نظرية الواقعية الجديدة والأمن السيبراني

Neorealism and Cybersecurity

أ.د. أنور محمد فرج محمود
كلية العلوم السياسية – جامعة السليمانية
Anwar.faraj@univsul.edu.iq

م. فرهاد جلال مصطفى سعيد
كلية العلوم السياسية – جامعة السليمانية
Farhad.mustaffa@univsul.edu.iq

تاريخ استلام البحث: ٢٠٢٤/٩/١٥ **تاريخ قبول النشر: ٢٠٢٤/١٢/٢٢**

الملخص:

يرمي هذا البحث إلى اختبار الأسس المفاهيمية والافتراضات النظرية والطروحات التحليلية للواقعية الجديدة في الفضاء السيبراني. ويركز البحث على وجه الخصوص على قضية الأمن بِعدّها واحدة من أهم القضايا لدى للواقعيين. هنا يتم تناول قضية الأمن السيبراني من منظور نظرية الواقعية الجديدة في ثلاث خطوات. في الخطوة الأولى، يتم دمج الأمن السيبراني في الطروحات الرئيسية للواقعية الجديدة، ومنها الفوضى الدولية، وسعي الدول لتعظيم قوتها/ أمنها، والمعضلة الأمنية. وفي الخطوة الثانية، سيتم العمل على عرض الردع السيبراني وتوازن الهجوم والدفاع في المجال السيبراني كأداتين لضمان الأمن السيبراني. وفي الخطوة الثالثة، تعرض الانتقادات والإشكاليات التي تعاني منها تحليلات الواقعية الجديدة في الفضاء السيبراني. وفي المجمل يسعى هذا البحث إلى المساهمة في سد الفجوة الموجودة في تحليل النظرية الواقعية الجديدة في الفضاء السيبراني. وهو يقوم بذلك من خلال تحديد الثغرات في النظرية بهدف دفعها نحو تطور نسخة من النظرية الواقعية للعالم السيبراني.

الكلمات المفتاحية: الأمن السيبراني، الواقعية الجديدة، الفوضى السيبراني، القوة السيبرانية، المعضلة الأمنية السيبرانية، الردع السيبراني، التوازن السيبراني.

Abstract:

This research aims to test the conceptual foundations and theoretical assumptions of neorealism in cyberspace. The research focuses in particular on the issue of security, as it is one of the most important issues for realists. Here, the issue of cybersecurity is addressed from the perspective of neorealism in three steps. First, cybersecurity is integrated into the main analytical elements of neorealism, including international anarchy, states' quest to maximize their power/security, and the security dilemma. Second, cyber deterrence and the balance of offense-defense in the cyber domain will be addressed as two ways to protect cybersecurity. Finally, the criticisms those neorealism analyses in cyberspace suffer from are presented. Overall, this research attempts to contribute to bridging the gap in the analysis of neorealism in cyberspace. It does do so by identifying gaps in the theory with the aim of pushing it towards developing a version of the realist theory for the cyber world.

Keywords: Cybersecurity, Neorealism, Cyber Anarchy, Cyber power, Cybersecurity Dilemma, Cyber Deterrence, Cyber Balance.

المقدمة

تقدم النظرية الواقعية منظورًا للسياسة العالمية يؤكد على الطبيعة التنافسية والصراعية للعلاقات الدولية. وهي تنظر إلى النظام الدولي باعتباره حالة طبيعية فوضوية، حيث تكون الدول هي الجهات الفاعلة الرئيسة، مدفوعة بالمصلحة الذاتية والسعي إلى القوة.

في إطار النظرية الواقعية، ظهرت عدة إتجاهات مختلفة، ولكل منها طروحات وافتراضات نظرية خاصة، كالواقعية التقليدية، الواقعية الجديدة، الواقعية الهيكلية، الواقعية الهجومية، الواقعية الدفاعية، والواقعية التقليدية الجديدة.

تاريخيا يرتبط الجذور الفكرية (للواقعية التقليدية، Classical Realism) بمفكرين مثل (ثوسيديدس، Thucydides)، (نيكولا ماكيافيلي، Niccolò Machiavelli)، (توماس هوبز، Thomas Hobbes) وغيرهم. أما كنظرية للعلاقات الدولية، فهي ظهرت في أعقاب الحرب العالمية الثانية على يد (إدوارد هـ. كار، Edward H. Carr) و(هانز ج. مورجنثاو، Hans J. Morgenthau) لمواكبة أجواء دولية حبلى بالتوتر والصراع وارتبط بتغيرات عميقة طالت بنية النظام الدولي. وكانت ظهورها بمثابة ثورة على توجهات المدرسة المثالية التي هيمنت على تحليل العلاقات الدولية منذ نهاية الحرب العالمية الأولى. ومع ظهورها سرعان ما بزغ نجمها في أُفق تحليل السياسة الدولية. وتركز على دور الطبيعة البشرية وسياسة القوة وأهمية رجال المصلحة الوطنية والأمن القومي في تشكيل السياسة الدولية.

وبعد أن هيمنت على تنظير العلاقات الدولية لمدة عشرين عاماً، أظهرت الواقعية في بداية سبعينيات القرن العشرين علامات التراجع، وكانت الهجمات تتوالى عليها خصوصاً من جانب السلوكيين، والتعدديين. إلا إن منظريها استحدثوا نسخة جديدة لها بإسم (الواقعية الجديدة، Neorealism).

طور (كينيث والتز، Kenneth Waltz) الواقعية الجديدة في نسخة (الواقعية الهيكلية، Structural Realism) وتؤكد على البنية الفوضوية للنظام الدولي كمحرك أساسي لسلوك الدولة. وتركز على توزيع القوة بين الدول وتوازن القوى كمحددات رئيسية للاستقرار الدولي. وبعد ذلك ظهرت إتجاهان نظريان، وهما (الواقعية الهجومية، Offensive Realism) و(الواقعية الدفاعية، Defensive Realism). تزعم الواقعية الهجومية أن الدول تسعى بطبيعتها إلى تعظيم القوة من أجل الهيمنة. أما الواقعية الدفاعية، فتزعم أن الدول تهتم في المقام الأول بالأمن وتسعى إلى الحفاظ على الوضع الراهن. وتؤكد على أهمية موازنة القوة وتجنب تراكم القوة المفرط. هكذا تتبنّى الواقعية الهيكلية أسلوبًا بنيويًا للتحليل، وتظهر كل علامات استعادة مكانتها السابقة المتفوقة مثلما يقول (ريتشارد ليتل Richard Little)[1].

أخيراً، تجمع (الواقعية التقليدية الجديدة، Neoclassical Realism) بين إفتراضات الواقعية التقليدية والواقعية الهيكلية، أي بين تأثيرات البيئة الخارجية والسياسة الداخلية. وهي تسعى إلى شرح كيف يؤثر النظام الدولي، وخاصة توزيع القوة بين الدول، على سلوك الدولة، وتحاول تحليل سياستها الخارجية، ولكنها تعترف أيضًا بدور العوامل المحلية في تشكيل قرارات السياسة الخارجية. وفي النهاية يمكن القول إن الواقعية التقليدية الجديدة هي نظرية للسياسة الخارجية للدول.

لقد كان للنظرية الواقعية تأثير كبير في تشكيل فهمنا للسياسة الدولية، وعلى الرغم من تعرضها لإنتقادات عديدة، تظل أداة قيمة لتحليل تعقيدات العلاقات الدولية إلى الحد الذي وسمها (فيليكس روش، Felix Rösch) و (ريتشارد نيد ليبو، Richard Ned Lebow) بأنها أهم عائلة نظرية في العلاقات الدولية[٢]، بل وأكثر من نظرية؛ إنها (نموذج معرفي، Paradigm) كما يصفها الدكتور (أنور محمد فرج)[٣].

