقيقي يردعه، وصعوبة منع الهجمات الصفرية، وعدم وجود أطر قانونية تنظم استخدام القوة السيبرانية في العلاقات الدولية". (Martin,2009:7) ورغم إمكانية تعريف المفهوم، وتحديد ركائز على المستوى النظري، فإن هذا التعريف لا يحظى بإجماع الدول على المستوى العلمي. والمثال على ذلك هو الولايات المتحدة والصين. ففي الوقت الذي تفضل فيه الولايات المتحدة استخدام مصطلح الأمن السيبرانى Cyber Securityللتركيز على التكنولوجيات والشبكات والأجهزة الآلية، تفضل دول، مثل الصين وروسيا، استخدام مصطلح أوسع، ألا وهو "أمن المعلومات" Security Information، ليشمل المعلومات التي تمر عبر الشبكات، وكذلك التقنيات المعلوماتية. ودون معجم مشترك، سيستمر الخلاف بشأن كيفية استخدام الإنترنت، وسياسات الردع وطبيعة الهجمات الواجب ردعها (رغدة البهي).

وبعيدًا عن جدال المفهوم، فإن إشكالية الردع السيبرانى، الذي يأتي ضمن مميزات الفضاء السيبراني، هي صعوبة إسناد الهجوم السيبراني إلى مرتكبيها، ويرجع هذا إلى استخدام الفاعلين الدوليين، أينما كانوا، تقنيات التشويش المتقدمة المتعددة الأشكال لتجنيب الكشف عن هوياتهم، (رغدة البهي). كما أنه من الصعب وضع الخصم في تهديد حقيقي، ويعود هذا إلى إنكار معظم الفاعلين الدوليين الاتهامات الموجهة إليهم، فالجميع يتهم، والجميع ينكر الفضاء السيبراني.

الدفاع السيبرانى

يقصد بالدفاع السيبرانى "مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثيرات الهجمات السيبرانية، والتخفيف من حدتها، والتعافي منها بسرعة. وقد عرّفت العقيد الفرنسية الدفاع الإلكتروني بأنه "مجموعة الوسائل الفنية وغير الفنية التي تُمنح لدولة بالدفاع في الفضاء السيبراني عن نظم المعلومات الحرجة".

وفي الاستراتيجية النمساوية، يشير مصطلح الدفاع السيبراني إلى "جميع التدابير اللازمة للدفاع عن الفضاء السيبراني بالوسائل المناسبة لتحقيق الأهداف العسكرية الاستراتيجية". ويعرفه البرلمان الأوروبي بأنه "عملية تطبيق الإجراءات الأمنية من أجل الحماية من الهجمات السيبرانية، والتعامل معها، بما يستهدف تأمين البنية التحتية لنظم الاتصالات والسيطرة" (إيهاب,2019 :6).

المحور الرابع

الإرهاب السيبراني

يمثل الإرهاب السيبراني خطرًا على الأمن القومي والعالمي في ظل مجتمع ما بعد المعلومات، من خلال توظيف التقنيات الذكية في تنفيذ عمليات إرهابية سيبرانية، سواء عبر هجمات سيبرانية فى الفضاء السيبراني، أو استخدام الروبوت والمسيّرات في شن عمليات إرهابية، أو استخدام الطابعات الثلاثية الأبعاد في تصنيع الأسلحة (إيهاب,2019 :141).

1-التقنيات الذكية والإرهاب السيبراني

تسعى الحركات الإرهابية دائمًا إلى توظيف جميع التقنيات الذكية والتطورات التكنولوجية لتحقيق أهدافها، وتسخيرها لنشر أفكارها التقليدية بصورة متطورة وذكية تتلاءم مع مستجدات العصر، فانتقلت "الدعوة" من مرحلة شرائط الكاسيت والفيديو إلى مواقع التواصل الاجتماعي، وتطبيقات الهواتف الذكية، مرورًا بالمنتديات والمدونات الإلكترونية. وأصبح "التجنيد" يتم من خلال غرف الدردشة وألعاب الفيديو، بعد أن كان مقتصرًا على "الزوايا" والمجالس الخاصة. وتطورت "الهجمات الإرهابية" من الحزام الناسف والدرّاجات النارية المفخخة إلى الهجمات السيبرانية، والدرونز المسيّرة، وتحولت من صناعة الأسلحة، بطرق بدائية ويدوية، إلى إمكانية صناعتها عبر استخدام الطابعات الثلاثية الأبعاد، فأصبحت التكنولوجيا من أبرز أسلحة الحركات الإرهابية لتحقيق أهدافها الدعائية والعسكرية.

وقد أسهمت هذه التطورات التكنولوجية في ظهور أنماط جديدة من الإرهاب لم تكن موجودة من قبل، منها نمط الذئاب المنفردة LONE WOLVES، وهو ذلك الإرهابي الذي يعتنق الفكر المتطرف دون أن يرتبط تنظيميًا بجماعة إرهابية، فيأخذ أفكارها المتشددة من خلال مواقع الإنترنت، ويقوم بصناعة الأسلحة من خلال الفيديوهات التعليمية الموجودة على صفحات التواصل الاجتماعي، ثم ينطلق منفردًا لتنفيذ مخططه الإرهابي.

