Dirasat: Human and Social Sciences, Volume 53, No. 6, 2026, 9115

Deanship of Scientific Research

Asymmetric Cyberwarfare Strategy in International Relations: A Study in Theory and Application of the Russian-Ukrainian War

Alshaimaa Mohamed Mahmoud Hassan*

Department of Public Law, King Faisal University, AlAhsa, Saudi Arabia.

Received: 22/9/2024
Revised: 25/11/2024
Accepted: 11/12/2024
Published online: 1/1/2026

* *Corresponding author:*
a.hassan@kfu.edu.sa

Citation: Mohamed, A. M. (2026). Asymmetric Cyberwarfare Strategy in International Relations: A Study in Theory and Application of the Russian-Ukrainian War . *Dirasat: Human and Social Sciences*, *53*(6), 9115.
https://doi.org/10.35516/Hum.2026.9115

Abstract

Objectives: This study aims to explore the understanding and interpretation of cyber war strategy and the controversy surrounding it, particularly its strategic overlap with concepts such as asymmetric warfare. It employs realist theories of international relations to provide explanations for the Russian-Ukrainian asymmetric cyber war strategy under study.

Methods: Given the novelty and complexity of the phenomenon with its multiple dimensions, this study relies on the inductive approach to examine the asymmetric Russian-Ukrainian cyberwarfare.

Results: The study concluded that the dynamic nature of the asymmetric Russian-Ukrainian cyber war highlights the inability and imbalance of the international system to address this type of conflict. This is particularly evident in the absence of a legal framework and a lack of international consensus on its classification, legitimacy, and legal adaptation—whether as "military" or unarmed armed conflict. As such, this war is uniquely complex, combining fifth-generation warfare, including cyber wars, and kinetic military action.

Conclusions: As states increasingly view cyberspace as integral to their political and strategic interests, the major divisions within new realism in international relations offer varied interpretations of states' intentions, interactions, and global policies. The study discusses the transformation of the Russian-Ukrainian conflict within the context of the new geopolitical and geostrategic order, providing realistic interpretations of the war strategy, its implementation tactics, legitimacy, and international positioning, along with its implications for international relations.

Keywords: Cyberwarfare; non-compliance; strategy; realism; international relations; Russian-Ukrainian war

استراتيجية الحرب السيبرانية غير المتماثلة في العلاقات الدولية (دراسة في النظرية والتطبيق للحرب الروسية الأوكرانية)

الشيماء محمد محمود حسن*

قسم القانون العام، كلية الحقوق، جامعة الملك فيصل، الأحساء، المملكة العربية السعودية

ملخّص

الأهداف: تهدف هذه الدراسة في البحث عن كيفية فهم وتفسير استراتيجية الحرب السيبرانية والخلاف الدائر حولها، لا سيما مع تداخلها الاستراتيجي مع مفاهيم ومصطلحات أخرى، مثل الحرب غير المتماثلة ومقاربتهما النظرية في النظريات الواقعية للعلاقات الدولية لتقديم التفسيرات الواقعية لاستراتيجية الحرب السيبرانية الروسية الأوكرانية غير المتماثلة محل الدراسة.

المنهجية: نظرا إلى حداثة الظاهرة ومن ثَمّ تعقدها وتعدد أبعادها على النحو الذي يقتضي عند دراستها، الاعتماد في هذه الدراسة على المنهج الاستقرائي في دراسة الحرب السيبرانية الروسية الأوكرانية غير المتماثلة.

النتائج: خلصت الدراسة إلى جملة من النتائج من أبرزها، أن الطبيعة الديناميكية للحرب السيبرانية الروسية الأوكرانية غير المتماثلة. أظهرت عجز النظام الدولي وعدم توازنه في التعامل مع هذا الحرب، خاصةً في ظل غياب الأساس القانوني لها وعدم وجود اتفاق دولي على تصنيفها وتحديد شرعيتها وتكييفها القانوني، إن كانت تقع تحت الصراع المسلح "العسكري" أو غير المسلح. لذا تعد ذلك الحرب فريدة من نوعها ومعقدة للغاية تجمع بين حروب الجيل الخامس الذي تشمل الحروب السيبرانية، والعمل العسكري الحركي.

الخلاصة: مع بدء الدول في النظر إلى الفضاء السيبراني كجزء من مصلحتها السياسية والاستراتيجية، وما تُقدمه الانقسامات الرئيسة للواقعية الجديدة في العلاقات الدولية من تفسيرات مختلفة لنيات الدول وتفاعلاتها وسياساتها العالمية. وتطبيقاً على الحرب السيبرانية الروسية الأوكرانية غير المتماثلة، ستناقش الدراسة تحول الصراع الروسي الأوكراني في سياق العلاقات الدولية للنظام الجيوسياسي والجيواستراتيجي الجديد. محاولة منها في كيفية تقديم التفسيرات الواقعية لاستراتيجية ذلك الحرب، والتكتيكات التي اتُّبِعَتْ في تنفيذها، وتحليل مشروعيتها والموقف الدولي منها، بالإضافة إلى تداعياتها وتأثيراتها على العلاقات الدولية.

الكلمات الدالة: الحرب السيبرانية، عدم الامتثال، الاستراتيجية، الواقعية، العلاقات الدولية، الحرب الروسية الأوكرانية.

المقدمة:

ان المداخل النظرية المتوطنة في الحقل المعرفي للعلاقات الدولية لم تعد قادرة على استيعاب التحولات والتغيرات التكنولوجية الاستثنائية التي يشهدها العالم اليوم من الحروب والتهديدات، التي أسهمت في بروز تقنيات تكنولوجية متطورة في ميدان التسليح واستحداث أدوات متقدمة غير تقليدية في اختراق الدول وأجهزتها ومنشأتها الحيوية، وإخضاع الخصوم عبر الحرب السيبرانية. حيث تجاوزت الحروب والمواجهات العسكرية التقليدية لتشمل توظيف أدوات واستراتيجيات جديدة أدت إلى صعود الاستراتيجيات السيبرانية أو الاستراتيجيات الهجينة (Hybrid Strategies) التي تمزج بين الحرب العسكرية التقليدية والحرب السيبرانية والحرب غير النظامية المتباينة. بالتالي تعُدُّ الحرب الدائرة بين روسيا وأوكرانيا من الحروب الحديثة التي تكتسب أهميةً خاصةً من حيثُ العمليات السيبرانية، الذي يرجع إلى امتلاك البلدين طيلة سنوات، عددًا كبيرًا من الخبراء والمتخصِّصين في المجال الرقمي وتكنولوجيا المعلومات والأمن والعمليات السيبرانية. فروسيا تعدّ واحدة من أهم دول العالم استخداماً للعمليات السيبرانية غير المتماثلة وتوظيفها في حروبها وسياستها الدولية، في الوقت ذاته سعت أوكرانيا بفعالية على استحداث وتحسين بنيتها التحتية الرقمية لمجابهة الخطر الروسي. مما أضحت دراسة الحرب السيبرانية غير المتماثلة الدائرة بين روسيا وأوكرانيا، أمرًا محوريًّا لترسيخ فهمنا لاستراتيجية الحرب السيبرانية، حيث أضحت التطبيقات والأدوات السيبرانية والرقمية مرتبطة ارتباطا جزئياً في الأعمال الحربية. مما دفع الكثير من منظري العلوم السياسية والاستراتيجيين العسكريين إلى إعادة التفكير من جديد في الحقائق والمسلَّمات حول الحرب السيبرانية التي لم تكن بمعزل عن أي عملية حربية أخرى.

أهمية الدراسة:

تكمن أهمية الدراسة في أنها جاءت من الناحية العلمية إلى توضيح مبدأ من أهم وأخطر المبادئ المستخدمة عالمياً، وهو مبدأ الحرب السيبرانية غير المتماثلة وكيف تم تطبيقها كاستراتيجية في الحرب الروسية الأوكرانية، وما مدى مشروعيه تطبيق هذه الاستراتيجية في علاقتها الدولية.

أما على الجانب العملي فتكمن الأهمية العملية لهذه الدراسة في أنها تمد الباحث العلمي بالمعلومات الكافية عن استراتيجية الحرب السيبرانية غير المتماثلة في العلاقات الدولية، ذلك بالتطبيق على استراتيجية الحرب الروسية الأوكرانية الحالية، وأيضا المهتم بالشأن الدولي بالمعرفة التامة عن الفكر الاستراتيجي الحديث للحروب السيبرانية المطبق في العلاقات الدولية.

كذلك إمداد المكتبة العلمية بمرجع مهم من الممكن الاستناد إليه في البحوث والدراسات المتعلقة باستراتيجيات الحروب السيبرانية غير المتماثلة، لما يحتويه من تفصيلاته معلومات قديمة وحديثه عن طبيعة وتطور مفهوم وأبعاد وأنماط هذه الحرب غير المتماثلة في النظريات الواقعية للعلاقات الدولية.

أهداف الدراسة:

تهدف هذه الدراسة في البحث عن كيفية فهم وتفسير استراتيجية الحرب السيبرانية والخلاف الدائر حولها، لا سيما مع تداخلها الاستراتيجي مع مفاهيم ومصطلحات أخرى، مثل الحرب غير المتماثلة. كذلك التعرف على أبرز أنماطها ومقاربتهما النظرية في النظريات الواقعية للعلاقات الدولية، لتقديم التفسيرات الواقعية لاستراتيجية الحرب السيبرانية الروسية الأوكرانية غير المتماثلة محل الدراسة واقع التفاعلات الدولية وشرعيتها، وتحليل تداعياتها ومخاطرها على العلاقات الدولية والأمن العالمي.

مشكلة الدراسة:

جاءت المشكلة البحثية ارتكازاً إلى التساؤل البحثي المركزي، الذي طرحته المشكلة البحثية، التي ستحاول الدراسة الإجابة عليه، ويدور في: **ماهي استر اتيجيات الحرب السيبر انية وتطبيقاتها في الحرب الروسية الأوكر انية؟**.

اتساقاً مع المشكلة البحثية والتساؤل الرئيسي الذي طُرح، تحاول الدراسة الإجابة على عدة تساؤلات فرعية، تدور حول ما يلي:

1. ما ماهية المقاربة النظرية بين المفهوم والأبعاد للحرب السيبرانية وبين عدم الامتثال في العلاقات الدولية؟.
2. ما مدى مشروعية الحرب السيبرانية الروسية الأوكرانية غير المتماثلة في القانون الدولي والموقف الدولي؟.
3. ما ماهية دلالات ديناميكية تطور استراتيجية الحرب السيبرانية الأوكرانية غير المتماثلة، وما مدى تأثير تداعياتها على العلاقات الدولية؟.