أهمية البحث: تتمثل أهمية البحث في محاولته لاختبار الواقعية الجديدة كنظرية رئيسية للتحليل في حقل العلاقات الدولية في مجال الفضاء السيبراني وخصوصاً فيما يتعلق بقضية الأمن والمقصود هنا هو الأمن السيبراني. ولذلك فإن البحث له قيمة علمية نظرية ويساهم في تطوير نظرية الواقعية الجديدة في تحليلاتها للأمن السيبراني.

هدف البحث: يهدف هذا البحث إلى استكشاف مدى معقولية البنى المفاهيمية الرئيسية وافتراضات الواقعية الجديدة لقضية الأمن في الفضاء السيبراني، وبالتالي محاولة لبناء إطار تحليلي للأمن السيبراني من منظور الواقعية الجديدة.

إشكالية البحث: مع بروز الظاهرة السيبرانية، طرحت تساؤلات حول مدى القوة التفسيرية لنظريات العلاقات الدولية تجاه هذه الظاهرة. وفي هذا الإطار، يلاحظ شكوك حول ملائمة نظريات العلاقات الدولية القائمة لتفسير سلوك الدولة في مشهد سريع التطور كعالم الفضاء السيبراني. ولكن سيكون من الخطأ تجاهل هذه النظريات دون اختبار تحليلاتها النظرية في مواجهة الحقائق الجديدة بشكل كافٍ. ومن هنا تتبلور إشكالية هذا البحث، وهي تتمثل في التساؤل: هل تتلائم البنى المفاهيمية والعناصر النظرية لنظرية الواقعية الجديدة لفهم الأمن السيبراني وبناء تصور حوله؟

فرضية البحث: ينطلق هذا البحث من فرضية مفادها: تتمتع النظرية الواقعية الجديدة بقوة استدلالية في المجال السيبراني تساعد في بناء تصور تحليلي للأمن في الفضاء السيبراني. ولاختبار صحة الفرضية، يتطرق البحث إلى تناول مجموعة من القضايا المتعلقة بالأمن السيبراني مثل المعضلة الأمنية السيبرانية، والردع السيبراني وتوازن الهجوم والدفاع في الفضاء السيبراني.

الإطار النظري للبحث: يتخذ البحث من نظرية الواقعية الجديدة إطاراً نظرياً له من أجل فهم الأمن السيبراني.

هيكل البحث: يتضمن البحث مقدمة عامة، خاتمة وثلاثة مطالب. يتناول المطلب الأول، الواقعية الجديدة والأمن السيبراني، ويتم التطرق فيه إلى الحديث عن مسائل الفوضى، وتعظيم القوة/الأمن، والمعضلة الأمنية من منظور سيبراني للواقعية الجديدة. أما المطلب الثاني فيحمل عنوان الواقعية الجديدة وضمان الأمن السيبراني، ويتناول الردع السيبراني، وتوازن الهجوم والدفاع السيبراني. ويعرض المطلب الثالث الإشكاليات التحليلية للواقعية الجديدة في مجال الأمن السيبراني.

المطلب الأول: الواقعية الجديدة والأمن السيبراني

نركز في هذا المطلب على أهم العناصر النظرية للواقعية الجديدة وعلاقتها بالأمن السيبراني. وتناول موضوع الفوضى السيبرانية من منظور الواقعية الجديدة، وفك ارتباط قضية تعظيم القوة السيبرانية أو تعظيم الأمن السيبراني، وأخيراً مسألة المعضلة الأمنية السيبرانية.

الفرع الأول: الواقعية الجديدة والفوضى السيبرانية

طبقا للواقعية الجديدة، الفوضوية هي أكثر المحددات تأثيراً لسلوك الدول في النظام الدولي. وفوضوية النظام الدولي هي السبب وراء بحث الدول عن القوة، وأن العلاقة بين القوة والأمن هي علاقة طردية[٤].

يتسم الفضاء السيبراني بالطابع الفوضوي على نطاق واسع[٥]، حيث لا توجد سلطة عليا تدير التفاعلات التي تحدث فيه[٦]، والتشريعات الدولية بهذا الصدد محدودة ولاتزال المنظمات الدولية، كالأمم المتحدة، عاجزة عن فرض سلطتها في هذا المجال[٧]، ومن الطبيعي أن تخشى الدول بعضها بعضاً[٨]، نتيجة لإنعدام الثقة فيها[٩]، واحتمال اندلاع حرب سيبرانية[١٠].

في بيئة كهذه الحفاظ على معايير السلوك أمراً بالغ الصعوبة[١١]، ويفرض هذا على الدول الإعتماد على الذات لتطوير قدراتها السيبرانية[١٢]. كما يرى (جيمس آدامز، James Adams)، وهو من الواقعيين الجدد، أن كل دولة تقف بمفردها أو مع حلفائها، الذين لا يمكنها أبدًا الوثوق بهم تمامًا، وتحاول يائسة بناء قوتها ودفاعاتها السيبرانية بينما تخشى أن يشكل كل اختراق تحققه دولة أخرى تهديدًا مباشرًا لأمنها [١٣].

عليه تشبه البيئة السيبرانية الدولية حالة الطوارئ الدائمة والحرب والقوة، أي إدامة حالة التهديد، حيث تكون الأمن عرضة لأشكال مختلفة من التهديد المستمر. أنها حالة لها العديد من أوجه التشابه مع حالة الطبيعة عند توماس هوبز[١٤]. إذن تتوقع نظرية الواقعية الجديدة إنهيار الثقة والمؤسسات الدولية بشكل كامل في ظل خوف كل دولة من هجمات وشيكة وغير معروفة، وبناء قوتها الخاصة[١٥].

الفرع الثاني: الواقعية الجديدة بين تعظيم القوة أو الأمن في المجال السيبراني

هناك نقاش بين الواقعيين الهجوميين والواقعيين الدفاعيين حول كيفية تأثير الفوضى على تصرفات الدول ومدى القوة المطلوبة لأمن الدول وبقائها. وهم لا يتفقون على هل الدول تسعى للهيمنة على النظام الدولي أو تسعى لتوازن القوة والحفاظ على النظام القائم الناشيء[١٦].

تزعم الواقعية الدفاعية أن الحرب تحدث بسبب المنافسة الدائمة بين الوحدات الساعية إلى الأمن والتي ترغب في الحفاظ على الوضع الراهن من خلال توازن القوى ضد التهديدات المتزايدة. وبالتالي، فإن الواقعية الدفاعية تتعامل مع التحركات الموازنة ضد التوسع أو العدوان باعتبارها آلية ردع فعالة.

يعتقد الواقعيون الدفاعيون، وفي مقدمتهم (كينز والتز)، بأن الدول تقوم في الواقع بتعظيم الأمن[١٧]. من وجهة النظر هذه، القوة هي مجرد وسيلة لتحقيق غاية لأنها مفيدة لضمان الأمن. عليه لابد للدول أن تهتم كثيراً بتعظيم أمنها السيبراني وليست الهيمنة السيبرانية.

أما الواقعيون الهجوميون، وفي مقدمتهم (جون ميرشايمر، John Mearsheimer)، فيعتقدون بِأنه في ظل البنية الفوضوية الدولية تسعى الدول إلى تعظيم القوة لأنها الوسيلة الأكثر موثوقة لضمان البقاء، والهدف النهائي للدول، وخاصةً الكبرى منها، هو الهيمنة [١٨]. ويعني هذا أن تمتلك دولة عظمى، مثل الولايات المتحدة الأمريكية، قدرات سيبرانية متفوقة وتستخدمها على نطاق عالمي وفرض الهيمنة السيبرانية على العالم. إن غياب التأثيرات المقيدة للجغرافيا في الفضاء السيبراني يدعم هذا المنطق.