وإلى جوار "الخلايا" التقليدية، ظهرت خلايا إرهابية "سيبرانية"، تنشط فقط على مواقع الإنترنت، ولا تقل مهمتها أهمية عن الخلايا التقليدية، فمنها التي تقوم بعمليات الدعوة والتجنيد وجمع التمويل عبر الإنترنت، ومنها مَن تقوم باختراق المواقع الإلكترونية وصفحات التواصل

الاجتماعي للضحايا للتأثير فيها معنويًا، ومنها مَن تقوم بشن هجمات إلكترونية على بنوك ومؤسسات مالية؛ بهدف السرقة والحصول على المال، أو على مؤسسات سياسية وعسكرية لجمع معلومات استخباراتية لتنفيذ العمليات الإرهابية، أو تسريب وثائق ومعلومات استراتيجية، فضلًا عن استهداف خدمات الحكومات الإلكترونية الذكية عبر الإنترنت، ووقفها، أو استهداف البنية التحتية للدولة، وأنظمتها المالية والمصرفية والاتصالية والعسكرية، وغيرها.

الطائرات بدون طيار (المسيّرات) DRONES

تعد الطائرات بدون طيار (DRONES) "المدنية"، والمخصصة للأغراض التجارية والترفيهية، سلاحًا ذا حدين. فكما يمكن أن تستخدم في توصيل الطلبات أو التصوير الفوتوغرافي، يمكن أيضًا استخدامها في تنفيذ هجمات إرهابية، حيث تستطيع المسيّرات أن تحمل سلاحًا موجهًا، أو قنبلة، أو عبوة ناسفة، وتفجّرها على الهدف المطلوب، أو أن تستخدمها في عمليات المراقبة والاستطلاع. فالوسيلة واحدة، والاستخدام واحد، ويتبقى فقط الهدف من الاستخدام، سواء حمل طرد توصيل أو قنبلة.

العملات الافتراضية

أصبحت العملات الافتراضية "مثل البيتكوين" العملة الرئيسية لجميع الأنشطة الإجرامية، لما لها من قدرات تشفيرية عالية، كما أنها لا تتطلب البيانات الشخصية للمستخدم. فأي مالك لعملة البيتكوين هو مجرد "رق" يمثل المحفظة المالية التي سيتم تحويل النقود منها وإليها، وبالتالي فهي توفر خاصية التخفي وعدم التعقب (إيهاب,2019 :141).

الطابعات الثلاثية الأبعاد

طبقًا لتصريحات "مارك رولى "، رئيس شرطة لندن، فإن الإرهابيين من الممكن أن يستخدموا تلك التقنية في طباعة "طائرات من دون طيار " أو في صناعة القنابل أو بنادق ورصاص. ولما كانت المواد المستخدمة في تلك المواد من الصعب اكتشافها بواسطة الأجهزة الأمنية، فإن ذلك يعد مهددًا كبيرًا وتطورًا خطيرًا فيما يتعلق بالأنشطة الإرهابية، حيث يمكن للجماعات المتطرفة استخدامها في تنفيذ عملياتها الإرهابية، سواء في تصنيع المتفجرات أو تهريبها عبر المطارات (Sarah.2017).

دوافع اللجوء إلى الإرهاب السيبرانى

تم تعريف الإرهاب السيبراني بأنه "التقاء الفضاء السيبراني والإرهاب في ساحة واحدة، حيث تنفذ الهجمات غير القانونية والتهديدات بالهجوم على أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيه؛ لتخويف أو إكراه حكومة أو شعبها؛ من أجل تحقيق أهداف سياسية أو اجتماعية. ولكي يعد ذلك إرهابًا، يجب أن يؤدي إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل التسبب في ضرر كاف لتوليد الخوف" (Fema,2002:2).

وبناء عليه، فإن هذا التعريف لا يتضمن استخدام الجماعات الإرهابية للإنترنت في عمليات الدعاية، وجمع المعلومات التي تسهم في التحضير للهجمات الإرهابية، ونشر المواد التدريبية، والتواصل، والتجنيد، والتمويل.

أما التعريفات الواسعة، فمنها تعريف "برينر" بأنه يشمل أي استخدام لتكنولوجيا المعلومات والاتصالات وأجهزة الكمبيوتر للانخراط في نشاط إرهابي (Susan: 457, 2006)، وهو تعريف يشمل في طياته أشكال الإرهاب كافة في ظل الاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات في مناحي الحياة كافة.

مميزات الإرهاب السيبرانى

- النتائج: يهدف لإحداث أضرار مادية ملموسة، وإلحاق خسائر جسيمة، سواء في الأرواح البشرية، أو الممتلكات أو البنية التحتية الحيوية، علمًا بأن الهدف المباشر هو إحداث تلك الحالة من الترويع والهلع.
- الإسقاط النفسي للخوف والترهيب: هو السمة الأخيرة للإرهاب السيبرانى، وهو الوسيلة التي يعتمد عليها الإرهابيون في نشر أفكارهم ومعتقداتهم بين قطاعات واسعة من الجماهير.
- تعدد الثغرات: حيث إن العنصر الأساسي في التطور التكنولوجي هو التحديث المستمر. ومن ثم، فإن الجهة القادرة على إحداث ذلك التطور يمكنها اكتشاف الثغرات في النظم الموجودة، وهو ما تعتمد عليه المنظمات الإرهابية؛ حيث تعمد إلى استغلال تلك الثغرات، وإحداث الاختراق أو الهجوم من خلالها.
- استغلال عنصر التعقد التكنولوجي: إثارة حالة من الخوف لدى العامة بإظهار القدرات في

التحكم التكنولوجي، الذي يرتبط في أذهان العامة بالعملية المعقدة؛ ما يضيف أبعادًا أكثر تعقيدًا؛ نتيجة لسيادة الاعتقاد بأن من يتحكم في التكنولوجيا تكون له اليد العليا في تغيير مجريات الأمور، وهو ما يتوافق مع تحقيق الأهداف الإرهابية في إثارة الخوف والهلع من خلال دمج هذين المصدرين للخوف من الإرهاب والتكنولوجيا (FEMA: 2002, 4).