فروض الدراسة:

لقد دار في الذهن عدد من الاستفسارات أثارتها المشكلة البحثية، تم الانتهاء منها إلى تصميم وصياغة فرضية أساسية مفادها:

"أن أيديولوجية روسيا وأوكرانيا في صلب استراتيجية الحرب السيبرانية غير المتماثلة بينهما، اتسمت بخصائص مختلفة عن نظيراتها التقليدية، من حيث ديناميكية مفهومها وأبعاد تداخلاتها وتطور نظريتها الواقعية، وأنماط وصور تلك الاستراتيجية. مما عبرت عن نمطين من القوة (الناعمة، الصلبة) في عملية توظيف القدرات السيبرانية والتفاعلات في الفضاء المعلوماتي، باعتبارها الأداة الأمثل في رسم استراتيجية "الحرب السيبرانية غير المتماثلة" كاستراتيجية جديدة في العلاقات الدولية".

ويترتب على ذلك مناقشة أو التأكد من صحة ثلاثة فروض عملية أخرى، تتلخص فيما يلي:

الفرض الأول: إن هناك مقاربة نظرية بين المفهوم والأبعاد للحرب السيبرانية، وبين عدم الامتثال في العلاقات الدولية.

الفرض الثاني: يوضح العلاقة بين ما تحققه الحرب السيبرانية غير المتماثلة من انتصارات لمستخدميها، وبين مدى مشروعية هذه الحرب والاعتراف بها دولياً.

الفرض الثالث: ترتب على استراتيجية الحرب السيبرانية غير المتماثلة التي طبقتها روسيا في حربها على أوكرانيا وفي علاقتها الدولية مزج بين (القوة الناعمة، والقوة الصلبة)، مما أثرت تداعياتها على العلاقات الدولية والتفاعلات السياسية.

منهجية الدراسة:

اعتمدت الدراسة على المنهج الاستقرائي الذي يقوم على ملاحظة الأبعاد الواقعية والأنماط والعلاقات المرتبطة بالظاهرة محل الدراسة؛ للانتقال من مستوى الفهم البسيط إلى مستوى الفهم المركب، وذلك باستقراء مفهومي وأبعاد الحرب السيبرانية وعدم الامتثال، والصور والأنماط التي ارتكزت عليها الحرب السيبرانية غير المتماثلة، لمعرفة طبيعة ذلك الحرب السيبرانية الروسية الأوكرانية غير المتماثلة، كذلك الاستراتيجيات والتكتيكات التي اتُّبِعَتْ في تنفيذها والآثار والتداعيات التي ترتبت من جرائها على العلاقات الدولية.

حدود الدراسة:

لحصر الدراسة في نطاق محدد فقد حددت الدراسة كلٍ من الإطار المكاني وهو التركيز على النموذج الروسي والأوكراني، والإطار الزمني ابتدأ من عام 2022 حيث الهجوم الروسي على أوكرانيا بسلسلة واسعة من الهجمات ضد المواقع التي تديرها الحكومة الأوكراني.

المبحث الأول: الحرب السيبرانية وعدم الامتثال ومقاربتهما النظرية بين المفهوم والأبعاد

مع انتقال الفضاء السيبراني إلى ساحة للتفاعلات الدولية، الذي أضحى يشكل دوراً بارزا وتغيرات جوهرية في العلاقات الدولية، حيث برز الكثير من الأنماط والأصعدة المختلفة في استخداماته، سواء على الصعيد المدني، أو السياسي، أو الاقتصادي، أو العسكري، مما برز شكل جديد من القوة هي "القوة السيبرانية"، التي جعلت الفضاء السيبراني ميدانا للصراعات المتباينة، لاستحواذ الفاعلين من الدول وغير الدول على قدر كبير من النفوذ والهيمنة السيبرانية المؤثرة.

في سياق ذلك، استحدثت ظاهرة "الحروب السيبرانية Cyber wars"، التي تميزت بسمات متباينة عن نظيراتها من الحروب العسكرية التقليدية، من حيث فحوى الأعمال والممارسات العدائية، والفواعل الدولية وغير الدولية، والتأثيرات في بنية وتشكيل الأمن العالمي، ومدى امتثالها وتكافؤها. حيث جسدت ذلك الحرب نمطين من القوة هما: (القوة الناعمة، والقوة الصلبة) في استخدامها للتفاعلات الدولية في الفضاء السيبراني، مما يظهر تزايد وتفاقم القدرات والتهديدات المتصاعدة والمتلاحقة لأمن البنية التحتية الحيوية الرقمية. فقضية الحرب السيبرانية من القضايا المستحدثة في النظام العالمي، نتيجة لقيامها بتحول الساحة الدولية إلى أرض معارك غير متماثلة في عالم افتراضي تقني يستلزم الرد الصارم من قبل المجتمع الدولي، في حال عدم تحقق شرط الدفاع عن النفس، وفي سياق ذلك انقسمت الآراء حول مشروعية الحرب السيبرانية غير المتماثلة إلى فريقيين (مؤيد، معارض). مما تحولت جهود ومساعي عدّة للضبط المفاهيمي لمصطلح الحرب السيبرانية، تحديداً وأنه لا يوجد اتفاق بين الباحثين والمتخصصين حول مفهوم الحرب السيبرانية.

المطلب الأول: مفهوم و أبعاد الحرب السيبرانية وتطوره في النظريات الواقعية للعلاقات الدولية

بتطبيق مقولات النظريات الواقعية على مفهوم الحرب السيبرانية وجدَّ أنه ذاع صيت استخدام هذا المفهوم على يد منظرو العلاقات الدولية الواقعيون الجدد الذين طوروا من مفاهيم "الحرب السيبرانية". حيث رأي جيمس آدم – أحد منظِّري الواقعية الجديدة– أن الفضاء السيبراني بات ساحة جديدة للقتال بين الدول، فكلما ازداد اعتماد الدول على التطورات التقنية والرقمية ازدادت قابليتها للاختراق (Adams, 2001, p.98).

كما أشار "نيلز ميلزر" إلى مصطلح "الحرب السيبرانية" إلى أنه: الحرب الذي تُجرى في الفضاء السيبراني باستخدام الوسائل والأساليب السيبرانية. في حين أن مصطلح "الحرب" يُفهم عمومًا على أنه يشير إلى سير الأعمال العدائية العسكرية في حالات النزاع المسلح. كذلك وصف "الفضاء السيبراني" بأنه شبكة مترابطة عالميًا من البنى التحتية الرقمية، متضمنة الإنترنت وشبكات الاتصالات السلكية واللاسلكية وأجهزة التحكم وأنظمة الحاسوب والمعلومات البيانات الرقمية الموجودة فيها. وبذلك، فإصابة شبكة حاسوب الخصم المحارب بفيروس خبيث من شأنه أن يمثل عملاً من أعمال الحرب السيبرانية، في حين أن القصف الجوي لقيادة إلكترونية عسكرية لا يشكل عملاً من أعمال الحرب السيبرانية. وحقيقة أن الحرب السيبرانية تجرى في الفضاء السيبراني لا تستبعد إمكانية حدوثها (Melzer, 2011, p.9).

أما عن كريستوفر بول وإلينور سلون فقد وضعا كلٍ منهما تعريفاً للحرب السيبرانية اتفقا فيه على أنها: «الاستخدام المندمج للقدرات الأساسية للقتال الإلكتروني، عمليات شبكة الحاسوب، العمليات النفسية، الخداع العسكري، وأمن العمليات، في تناغم مع الدعم الخاص والقدرات ذات العلاقة، للتأثير،

تمزيق، إفساد، أو غصب عدائي للإنسان وصناعة القرار الآلي مع حماية الخصوصية» (Paul, 2008, p.2 & Sloan, 2012, pp. 85-87).

وأخيراً، وبعد ما عُرِض من مفاهيم متعلقة بالحرب السيبرانية وتطورها من واقع النظرية الواقعية في العلاقات الدولية وتنوعها وتعدد ضروبها وبواعث ديناميكيتها - بالرغْم من عدم وجود تعريف واضح ومحدد متفق عليه نظراً لاتساع المفهوم بسبب التقدم التقني وتعدد وتنوع أشكال ذلك الحرب - أوضحت أدبيات العلاقات الدولية بأن النظريات الواقعية تعدّ الأكثر قابلية للتطبيق على القضايا المتعلقة بالحرب السيبرانية. ومن الممكن أن تساعد تلك النظريات في تفسير كيفية استخدام الدول للتكنولوجيات السيبرانية؛ لتعزيز مصالحها في المجالات الأمنية والحربية. وبتفسير مفاهيم الحرب السيبرانية التي عُرِضَت من واقع النظريات الواقعية في العلاقات الدولية، اتضح أن لها خمسة مظاهر تبين طرقاً وآلية عملها، أولها: أن الحروب السيبرانية تستهدف فئات محددة، ربما تكون أفرادا، أو دولاً، أو مؤسسات، أو منظمات. وثانيها: استهداف البيئة الرقمية للمعلومات في الحرب السيبرانية، بينما يتمثل ثالثها في: أن (القرصنة الناعمة) تعُد سلاح هذا الحرب، والمتمثلة في النظم والأدوات التقنية والمنصات الرقمية والشبكات المعلوماتية بكافة أشكالها، أما رابعها فيتمثل في: أن لهذا الحرب تكاليف بالغة الثمن ومتعددة، تتمثل في التكاليف السياسية والاقتصادية والعسكرية والأمنية والاجتماعية، لكنها في الوقت ذاته تعد تكاليف بسيطة مقارنة بتكاليف الحروب العسكرية التقليدية، أما خامسا: المظاهر والتكتيكات الأيديولوجي الذي قد تعتلي تطبيقات ذلك الحرب في الفضاء الرقمي. فهذه المفاهيم ومظاهرها أوضحت أن هذا الحرب مثال لعدم التماثل في القوة بصرف النظر عن كيفية تعاريفها وتوضيح جوانبها.

المطلب الثاني: طبيعة مفهوم و أبعاد عدم الامتثال وتداخلاته الاستر اتيجية

يعود مفهوم عدم الامتثال إلى الجنرال هنري شيلتون "Henry Shelton" رئيس هيئة أركان القوات المشتركة الأمريكية، الذي قدم تعريفه "للحرب غير المتماثلة"، بأنها: "سعي طرف يعادي أمريكا والتفافه نحو قوتها واستغلاله لنِقَاط ضعفها، معتمداً على طرق وأدوات مختلفة كلياً عن نوع الأعمال التي يمكن التعامل معها وتوقعها من قبل الجيش الأمريكي. وعدم الامتثال، يعني أن يستغل هذا الطرف المعادي توظيف الحرب النفسية وما ينتج عنها من تشتيت الخصم وإضعافه لكي ينتزع الروح القتالية من الخصم، ويتحكم هو في زمام الأمور والمبادرة في حرية التحرك والتأهب، واستخدام أساليب وطرق قتالية مستحدثة، وتكتيكات ووسائل تكنولوجية غير تقليدية، جرى التوصل إليها عن طريق التفكير الاستراتيجي غير المعتاد الذي لا يستطيع تقديره أو تصوره؛ لتطبيقه على كافة مستويات وعمليات الحرب" (McNamara, 1968, p. 108).