عليه القوى العظمى لديها الحافز لتعظيم قوتها السيبرانية، وليس موازنة قوتها السيبرانية باستخدام وسائل هجومية أو صراع سيبراني مهيمن لتحقيق غلبة القوة السيبرانية العالمية لردع العدوان وتعزيز الأمن في الفضاء السيبراني. والمنطق هنا فكلما كنت أقوى في الفضاء السيبراني، قل احتمال تعرضك للهجوم من قِبَل الآخرين.

على الرغم مما سبق، يبدو أن القوة المطلقة في هذا السياق لها معنى أقل مما كانت عليه في السياق الأكثر وضوحًا للتكنولوجيا الصناعية. على سبيل المثال، قد يُنظر إلى الولايات المتحدة بالفعل على أنها تمتلك نسبة غير مسبوقة من القوة، ومع ذلك يبدو أنها غير كافية لضمان الأمن في المجال السيبراني. كما من المحتمل أن تصبح بعض الجهات الفاعلة الصغيرة، بما في ذلك الجماعات الإرهابية والدول الأقل نمواً، والتي كان يُنظر إليها سابقًا على أنها تمتلك القليل من القوة، قوية نسبيًا في الفضاء السيبراني. لذلك أن وجهة نظر تعظيم الأمن لها تأثير أكبر هنا من وجهة نظر تعظيم القوة[١٩].

الفرع الثالث: الواقعية الجديدة والمعضلة الأمنية السيبرانية

ترتبط إحدى التحديات الرئيسية بحالة عدم اليقين الموجودة في السياسة الدولية. طبقاً للواقعية الدفاعية، يمكن لطبيعة النظام الدولي أن تؤدي إلى معضلة الأمن. تعني معضلة الأمن حالة تؤدي جهود دولة واحدة لتحسين أمنها إلى تقليل أمن الدول الأخرى. وردًا على ذلك، تحاول دولة أخرى تعزيز قدراتها الدفاعية. تؤدي مثل هذه الخطوات المتتالية إلى سباق تسلح، وتدهور العلاقات الدبلوماسية، وحتى إلى صراع مفتوح[٢٠].

وفق منطق فرضيات النظرية الواقعية الجديدة، فإن زيادة القوة السيبرانية لأحد الأطراف سوف تكون بالضرورة على حساب أمن الآخرين، وأن الأطراف الضعيفة أو التي لا تستطيع حماية نفسها أو تتهاون في تعزيز قدرات دفاعها يجب أن تدفع ثمن الاعتداءات السيبرانية[٢١].

يقدم (بين بوكانان، Ben Buchanan) حجة مقنعة لتطبيق معضلة الأمن على تفاعلات الدول في الفضاء السيبراني. فهو يلاحظ أن العمليات التي تسعى إلى جمع المعلومات والحصول على الاستخبارات، بغض النظر عن الطريقة التي يتم بها إجراؤها، يمكن أن تشكل تهديدًا للدول التي يتم إجراؤها ضدها[٢٢]. وتقود هذه الواقعة إلى نوع من سباق تسلح سيبراني، وبدوره إلى معضلة أمنية سيبرانية.

وتعني المعضلة الأمنية السيبرانية، أن الجهود التي تبذلها دولة واحدة لتعزيز أمن بنيتها التحتية السيبرانية تقلل من الأمن السيبراني للدول الأخرى[٢٣]. يلعب هنا عامل صعوبة التمييز بين الأسلحة الهجومية والدفاعية وصعوبة معرفة نوايا الدول دوراً مركزياً في نشوء المعضلة الأمنية السيبرانية.

تجد الدول حافزا لاختراق شبكات الدول الأخرى من أجل الدفاع عن نفسها ضد العدوان المستقبلي. ومن خلال غزو شبكات الدول الأخرى، يمكنها جمع معلومات استخباراتية بالغة الأهمية حول قدرات الخصوم المحتملين وتعزيز دفاعاتها من خلال معرفة كيفية هيكلة الدول الأخرى لقيادتها وضوابطها السيبرانية. والنتيجة هي أنه بمجرد اقتحام دولة لشبكة دولة أخرى، يصبح من المستحيل تقريبا التمييز بين النوايا الهجومية والدفاعية. وعلاوة على ذلك، يمكن أن تتغير النوايا بين عشية وضحاها. ونتيجة لهذا فإن الدول تميل إلى إفتراض الأسوأ عندما تدرك أنها تعرضت للاختراق، فتقوم بعمليات تسلل خاصة بها، ومن هنا تأتي المعضلة الأمنية السيبرانية، كما حللها بوكانان بدقة وإن كانت سهلة الفهم[٢٤].

إنطلاقاً مما سبق، يمكننا القول إن الفضاء السيبراني هو فضاء فوضوي بالمفهوم الواقعي. وهذا يحث الدول إلى بناء قوة سيبرانية تمكنها من بسط النفوذ وفرض الهيمنة في هذا الفضاء، سبيلاً للحفاظ على أمنها السيبراني. ومع ذلك، فإن أي خطوة تتخذها دولة ما في هذا الاتجاه تشكل تهديدًا للأمن السيبراني لدولة أخرى، مما يدفعها في النهاية إلى اتخاذ نفس الخطوة لمواجهة هذه التهديدات السيبرانية. وهكذا تدخل الدول في سباق تسلح سيبراني كنتيجة لإنخراطها في معضلة أمنية سيبرانية دولية.

المطلب الثاني: الواقعية الجديدة وضمان الأمن السيبراني

تشكل التقنيات السيبرانية المفهوم الواقعي المألوف للأمن بين الدول في نظام فوضوي. من هنا تكتسب التكنولوجيات السيبرانية المزيد من الاهتمام باعتبارها أدوات أو حتى "أسلحة" للتعطيل وانعدام الأمن في أيدي الجهات السياسية الفاعلة، وهي الدول غالبا[٢٥]. ولكن لنتسائل: كيف يتم ضمان الأمن في الفضاء السيبراني؟

إن محاولة الإجابة عن السؤال أعلاه من خلال التفكير مع الواقعية الجديدة يقودنا إلى الحديث عن الردع السيبراني وميزان القوة السيبرانية من ناحية الهجوم والدفاع كطرق لحماية الأمن السيبراني للدول.

الفرع الأول: الردع السيبراني

إحدى وسائل ضمان الأمن لدى النظرية الواقعية هي الردع. ولكن كيف يتحقق الردع؟ هل يتحقق عن من خلال الهيمنة أم توازن القوة؟ والحديث هنا هو بخصوص الردع السيبراني.

يقارن (يافوز أكداغ Yavuz Akdağ) بين الواقعية الدفاعية والواقعية الهجومية في موضوع الردع السيبراني. حسب أكداغ أن الردع السيبراني عن طريق توازن القوى حسب منظور الواقعيين الدفاعيين ربما يكون نهجًا غير مناسب في الصراع السيبراني والحرب السيبرانية. وبدلاً من ذلك، يمكن أن يكون منظور الواقعية الهجومية لفرض الهيمنة أفضل للردع السيبراني وتعزيز الأمن السيبراني. من هذا المنطلق يرى أكداغ أن الولايات المتحدة في وضع أفضل لمواصلة الهيمنة السيبرانية من خلال استراتيجيات سيبرانية هجومية لردع وضمان الأمن السيبراني، حيث لا يمكن لأي دولة عاقلة أن تجرؤ على تصعيد الصراع السيبراني ضد القوة السيبرانية المهيمنة [٢٦].

هناك آراء بأن الردع مفهوم صعب في الفضاء السيبراني. وتكشف الأدبيات المتعلقة بالردع السيبراني عن العديد من التحديات التي تواجه هذا المفهوم ذاته، ومن أهم هذه التحديات[٢٧]:

١. صعوبة إسناد الهجمات السيبرانية إلى مرتكبيها.

٢. سهولة الحصول على الأسلحة السيبرانية وتنفيذ الهجمات السيبرانية.

٣. النطاق الواسع للجهات الفاعلة الحكومية وغير الحكومية التي تشن هجمات سيبرانية لأسباب متعددة وضد أهداف حكومية وغير حكومية.