- صعوبة تحديد هوية الإرهابيين السيبرانيين: حيث تتيح التقنيات المتطورة للشبكات المعلوماتية عدم الكشف عن هوية القائمين بالهجمات الإرهابية السيبرانية، الأمر الذي يعتمد في الأغلب على مجرد التخمينات، ومحاولة الربط بين الأحداث دون وجود دليل قاطع؛ حيث تظل الحدود الجغرافية أو ملامح الجهات الفاعلة غير واضحة في الفضاء السيبرانى؛ ما يتيح للمهاجم تجنب اكتشافه، والقبض عليه. هنا، يمكن إضافة بُعد آخر يرتبط بانعكاس ذلك على تعقد الصعوبة التي تنطوي عليها عمليات تنفيذ قوانين الإرهاب السيبرانى.
- جذب الانتباه: حيث توفر الشبكات المعلوماتية من خلال تعاظم درجة الاعتماد عليها، وتزايد أعداد المستخدمين، فرصة واسعة أمام الجماعات الإرهابية لتأكيد هويتها ونشاطها، ومحاولة جذب الانتباه للقضايا التي تعبر عنها، خصوصًا أن الإرهاب تتم ممارسته في الأغلب من جانب جماعات يبرز لديها الجانب العقائدي. هنا، من المرجح أن تكتسب العمليات الإرهابية السيبرانية تغطية إعلامية واسعة، فضلًا عن اهتمام الحكومة والجمهور بها.
- انخفاض التكلفة وسهولة التنفيذ: حيث أسهمت الممارسات المتواترة للهجمات السيبرانية في نشوء سوق سوداء أكثر تطورًا للأسلحة السيبرانية. وحيث تتعاظم الآثار المدمرة لها، فإن تكلفتها في تناقص مستمر، حيث تتوافر مجموعة واسعة من البرامج السهلة الاستخدام والمتاحة عبر آلاف المواقع على شبكة الإنترنت، بالإضافة إلى انضمام أجيال جديدة من القراصنة ذوي القدرات التقنية العالية إلى الجماعات الإرهابية، أو تجنيدهم ليصبحوا إرهابيين سيبرانيين يعملون لمصلحتهم بمقابل مادي.
- محدودية الخسائر بالنسبة للإرهابي: حيث لا يترتب، في الأغلب، على الإرهاب السيبراني خسائر بشرية أو مادية تذكر من جانب العناصر الإرهابية، فهو لا يتطلب التعامل مع المتفجرات أو المواد الكيميائية الحيوية أو القيام بمهمة انتحارية.

نتيجة لما سبق، يعد الإرهاب السيبرانى من أخطر أشكال الجرائم السيبرانية، حيث قد تؤدي

أهدافه وآثاره إلى تدمير البنية التحتية للدول دون وجود سبب مباشر أو فرصة للمساومة (Michael,2015).

مثال على ذلك ما حدث في أبريل 2015 بفرنسا، حيث قام متسللون يزعمون انتماءهم لداعش باختراق شبكة التليفزيون العامة الفرنسية، وقطع البث التليفزيوني، وكذلك اختراق الموقع الإلكتروني الخاص بالقناة وحسابات الوسائط الاجتماعية، ونشر صور مؤيدة لداعش؛ بغرض ترويع الفرنسيين بتمكنهم من اختراق شبكة التليفزيون الرسمية الخاصة بهم (محمد.2016).

المحور الخامس

الوكالة السيبرانية

للحرب أشكال وتقنيات متعددة، فهي" تقليدية"؛ حيث تستعمل فيها معدات القتال، عدا أسلحة الدمار الشامل. أما "غير التقليدية"، فقد استُحدثت في العصر الحديث، وعلى مستويات أخرى، منها الحروب الاقتصادية، والنفسية، والسياسية، والإعلامية. وقد تستغرق الحرب أيامًا قليلة، أو تدوم لسنوات عديدة. وتبذل الدول عادة ما في وسعها لتقصير أمد الحرب؛ لما يترتب عليها من معاناة وخسائر مادية وبشرية.

لهذا، تسعى الدول إلى إيجاد أشكال من الحروب تجنّبها المساءلة القانونية والإنسانية والتكلفة المادية على المستويين المحلي والدولي. وفي الوقت نفسه، تحقق لها أهدافها الاستراتيجية داخل النظام العالمي والإقليمي؛ وهذا ما تستهدفه الحروب بالوكالة.

شهد مصطلح "الحرب بالوكالة" شعبية جديدة في بؤر الصراعات الدولية، على الرغم من أن أول حرب بالوكالة تم تسجيلها عام 1953م، إلا أنه لم يكن بالمصطلح الشائع، حتى اندلعت الحرب الباردة بسبب الاختلافات الأيديولوجية والسياسية بين المنتصرين من الحرب العالمية الثانية؛ حيث إن القوتين العظميين المسلحتين بالنووي لم ترغبا في المواجهات المباشرة التي قد تؤدي إلى حرب نووية مدمرة، وإنما سارعتا إلى نشر نفوذهما الخاص في جميع أنحاء العالم Proxy (war,2016).