ورغم مرور أكثر من عَقْدَين من الزمن منذ بدء تداول مصطلح "عدم الامتثال" فإنه لا يوجد حتى في تلك الأثناء تعريف متفق عليه يُفسِّر مفهوم استراتيجية الحرب غير المتماثلة بشكل قاطع وواضح، بل هناك في حقيقة الأمر تعاريف متعددة بعضها من التعريفات التأسيسية، عُرفت على أنها استخدام نوع ما من الاختلاف للحصول على ميزة على الخصم (Metz, 2001, p.2). أما عن التعريفات الأكثر شيوعاً التي تشير إلى أن عدم الامتثال هي تقريبًا أي شيء قد يفعله ممثل ضعيف عندما يواجه خصمًا أقوى بكثير، خاصة إذا كان هذا الإجراء مفاجئًا أو مبدعًا إلى حد ما "فالحرب غير المتماثلة هي عمل عنيف يقوم به "لا يملكون" ضد "من يملكون" حيث يسعى من لا يملكون، سواء كانوا من الدول أو الجهات الفاعلة دون الدول، إلى إحداث تأثيرات عميقة، بواسطة توظيف مزاياهم النسبية الخاصة في مواجهة نِقَاط الضعف لدى خصوم أقوى بكثير" (Thornton, 2007, p. 9).

ودون الإسهاب في الإشارة إلى المزيد من التعريفات، فإن الخطط المدروسة المستخدمة في هذا النوع من الحروب والقدرات التقنية الفائقة هما السمات الأساسية التي تتطلبها استراتيجية عدم الامتثال، وهذا ما ستوضحه الدراسة في الحالة الروسية الأوكرانية للحرب السيبرانية غير المتماثلة، التي حظيت باهتمامً بالغ وجهوداً تحليلية حولها من قبل الدراسين والمنظرين الاستراتيجيين والسياسيين، نظراً لما تشكله من أهمية بالغة الخطورة على النظام الدولي في تحقيق أغراض متداخلة (سياسية، وعسكرية، واقتصادية، واجتماعية، وإجرامية، وغيرها)، ذات أبعاد وتوجهات جديدة غير معروفة وغير مدروسة للمجتمع التحليلي.

المطلب الثالث: صور و أنماط استر اتيجية الحرب السيبر انية غير المتماثلة

تعددت وتنوعت صور وأنماط استراتيجية الحرب السيبرانية غير المتماثلة من حيث درجة الشدة من عدمه، التي تسهم في ديناميكيتها أو استمراريتها وفي تحويلها أو انتهائها، وفقاً للأدبيات السياسية الواقعية المتعددة؛ وإمكانية التنبؤ بالأزمات الناجمة عنها، فتراوحت بين ما يلي:

النمط الأول: الحرب السيبر انية الباردة منخفضة الشدة Low intensity: يعبر هذا النمط من الحرب عن صراع مستمر بين الفاعلين المتنازعين، يتم فيه استخدام الفضاء السيبراني كساحة للحرب منخفضة الشدة، ويكون ذا طبيعة ممتدة له طابع غير سلمي، بخلاف أنه له بعد سياسي واقتصادي وتاريخي وديني وأيدلوجي واجتماعي عميق الجذور ومتداخل وممتد، كأن تكون جزءا من الصراعات السياسية والعسكرية التقليدية الطويلة الممتدة مثل: (الصراع العربي الإسرائيلي). التي في العادة ما يُلْجَأ إلى القوة الناعمة لاستراتيجية الحروب السيبرانية في مثل صراعات كهذه تمزج بين الجيلين الرابع والخامس، متضمنة عدة أدوات، كالحروب النفسية وحرب الأفكار والعقائد والاختراقات المتعددة والتجسس والمنافسة بين الشركات التقنية والرقمية العالمية وأجهزة الاستخبارات الدولية. ويستخدم هذا النمط من الحروب السيبرانية أسلوب خلق وافتعال الأزمات السياسية لإثارة الرأي العام والاضطرابات ضد الدولة، وبث وترويج الإشاعات للإضرار بالاقتصاد والأمن القومي، وخلق مناخ وبيئة غير آمنة على المستوى السياسي والأمني

والاستثماري، وغيرهم. وقد وجدنا منها أشكالاً ونماذج عدة مع بدء تنفيذ استراتيجية الفوضى الخلاقة عام 2011 وظهور ما يسمى بثورات التغيير العربي، كذلك جماعة "ويكليليكس"، و "أنونيموس" التي تقوم بتنشيط القرصنة للتعبير عن مواقف سياسية، أو حقوقية، أيضاً في حالات الأزمات الدولية، مثل التوتر بين استونيا وروسيا في عام 2007، وكذا الاختراقات المتبادلة بين الصين والولايات المتحدة وروسيا، وقد تعرضت روسيا للاتهام بالقرصنة الإلكترونية في الانتخابات الرئاسية الأمريكية التي جرت عام 2016 لدعم المرشح الجمهوري دونالد ترامب في مواجهة منافسته الديمقراطية هيلاري كلينتون (الدويك، 2019، حكيم، 2020، ص97).

النمط الثاني: الحرب السيبرانية متوسطة الشدة Medium intensity: يبرز هذا النمط من الحرب حينما انتقل الصراع عبر الفضاء السيبراني إلى ساحة مماثلة لحرب عسكرية تقليدية جارية في أماكن متفرقة من أنحاء العالم. مما نجم عنها جملة متشابكة من الأزمات التقليدية المتداخلة، تكون تعبيراً عن حدة الصراع القائم بين الأطراف، تمهيداً لحرب عسكرية. وهي ليست بحاجة إلى بدائل وسيناريوهات كما في حال الأزمات السياسية، فالمسألة تتوقف على القدرات السيبرانية، وامتلاك برامج قادرة على الردع الهادف أو الهجوم المحدود أو الموسع، مما ينجم عنه البعض من الأزمات الناتجة على عدم التحكم في أنظمة الشبكات، ومنها اختراق المواقع الإلكترونية الحيوية وتدميرها، وقرصنة وإتلاف المعلومات، وشن حرب نفسية ضد الخصوم، وتعطيل شبكات ومحطات توليد الطاقة الكهربائية، وجميع شبكات النقل سواء البري أو الجوي أو البحري، والشبكات البنكية، وإدارة محطات المفاعلات النووية. ويستمد هذا النمط من الحروب السيبرانية قوته من شدة وقوة أطرافه، وارتباطها الوثيق بالأعمال العسكرية التقليدية، ومن نماذج هذا النمط: الحرب الروسية الجورجية عام 2008، والحرب الأمريكية الإيرانية عام 2010، والحروب الروسية الأوكرانية 2022/2018/2016 (الدويك، 2019، حكيم، 2020، ص97-98).

النمط الثالث: الحرب السيبرانية الساخنة مرتفعة الشدة وأزماتها الكارثية High intensity: ينعكس ذلك النمط عن ظهور حروب منفردة في الفضاء السيبراني، وغير متماثلة مع العمليات العسكرية التقليدية. حيث يتضمن هيمنة البعد التقني والرقمي على إدارة العمليات العسكرية، ذلك باستهداف الأدوات السيبرانية منشآت العدو، واللجوء إلى الروبوتات والطائرات بدون طيار في الحروب المسلحة، والتحكم فيها عن بعد، هذا بخلاف تطوير واستحداث القدرات القتالية في ميداني الهجوم والدفاع السيبراني، والاستحواذ على القوة السيبرانية. والهدف من وراء ذلك تحقيق "الهيمنة السيبرانية واسعة النطاق" بصورة عاجلة في حالة نشوب حرب. ويرى البعض من الدارسين والخبراء أن النموذج الأقرب لهذا النمط من الهجمات السيبرانية، هو خوض إسرائيل بالتعاون مع الولايات المتحدة عام 2010، هجمات فيروس "ستاكسنت Stuxnet" المعلوماتي ضد المنشآت والمواقع النووية الإيرانية (McMillan, 2014, Broad, 2011).

المبحث الثاني: الموقف الدولي من الحرب السيبرانية الروسية الأوكرانية غير المتماثلة

في هذا المبحث يثور التساؤل حول مدى مشروعية هذا الحرب السيبرانية الروسية الأوكرانية غير المتماثلة وفقا لقواعد القانون الدولي الخاصة بإنفاذ حظر استخدام القوة، فضلاً عن الموقف الدولي المتمثل في الأمم المتحدة ومجلس الأمن والدول من ذلك الحرب.

المطلب الأول: تحليل مشروعية الحرب السيبرانية الروسية الأوكرانية غير المتماثلة

تعد قضية الحرب السيبرانية من القضايا العالمية المستجدة في النظام القانوني الدولي، نتيجة لقيامها على استحداث جيل جديد من أدوات الصراع والاشتباك انتقلت بواسطتها جبهات القتال إلى ساحة الفضاء السيبراني بشكل غير متماثل، مما ساهم هذا الاستحداث في إعادة النظر في هيكلة حركية وديناميكية الصراع، كذلك ظهور ما يسمى بعصر "القوة النسبية"، مما جعل "القوة العسكرية" وحدها لا تكفي لتأمين أمن الدول وبنيتها التحتية الحيوية، فخلف آثارا استراتيجية بالغة على مدى نسق النظام الدولي وتوازناته خاصةً في ظل عدم وضوح المعنى الدقيق لمصطلح "استخدام القوة" المشار إليه في المادة (الثانية) الفَقَرة (الرابعة) 4/2 من ميثاق الأمم المتحدة، فضلا عن خلو الاتفاقيات والأعراف الدولية من ذلك المصطلح. ولكن بعد أن أُثير استثناء تفعيل المادة 51 من الميثاق؛ التي أباحت الدفاع الشرعي الوقائي عن النفس في الحروب والهجمات السيبرانية حتى ترتقي إلى درجة الهجوم المسلح، فتعطي للدولة المعتدي عليها فرصة تفعيل المادة 51، وتطبيقاً لنص هذه المادة ذهب جانب من الفقه الدولي بإباحة الدفاع الشرعي للحرب السيبرانية الروسية الأوكرانية. في المقابل ظهر اتجاه فقهي معاكس لهذا الجانب من التدخلات المستحدثة نتيجة للتمدد والتوسع غير المتماثل في تفسير الدول الكبرى لمصطلح الدفاع عن النفس.

وبذلك ينقسم الفقه الدولي تجاه الحرب السيبرانية الروسية الأوكرانية غير المتماثلة حول مدى مشروعية الحرب السيبرانية الروسية الأوكرانية غير المتماثلة، فهناك من أيد مشروعية هذا الحرب وهناك من عارضها بشدة وهذا ما ستتناوله الدراسة فيما يلي:

أولاً: الفريق المؤيد لمشروعية الحرب السيبرانية الروسية الأوكرانية غير المتماثلة

هناك جانب من الفقه الغربي يؤيد مشروعية الحرب السيبرانية بوجه عام، مستنداً على ذلك بأنه في سياق الدفاع الشرعي لا تنتهي عند وقوع هجوم عسكري أو اعتداء مسلح، ربما تمتد أيضاً إلى سياق الهجوم السيبراني غير المتماثل الذي يرتقي إلى الهجوم والاعتداء العسكري المسلح الوارد في المادة

51 من ميثاق الأمم المتحدة، التي أقرت للدول سواء فرادى أو جماعات بالحق الطبيعي لهم في الدفاع عن أنفسهم دون قيود.