٤. التحديات المرتبطة بتجنب التصعيد.

٥. تجنب الانتقام أو الرد المضاد، حيث يصعب السيطرة على الهجمات السيبرانية أو التنبؤ بها. ولذلك، ستطول المسافة الزمنية بين الهجوم والرد.

٦. المصداقية: من بين العوامل التي تؤثر في الردع السيبراني هو ثقة المهاجم في قدرة الدولة على الانتقام والرد. ولكن في المجال السيبراني، الأسلحة السيبرانية خفية وغير مرئية إلى أن يُقدم طرف ما على استخدامها. ولذلك، لا يمكن للمهاجم أن يعرف إذا امتلك الخصم القدرة على الرد أو الانتقام.

ومهما يكون الأمر، فقد يكون من المناسب أكثر الاعتراف بأن الردع هو أداة ضعيفة في عالم الفضاء السيبراني. ونرى سبب ذلك بشكل كبير في عدم الوضوح في كيفية الرد على الهجمات السيبرانية عليهم، إذ لا يزال من غير الواضح كيف تستجيب الدول للهجمات السيبرانية، خاصة وأن ظاهرة الهجمات السيبرانية جديدة نسبياً ولا يوجد استنتاج عام يستند إلى تجارب متراكمة حول تعامل الدول في حال تعرضها لهجمات سيبرانية. على سبيل المثال، هل ترد الدولة التي تعرضت لهجوم سيبراني بالمثل، أي سيبرانياً؟ أو بدلاً من ذلك تنتقل الرد إلى العالم المادي؟ أو تختار عدم الفعل أي عدم الرد؟ أو ماذا؟ إن هذا الغموض في التفاعلات السيبرانية الدولية أفضى إلى إضعاف الردع في المجال السيبراني.

فضلاً عن ذلك، ويتوقف أيضاً جزءاً من ضعف الردع السيبراني على إختلال التوازن بين الهجوم والدفاع في الفضاء السيبراني لصالح الهجوم، مما أنتج بعدم فعالية الردع كأداة لضمان الأمن السيبراني، كما يتبين في الفرع التالي أدناه.

الفرع الثاني: توازن الهجوم والدفاع السيبراني

يشير توازن الهجوم والدفاع إلى "مدى سهولة أو صعوبة غزو منطقة ما أو إلحاق الهزيمة بمدافع في المعركة. فإذا كان التوازن لمصلحة المدافع، يكون الغزو صعباً وبالتالي ليس من المرجح أن تكون هناك حرب. ويحدث العكس إذا كان التوازن لمصلحة الهجوم"[٢٨]. إن هذا التوازن هو الذي يحدد شدة المنافسة الأمنية بين الدول[٢٩]. ومن المعلوم أن الواقعية الهجومية تنادي بميزة الهجوم على الدفاع، في حين المعادلة معكوسة عند الواقعية الدفاعية.

والسؤال هنا هو: هل تكنولوجيا السيبرانية تفضل الهجوم أم الدفاع؟ إن هذا السؤال هو بالغ الأهمية بالنسبة للأمن السيبراني. ويمكن ملاحظة إتفاق شبه عام بين الباحثين في الوقت الحالي في الإفتراض بتفوق الهجوم على الدفاع في العمليات السيبرانية.

وفقاً لـ (جون أركويلا، John Arquilla) يُعزى هذا الإفتراض جزئيًا إلى التصميم الأصلي للفضاء السيبراني، والذي تطور في البداية من شبكة (آربانيت ARPANET) التابعة لوزارة الدفاع الأمريكية. لقد تم تصور الفضاء السيبراني في المقام الأول كوسيلة شديدة التعقيد ومترابطة تهدف إلى الاتصال المفتوح وغير المحدود بين مجموعة متنوعة من المستخدمين دون الأخذ بالحسبان نقاط الضعف داخل النظام ستظل قابلة للاستغلال[٣٠]. وهذا يمنح الخصوم ميزة وجود العديد من الفرص للمهاجمة، قد تكون نقطة ضعف واحدة كافية للمهاجم لدخول الشبكة بينما يحتاج المدافعون إلى حراسة العديد من الأنظمة، وغالبًا ما يكون ذلك بدون موارد كافية[٣١]. لذلك يمكننا أن نستنتج أن هناك اختلالا في التوازن بين الهجوم والدفاع، أو كما يقول (جورج لوكاس، George Lukas) "إن الميزة، كما يعترف خبراء الأمن السيبراني أنفسهم، تكمن دائمًا في الهجوم"[٣٢].

هناك أسباب تفسَر أفضلية الهجوم على الدفاع في الفضاء السيبراني وفي الوقت الحالي. على سبيل المثال، يشير (بروس شناير، Bruce Schneier) إلى بعض من هذه الأسباب كالآتي[٣٣]:

١. يسهل تحطيم الأشياء ولكن يصعب إصلاحها.

٢. يعدُ التعقيد العدو الأسوأ للأمن، وتسير نظم المعلوماتية بإطّراد نحو مزيد من التعقيد.

٣. تسهل طبيعة الفضاء السيبراني للمهاجم العثور على نقطة ضعف قابلة للإستغلال، فيما يجب على المدافع معرفة نقاط الضعف كلها ثم العمل على إصلاحها.

٤. يستطيع المهاجم أن يختار هجمة ما ويركز جهوده عليها، فيما يفترض بالمدافع أن يتحسّب لأنواع الهجمات كلها.

٥. غالبية البرامج الرقميّة ضعيفة أمنيّاً.

وكذلك يمكن إضافة أسباب أُخرى، ومنها:

١. الهجوم السيبراني أسهل وأسرع من الدفاع السيبراني، وعوامل الوقت لتصور الهجوم القادم وكذلك المساحة العازلة المادية لمقاومته –كما في الحرب التقليدية– لا تعمل في الفضاء السيبراني[٣٤].

٢. إنخفاض معدل الردع المتبادل في الفضاء السيبراني[٣٥].

٣. من وجهة نظر التكلفة، فإن تصميم الأسلحة الهجومية السيبرانية أرخص كثيراً من إنشاء الأسلحة الدفاعية السيبرانية، لأن القدرة السيبرانية الهجومية تترجم مباشرة إلى قوة، في حين لا يمكن قياس القدرة السيبرانية الدفاعية إلا من خلال تقييمات المخاطر المعقدة وغير الواضحة إلى حد ما [٣٦].

٤. سوف يفشل الدفاع السيبراني في الحرب السيبرانية. والمشكلة هي كيفية تجنب الهجمات على جميع الشبكات الوطنية. ربما يمكن لجيش دولة ما الدفاع عن أنظمة الكمبيوتر الخاصة بالدولة. ومع ذلك، في الحرب السيبرانية لا يهاجم المتسلل البنية التحتية الرقمية للدولة فحسب، بل يهاجم أيضًا البنية التحتية الرقمية الخاصة مثل الأنظمة المصرفية. علاوة على ذلك، يتم تشغيل الكثير من البنية التحتية اليوم من قبل شركات خاصة، بما في ذلك شبكات الطاقة والنقل. كيف سيبنون دفاعًا سيبرانيًا قويًا مثل الدفاع السيبراني العسكري؟ [٣٧].

٥. صعوبة تحديد هوية المهاجم بالنسبة للضحية. ويمكن شن الهجمات السيبرانية في أي مكان، حتى من خارج الدولة التي ترعاها. فضلاً عن ذلك، وبما أن الحرب السيبرانية مصممة لدعم الصراع المادي، فإن المهاجم المحتمل يصبح أكثر ميلاً إلى شن الهجوم، لأن الخسائر في الأرواح سوف تكون أقل[٣٨].