تشكل الحرب بالوكالة شكلًا من أشكال الصراع لردع الدول المتنافسة عن امتلاك موارد استراتيجية خاصة بها. ويعتمد هذا الجزء على حساب نسبة المخاطر السياسية والرغبة في تعظيم

المصلحة الوطنية، وعلى قدرة قوة الخصم في الاستجابة. ويتبنى هذا المنهاج "خط المقاومة الأقل بالمعنى المادي" وخط التوقع الأقل "بالمعنى النفسي"، عن طريق إضعاف العدو بواسطة الكدمات عن الضربات، خاصة عندما ترى الدول المستهدفة قدرتها العسكرية الضعيفة، مع رؤية قادة هذه الدول أن استنزاف العدو في التصدي لأفعال الطرف الموكل أكبر من التكلفة نفسها.

وتأتى أشكال التدخل بالوكالة إما بطرق مباشرة أو غير مباشرة، بواسطة دولة أو مجموعة دول (أ) في الدولة (ب) للقيام بالأعمال التخريبية نيابة عنها. ويأتي تدخل الوكلاء بناء على إدراك المخاطر في التدخل المباشر في أي نزاع، مبررًا كان أو غير مبرر، مع حساب تكلفة التدخل، سواء كان سياسيًا أو ماديًا أو قانونيًا. ولهذا، فكل وكيل يقدم مصلحته الوطنية كهدف رئيسي، وهذا ما تحدده العلاقة بين الممول والوكيل (Andrew, 2013).

دوافع اللجوء إلى الحروب بالوكالة

ترجع أهداف اللجوء للحروب بالوكالة إلى:

1. تجنب الدول الكبرى المواجهات المباشرة؛ بسبب عدم تحملها تكاليف هذه المواجهات. وفي الوقت نفسه، لا تتنازل عن أهدافها لتأمين مصلحتها الوطنية.
2. ظهور مجموعة جديدة من الفاعلين الدوليين في المشهد السياسي الدولي (الشركات العسكرية الخاصة، والاهتمام بها في الحروب الحديثة، قراصنة الإنترنت...). هؤلاء المحاربون الجدد تستوعبهم الدول في مرحلة يتضاءل فيها التجنيد العسكري الوطني، وتتقلص فيها ميزانية الدفاع.
3. النتيجة الحتمية للحرب على الإرهاب التي تتبناها أمريكا، بعد أحداث 11 سبتمبر 2001 لشن حروب لتغيير نظم داخل الدول، هي الاتجاه للحروب بالوكالة لتحقيق أهدافها، ولتقليل المواجهة السياسية والعسكرية.
4. العنصر النفسي يأتي عن طريق حساب وتحليل المخاطر القابلة للتطبيق وكيفية اتخاذ القرار؛ من أجل الحصول على مكاسب أكبر باستخدام وسائل الحروب الحديثة، ومنها دعم عدو عدوي وتسليحه (Andrew. 2017).
5. اتجاه دول الغرب لخصخصة السلع والخدمات، بما فيها الشؤون العسكرية. فالاعتماد الأكبر

من جانب الدول على الشركات العسكرية الأمنية الخاصة سمة مميزة للسياسة الأمنية المعاصرة في الغرب، إذ تتعدد مهام هذه الشركات من شراء الأسلحة والتدريب وجمع المعلومات الاستخبارية وحماية الشخصيات*.

6. تعد الحرب السيبرانية إحدى آليات إخفاء هوية الممولين، خاصة لاعتماد المجتمع المعاصر على الفضاء السيبراني، حيث يصعب التوصل إلى أصل الهجمات السيبرانية. فهذه الآلية من الحرب بالوكالة أبطلت الاعتقاد السائد في القرن العشرين بمبدأ "القوات في الميدان" كضرورة للحروب بالوكالة، حيث يمكن لأجهزة الكمبيوتر الآن إحداث ضرر في البنية التحتية لدولة أجنبية من النوع الذي لا تستطيع الجيوش البديلة القيام به؛ مثل (فيروس ستوكسنت العالمي) Stuxnet الذي صممه الأمريكيون والإسرائيليون لوقف تخصيب اليورانيوم في منشأة إيران النووية عام (2010).

تبرز الحروب بالوكالة في عملياتها داخل الدولة التي تسعى لانهيار سلطة الدولة المركزية (إسقاط نظام) عن طريق تشتيت وسائل العنف بين السكان، أو عن طريق الميليشيات والشركات العسكرية والأمنية الخاصة التابعة للمُمَول (Alex,2016:190).

الوكالة السيبرانية

لم تعد الجيوش العسكرية الضخمة أحد متطلبات حروب الوكالة، بعد أن قوضت التطورات، على صعيد الاتصالات وتكنولوجيا المعلومات، حتمية وضرورة الوجود على الأرض للقوى كأحد متطلبات تلك الحروب، إذ يمكن لأجهزة الكمبيوتر أن تُحدث أضرارًا في البنى التحتية للدول على نحو تعجز الجيوش العسكرية عن إحداثه. وبالتالي، فمن المحتمل أن يشهد القرن الحادي والعشرون حروبًا بالوكالة من قِبل خوادم (Proxy Servers) لا قوات (Proxy Forces). يدلل على ذلك التقرير الصادر عن وزارة الدفاع البريطانية في عام 2010 بعنوان "الطابع المستقبلي للصراع"، الذي ذكر فيه أن خصوم المستقبل هم الدول والفاعلون من غير الدول والوكلاء، وهو ما أوعزه إلى تغيرات رئيسية عدة في طبيعة الحرب الحديثة، منها تصاعد أهمية الشركات العسكرية الخاصة، والاستخدام المتزايد للفضاء السيبراني كمنصة لشن الحروب بشكل غير مباشر، وغير ذلك (Andrew,2013:8) .