كذلك أن مشروعية حق الدفاع عن النفس ليست بوليدة ميثاق الأمم المتحدة، بل أقرتها الأعراف والمحاكم الدولية مستندة على حالة الضرورة القصوى التي لا يكون لديها أي مجال أو وسيلة أخرى لدفع هذا الخطر، وجوباً أن يكون الخطر داهماً ووشيك الوقوع يهدد ضرراً مادياً للأفراد والممتلكات والمرافق والبنية التحتية للدولة المعتدى عليها، فضلاً على أن تكون الإجراءات الوقائية بواسطة الهجمات السيبرانية التي تزاولها الدولة مقبولة ومحددة بموجب الحماية فقط.

أيضاً يتبني هذا الجانب رأيه في شرعية الدفاع عن النفس للحرب السيبرانية بناءً على اعتبار أن جميع أسلحة الدمار الشامل من أسلحة نووية أو كيماوية أو البيولوجية أو حتى قواتهم التدميرية، تعد حصيلة الثورة التقنية الهائلة التي يشهدها العالم اليوم. لذا يتوجب منح الدولة المعتدى عليها توجيه ضربة وقائية بواسطة الهجمات السيبرانية إسناداً إلى حق الدفاع عن نفسها، التي تفتح على وجه الخصوص "قدرات غير متماثلة واسعة النطاق لتقليل القدرة القتالية للعدو" وكان هذا واضح بشكل خاص في اعتماد روسيا على أمن المعلومات في عقيدتها الأمنية، ذلك بتوظيف أجهزة الدعاية بواسطة الفضاء الإعلامي والحرب المعلوماتية واسعة النطاق الذي ذهبت روسيا للعمل عليها في حربها على أوكرانيا، باستهداف نِقَاط الضعف للخصم وتجنب المواجهة العلنية حتى المراحل النهائية للصراع.

أما عن حديث الفقه العربي حول مشروعية الدفاع السيبراني فقد أقر جانب منهم بهذا الحق، على اعتباره أنه ليس استثناء جديد، بل يتفق مع أحكام ونصوص ميثاق الأمم المتحدة، حيث يعد جزءً من الاستثناء الوارد في نص المادة 51 من الميثاق حول جانب الدفاع عن النفس، لذا فإنّ مشروعيه هذا الحق تعد وفقاً لما أقروه من ضرورات حفظ الأمن والسلم الدوليين بصرف النَّظر عن وصف العمليات السيبرانية غير المتماثلة بأنها "قوة" أو هجوم مسلح.

وبحسب وجهة نظر هذا الرأي الذي برر مشروعية الحرب السيبرانية غير المتماثلة، إلى أن إقرار "حق الدفاع عن النفس" وفقاً للمادة 51 من الميثاق جاء في سياق عام ومطلق ولم يخصص، لذا يتوجب حق الدفاع عن النفس بالحرب السيبرانية بالطرق الذي تتفق مع مقاصد الأمم المتحدة وميثاقها. وهذا ما استندت إليه روسيا في حربها غير المتماثلة على أوكرانيا واستعمال حقها في الدفاع الشرعي عن نفسها، حيث استخدمت ذات الوصف – الدفاع الشرعي – في رسالة الرئيس الروسي فلاديمير بوتين إلى محكمة العدل الدولية لإثبات دفعها بعدم الاختصاص بنظر الدعوى الذي رفعتها أوكرانيا ضد روسيا، وأرفقت روسيا مع هذه الرسالة نسخه كاملة مع خطاب الرئيس الروسي (الذي أُذيعَ متلفزاً في 24 فبراير/ شباط 2022) إلى محكمة العدل الدولية، وكذلك أرفقت نسخة لمجلس الأمن؛ لإخطاره من منطلق الوفاء عند استخدام حقها الشرعي في الدفاع عن النفس وفقاً للمادة 51 من ميثاق الأمم المتحدة (United Nations Dag Library, 2022).

ثانياً: الفريق المعارض لمشروعية الحرب السيبرانية الروسية الأوكرانية غير المتماثلة

في الجانب الآخر هناك فريق كاد أن يجمع على عدم مشروعية الدفاع الشرعي للحرب السيبرانية الروسية الأوكرانية تأسيسا للمادة 51 من ميثاق الأمم المتحدة، التي يستوجب لممارسة حق الدفاع عن النفس ووقوع عدوان مسلح فعلي ووشيك، ومن ثم فلا يكفي الهجمات السيبرانية. حيث يرى أصحاب هذا الرأي أن هذا الحق منذ نشأة الأمم المتحدة حتى وقتنا هذا محصور في وجوبية وقوع اعتداء مسلح على إقليم الدولة، مستنداً إلى الممارسات الدولية منذ عام 1945 المقتصرة على حق الدفاع الشرعي عن النفس في حال وقوع أي اعتداء مسلح، ما يعني هنا من وجهة نظر أصحاب هذا الرأي أن الدفاع الشرعي للحرب السيبرانية عمل غير مشروع وفقاً لميثاق الأمم المتحدة.

حيث يعدّ ميثاق الأمم المتحدة أن الدفاع الشرعي للحرب السيبرانية غير مشروع، ذلك نظراً لمخالفته لنص المادة 51 من الميثاق، والدليل على ذلك حسب هذا الرأي أن التفسير العلمي لنص تلك المادة يستلزم ربطها بنص المادة 4/2 من الميثاق والمتضمنة مبدأ الامتناع عن استعمال القوة أو استخدامها ضد سلامة أراضي أية دولة أو استقلالها السياسي؛ تتخذ الأمم المتحدة إزاءها عملاً من أعمال المنع أو القمع، أو بأية طريقة أخرى.

ورداً على الرأي المؤيد للدفاع الشرعي للحرب السيبرانية ومشروعيتها، الذي لا يستوجب وقوع هجوم مسلح فعلياً، يثور تساؤل حول مدى وصف العمليات السيبرانية بأنها "قوة" بالمعنى المقصود في هذا الحظر الذي يُعطى المصطلح في سياقه وفي ضوء هدف الميثاق وغرضه، فكيف يمكن تشخيص ذلك دفاعاً وقائياً شرعيا؟.

بالرغم من أن المعنى العادي لمبدأ "القوة" واسع بشكل واضح بما يكفي ليشمل أشكال الإكراه المسلح وغير المسلح، فإن الغالبية العظمى من مؤيدي هذا الرأي يرون أن مصطلح "القوة" تأسياً للمادة 4/2 من ميثاق الأمم المتحدة مرادفًا عمليًا لـ "القوة المسلحة" أو "العسكرية"، وهذا لا يعني بالضرورة أن حظر القوة بين الدول يقتصر على استخدام الأسلحة الحركية، أو الكيميائية، أو البيولوجية، أو النووية. ووفقاً لمحكمة العدل الدولية، ينطبق الحظر على أي استخدام للقوة. لذا يرون أنه ليس من المثير للجدل نسبياً أن العمليات السيبرانية تندرج تحت الحظر المنصوص عليه في استعمال القوة بموجب المادة 4/2 من ميثاق الأمم المتحدة. فآثارها مماثلة لتلك الذي يحتمل أن تنجم عن لك الأسلحة الأخرى. ومن المؤكد أن هذا يشمل استخدام العمليات السيبرانية كأداة هجومية أو دفاعية مصممة للتسبب في وفاة أو إصابة الأشخاص أو تدمير أجهزتها الأمنية والمعلوماتية والمرافق والبنية

التحتية الحيوية للدولة، بصرف النظر عما إذا كان هذا التدمير ينطوي على ضرر مادي أو ضرر وظيفي أو مزيج من الاثنين معًا. ومن الأمثلة الواضحة على استخدام "القوة" بالمعنى المقصود في المادة 4/2 من الميثاق، عمليات التجسس السيبراني على أجهزة الدولة والعمليات السيبرانية التي تتلاعب استهداف أنظمة الحاسوب للتسبب في انهيار محطة للطاقة النووية، أو فتح بوابات سد فوق منطقة مكتظة بالسكان، أو تعطيل مراقبة الحركة الجوية في مطار مزدحم خلال الظروف الجوية السيئة، ولكل منها عواقب وخيمة محتملة من حيث الوفاة والإصابة والدمار، مما يبرر هذا النوع من الحروب انتهاكاً لنظام الميثاق (Melzer, 2011, p.7).

المطلب الثاني: الموقف الدولي والأممي من الحرب

في ضوء العرض السابق، أتضح أن الرأي الغالب في الفقه الدولي ذهب -كما سبق وأن بينَّا- إلى أن روسيا قد انتهكت مبدأ حظر استخدام القوة بحربها السيبرانية على أوكرانيا. وبفرض صحة ذلك، يثور التساؤل حول الموقف الدولي لمواجهة وردع الاستخدام غير المشروع للقوة، في ضوء مستجدات الحرب السيبرانية الروسية الأوكرانية غير المتماثلة.

فقد أدانت العديد من الدول الحرب الروسية غير المتماثلة ضد أوكرانيا، ووصفتها بالعدوان، ومن بينها ثلاث من الدول دائمة العضوية في مجلس الأمن. حيث قامت كلٍ من الولايات المتحدة الأمريكية والمملكة المتحدة وألمانيا وحلف شمال الأطلسي والاتحاد الأوروبي منذ اندلاع ذلك الحرب بتطبيق إجراءات عقابية شديدة على روسيا.

طرحت الولايات المتحدة الأمريكية في 25 فبراير/ شباط 2022 وألبانيا على مجلس الأمن للتصويت، مشروع قرار يُدين الحرب الروسية ضد أوكرانيا. وقد حظي هذا المشروع بدعم أغلبية 11 عضوًا في المجلس، فيما امتنعت الصين والهند والإمارات العربية المتحدة عن التصويت، وبموجب المشروع أيضا، فإن المجلس المكون من 15 عضوا كان سيستنكر، العدوان الروسي باعتباره انتهاكا للمادة 4/2 من ميثاق الأمم المتحدة، لكن في النهاية فشل اعتماد القرار بسبب استخدام حق النقض (الفيتو) من قبل روسيا (الأمم المتحدة 2022، United Nations, 2022). هذا بجانب ما اتخذته تلك الدول من حظر الرحلات الجوية الروسية، والعقوبات الاقتصادية، والطرد من نظام المال الدولي لجمعية الاتصالات المالية العالمية بين البنوك (سويفت) (Aladekomo, 2022, p.9). كذلك قامت أمريكا في 8 مارس/ آذار 2022، بفرض حظر على استيراد النفط الخام الروسي والغاز الطبيعي المسال والفحم، لإضعاف روسيا اقتصاديًا (Partington, 2022, p.9). وقد وُصفت العقوبات على روسيا بأنها الأكثر شمولًا على الإطلاق (Ukraine, 2022, p.9). كما توسعت أمريكا وحلفاؤها في نشر قوات سيبرانية لدعم وحماية دفاعات الشركاء. والأدهى، أن الحرب الروسية ضد أوكرانيا قد دفعت حلف الناتو إلى وضع المزيد من القوات في شرق أوروبا كما أدت إلى تحالف دول أخرى مع الناتو مثل السويد وفنلندا (Bildt, 2022). فضلاً عن اعتماد البرلمان الأوروبي في يونيو/ حزيران 2022 قراراً بشأن الأمن في الشراكة الشرقية (EaP) ودور سياسة الأمن والدفاع المشتركة، الذي يدعو الاتحاد الأوروبي إلى توسيع آليات الدعم لزيادة مشاركة دول (EaP) في المهام والعمليات المدنية والعسكرية لسياسة الأمن والدفاع المشتركة (CSDP) للدفاع ضد غزو عسكري سيبراني متعدد الأبعاد، ذلك بوضع استراتيجيات منسقة وشاملة لتعزيز الدفاعات ضد مجموعة من الهجمات السيبرانية المدمرة. ذلك في إطار مشروع التعاون المنظم الدائم PESCO - الذي يعد جزءً من سياسة الأمن والدفاع للاتحاد الأوروبي- لفرق الاستجابة السريعة السيبرانية والمساعدة المتبادلة في الأمن السيبراني (CRRTs)، يستطيع الاتحاد الأوروبي تجميع قدرات الأمن السيبراني للدول الأعضاء وتقديم الدعم عند الطلب. وذلك ما قام به الاتحاد الأوروبي بتنشيط فرق CRRT الخاصة به لدعم الدفاع السيبراني لأوكرانيا أول مرة في سياق عملياتي، وذلك بعد طلب من الحكومة الأوكرانية قبل أسبوع من الغزو في فبراير/ شباط 2022 (Duguin, 2023, p.15, p.16).