مع كل ما تطرقنا إليه أعلاه، هناك في المقابل مساندة لجهة فوائد الدفاع السيبراني في المواجهات السيبرانية، ومن هذا المنطلق يشير الباحث (ريتو إنفيرسيني، Reto Inversini)*[٣٩]:

١. لا ينبغي لميزة المهاجم أن تؤدي إلى سباق تسلح يهمل الدفاع؛ أي لماذا نستثمر في الدفاع، إذا كانت للهجوم دائما الأفضلية؟ بل يمكن تعزيز أمن ومتانة البنية التحتية السيبرانية. فكلما كان الأمان أفضل، كلما ارتفع ثمن الهجمات الناجحة، مما يجعل الهجمات أقل احتمالاً. كما أنه يساعد على تقليل احتمالية وتأثير الأضرار الجانبية التي لم يقصدها المهاجم ولكنها قد تؤدي في حد ذاتها إلى تصعيد خطير.

٢. لا ينبغي لنا أن نقلل من مدى تعقيد مهمة المهاجم. يتمتع المدافعون بإشراف جيد على شبكاتهم ويتصرفون بأنظمة مراقبة متقدمة. وعلى النقيض من ذلك، يجب على المهاجم إلقاء نظرة خاطفة من خلال ثقب المفتاح ومحاولة فرز البيانات والأنظمة المثيرة للاهتمام دون ارتكاب الكثير من الأخطاء وعدم اكتشافه.

٣. يرتكب كل مهاجم أخطاء (كل جهة اتصال تترك أثرًا". والأمر متروك للمدافع للعثور على هذه الآثار في أسرع وقت ممكن للكشف عن المهاجم قبل حدوث ضرر جسيم.

٤. في حالة الهجمات يجب أن يكون لدى المهاجم معرفة خاصة ليس فقط حول الأداء العام ولكن أيضًا حول التنفيذ الفعلي. إنها مهمة تستغرق وقتًا ومالًا لتحقيق مثل هذه المعرفة، ولا يمكن للمهاجمين القيام بذلك إلا إذا كان الثمن يستحق ذلك.

إنطلاقاً مما سبق، يتعلق مسألة الأمن السيبراني بكفة الميزان بين الدفاع والهجوم في الفضاء السيبراني، ويبدو في الوقت الحالي هناك اختلال في هذا التوازن لصالح الهجوم. وذلك بسبب حداثة اللجوء إلى استخدام السيبرانية كسلاح في العلاقات الدولية وعدم وجود أسلحة سيبرانية دفاعية تضمن الإستقرار على غرار السلاح النووي المعلوم لنا. ولتحقيق التوازن في كفة الميزان هذه، سوف يستغرق الأمر بعض الوقت لفهم أنواع الأسلحة السيبرانية وكيفية تنفيذ الهجمات، وبالتالي إبتكار أسلحة وجدران سيبرانية دفاعية تجاهها، وفي المجمل صياغة سياسات دفاعية سيبرانية.

المطلب الثالث: إشكاليات الواقعية الجديدة في مجال الأمن السيبراني

على الرغم من إقرارنا بأن الواقعية لها قدر كبير من الجدارة للنظر إلى قضية الأمن بشكل عام، وضمنها الأمن السيبراني، إلا أنها تواجه عدد من الإشكاليات التحليلية، من أهمها إشكالية الفاعلين، إشكالية تقدير القوة السيبرانية وإشكالية ميزان السيبراني بين الهجوم والدفاع.

الفرع الأول: إشكالية الفاعلين

إن التحدي الخاص الذي يواجه أي شخص مهتم بتكييف مبادئ وافتراضات النظريات الواقعية الجديدة لتفسير ديناميكيات الصراع في عصر المعلومات هو تفسير دور وأهمية الجهات الفاعلة غير الحكومية[٤٠].

يركز الواقعيون على الدول في تحليلهم فقط أو في أحسن الأحوال كفاعل أساسي، وقد يكون ذلك مناسبًا في تحليل الصراعات التقليدية، إلا إن الأمر ليس كذلك في الفضاء السيبراني. إذ إن التركيز على الدولة قد لا تقدم بالضرورة أفضل نموذج لفهم الفضاء السيبراني[٤١]. فلا يمكن إنكار أن الدول لديها المزيد من الموارد المالية والتكنولوجية، لكن شركات تكنولوجيا الإتصالات والمعلومات العملاقة، ومجموعات المصالح الخاصة، والمنظمات الإرهابية، ومجموعات القرصنة الإجرامية، وبعض المنظمات الدولية المعنية بتنظيم وإدارة الإتصالات الدولية –كالاتحاد الدولي للاتصالات–وحتى الأفراد جميعهم قادرون على التسبب في تهديدات أمنية سيبرانية [٤٢].

إن صعود قوة فاعليين من غير الدولة في مجال الأمن السيبراني، واختراق الحدود السيادية في الهجمات السيبرانية، لا يحظى إلا بقليل من الاهتمام أو لا يحظى بأي اهتمام في التحليلات الواقعية[٤٣].

في المقابل تصر الواقعية على إفتراضها إستمرار الدور الأساسي للدولة في تطور تكنولوجيا المعلومات والإتصالات كآلية لتعزيز قوتها والتحكم الإجتماعي وتحقيق الأمن داخلياً وخارجياً. كما وفي ذلك تتفوق على الشركات والقطاع الخاص، وتتمتع بالقدرة على دمج البيانات من مصادرها الحكومية وغير الحكومية [٤٤].

إضافة إلى ذلك، نرى إن الفاعليين من غير الدولة ومن خلال هجماتهم السيبرانية لا يشكلون تهديداً للبنى الهيكلية للدولة. قد تكون لهذه السلوكيات أضراراً ببعض القطاعات الخدمية وإقتصاد الدولة، ولكنها لاتصل إلى تعرض وجود هذه الدولة للخطر إلا عندما ترعاها أو تنفذها دولة أُخرى.

الفرع الثاني: إشكالية تقدير القوة السيبرانية

بالنسبة للواقعية، فإن التكنولوجيا تمثل ببساطة أحد مكونات تعريف القوة بإعتبارها القدرات العسكرية والاقتصادية والتكنولوجية للدول[٤٥]. وترتكز الواقعية الجديدة في تحليلاتها على بنية النظام الدولي أي توزيع القوة فيما بين الدول وعلى وجه الخصوص الدول الكبرى. ومع ذلك، من الصعب التنبؤ بمثل هذه الأمور في الفضاء السيبراني. يساعد المنظور الواقعي لفهم القوة في العلاقات الدولية في سياق التكنولوجيا الصناعية، ولكن لا تأخذ في الاعتبار السمات المميزة لتكنولوجيا المعلومات والاتصالات التي يمكن أن تجعل طبيعة القوة والتعبير عنها أكثر تعقيدًا[٤٦].

من الصعب تحديد من هي القوة العظمى في الفضاء السيبراني. كل دولة لديها قدراتها السيبرانية الخاصة بها، بما في ذلك الدول الصغيرة، والدول الاقتصادية الضعيفة، والدول ذات القوة العسكرية الضعيفة. هذا لا يعني أنها قوة ضعيفة في الفضاء السيبراني[٤٧].

في العالم المادي يمكننا قياس قوة الدولة بدقة إلى حد ما، ولكن ليس الأمر كذلك في الفضاء السيبراني. على سبيل المثال، الولايات المتحدة قوة عسكرية واقتصادية عظيمة ولكن في الفضاء السيبراني، تتعرض لهجمات سيبرانية متكررة[٤٨]. لذا، تفشل الواقعية الجديدة في تفسير تكوين القوة في الأنظمة الدولية السيبرانية بشكل كافٍ. ومن الصعب القول ما إذا كانت بعض الدول أكثر أو أقل قوة من

غيرها[٤٩]، وعلى وجه الخصوص في حالات الصراع السيبراني الذي لا يمكن فيه تصفية الخصم نهائياً [٥٠]. وهذا إطار إشكالي مضاف بالنسبة للواقعية الجديدة في تحليلاتها للتفاعلات الدولية السيبرانية، نظراً للافتقار العام إلى العنف الصريح في هذه التفاعلات[٥١].