أثرت الثورة التكنولوجية في نظرية الوكالة، خاصة بعد أن بات الفضاء السيبراني وكيلًا

عن الفضاء المادي، لينشئ بذلك حدودًا جغرافية جديدة بين مختلف الفاعلين (Bradford W. Reyns.2011: 1152) . فقد بات الإنترنت مساحة جديدة للمعارك، وهي الساحة التي يصعب في إطارها معرفة هوية الخصوم على وجه الدقة، بما يؤجج استراتيجيات الحروب السيبرانية الطويلة الأمد. فقد يسفر استخدام الشركات العسكرية والأمنية عن اندلاع حروب عسكرية بالوكالة على المدى الطويل. إلا أن حروب الوكالة السيبرانية تمتاز بالمجهولية، في ظل تعدد الآليات التي من شأنها أن تخفي هويات الأطراف المتصارعة إلى حد كبير. ففي ظل الاعتماد المتزايد على أجهزة وشبكات الكمبيوتر، تعد الحروب السيبرانية استراتيجية مثالية للوكلاء السيبرانيين بفعل صعوبات تتبع مصدر الهجمات السيبرانية. كما يسهل إمداد الوكلاء السيبرانيين بالتقنيات التكنولوجية اللازمة، مقارنة بالأسلحة التقليدية (Andrew,2013:9).

لذلك، تزايد توظيف الوكلاء السيبرانيين من قِبل الدول ضد مختلف الأهداف، خاصة أن ذلك يحول دون تورط الدول المحرضة وسهولة التنصل من الهجمات السيبرانية (Aaron.2018:41)، وصعوبة إسناد الهجمات إلى مرتكبيها، لاسيما أن ذلك ينطوي – عادة – على مشاركة معلومات استخباراتية. فعلى مدى العقد الماضي، أصبحت العمليات السيبرانية الهجومية أداة أساسية لأغراض التجسس والإكراه. (Lior Tabansky).

ففي الفضاء السيبراني، هناك ثلاثة أطراف رئيسية، أولها الرعاة، ثانيها الوكلاء السيبرانيون، ثالثها الفاعل المستهدف. وكل طرف من الأطراف الثلاثة قد يكون دولة أو فاعلًا من غير الدول. وبطبيعة الحال، ينصب التركيز على الرعاة والوكلاء فحسب، وعليه قد تلجأ دولة ما لتوظيف أخرى لتحقيق أهدافها، أو قد توظف فاعلًا من غير الدول على شاكلة المرتزقة، والقراصنة، والميليشيات السيبرانية، وغيرهم. في المقابل، قد يستغل فاعل من غير الدول بعض الدول الهشة للعمل من خلالها، أو قد يوظف فاعلًا آخر على شاكلته؛ كاستعانة القراصنة ببعضهم بعضاً لتحقيق مختلف الأهداف.

يلجأ الرعاة إلى توظيف الوكلاء السيبرانيين للحيلولة دون تصاعد الصراع على خلفية الهجمات السيبرانية. فإذا شنت دولة ما علنًا على أحد خصومها، على سبيل المثال، فقد تتعرض للانتقام، إما في الفضاء السيبراني، أو في مجالات تقليدية أخرى. فمن شأن توظيف الوكلاء السيبرانيين أن يحول دون تورط الرعاة في عمليات ذات تكلفة سياسية أو مادية مرتفعة من ناحية،

فضلًا عن امتلاك بعض الوكلاء السيبرانيين عددًا من الأدوات، والمهارات والإمكانات التي قد تفتقر إليها الدول، أو تتزايد تكلفة تطويرها محليًا من ناحية أخرى. إلى جانب الأهداف السابقة، قد يهدف الرعاة إلى تجنب الكشف عن قدراتهم، أو الحفاظ على الغموض الاستراتيجي مع التطورات التكنولوجية المتلاحقة، أو استغلال الفضاء السيبراني لجمع مختلف المعلومات الاستخباراتية عن الأهداف الحكومية، والعسكرية، والصناعية، والاقتصادية، دون اكتشاف طبيعة أنشطة الرعاة الحقيقية داخل الفضاء السيبراني (Ministry of Defence,2016:22).

الفاعلون الدوليون للوكلاء السيبرانيين

صاحب الثورة التكنولوجيا إلغاء الطرق التقليدية والقديمة الثابتة للتفكير في الحروب، والفاعلين الدوليين ومجالات القوة. فظهرت أنواع جديدة من الحروب والنزاعات لم تعتدها الدول من قبل، كتلك ذات الصبغة السيبرانية، التي تهدد الأمن القومي للدول الكبرى والصغرى على حد سواء. ولم يعد استخدام التكنولوجيا في الجوانب مقتصرًا على الدول الكبرى التي تتنافس فيما بينها في استخدام التطورات التكنولوجية الحديثة في تحديث جيوشها، وتعزيز قوتها العسكرية. لكن مع إتاحتها لجميع الفاعلين الدوليين، أضحت سلاحًا في أيدي أفراد عاديين، ما يمكّنهم من تهديد أمن الدول من وراء الحدود (عمر, 1:2019).

بشكلٍ عام، تتعدد سمات وخصائص الفاعلين الدوليين للوكلاء السيبرانيين، فيمكن إجمالهم على النحو الآتي:

أ- الدولة: يمكن للدول شن هجمات سيبرانية هجومية، عبر وكالاتها الحكومية المتخصصة عبر القيادة السيبرانية، ووكالة الأمن القومي، إما منفردة أو ضمن تحالف غير معلن. (Frederic.2015: 10) يمكن تعريف الوكلاء السيبرانيين بوصفهم "وسطاء يقومون أو يسهمون بشكل مباشر في الهجمات السيبرانية بما يحدث تأثيرًا يستفيد منه آخر، أو هم الخوادم الوسيطة بين المستخدمين والشبكة العالمية، أو مجموعة من المتسللين بعمليات سيبرانية نيابة عن الرعاة"(Ministry of Defence,2016:85).