وفي 30 سبتمبر/ أيلول 2022، تقدمت مرة أخرى الولايات المتحدة وألبانيا بمشروع قرار لمجلس الأمن لإدانة الضم غير القانوني لمناطق أوكرانية معينة (دونيتسك، ولوغانسك، وخيرسون، وزابوريجيا)، بعد تنظيم الاستفتاءات التي أجريت في 23 و27 سبتمبر/ أيلول 2022، وقد تم التصويت على مشروع القرار بالرفض بسبب استخدام روسيا لحق الفيتو، وذلك بعدما صرح المندوب الدائم لروسيا في الأمم المتحدة حينها: "إن سكان هذه المناطق لا يريدون العودة إلى أوكرانيا وكان خيارهم مستنيرا وحراً" (الأمم المتحدة، 2022).

كما انتقدت النرويج حق النقض (الفيتو) في مجلس الأمن وصرحت: «إن استخدام حق النقض من قبل المعتدي يقوض الغرض من الميثاق. حيث يعد انتهاك لأساس ميثاق الأمم المتحدة ذاته. إضافةً إلى ذلك - بروح ميثاق الأمم المتحدة - كان يجب على روسيا أن تمتنع عن التصويت على مشروع القرار لكونها طرفًا في النزاع» (Security Council, 2022).

من جهة أخرى تقدمت روسيا في 2 نوفمبر/ تشرين الثاني 2022، بمشروع قرار إلى مجلس الأمن يهدف إلى إجراء تحقيق بتفويض من مجلس الأمن بشأن حيازة أوكرانيا أسلحة بيولوجية، وذلك استنادًا إلى المادة السادسة من اتفاقية الأسلحة البيولوجية لعام 1972 التي تحظر استحداث وإنتاج ونقل وتخزين وحيازة واستخدام الأسلحة البيولوجية والتكسينية. وقد فشل تبني القرار بسبب (حق الفيتو) من ثلاث دول هي الولايات المتحدة الأمريكية وفرنسا والمملكة المتحدة، وامتناع 10 دول عن التصويت، فيما صوت لصالح القرار روسيا والصين خلال جلسة مجلس الأمن الدولي المنعُقدة ضمن جدول أعمال "الأخطار التي تهدد السلام والأمن الدوليين" (الأمم المتحدة، 2022).

بهذا الشكل، فإن مجلس الأمن قد فشل في اتخاذ القرارات اللازمة في المسائل المتعلقة بدوره الرئيس في حفظ السلم والأمن الدوليين نتيجة لاستخدام حق الاعتراض (الفيتو) من قبل كافة الأعضاء الدائمين في مجلس الأمن -باستثناء الصين- مما أدى إلى تدخل الدول لسد هذا النقص، ولكن هذا التدخل يعوزه بشكل كبير الأساس القانوني. فمن ناحية، لا يُمكن أن تُترك ضحية الحرب غير المتماثلة دون موقف من قبل الدول، في ظل غياب دور واضح لمجلس الأمن. ومن ناحية أخرى لا يمكن إطلاق دور الدول في دعم أحد أطراف النزاع دون تحديد تصنيف وشرعية هذا الحرب السيبرانية غير المتماثلة، خاصة مع غياب الأساس القانوني مما جعلها حرباً فريدة من نوعها ومعقدة للغاية تجمع بين حروب الجيل الخامس الذي يشمل الحروب السيبرانية، والعمل العسكري الحركي.

المبحث الثالث: ديناميكية تطور استراتيجية الحرب السيبرانية الروسية الأوكرانية وتداعياتها على العلاقات الدولية

يشير جل المتخصصين في العلاقات الدولية والمُنظرين في مجال الاستراتيجيات، إلى أن الطبيعة الديناميكية التي تتسم بها استراتيجية حروب اليوم المعاصرة أصبحت حروبا هجينة غير متماثلة، تلعب الأدوات والفضاء السيبراني فيها دورا رئيساً. فمع ظهور أنماط جديدة من هذه الحروب أصبحت "استراتيجية الحرب السيبرانية" تتصف بقدر كبير من التطور المتلاحق والمتسارع والمنافسة البالغة غير المتماثلة؛ تنبع من دوافع وعوامل تسوق الدول لتبني هذا النوع من الاستراتيجيات المستحدثة في مجال السياسة الخارجية.

المطلب الأول: استراتيجية الحرب السيبرانية الروسية الأوكرانية غير المتماثلة

تمثل روسيا ثقل إستراتيجي سيبراني عالمي نظراً لتفوقها في مجال الاتصالات والاستخبارات السيبرانية وردع الفيروسات المضادة، حيث تتبوأ وكالة "زيكوريون" للاستشارات الأمنية وتحليل المعلومات، ومقرها موسكو المرتبة الأولى كواحدة من أفضل خمسة جيوش سيبرانية في العالم في خدمات وأعمال القرصنة (فتحي، 2019، ص6). بذلك تعد روسيا من الدول الأوائل التي استخدمت الفضاء السيبراني في مجال استراتيجياتها العسكرية، وارتكزت على الاهتمام بالبحث والتطوير لتضاعف قدراتها الهجومية في هذا المجال، خلفاً عن السلاح النووي بتكلفة أقل ولا يتطلب إلى حدود جغرافية معينة، على عكس ما تحتاج إليه الحروب التقليدية العسكرية من قوة مادية بالغة التكلفة. ويمكن الاستشهاد بذلك في الحرب السيبرانية الروسية الأوكرانية، التي يمكن تسميتها باستراتيجية "حرب الظل": فما هي الطبيعة الديناميكية لهذه الاستراتيجية السيبرانية، وما هي الأدوات الحديثة التي انتهجتها روسيا بطرق غير مباشرة وغير متماثلة لتنشأ في مجملها حربا سيبرانية تؤجج الصراع بين موسكو وكييف؟.

أولاً: دلالات تطور استراتيجية الحرب السيبرانية الروسية

تتبلور العقيدة الاستراتيجية للحرب السيبرانية الروسية من وثيقة وزارة الدفاع الروسية الصادرة باسم (مفهوم الأنشطة الفضائية السيبرانية المعلوماتية للقوات المسلحة الروسية) لتظهر الحيز الهام الذي تمثله السيبرانية المعلوماتية في السياق الاستراتيجي الروسي، حيث اعتمدت روسيا على عقيدة الأمن السيبراني للمعلومات في استراتيجيتها، وأكدت الوثيقة على البعد العسكري لمسألة المعلومات كأساس لأمن الدولة، وتحدد الأسلحة السيبرانية باعتبارها إحدى الأدوات البارزة لتحقيق الأهداف السياسية (فتحي، 2019، ص4-6). إذ تستهدف روسيا من جرّاءِ توظيفها النسبي لاستراتيجية الحرب السيبرانية عدة أهداف، تدور مضامينها حول الآتي:

1. **خلق بنية متسامحة والتأثير في الرأي العام:** حيث تستهدف الحرب السيبرانية خلق بنية متسامحة تجاه المصالح والرؤية الروسية، ويُجرى ذلك بواسطة وسائل الإعلام الجماهيري والاجتماعي لإحداث تأثير في توجهات وآراء الجماهير العادية، مما يجعلهم أكثر تقبلاً وتسامحاً مع الرؤية الرسمية لروسيا، ومن ثم تخفيف حدة الصراع لسياسة روسيا تجاه الحرب الأوكرانية (ساثر، 2017، ص14).
2. **تقويض الثقة والقدرة على المواجهة:** فالعديد من عمليات الحرب السيبرانية الروسية، ولا سيما المتعلقة بالقرصنة الرقمية التي تضعف من إمكانات الخصم وقدرته على المواجهة، وهو ما يظهر بشكل جلي في الحرب الروسية الأوكرانية. حيث إن الاختراقات السيبرانية الروسية تستهدف ما أبعد من ساحة المعركة، ذلك باستهدافها للمنشآت الحيوية الأوكرانية. إذ تسعى جاهدة إلى إضعاف الثقة في كييف وخلق شعور بفقد السيطرة، بما يحشد المواطنين الأوكرانيين على الدولة لفشلها في حماية بنيتها المجتمعية، ومن ثم زعزعة استقرار الحكومة التي يؤدي إلى انهيار وسقوط متكامل يتيح لموسكو السيطرة على كييف أو الضغط عليها وتقديم تنازلات (علي، 2024).
3. **حرب السرديات وتشويه القوى المناهضة:** حيث وظفت روسيا استخدامها للفضاء السيبراني بشن "حرب السرديات" لتشويه الخصم، وفي الوقت نفسه تكوين صور إيجابية لحلفائها. إذ ترتكز على استنزاف الثقة العالمية في أوكرانيا باستخدام الدعاية الإعلامية والرقمية، والترويج لمقولات "الثورات الملونة" التي شهدتها أوكرانيا، وكانت نتاجاً لجماعة من المحرضين المدعومين من الخارج من أجل إخراج أوكرانيا من المدار الروسي. وتتضمن هذه الأدوات والأساليب التي انتهجتها روسيا في تلك الاستراتيجية؛ إنشاء حسابات وهمية على صفحات وسائل التواصل الاجتماعي، لاستهداف المحتوى، ذلك باستخدام مجموعات من المؤثرين الفريدين في تغيير الأحداث والمواقف العامة.
4. **الحرب النفسية والخداع الاستراتيجي:** سعت روسيا في استراتيجية حربها السيبرانية إلى حملة التضليل، ونشر معلومات مضللة ضد أوكرانيا لتقويض الدعم الدولي لها، ذلك لتشكيل مواقف دول الجنوب العالمي إزاء الحرب، وإن كان ذلك لا يؤدي دوراً حاسماً حتى في أثناء القتال المكثف (علي، 2024).