مع الإقرار بجدية الإنتقاد الموجه أعلاه للواقعية الجديدة، فإن هذا لن يقلل من شأن النظرية ولا من جدوى تحليلاتها القيمة، وذلك لأن الواقعية الجديدة هي نظرية للوقائع والأحداث الكبرى والمؤثرة في التفاعلات السياسية الدولية كحالات الصراع الدولي من نوع الحرب والردع وصراعات القوة، أي إنها تهتم بالقضايا التي تندرج ضمن "سياسات عليا" للدول وليست قضايا "سياسات الدنيا". عليه، تركز الواقعية الجديدة على التفاعلات تي قد تهدد الأمن السيبراني للدول، وليست الحالات التي قد تشكل ضرراً أو خطراً ذات وزن قليل نسبياً.

الفرع الثالث: إشكالية ميزان السيبراني بين الهجوم والدفاع

نرى بأن إفتراض الواقعية الهجومية بميزة الهجوم على الدفاع في الفضاء السيبراني صحيح مؤقتاً وليس إلى الأبد، وذلك لأن عامل الوقت يلعب دوراً في هذا الأمر. إن رأينا هذا يستند إلى حقائق من تأريخ العلاقات الدولية والتجارب في السياسة الدولية.

يزعم جون ميرشايمر، وهو من الواقعيين الهجوميين، أن الدول التي تبادر إلى العدوان تفوز بالحروب في (٦٠%) من الحالات. ويستند في ذلك على معطياة (٦٣) حرباً بين عامي (١٨١٥-١٩٨٠) وانتصر فيها المعتدي (٣٩) مرة [٥٢]. غير من أجل الخروج باستنتاج أدق من هذه المعطياة التأريخية، ربما من الأفضل أن نتمعن أكثر من منطلق نسبة الإنتصار والهزيمة في الفترات التأرخية للحروب.

تشير دراسة (دان ليندلي' Dan Lindley) و(ريان شيلدكراوت، Ryan Schildkraut) في عام (٢٠٠٤) انهما قاما بقياس نتائج (٧٩) حرباً بين (١٨١٥) و (١٩٩٧)، وتبين لهم أن نتائج هذه الحروب كانت على النحو المبين في الجدول رقم (١)[٥٣]:

الجدول رقم (١): نتائج (٧٩) حرباً لفترة (١٨١٥-١٩٩٧)

نتائج الحرب	عدد الحروب	النسبة المئوية
فوز المبادر بالحرب	٣٩	% ٤٩
خسارة المبادر بالحرب	٢٤	% ٣٠
دون تحقيق نصر مبين	١١	% ١٤
الإنتهاء بمساومات	١	% ١
دون نتيجة واضحة	٤	% ٥

المصدر: Dan Lindly and Ryan Schildkraut, Is War Rational: The Extent of Miscalculation and Misperception as causes of war, 2005

لاحظ الدكتور (وليد عبدالحي) في نتائج هذه الدراسة انه عند تقسيم الفترة الزمنية من (١٨١٥) الى (١٩٩٧)، تبين انه في كل مرحلة كانت نسبة انتصار المبادر بالهجوم تتراجع نظرا لتزايد هائل في المتغيرات الجديدة وتعقيدات الحياة الدولية المعاصرة وتشابك ابعادها. وتدل النتائج على ان حوالي نصف الحروب انتهت الى غير ما كان يأمله المبادر بها[٥٤].

استنادا إلى هذا الإستنتاج، نميل إلى التنبوء بتغيير الواقع الراهن لميزان الهجوم–الدفاع في القوة السيبرانية مع مرور الوقت تدريجياً. هذا يعني إن الواقع الراهن بتفوق الهجوم على الدفاع طبيعي بالنسبة لنا، وذلك كون التكنولوجيا السيبرانية حديثة النشأة والأسلحة السيبرانية جديدة وقليلة الإنتشار وبالتالي من يمتلكها يتمتع بالتفوق على غيرها. ولكن مع مرور الوقت قد تتراجع في كل فترة نسبة تفوق الهجوم على الدفاع طبقاً لإستحداث وإنتشار أدوات وبرامج وأسلحة سيبرانية دفاعية.

على الرغم من الإشكاليات النظرية التي تؤثر في قوتها التحليلية، تظل النظرية الواقعية الجديدة، بأدواتها المفاهية وإفتراضاتها التحليلية، النظرية الرئيسة لفهم التفاعلات السيبرانية الدولية في البيئة الفوضوية الدولية بين الفاعليين المهمين، وهم الدول وبالأخص الدول الكبرى. وتقع قضايا القوة السيبرانية، توازن القوة السيبرانية، التوازن بين بين الدفاع والهجوم سيبرانياً والأمن السيبراني في تحليلات النظرية.

الخاتمة

يشكل ظهور الفضاء السيبراني في العلاقات الدولية تحدياً جديداً لنظريات العلاقات الدولية وقوة طروحاتها التحليلية بشكل عام. إحدى هذه النظريات هي نظرية الواقعية الجديدة التي تساعد بنيتها المفاهيمية وافتراضاتها الرئيسة على فهم التفاعلات السيبرانية الدولية بدقة مقبولة. من البدء، إن تصور الواقعية الجديدة لفوضوية النظام الدولي هي الصورة أكثر دقة للفضاء السيبراني الفوضوي. وتعد الدول أهم الفاعلين المؤثرين في الفضاء السيبراني، وخاصة الدول الكبرى. وفي بيئة سيبرانية فوضوية، لا تثق الدول ببعضها البعض، وعدم اليقين والشك في قدرات ونوايا بعضها البعض هما الحالة السائدة في العلاقات بين الدول. عليه، تسعى الدول إلى تعظيم قوتها السيبرانية إلى حد فرض هيمنتها في الفضاء السيبراني سبيلاً لضمان أمنها السيبراني. ولكن ستكون هذه الخطوة على حساب أمن الآخرين، مما تدفعهم إلى اللجوء هم أيضاً لإتخاذ الخطوة نفسها من أجل ضمان أمنهم السيبراني أيضاً. وتستمر هذه الخطوات إلى أن تجد الدول نفسها في معضلة أمنية سيبرانية نتيجة سباق تسلح سيبراني دولي. في بيئة سيبرانية كهذه، سيكون الردع السيبراني كأداة للحفاظ على الأمن السيبراني ضعيفًا، كما يختل التوازن السيبراني بين الهجوم والدفاع لصالح الهجوم.

وعلى الرغم من القوة التي تتمتع بها مفاهيم وافتراضات نظرية الواقعية الجديدة لتطبيقها على الفضاء السيبراني، إلا أن النظرية لا تزال تعاني من بعض القصور والإشكاليات في التحليل، وعلى وجه الخصوص في تجاهلها لتأثير الفاعلين من غير الدولة في الفضاء السيبراني، وإشكالية قياس القوة السيبرانية وتفسير التفاعلات السيبرانية الدولية محدودة الحدة والعنف والتهديد. بالإضافة إلى ذلك، يلعب

عامل الوقت دوراً في تغيير إختلال التوازن بين الهجوم والدفاع في الوقت الراهن لصالح الهجوم نحو حالة التوازن أو حتى تفوق الدفاع مستقبلاً في المجال السيبراني.

وأخيراً، وعلى الرغم من الانتقادات والقصور التحليلية، تقدم نظرية الواقعية الجديدة إطارًا تحليليًا مهمًا لفهم تعقيدات الفضاء السيبراني بشكل عام، والأمن السيبراني بشكل خاص.

الهوامش:

([1]) Richard Little, Structuralism and Neo-Realism, in: Margot Light and A. J. R. Groom (eds.), International Relations: A Handbook of Current Theory, 2nd ed., (London: Bloomsbury Academic, 2016), 74.