ب- الفاعلون من غير الدول: أينما كان الفاعلون، أفرادًا كانوا، أو جماعات، أو منظمات إرهابية، أو شركات متعددة الجنسيات، أو منظمات إرهابية، فإنه يتم توظيفهم، بالتوازي مع الأدوات العسكرية، وهو ما تجلى فيما فعلته روسيا في أوكرانيا عام 2015 من تعطيل شبكة كهرباء

بدلًا من تفجيرها. ويمكن للدول أن تعمل في الفضاء السيبرانى بشكل مباشر وغير مباشر عن طريق الوكلاء، ما يشجع أو يوجه سلوك المتسللين، أو مجرمي الإنترنت. & Martha (Duncan,2016:435-436)

يمكن تقسيم الفاعلين من غير الدول للوكلاء السيبرانين كالآتي:

الأفراد: الذين يمتلكون معرفة تكنولوجية عالية والقدرة على توظيفها، وعادة ما تكون هناك صعوبة في الكشف عن هوياتهم، ومن الصعب ملاحقتهم.

فأصبح الفرد بفضل الفضاء السيبراني فاعلًا مؤثرًا في العلاقات الدولية، ومن أبرز النماذج ظاهرة الويكيليكس" Wikileaks" الذي نجح في نشر ملايين الوثائق السرية للإدارة الأمريكية وقنصلياتها؛ ما خلق مشكلات دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها.

الشركات المتعددة الجنسيات

تمتلك شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي ما زالت حكرًا على الدول. فخوادم شركات مثل: جوجل Google وفيسبوك Facebook وميكروسوفت Microsoft وآبل Apple وأمازون Amazon تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف الأسواق وتستغل، وتؤثر في اقتصادات الدول وفي ثقافة المجتمعات وتوجهاتها، وهذا ما حدث في الأزمة بين شركة "جوجل" والصين حول المحتوى، أو فضيحة تسريب بيانات مستخدمي فيسبوك لمصلحة شركة "كامبردج أناليتيكا" التي تمت الاستعانة بها لمصلحة الحملة الانتخابية للرئيس الأمريكي ترامب.

المنظمات الإجرامية

تقوم بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الإنترنت العميق Deep internet لتجارة المخدرات والأسلحة والبشر، حيث تكلف هذه الجرائم السيبرانية مليارات الدولارات سنويًا.

الجماعات الإرهابية

تعد من أبرز الفواعل الدولية، خاصة بعد أحداث 11 سبتمبر؛ حيث تستغل الفضاء السيبرانى في عمليات التجنيد والتعبئة، والدعاية، وجمع الأموال، والمتطوعين. كما تحاول جمع

المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول. (إسماعيل، 2019 :1020-1021)

أنماط الوكلاء السيبرانيين

صنف كل من ايريكا بورجارد، وشون لونرجران الوكلاء السيبرانيين تبعًا لمعيارين رئيسيين، هما: طبيعة الوكلاء (سواء كانوا أفرادًا أو جماعات)، ونوعية الأهداف التي يسعون لتحقيقها (سواء كانت سياسية أو اقتصادية). ووفقًا لهما، يشمل الوكلاء السيبرانيون مجموعة واسعة نسبيًا من الفاعلين تضم: المتسللين الوطنيين والمنظمات الإجرامية والإرهابيين السيبرانيين، وغيرهم؛ حيث يصنف مختلف الوكلاء السيبرانيين تبعًا لمعيارين أساسيين، هما: مدى ومستوى التنظيم، والأهداف المرجوة، وهو ما يتضح من الجدول رقم (1).

جدول (1) أنماط الوكلاء السيبرانيين

الأهداف	أفراد أو جماعات	جماعات منظمة
السياسية	المتسللون الوطنيون القراصنة الإرهابيون السيبرانيون نشطاء الإنترنت (جماعة أنونيموس) *، وغيرها	الميليشيات السيبرانية منظمة "تاشي" فى روسيا الجيش السيبراني السوري الجيش السيبراني الهندي الجيش السيبراني الباكستاني
الاقتصادية	المهندسون المستأجرون Geeks- for – hire مثل: فيروس I Love You	الشبكات الإجرامية مثل: Rnn Asian Trads

فيما صنّف تيم موريز الوكلاء السيبرانيين إلى فئات عدة، وذلك على النحو الآتي:

أ- الفئة الأولى: وتضم بعض المؤسسات الوطنية التي يتم الاعتماد عليها كليًا من قِبل الدول؛ مثل: أجهزة الدولة، أو مؤسسات الدولة الحكومية.

ب- الفئة الثانية: وتضم فاعلين من غير الدول، لكن تحت إشراف أو سيطرة

الدولة؛ ما يعنى أن عملياتهم تخضع للدول.

ج- الفئة الثالثة: تضم فاعلين من غير الدول لا يخضعون لسيطرة الدولة الشاملة؛ بمعنى أن الدولة لا تسيطر عليهم بشكل مباشر، أو على عملياتهم، لكنها تمارس شكلًا من أشكال السلطة العامة، من خلال المشاركة في التخطيط، أو الإشراف، أو التنظيم، أو التنسيق، بل وحتى التوقف.