5. **إثارة المشكلات الداخلية**: حيث توحي الحرب السيبرانية الروسية على الترسيخ لقضايا داخلية وأوضاع متأزمة في أوكرانيا تتضمن دلالات سلبية في المجتمع الأوكراني، ذلك في محاولة منها بممارسة الضغط على الحكومة الأوكرانية.

6. **مواجهة العقوبات الغربية الأمريكية والإخلال بمعادلة الدعم الغربي الأمريكي لأوكرانيا:** فحينما تبنت الدول الأوروأمريكية آلية للعقوبات القسرية ضد روسيا، قامت روسيا بدمج وتوظيف التأثيرات السيبرانية (الرقمية) والتقليدية (العسكرية) في ميدان المعركة وخارجها، ذلك بإحداث موجة من الهجمات الردعية السيبرانية ضد البنية التحتية الحيوية الأوروأمريكية، واستغلال الدعاية الرقمية المضللة والمؤثرة، للتقليل من الدعم الأوروأمريكي للحرب في أوكرانيا.

ثانياً: البنى التأثيرية في استراتيجية الحرب السيبرانية الروسية

تندرج مجالات القوة والتفوق الروسي نحو التأثير الكبير للدعاية الرقمية الروسية فضلاً عن عمق التأثير للحرب السيبرانية العسكرية لاعتبارات استراتيجية تتعلق بتفوق الروس في منظومات التشويش والتضليل العسكري الممنهج، فضلا عن القوة الردعية الروسية في خلق الفيروسات ومنع الاختراقات المضادة، كذلك الإمكانات العالية في مجال الاستخبارات والاختراق السيبراني. لذا يمكن تحديد الوسائل الارتكازية للتأثير في العقيد الاستراتيجية للحرب السيبرانية الروسية بالآتي (فتحي، 2019، ص6-7):

1. التجسس والاستخبارات السيبرانية.
2. الهجمات السيبرانية، التي تسبب أذى البنية التحتية لأوكرانيا.
3. حروب المعلوماتية في وسائل الإعلام وشبكات التواصل الاجتماعي.

ثالثاً: البنى العقائدية لاستراتيجية الحرب السيبرانية الروسية

ينظر منظرو الفكر الاستراتيجي السيبراني على أن الاندفاع والانغماس السيبراني ينبع من عقيدة روسيا الاستراتيجية للحرب السيبرانية، التي تتمثل في كيفية استخدام قدرات الاتصال بالإنترنت وتنظيم الوسائل الرقمية من أجل مضاعفة الجهد الحربي التقني، ذلك من أجل تعضيد النهج الاستراتيجي الروسي للحرب السيبرانية، ومعالجتها سواء من حيث نظريته أو أسسه العملية. فالسيبرانية الهجومية والدفاعية تلعب دوراً هاماً وكبيراً في عقيدة الجيش الروسي التقليدي، وربما تلعب دوراً في المستقبل في استراتيجية روسيا التي يطلق عليها "إطار الردع"، مع أنّ الجيش الروسي كان بدايةً بطيئاً في احتضان السيبرانية لأسباب استراتيجية وهيكلية وعقائدية على حد سواء (فتحي، 2019، ص7، 8). لكن تجارب الحرب في أوكرانيا أتاحت فرصة كبيرة لروسيا من أجل ثقل وتعديل استراتيجيتها وتكتيكاتها السيبرانية، من أجل تعضيد القوة العسكرية التقليدية خصوصاً في الجناح الشرقي لأوروبا، وإعادة التموضع وخفض مستوى الإخفاقات في مجال الحرب السيبرانية غير المتماثلة، وصولاً إلى إثبات ذاتها وقدراتها على الساحة العالمية واسترجاع استراتيجية الذات الروسية المفتقدة.

وهذا ما أوضحته دلائل ومؤشرات استخدام روسيا للعمليات السيبرانية لمداهمة مواقع أوكرانية، والتشويش على مواقع القيادة وتعطيلها، والسيطرة منذ بدء الحرب بنشر روسيا لبرامج ضارة عطلت نظام الأقمار الاصطناعية وأدت إلى انقطاع أكثر من 30 ألف اتصال بالإنترنت مؤقتاً في جميع أنحاء أوروبا، بما في ذلك 5 آلاف توربينة رياح، إلى جانب أنه ومنذ بدء الحرب وردت تقارير عن اكتشاف برامج ضارة في البنية التحتية الحيوية في البلدان التي تدعم أوكرانيا بمساعدة عسكرية أجنبية. ففي الولايات المتحدة الأمريكية تم اكتشاف برامج روسية ضارة في البنية التحتية الحيوية المرتبطة بتوليد وتوفير الكهرباء في وقت مبكر من الصراع، وفي المملكة المتحدة أضحت هناك تخوفات من مساعي روسيا المتزايدة لاستهداف البنية التحتية الحيوية منذ بدء الحرب في أوكرانيا (علي، 2024). مما بات بمثابة أساس تترابط فيه مفردات استراتيجية روسيا للحرب غير المتماثلة وتتفاعل عوامل ديناميكيتها فوق المستوى الذي يكفل لإشارة أو ردع أوكرانيا وخصوم روسيا.

رابعاً: استراتيجية الردع السيبراني الأوكراني

تجلَّى في حرب الشبكات السيبرانية غير المتماثلة بين روسيا وأوكرانيا مفهوم استراتيجية الردع السيبراني. حيث قامت استراتيجية الردع الموجَّه ضد روسيا على أربع دعائم رئيسة: أولًا- تطوير أوكرانيا لبنيتها التحتية السيبرانية الأمنية. وثانيًا- التحالف الدولي الأمني السيبراني لمعسكر الغرب ومن ضمنهم أوكرانيا. وثالثاً- التحالف والتعاون الوثيق بين القطاعَيْن الحكومي والخاص من جهة، والتحالف مع منظمات دولية من جهة أخرى. رابعاً وأخيرًا: الردع والهجوم السيبراني المضاد.

وقد برعت أوكرانيا في إنشاء جيش "أوكرانيا السيبراني" يتبنى تكتيكات حروب القرصنة الناعمة بتركيزها على الدعاية والتأثير الإعلامي والجماهيري، لتعزيز قدرات الدفاع الذاتية. حيث وظَّفت هذه التكتيكات في دعم وتعزيز سرديتها عن الحرب من جهة، وبثِّ روح العزيمة والصمود في الحاضنة الأوكرانية من جهة أخرى. وكان ذلك واضحًا خلال الدخول الكثيف للرئيس الأوكراني على خطِّ هذه التكتيكات بواسطة الفيديوهات التي كان يخرج بها على شعبه بشكل مباشر من شوارع العاصمة "كييف" عبر تطبيقات منصات التواصل الاجتماعي. هذا فضلاً عن عدد المتطوعين السيبرانيين الذي أبدوا استعدادهم للإسهام في تنفيذ هجماتٍ سيبرانية نيابةً عن الجانب الأوكراني (عودة، 2022، ص 5-6).

من هنا أثبت النموذج الأوكراني على أن الردع والدفاع في عصر السيبرانية لا يقتصران على إنشاء أقوى الأنظمة والجيوش، وإنما القدرة والمرونة على الاندماج في أنظمة أخرى، وكذلك التأثير الدولي. وللتدليل على الاندماج والتأثير من قبل النموذج الأوكراني، فقد تمَّ توقيع اتفاقية بين دائرة الأرشيف الحكومية في أوكرانيا والأرشيف الوطني للمملكة المتحدة بشأن النقل المؤقت لقاعدة البيانات السحابية والنسخ الاحتياطية للمواد الرقمية لمؤسسات الأرشفة الحكومية الأوكرانية في حالة فقدانها المحتمل جراء هجمات سيبرانية روسية عبر أسلوب الفيروسات الماسحة Wiper Malware (عودة، 2022، ص 5-6). وعن اندماج الأنظمة لخلق شبكة معقدة يصعب اختراقها أو تعطيلها؛ فقد تم نشر فريق الاستجابة السيبرانية السريع التابع للاتحاد الأوروبي وترأسه ليتوانيا، للمساعدة في تعزيز الدفاعات الأوكرانية ضد الهجمات السيبرانية الروسية، باكتشاف مجموعة متنوعة من التهديدات الروسية والاستجابة لها. كما وقَّع حلف شمال الأطلسي (الناتو) قبيل الغزو الروسي اتفاقيةً تعاون مشترك مع أوكرانيا وقبولها كمشارك مساهم في مركز التميز للدفاع السيبراني التعاوني؛ بهدف تعزيز التعاون السيبراني مع أوكرانيا، وتعزيز قدراتها ودفاعاتها السيبرانية. في حين أطلقت وكالة الأمن السيبراني الوطنية في رومانيا وشركة أمن سيبراني تسمى Bitdefender شراكةً بين القطاعَيْن العام والخاص لتقديم الدعم الفني والاستخباراتي المجاني للحكومة والمواطنين والشركات الخاصة في أوكرانيا "طالما كان ذلك ضرورياً. لقد كان للتعاون والاندماج بين القطاعين الخاص والعام أثر واضح في تعزيز المرونة السيبرانية. فمركز استخبارات التهديدات التابعة لشركة ميكروسوفت كان على أهبة الاستعداد والتواصل الدائم مع المسؤولين في البيت الأبيض والمسؤولين الأوكرانيين، وأسهم في رصد فيروس Foxblade، وقبل ذلك فيروس WhisperGate. ومن جانبها، أسهمت شركة الأمن السيبراني ESET، ومقرها سلوفاكيا، في الكشف عن الشفرة الضارة لفيروس HermeticWiper في الأيام الأولى للغزو الروسي(Hakmeh, 2022). أما شركة إيلون ماسك ومن خلال خدمة الإنترنت الفضائي Starlink، فقد استطاعت الإبقاء على أوكرانيا متصلة بشبكة الإنترنت معظم الوقت (Lerman, 2022).

المطلب الثاني: تداعيات الحرب السيبرانية غير المتماثلة على العلاقات الدولية:

أردفت الحرب السيبرانية الروسية الأوكرانية غير المتماثلة مدخلاً مستحدثاً في العلاقات الدولية، تحديداً في حقل الاستراتيجيات العسكرية والحربية، حيث بات هناك نوع من الحرب الهجينة الخفية أو ما يطلق عليها "حرب الظل"، تشنها الدول فيما بينها. وقد أدى ازدياد عِلاقة الدول بالفضاء السيبراني أو الرقمي، وما أعقبته هذا الحرب إلى مجموعة من التهديدات والتداعيات على تفاعلات العلاقات الدولية، من أبرزها:

1. **تفاقم التهديدات والمخاطر السيبرانية:** تحديداً مع استعداد المنشآت والأجهزة الحيوية سواء العسكرية أو المدنية في الدول للهجمات السيبرانية عليها عن طريق وكيل، أو تعطيل أنظمتها الرقمية والمعلوماتية، ما من شأنه التأثير في قيام تلك المنشآت بوظائفها في التحكم في تنفيذ تلك الهجمات، التي تعد أداة بالغة الأهمية في السيطرة الاستراتيجية، سواء أكان في وقت الحرب أو وقت السلم (عبدالصادق، 2016، ص 22-26).