([2]) Felix Rösch and Richard Ned Lebow, A Contemporary Perspective on Realism, in: Stephen McGlinchey, Rosie Walters and Christian Scheinpflug (Eds.), International Relations Theory, (Bristo: E-International Relations Publishing, 2017), 138.

([3]) د. أنور محمد فرج، نظرية الواقعية في العلاقات الدولية: دراسة نقدية مقارنة في ضوء النظريات المعاصرة، (السليمانية: مركز كوردستان للدراسات الإستراتيجية، ٢٠٠٧)، ١٦٩.

([4]) Steven E. Lobell, Structural Realism/Offensive and Defensive Realism, The International Studies Compendium Project (Oxford: Wiley-Blackwell, 2010), 6651.

([5]) Madeline Carr, US Power and the Internet in International Relations: The Irony of the Information Age, (Hampshire: Palgrave Macmillan, 2016), 39.

([6]) د. إيهاب خليفة، الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، (القاهرة: العربي للنشر والتوزيع، ٢٠٢١)، ٢٧.

([7]) أنديرا عراجي، "القوة في الفضاء السيبراني: فصل عصري من التحدي والإستجابة،" (رسالة دبلوم دراسات عليا، الجامعة اللبنانية، ٢٠١٥-٢٠١٦)، ص٢٥.

([8]) د. ماجد محمد الحنيطي، تكنولوجيا الصراعات الدولية المعاصرة، (عمان: الآن ناشرون وموزعون، ٢٠٢١)، ٢٤٠.

([9]) Muhammad Abdurrohim, Indah Kumalasari and Fathur Rosy, "The Paradox of Indonesia Cyberspace Policy and Cooperation: Neoclassical Realism Perspective," Jurnal Hubungan Internasional 11: 2 (2023): 20.

([10]) George Lucas, Cybersecurity and Cyber Warfare: The Ethical Paradox of Universal Diffidence, in: Markus Christen, Bert Gordijn and Michele Loi (eds.), The Ethics of Cybersecurity, (Switzerland: Springer Open, 2020), 248.

([11]) Zachary A. Poindexter, "Effects of Defend Forward on Security; Stability and U.S. Interest in the Cyber Domain," (Master's Thesis, Naval Postgraduate School, 2022), 48.

([12]) د. هبة جمال الدين، "الأمن السيبراني والتحول في النظام الدولي،" مجلة كلية الإقتصاد والعلوم السياسية ٢٤: ١ (كانون الثاني ٢٠٢٣): ٢٠٥.

([13]) James Adams, "Virtual Defense," Foreign Affairs 80: 3 (May - Jun., 2001): 98.

([14]) Joseph Da Silva, "Cyber Security and the Leviathan," Computers & Security 116 (May 2022): 3.

([15]) Constantine J. Petallides, "Cyber Terrorism and IR Theory: Realism; Liberalism; and Constructivism in the New Security Threat," Inquiries Journal 4:3, (2012), Available at:

http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat, (Accessed August 17, 2023).

([16]) Michael McKoy, Neoconservatism: A Death Prematurely Foretold, in: Edwin Daniel Jacob (ed.), Rethinking Security in the Twenty-First Century: A Reader, (New Jersy: Palgrave Macmillan: 2017), 285.

([17]) Steven E. Lobell, "Structural Realism/Offensive and ….," Op. cit., 6651.

([١٨]) جون ميرشايمر، مأساة سياسة القوى العظمى، تر. د. مصطفى محمد قاسم، (الرياض: النشر العلمي والمطابع– جامعة الملك سعود، ٢٠١٢)، ٣٧.

([19]) Madeline Carr, US Power and the …. Op., cit., 78.

([٢٠]) فرهاد جلال مصطفى، الأمن ومستقبل السياسة الدولية، (السليمانية: أكاديمية التوعية وتأهيل الكوادر، ٢٠١٠)، ١٤٥.

([٢١]) د. عامر مصباح، "الفضاء السيبراني نموذج لتوسيع عقيدة الدفاع الإستراتيجي،" ستراتيجيا ٨: ٢ (كانون الثاني ٢٠٢١): ٤٢.

([22]) Ben Buchanan, The Cybersecurity Dilemma: Hacking; Trust and Fear between Nations, (London: Hurst and Company, 2016), 23.

([23]) Ilona Stadnik, "What is an International Cybersecurity Regime and How We Can Achieve It," Masaryk University Journal of Law and Technology 11:1 (Summer 2017): 137-138.

([24]) Ben Buchanan, The Cybersecurity Dilemma …., Op. Cit. 41-42.

([25]) Myriam Dunn Cavelty, "Cybersecurity Research Meets Science and Technology Studies," Politics and Governance 6:2 (June 2018): 26.

([26]) Yavuz Akdağ, "Great Power Cyberpolitics: Re-interpreting Offensive Realism and Power Transition Theory for Cyber Deterrence," (PhD Diss., University of South Florida, November 2023), 25.

([27]) Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," Joint Force Quarterly 77:2 (April 2015): 11. وكذلك: د. رغدة البهي، "الردع السيبراني: المفهوم والإشكاليات والمتطلبات،" مجلة العلوم السياسية والقانون ١ (كانون الثاني ٢٠١٧): ٥٥–٥٨.

([٢٨]) تيم دان، ميليا كوركي وستيف سميث (محررون)، نظريات العلاقات الدولية: التخصص والتنوع، تر. ديما الخضرا، مر. بشير محمد الخضرا، (الدوحة: المركز العربي للأبحاث ودراسة السياسات، ٢٠١٦)، ٧٥٥.

([29]) Patrick James, Realism and International Relations: A Graphic Turn Toward Scientific Progress, (New York: Oxford University Press, 2022), 448.

([30]) John Arquilla, "Cyberwar is Already Upon Us: But can it be Controlled", Foreign Policy, February 27, 2012, Available at: https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/, (Accessed November 2, 2022).

([31]) Reto Inversini, Cyber Peace: And How It can be Achieved, in: Markus Christen, Bert Gordijn and Michele Loi (eds.), The Ethics of Cybersecurity, (Switzerland: Springer Open, 2020), 267.

([32]) George Lucas, Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare, (New York: Oxford University Press, 2017), 127.

([33]) Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, (New York: W.W. Norton and Company, 2015), 103 (in PDF copy).

([34]) Ilona Stadnik, "What is an International Cybersecurity …., Op., Cit., 138.

([35]) Reto Inversini, Cyber Peace: And How …, Op. Cit., 267.

([36]) P. W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, (New York: Oxford University Press, 2014), 155.

([37]) Rika Isnarti, "A Comparison of Neorealism; Liberalism; and Constructivism in Analysing Cyber War," Andalas Journal of International Studies 5: 2 (November 2016): 156-157.

([38]) Ibid, 157.

* ريتو إنفرسيني هو باحث في جامعة العلوم التطبيقية في بيرن بالفدرالية السويسرية يبحث في مجالات الاستجابة للحوادث الأمنية وتصميم الشبكات وهندسة الأمن.

([39]) Reto Inversini, Cyber Peace: And How …., Op. Cit., 267-268.

([40]) Christopher Whyte and Brian M. Mazanec, Understanding Cyber Warfare: Politics, Policy and Strategy, 2nd ed., (London: Routledge, 2023), 48.

([41]) Richard David Hallows, "Securitization and the Role of the State in Delivering UK Cyber Security in a New-Medieval Cyberspace," (PhD Diss., University of Buckingham, 2020), 41.

([42]) Brain C. Schmidt, The Primacy of National Security, in: Steve Smith, Amelia Hadfield and Tim Dunne (Editors), Foreign Policy: Theories; Actors; Cases, 3rd. ed., (Oxford: Oxford University Press, 2016), 208.