د- الفئة الرابعة: تشمل رعاية الدولة الإيجابية لأحد الفاعلين من غير الدول، دون أن يتلقى الأخير دعمًا محددًا، لكنه عام. فعلى سبيل المثال، وصف المرشد الإيراني "آية الله الخميني مجموعة من طلاب الجامعات بعملاء الحرب السيبرانية".

هـ- الفئة الخامسة والأخيرة: وكلاء سيبرانيون فاعلون من غير الدول يتم التعامل معهم من جانب الدولة، بناء على مدى الاستفادة مما حققه من أهداف سيبرانية. (Tim,2016 383:403)

الخاتمة

من الشعار الذي اتخذته الحروب غير التقليدية "التدمير الذاتي، أقل دماء، ولكن أكثر خسائر وتدميرًا"، لم توجد ساحة أفضل لتطبيق شعارها من الفضاء السيبراني.

لقد اختصر الفضاء السيبرانى حاجزَي الزمان والمكان، وتجاوز سيادة الدولة، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي. ومن ثم، برزت فضاءات جديدة للصراع بأدوات مختلفة، وأنماط جديدة تختلف عن الصراعات التقليدية.

وقد أدت الابتكارات التكنولوجية الحديثة، وتبني نماذج الحكومات الذكية والمدن الذكية، وتزايد الاعتماد على التقنيات المتطورة في إدارة شئون الحياة اليومية كافة، إلى تغير المفاهيم التقليدية للعلاقات الدولية، خاصة تلك المرتبطة بالأمن القومي، مثل القوة والحرب والصراع والردع والدفاع، إلى الوكالة السيبرانية والإرهاب السيبراني. فلقد وضعت الجميع تحت التهديد، سواء المؤسسات أو الأفراد على حدٍ سواء. فلا تمييز بين أهداف مدنية أو عسكرية، أو بين أفراد مدنيين أو عسكريين، فالكل في مرمى الهدف.

أصبح الفضاء السيبراني ساحة مستحدثة للصراع، بعد البر والبحر والجو والفضاء، إلا أنه من صنع الإنسان. كما أنه عكس النزاعات التي تخوضها الدول والفاعلون من غير الدول، بل

إنه أعطى أفضلية عن باقي ساحات الصراعات، تمثلت في صعوبة منع ومعرفة مصدر الهجمات والتكلفة المنخفضة؛ حتى فشلت منهجية الردع التقليدية.

مع ظهور القوة السيبرانية، باتت الدولة لا تحتكر القوة، بل أصبحت في متناول الفاعلين من غير الدول، الأمر الذي زاد من مخاطر الإرهاب والوكلاء السيبرانين، ما يهدد السلم والأمن الدوليين.

فعندما أعلن الرئيس الأمريكي السابق ترامب عام 2019 القضاء على أحدث التنظيمات الإرهابية، تنظيم الدولة الإسلامية فى العراق والشام " داعش"، لم يعلن القضاء عليه كتنظيم إرهابي سيبراني أو كوكيل سيبراني. فعوامل النصر أو الهزيمة في هذا الفضاء لا تقاس بعوامل مسارح العلميات التقليدية، ما يهدد بطول أمد الصراعات الدولية والإقليمية.

وبما أن عجلة الزمن لا تعود للوراء، فالمستقبل القريب يحمل لنا تهديدات لا حصر لها على جميع الفاعلين، أفرادًا وجماعات ودولًا، من الفضاء السيبراني. فالعالم سوف تُدار تفاعلاته في السلم أو الحرب بواسطة الآحاد والأصفار داخل العالم الافتراضي، فهو أمر حتمي، لا اختيار فيه ولا مهرب منه.

قائمة المراجع

أولًا: المراجع باللغة العربية

- **الكتب:**

1. إيهاب خليفة، مجتمع ما بعد المعلومات، سلسلة كتب المستقبل والمستقبل للأبحاث والدراسات المتقدمة، العربي للنشر والتوزيع، القاهرة 2019.
2. فرد كابلات، المنطقة المعتمة، التاريخ السري للحرب السيبرانية، عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب: الكويت، مارس 2019.
3. محمد عبد الله يونس، أسباب ودلالات الهجوم الإرهابي على "نيس"، المستقبل للأبحاث والدراسات المتقدمة: أبو ظبي، يوليو 2016، على الموقع: www.futureuae.com (تاريخ الاطلاع :2020/7/15)

- **دوريات:**

1. إسماعيل زروقة، الفضاء السيبرانى والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 1 ،2019 .

2. أهمية الوحدات الرقمية داخل أجهزة الاستخبارات ومخاطر الهجمات الإلكترونية، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، ألمانيا، هولندا، 2020.
3. إيهاب خليفة، الأمن السيبراني: الماهية والإشكاليات، رؤية مصرية، مركز الأهرام للدراسات الاجتماعية والتاريخية، القاهرة، العدد 57 أكتوبر، 2019.
4. دلال محمود السيد، "تحولات الحرب التقليدية: تطور في الأدوات أم تغير مفاهيمي؟" مجلة السياسة الدولية، ملحق تحولات استراتيجية، القاهرة، العدد 211، يناير 2018.
5. رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، على الموقع: www.politics-dz.com (تاريخ الاطلاع :2020/1/1).
6. رغدة البهي، "الردع السيبرانى: المفهوم والإشكاليات"، المركز المصري للفكر الاستراتيجي، على الموقع https://ecss.com.eg (تاريخ الاطلاع :1/10/ 2019).
7. عمرو عبد العاطي، "التطورات التكنولوجية ومستقبل الحرب"، مجلة السياسة الدولية، الأهرام، القاهرة، العدد 215 يناير 2019.
8. المجال الخامس – الفضاء الإلكتروني: دراسات أمنية، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية على الموقع www.politics-dz.com (تاريخ الاطلاع:2020/2/1.)
9. مفاهيم عسكرية: الحروب اللاتماثلية، دراسات أمنية، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية: الجزائر، على الموقع www.politics-dz.com. (تاريخ الاطلاع :2019/12/3).
10. نوران شفيق، أشكال التهديدات الإلكترونية ومصادره، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، ألمانيا، هولندا، على الموقعwww.europarabct.com (تاريخ الاطلاع2021/2/1)
11. يحيى مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد 23، 2014.