2. **تعزيز القوة السيبرانية المؤسسية وانتشارها:** حيث عززت الحرب السيبراني الروسية الأوكرانية غير المتماثلة الفضاء السيبراني ما يُسمي بـ "القوة السيبرانية المؤسسية" في العلاقات الدولية، وتعني أن يصبح لها دور فعال في قوة الفاعلين الدوليين وغير الدوليين وتحقيق قيمهم وأهدافهم، في ضوء التنافسية والتسابق العالمي، الذي يؤثر إلى حد بعيد في تشكيل السياسة والعالمية (Held, 1999, p.85, p.88). لذلك فإن سهولة الحصول على تلك القوة السيبرانية أدت إلى ما يطلق عليه بإعادة تشكيل قدرة الأطراف المؤثرة ونشر القوة، وفقاً لانتقالها من التركز في أيدي الدول الكبرى؛ لتتوزع بين أكبر عدد من الفاعلين الدوليين من الدول المتوسطة والصغيرة، وكذلك الفاعلين غير الدوليين، مما يعني ذلك ضعف سيطرة الدولة وارتفاع حجم التهديدات التي تواجه النظام الدولي، حينما أزداد قدرة الفاعلين الأصغر في السياسة والعلاقات الدولية على ممارسة كل من القوة الصلبة والقوة الناعمة في استغلال الفضاء السيبراني (عبد العزيز، 2017، ص16). كالحالة الأوكرانية في مواجهة العمليات السيبرانية الروسية وتخصيص جهودها لبنيتها التحتية الرقمية بما يعزز من استمرارية الحكومة خلال ذلك الحرب الدائرة.

3. **عسكرة الفضاء السيبراني:** لردع تهديداته ومخاطره على أمن الفضاء السيبراني، وبرزت في ضوء هذا النطاق اتجاهات عدة، أهمها التوسع والاستحداث في السياسات الدفاعية والأمنية السيبرانية، وتعزيز القدرات في سباق التسلح السيبراني، وانتهاج الدول في أجهزتها الدفاعية الأمنية سياسات دفاعية سيبرانية، وتزايد الاستثمار في نطاق تطوير استراتيجية وأدوات الحرب السيبرانية داخل الجيوش التكنولوجية والرقمية الحديثة، وزيادة الإنفاق على الأمن السيبراني منها روسيا، والولايات المتحدة الأمريكية وغيرهما من الدول الأخرى.

4. **تحديث القدرات العسكرية الدفاعية والهجومية:** حيث سعت الدول جاهدة إلى تحسين العمليات الدفاعية وتحديثها، لمجابهة تهديدات ومخاطر الحرب السيبرانية غير المتماثلة، والاستثمار في البنية التحتية الرقمية، وتأمينها، وتطوير القدرات العسكرية، وتعزيز الجاهزية لذلك الحرب ورفع كفاءتها عن طريق التدريب، والمشاركة الدولية في حماية الأمن السيبراني والبنية الرقمية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الأمنية والوطنية المختصة. وهنا يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استغلال تلك الهجمات السيبرانية في سياق إدارة الصراع والتوتر مع دول أخرى (عبدالصادق، 2012، ص 30).

5. **دمج الفضاء السيبراني وإدراجه ضمن الأمن القومي للدول:** ذلك باستحداث وتحسين الجيوش والاستراتيجيات الأمنية والحربية، وإطلاق وحدات مختصة فقط بالحروب السيبرانية، وإنشاء هيئات وأجهزة قومية متخصصة في الدفاع والهجمات السيبرانية، والعمل على التدريبات اللازمة

لتلك الهجمات، وإجراء المناورات لتكريس الدفاعات السيبرانية وتعزيز قدراتها، والعمل على توطيد العلاقات الدولية والتعاون الدولي في سياق أمن الفضاء السيبراني لارتباطه بالأمن القومي لأغلب الدول، والعمل على تدشين مشروعات دولية ووطنية للأمن السيبراني في الدول.

6. **الاستعداد لحروب المستقبل:** حيث تبنت روسيا والولايات المتحدة والعديد من الدول استراتيجية الحرب السيبرانية، بحسبانها حربا للمستقبل تأتي في مقدمة الصفوف الأولى كأخطر التهديدات وأكبرها، التي تؤثر بشكل جلي على سلامة وأمن الفضاء السيبراني، ويتم شنها لتشتيت، وإثارة الاضطرابات لدى الخصم، عبر اختراق أجهزتهم وأنظمتهم، واستهداف الأنظمة العسكرية "غير المتصلة بالإنترنت" جزئيا، بواسطة تسخير التكنولوجيا الناشئة التي تستخدم إشارات الراديو لإدخال تشفير الكمبيوتر في الشبكات عن بعد واستخدامها في نقل معلوماتهم، للتأثير على عملية صنع القرار لدى الخصم. وهنا، تري الدول الكبري - من أبرزها الولايات المتحدة الأمريكية - أن من يحدد مصير تلك الحروب المستقبلية ليس فقط من يملك القوة، وإنما الذي لديه القدرة على إضعاف القوة، واختراق المعلومة والتشويش عليها (Nakashima, 2012).

وتفسيراً لما تم طرحه من تلك التداعيات، أوضحت الدراسة أن الحرب السيبرانية غير المتماثلة باتت من الحروب الأكبر مخاطراً وانتشاراً اليوم، والأكثر تهديداً للأمن القومي والعلاقات الدولية. فالمجتمع الدولي لا يملك القدرة السريعة على التدخل لاحتوائها مثل حالة الحروب التقليدية، وليس هناك مجال لتفعيل آلية المراقبة والتفتيش كحالة التفتيش النووي. لذا ستبقى معضلة دخول العالم سباق التسلح السيبراني A Cyber Arms Race في ترسيم طبيعة وفحوى ذلك النوع الجديد من الأسلحة التي يمتلكها الغير، قائمة وأصبحت واقعاً يشكل خطراً يهدد الأمن القومي للدول والعلاقات الدولية فيما بينهم.

الخاتمة

بعد الدراسة والاستقراء، وللإجابة على التساؤل الرئيس للدراسة وتساؤلاتها الفرعية، توصلت الدراسة إلى مجموعة متباينة من النتائج والتوصيات يمكن بلورتها على النحو الآتي:

أولاً: النتائج

لقد توصلت الدراسة إلى مجموعة من النتائج من واقع الإشكالية الرئيسة التي تم طرحها للتأكد من صحة فروض الدراسة، ومن ثم تحقيق الأهداف المرجوة، حيث تمخضت النتائج في التالي:

1. من أبرز النتائج الأساسية التي أتت بها الدراسة في المحور الأول **"الحرب السيبرانية وعدم الامتثال ومقاربتهما النظرية بين المفهوم والأبعاد":** هي أنه بالرغم ما كشفت عنه الدراسة من الافتقار إلى الوضوح التعريفي للحرب السيبرانية وعدم الامتثال، حيث إن ليس ثمة اتفاق بين المنشغلين من المتخصصين والأكاديميين بمجال العلاقات الدولية، حول تعريف واحد شامل لاستراتيجيات الحرب السيبرانية غير المتماثلة، كذلك الأمر لاستراتيجيات عدم الامتثال أن هنالك خلطاً كبيراً بين استراتيجيات عدم الامتثال (بدلالة الحرب السيبرانية) والاستراتيجيات الأخرى. إلا أن أدبيات العلاقات الدولية أوضحت بأن النظريات الواقعية الجديدة تعدّ الأكثر قابلية للتطبيق على القضايا المتعلقة بالحرب السيبرانية، إذ جاءت هذه المفاهيم لتوضح أن الحرب السيبرانية مثال لعدم التماثل في القوة بصرف النظر عن كيفية تعاريفها وتوضيح أبعادها وجوانبها.

أيضاً، ومن واقع النظرية الواقعية في العلاقات الدولية خلصت الدراسة، إلى أنه ثمة العديد من الأشكال والأنماط لاستراتيجية الحرب السيبرانية غير المتماثلة في مجال العلاقات الدولية، وبالرغم من تباين أنماط هذه الاستراتيجية وتنوعها وتعدد ضروبها وبواعث ديناميكيتها، غير إنه يجمعها قاسم واحد مشترك ألا وهو خاصية الطبيعة الديناميكية، التي قد تمخض عنها ظهور ما يسمى بـ"عصر القوة النسبية" التي أشارت إلى أن "القوة العسكرية" وحدها ليست بكافية في تأمين البنية التحتية الحيوية للدول، مما يتعاقب عنها آثاراً استراتيجية بالغة على مدى بنية وتركيبة النظام العالمي الجديد وتوازناته الدولية.

2. أما المحور الثاني **"الموقف الدولي وتحليل مشروعية الحرب السيبرانية الروسية الأوكرانية غير المتماثلة":** فقد كشفت الدراسة بأن هناك خلاف بين ما تحققه الحرب السيبرانية الروسية الأوكرانية غير المتماثلة من انتصارات لمستخدمها، وبين تحديد تصنيف مشروعية هذه الحرب أو عدم مشروعيتها. حيث أظهرت الدراسة عجز النظام الدولي وعدم توازنه في التعامل مع هذا النوع من الحروب الجديدة، خاصةً في ظل غياب الأساس القانوني لها وعدم وجود اتفاق دولي على تصنيفها وتحديد شرعيتها وتكييفها القانوني، فهي لا زالت شرعيتها غير محسومة إن كانت تقع تحت الصراع المسلح "العسكري" أو غير المسلح، لذا تعد ذلك الحرب فريدة من نوعها ومعقدة للغاية تجمع بين حروب الجيل الخامس التي تشمل الحروب السيبرانية، والعمل العسكري الحركي. ففي ظل تلك الانقسامات الرئيسة للواقعية الجديدة وما قدمته من تفسيرات مختلفة لنوايا الدول وتفاعلاتها حول تصنيف مشروعية ذلك الحرب وعدم وجود غطاء شرعي لها حتى وقتنا هذا، التي كشفت عن نظام دولي يسوده الفوضوية. تستنتج الدراسة أن الواقعية ليست كافية في حد ذاتها لفهم أو شرح الظاهرة التجريبية الجديدة للحرب السيبرانية الروسية الأوكرانية.

3. بينما كشفت الدراسة في المحور الثالث والأخير **"ديناميكية تطور استراتيجية الحرب السيبرانية الأوكرانية غير المتماثلة، وتداعياتها على**

العلاقات الدولية": أن هناك اختلاف في توظيف القوة السيبرانية الروسية عن توظيف القوة الردعية الأوكرانية؛ حيث سعت فلسفة روسيا في صلب استراتيجيتها الشاملة لاستخدام القوة الناعمة في حربها السيبرانية ضد أوكرانيا، والقوة الصلبة في الهجمات السيبرانية والعسكرية واستهداف البنية التحتية الحيوية لأوكرانيا. بينما ركزت أوكرانيا في القوة الناعمة فقط، انطلاقًا من استراتيجية الردع السيبراني الموجَّهة ضد روسيا، وتبنيها لتكتيكات حروب القرصنة الناعمة وتوظيفها في دعم سرديتها عن الحرب، وتعزيز قدراتها الدفاعية الذاتية في التأثير الدولي والجماهيري.

لذا فأن ديناميكية تطور استراتيجية الحرب السيبرانية الروسية الأوكرانية غير المتماثلة، ترتب عليها مزج بين (القوة الناعمة، والقوة الصلبة) في عملية توظيف القدرات السيبرانية والتفاعلات في الفضاء المعلوماتي، باعتبارها الأداة الأمثل في رسم استراتيجية "الحرب السيبرانية غير المتماثلة" أو ما يطلق عليها بـ"استراتيجية حرب الظل" كاستراتيجية جديدة، مما أثرت تداعياتها على العلاقات الدولية والتفاعلات السياسية، حيث تعد من الحروب الأكبر مخاطراً وانتشاراً، التي لا يملك المجتمع الدولي القدرة السريعة على التدخل لاحتوائها مثل حالة الحروب التقليدية، مما أصبحت واقعاً يشكل خطراً يهدد الأمن الدولي والعلاقات الدولية.

ثانياً: التوصيات

بناءَ على ما تقدم يمكن للدراسة اقتراح مجموعة من التوصيات تتمثل في:

1. وضع إطار معياري للواقعية الجديد يوفر خط أساس واضح في الاتفاق على تحديد تعريف شامل لمفهوم الحرب السيبرانية وعدم الامتثال يتبناهم المجتمع والنظام الدولي، ويخضع للتغيرات بمرور الوقت وفي ظل التطورات الحديثة، مما تضيف أوجه تناسق جديدة للعديد من أبعادها وأنماطها.

2. العمل على تحديث الأمم المتحدة من أجل مواكبة التطورات الدولية في ظل الثورة المعلوماتية والتكنولوجية، خاصة تفعيل المواد والنصوص المرتبطة باختصاصات وصلاحيات الأمم المتحدة في الشأن الخاص بتكوين "جيش دولي للأمن السيبراني" قادر علي ردع الدول المعتدية ودرئها على اختراق سيادة الدول الأخرى واختراق بنيتها الحيوية، كذلك تحديث مجلس الأمن الدولي على وجه الأخص، حتى يتخلص من سطوة وهيمنة حق النقض "الفيتو" للدول الدائمة العضوية التي تسعى في المقام الأول والأخير البحث عن مطامعها ومصالحها الخاصة.

3. العمل على تفعيل الدور القانوني على المستوى الدولي، ذلك بصياغة المنظمات الإقليمية والدولية آليات وقواعد تتناسب مع هذا النوع من الحروب الحديثة، وتتواكب مع تطوراتها التكنولوجية والرقمية السريعة والمتلاحقة، والعمل على تكثيف الجهود الدولية لسن مواد ونصوص قانونية تنص صراحةً في ميثاقها على أطر قانونية واضحة ومحددة، تكون بمثابة قاعدة قانونية لها قوة الإلزامية في تحديد العقوبات الحاسمة على استغلال الفضاء الجديد واستعماله في شن هجمات سيبرانية متعددة تهدد الأمن الوطني والدولي، وأيضا التعامل مع التحديات التي تفرضها تلك الهجمات غير المتماثلة على الساحة الدولية.

4. خلق بيئة دولية سيبرانية آمنة، بجهود دولية تسعى إلى العمل على رسم استراتيجية دولية خاصة بمنظومة الأمن السيبراني، تعتمد نهج متكامل نحو كيفية التأهب والجاهزية لسيناريوهات الاستخدام المحدود للإنترنت في حال الهجمات السيبرانية، مما تكون لديها القدرة على الجاهزية الاستباقية والمواجهة الرادعة للهجمات السيبرانية. هذا بالإضافة إلى اتخاذ التدابير الأمنية وأنظمة الحماية اللازمة للحد من الهجمات والاختراقات السيبرانية المدمرة للمنشآت والبنية التحتية الحيوية للدول، ذلك للحيلولة دون قيام حرب سيبرانية عالمية غير متماثلة وشاملة كما هو واضحا وظاهراً في الحرب الروسية الأوكرانية اليوم.

الشكروالتقدير

«تتقدم الباحثة بخالص الشكر والتقدير على الدعم المقدم لهذا المشروع من قبل عمادة البحث العلمي، وكالة الجامعة للدراسات العليا والبحث العلمي، جامعة الملك فيصل، المملكة العربية السعودية (رقم المنحة: KFU242787)».

المصادر والمراجع

الأمم المتحدة. (2022). الفيتو الروسي يحول دون تمرير مشروع قرار حول الوضع في أوكرانيا. *أخبار الأمم المتحدة*، https://news.un.org/ar/story/2022/02/1095042.

الأمم المتحدة. (2022). أوكرانيا: الجمعية العامة تطالب روسيا بعكس مسار "الضم غير القانوني" للمناطق الأوكرانية. *أخبار الأمم المتحدة*، https://news.un.org/ar/story/2022/10/1113922.

الأمم المتحدة. (2022). روسيا تفشل في تمرير مشروع قرار في مجلس الأمن بشأن مزاعم الأنشطة البيولوجية في أوكرانيا للمناطق الأوكرانية. *أخبار الأمم المتحدة*، https://news.un.org/ar/story/2022/11/1114987.

الدويك، ع. (2019). الأزمات والحروب السيبرانية... تهديدات تتجاوز الفضاء الإليكتروني. دراسة. *في مركز الأهرام للدراسات السياسية والاستراتيجية*، https://acpss.ahram.org.eg/News/16843.aspx#_ftnref4.

حكيم، غ. وصبرينة، ش. (2020). تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران فيروس ستكنست. *دفاتر السياسة والقانون*، 12(3)، 92-107.

ساثر، ج. (2017). الحرب السيبرانية الجديدة بين روسيا والولايات المتحدة الامريكية. *صحيفة الأيام*، (7686)، 14.

عبدالصادق، ع. (2012). القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني. *السياسة الدولية*، 48(188)، 28-35.

عبدالصادق، ع. (2016). *العلاقات الدولية والفضاء الالكتروني: دراسة في النظرية والتطبيق*. (ط3)، القاهرة: المركز العربي لأبحاث الفضاء الالكتروني.

عبد العزيز، س. (2017). التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية. *اتجاهات الأحداث-المستقبل للأبحاث والدراسات المتقدمة*، (20)، 8-19.

علي، ع. (2024). تكتيكات متبادلة: حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية. *المستقبل للأبحاث والدراسات المتقدمة*، https://futureuae.com/ar-AE/Home/Index/2/%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9.

عودة، ن. (2022). "العمليات السيبرانية في الحرب الروسية الأوكرانية طبيعتها وأنماطها". *الشرق للأبحاث الاستراتيجية*، 4-34 https://research.sharqforum.org.

فتحي، ع. (2019). العمليات السيبرانية الأوروأطلسية ومهددات الجيوسيبرانية الروسية «رؤية في الاشتباك السيبراني الأورو - روسي». *مجلة حمورابي*، 7(30)، 3-16.

مليح، ي. (2022). الحرب السيبرانية والأزمة الروسية الأوكرانية. *جريدة هسبريس*، https://www.hespress.com .

References

Adams, J. (2001). Virtual defense. *Foreign Affairs, 80*(3), 98-112.

Aladekomo, A. (2022). Russian aggression against Ukraine, sovereignty, and international law. *Available at SSRN*. https://ssrn.com/abstract=4064020 or http://dx.doi.org/10.2139/ssrn.4064020

Bildt, C. (2022). Are Sweden and Finland moving to apply for NATO membership? *The Washington Post*. https://www.washingtonpost.com/opinions/2022/03/16/are-sweden-finland-moving-apply-nato-membership/

Broad, W., et al. (2011). Israeli test on worm called crucial in Iran nuclear delay. *The New York Times*. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Duguin, S., & Pavlova, P. (2023). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. *Workshop, European Union: Directorate General for External Policies of the Union*. https://n9.cl/aa2l1

Hakmeh, J., & Naylor, E. (2022). How the tech community has rallied to Ukraine's cyber-defence. *The Guardian*. https://www.theguardian.com/commentisfree/2022/mar/07/tech-community-rallied-ukraine-cyber-defence-eu-nato

Held, D., et al. (1999). *Global transformations: Politics, economics, and culture*. Stanford University Press.

Lerman, R., & Zakrzewski, C. (2022). Elon Musk's Starlink is keeping Ukrainians online when traditional internet fails. *The Washington Post*. https://www.washingtonpost.com/technology/2022/03/19/elon-musk-ukraine-starlink

McMillan, R. (2014). Was Stuxnet built to attack Iran's nuclear program? *PC World*. https://www.pcworld.com/article/503296/was_stuxnet_built_to_attack_irans_nuclear_program.html

McNamara, R. (1968). *The essence of security: Reflections in office* (1st ed.). Strategic Studies Institute.

Melzer, N. S. (2011). Cyberwarfare and international law. *Center for Security Studies, Switzerland*, 8-17. https://coilink.org/20.500.12592/k75k4mCOI

Metz, S., & Johnson, D. V. (2001). Asymmetry and U.S. military strategy: Definition, background, and strategic concepts. *Strategic Studies Institute, U.S. Army War College*. http://www.jstor.org/stable/resrep11225

Nakashima, E. (2012). U.S. accelerating cyberweapon research. *The Washington Post*. https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html

Partington, R. (2022). G7 nations strip Russia of 'most favoured nation' status. *The Guardian*. https://www.theguardian.com/world/2022/mar/11/g7-nations-drawing-up-plans-impose-heavy-tariffs-russia-ukraine#top

Paul, C. (2008). *Information operations—Doctrine and practice: A reference handbook* (Contemporary Military, Strategic, and Security Issues). Praeger Security International.

Security Council. (2022). UN Security Council provisional verbatim record of 8979th meeting. *United Nations, Security Council, UN Doc. S/PV.8979*. https://www.legal-tools.org/doc/s3ykgp/pdf

Sloan, E. C. (2016). *Modern military strategy: An introduction* (2nd ed.). Routledge Taylor & Francis Group.

Thornton, R. (2007). *Asymmetric warfare: Threat and response in the 21st century* (1st ed.). Polity Press.

Ukraine. (2022). What are the sanctions on Russia and have they affected its economy? *BBC News*. https://www.bbc.com/news/world-europe-60125659

United Nations Dag Hammarskjöld Library. (2022). Letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General. *UN Doc. S/2022/154*. https://digitallibrary.un.org/record/3959647

النص الأصلي على الرابط التالي:

Retrieved from http://www.en.kremlin.ru/events/president/transcripts/67843.

United Nations, (2022)**,** Security Council Fails to Adopt Draft Resolution on Ending Ukraine Crisis, as Russian Federation Wields Veto, *United Nations*, Meetings Coverage Security Council, Retrieved from https://press.un.org/en/2022/sc14808.doc.htm .