ثانيًا: المراجع باللغة الأجنبية

- **BOOKS:**

1.Aaron F. Brantly, The Cyber Deterrence Problem, 201810th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, 2018.
2.Denise M.Carter (2020) "Cyberspace and Cyberculture" International Encyclopedia of Human Geography (Second Edition) 2020
3.Lior Tabansky, Iran's Cybered Warfare Meets Western Cyber-Insecurity, in: Fabio Rugge (ed.), Confronting an "Axis of Cvber"? China, Iran, North Korea, Russia in Cyberspace (Milano Italy: Le)
4.Tim Maurer, proxies and cyber space, journal of conflict security law, Oxford University press,2016.

- **PERIODICALS:**

1. **Alex Marshall, from civil war to proxy war: past and current dilemmas, small wars & Insurgencies, 2016.**
2. **Andrew Mumford, Proxy warfare and the future of conflict. The Rusi Journal,28/4/2013,https://www.tandfonline.com/doi/full/10.1080/03071847.2013.787733 (accessed 28/4/2020).**
3. **Andrew Mumford,The New Era of the Proliferated Proxy War,Real Clear Defense, 16/11/2017 https://www.realcleardefense.com/articles/2017/11/16/the_new_era_of_the_proliferated_proxy_war_112648.html (accessed 16/11/2020)**
4. **Andrew Murmford. Proxy Warfare (Cambridge & Malden: John Wiley & Sons, 2013).**
5. **Bradford W. Reyns, Billy Henson, Bonnie S. Fisher, Being Pursued Online Applying berlifestyle Routine Activities Theory to Cyberstalking Victimization, Criminal Justice and Behavior, Vol. 38, No. 11, November 2011.**
6. **Dmitri Alperovitch, Towards Establishment of Cyberspace Deterrence Strategy, In: Cyber Conflict ICCC, 2011 rd International Conference, Tallinn, Estonia, June 2011.**
7. **Dorothy Deadening, Rethinking the Cyber Domain and Deterrence, JFQ, 2015, 2nd Quarter.**
8. **Frederic Lemieux, Trends in Cyber Operations: An Introduction, In: FredericLemieux (ed.), Current and Emerging Trends in Cyber Operations, (London: Pal grave Macmillan, August 2015.**
9. **Joseph S. Nye m., Cyber Power, Harvard Kennedy School, 2010.**
10. **Kenneth Geers, The Challenge of Cyber Attack Deterrence, Computer Law & Security Review, No. 26, 2010, pp. 298-303.**
11. **MAJ Lee Hsiang Wei, The Challenges of Cyber Deterrence, POINTER, JOURNAL OF THE SINGAPORE ARMED FORCES,2016.**
12. **Martha Finnemore & Duncan B. Hollis, Constructing Norms for Global Cybersecurity, The perican Journal ofInternational Law, VoL 110, No. 3, July 2016.**
13. **Martin C. Libick, cyber deterrence and cyberwar, Santa, CA; RAND,2009.**

14. Michael Kenney,"Cyber- Terrorism In A Post-Stuxnet World" The Foreian Policv ,Research Institute (FPRI), https://www.fpri.org/article/2015/01/cyber-terrorism-in-a-post-stuxnet-world/ ,(accessed 1/25/2019)
15. Ministry of Defense's, Cyber Primer, Development, Concepts and Doctrine Centre Ministry of Defense's Cyber Good Practice Guide to Protecting Yourself in Cyberspace (2nd Edition), July 2016.
16. Muhammad Mudassar Yamin⁎, Basel Katt, Mariusz Nowostawski (2021) "Serious games as a tool to model attack and defense scenarios for cyber-security exercises" Computers & Security, Vol. 110, November 2021.
17. Paulo & Janu Shakarian, Andrew Ruef, Introduction to Cyber warfare A multidisciplinary Approach, Ehevier, 2013.
18. Richard A. Clark, Cyber War: The Next Threat to National Security and What to Do About It Paperback – August 5, 2011
19. Sarah Anderson Goehrke.,UK Police Note Potential for 3D Printing Uses in Terrorist Activity,on on , https://3dprint.com/59830/uk-anti-terror-3d-printing/ ,(accessed 1/3/2019.)
20. Susan W. Brenner, "Cybercrime, CyberterrorismAnd Cyberwarfare", EresRevue Internationale De DroitPenal, Vol. 77, no. 3, (2006.
21. Tabansky, Lior (2016) "Cyber Power in the Changing Middle East" Turkish Policy Quarterly, Vol. 15, Issue 1.
22. The Federal Emergency Management Agency (FEMA), "Appendix D: Cyberterrorism, Interim Tool Kit", 2002.
23. The Federal Emergency Management Agency (FEMA). "Appendix D: Cyberterrorism, Interim Tool Kit", July 2002.
24. What is a Proxy war? The Vietnam war / Proxy war. May 5. 2016
25. Wolff Heintschel Von Heinegg, "Territorial Sovereignty and Neutrality" Cyberspace Intonation Law Studies, Vol. 89, No. 1.