([43]) Johan Eriksson and Giampiero Giacomello, International Relations; Cybersecurity, and Content Analysis: A Constructivist Approach, in: Maximilian Mayer, Mariana Carpes and Ruth Knoblich (eds.), The Global Politics of Science and Technology: Perspectives; Cases and Methods, Vol.2, (n. p.: Springer, 2014) 208.

([٤٤]) على جلال معوض، "تأثير البيانات الضخمة في نظريات العلاقات الدولية،" السياسة الدولية، ملحق إتجاهات نظرية في تحليل السياسة الدولية ٢١٩ (يناير ٢٠٢٠): ١٠.

([45]) Stefan Fritsch, Conceptualizing the Ambivalent Role of Technology in International Relations: Between Systemic Change and Continuity, in: Maximilian Mayer, Mariana Carpes and Ruth Knoblich (eds.), The Global Politics of Science and Technology: Concepts from International Relations and Other Disciplines, Vol.1, (Heidelberg: Springer, 2014), 121, 130.

([46]) Madeline Carr, US Power and the … Op., cit., 16.

([47]) Rika Isnarti, "A Comparison of Neorealism; Liberalism," …, Op. Cit., 157.

([48]) James Adams, "Virtual Defense," Op., Cit., 98.

([49]) Rika Isnarti, "A Comparison of Neorealism; Liberalism," …, Op. Cit., 157.

([٥٠]) د. إيهاب خليفة، الحرب السيبرانية: الإستعداد ...، مرجع سابق، ٣١.

([51]) Thomas Rid, "Cyber War Will Not Take Place," Journal of Strategic Studies 35: 1, (February 2012): 8.

([٥٢]) جون ميرشايمر، مأساة سياسة القوى العظمى، مرجع سابق، ٤٩–٥٠.

([53]) Dan Lindly and Ryan Schildkraut, "Is War Rational: The Extent of Miscalculation and Misperception as Causes of War", 2005, Available at: https://www3.nd.edu/~dlindley/IWR/IWR%20Article.htm, (Accessed June 14, 2023).

([٥٤]) وليد عبد الحي، "نموذج اتخاذ القرار في الحرب السعودية على اليمن"، الخليج الجديد، الاثنين ١١ أكتوبر ٢٠٢١، https://thenewkhalij.news/article/245591، (تأريخ زيارة الموقع: ٥ شباط، ٢٠٢٢).

قائمة المراجع

أولاً: الكتب

١) الحنيطي، ماجد محمد. تكنولوجيا الصراعات الدولية المعاصرة. عمان: الآن ناشرون وموزعون. ٢٠٢١.

٢) خليفة، إيهاب. الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس. القاهرة: العربي للنشر والتوزيع. ٢٠٢١.

٣) دان، تيم. كوركي، ميليا. سميث، ستيف (محررون). نظريات العلاقات الدولية: التخصص والتنوع. تر. ديما الخضرا. مر. بشير محمد الخضرا. الدوحة: المركز العربي للأبحاث ودراسة السياسات. ٢٠١٦.

٤) فرج، أنور محمد. نظرية الواقعية في العلاقات الدولية: دراسة نقدية مقارنة في ضوء النظريات المعاصرة. السليمانية: مركز كوردستان للدراسات الإستراتيجية. ٢٠٠٧.

٥) مصطفى، فرهاد جلال. الأمن ومستقبل السياسة الدولية. السليمانية. أكاديمية التوعية وتأهيل الكوادر. ٢٠١٠.

٦) ميرشايمر، جون. مأساة سياسة القوى العظمى. تر. د. مصطفى محمد قاسم. الرياض: النشر العلمي والمطابع–جامعة الملك سعود. ٢٠١٢.

7) Buchanan, Ben. The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations. London: Hurst and Company. 2016.

8) Carr, Madeline. US Power and the Internet in International Relations: The Irony of the Information Age. Hampshire: Palgrave Macmillan, 2016.

9) Eriksson, Johan. and Giacomello, Giampiero. International Relations; Cybersecurity and Content Analysis: A Constructivist Approach, in: The Global Politics of Science and Technology: Perspectives; Cases and Methods. Edited by Mayer, Maximilian. Carpes, Mariana. and Knoblich, Ruth. Vol.2. n. p.: Springer, 2014.

10) Fritsch, Stefan. Conceptualizing the Ambivalent Role of Technology in International Relations: Between Systemic Change and Continuity. In: The Global Politics of Science and Technology: Concepts from International Relations and Other Disciplines. Edited by Mayer, Maximilian., Carpes, Mariana. and Knoblich, Ruth. Vol.1. Heidelberg: Springer. 2014.

11) Inversini, Reto. Cyber Peace: And How It can be Achieved. In: The Ethics of Cybersecurity. edited by Christen, Markus., Gordijn, Bert. and Loi, Michele. Switzerland: Springer Open. 2020.

12) James, Patrick. Realism and International Relations: A Graphic Turn Toward Scientific Progress. New York: Oxford University Press, 2022.

13) Lebow, Richard Ned., and Felix, Rösch. A Contemporary Perspective on Realism. in: International Relations Theory. edited by McGlinchey, Stephen., Walters, Rosie. and Scheinpflug, Christian. Bristo: E-International Relations Publishing. 2017.

14) Little, Richard. Structuralism and Neo-Realism. In: International Relations: A Handbook of Current Theory, 2nd ed., edited by Light, Margot. And Groom, A. J. R. London: Bloomsbury Academic. 2016.

15) Lobell, Steven E. "Structural Realism/Offensive and Defensive Realism." in: The International Studies Compendium Project. Oxford: Wiley-Blackwell, 2010.
16) Lucas, George. Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. New York: Oxford University Press, 2017.
17) Lucas, George. Cybersecurity and Cyber Warfare: The Ethical Paradox of Universal Diffidence. In: The Ethics of Cybersecurity. edited by Christen, Markus., Gordijn, Bert. and Loi, Michele. Switzerland: Springer Open. 2020.
18) McKoy, Michael. Neo-conservatism: A Death Prematurely Foretold. In: Rethinking Security in the Twenty-First Century: A Reader. edited by Jacob, Edwin Daniel. New Jersey: Palgrave Macmillan. 2017.
19) Schneier, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton and Company, 2015.
20) Schmidt, Brain C. The Primacy of National Security, in: Foreign Policy: Theories; Actors; Cases. Edited by Smith, Steve. Hadfield, Amelia. and Dunne, Tim. 3rd ed. Oxford: Oxford University Press. 2016.
21) Singer, P. W., and Friedman, Allan. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press. 2014.
22) Whyte, Christopher, and Mazanec, Brian M. Understanding Cyber Warfare: Politics; Policy and Strategy, 2nd ed. London: Routledge, 2023.

ثانياً: المجلات والأوراق علمية

١) البهي، رغدة. "الردع السيبراني: المفهوم والإشكاليات والمتطلبات." مجلة العلوم السياسية والقانون ١ (كانون الثاني ٢٠١٧): ٤٨-٦٦.
٢) جمال الدين، هبة. "الأمن السيبراني والتحول في النظام الدولي." مجلة كلية الإقتصاد والعلوم السياسية ٢٤: ١ (كانون الثاني ٢٠٢٣):
٣) مصباح، عامر. "الفضاء السيبراني نموذج لتوسيع عقيدة الدفاع الإستراتيجي." ستراتيجيا ٨: ٢ (كانون الثاني ٢٠٢١):
٤) معوض، على جلال. "تأثير البيانات الضخمة في نظريات العلاقات الدولية." السياسة الدولية، ملحق إتجاهات نظرية في تحليل السياسة الدولية ٢١٩ (يناير ٢٠٢٠):
5) Abdurrohim, Muhammad. Kumalasari, Indah. And Rosy, Fathur. "The Paradox of Indonesia Cyberspace Policy and Cooperation: Neoclassical Realism Perspective." Jurnal Hubungan Internasional 11: 2 (2023): 13-23.
6) Adams, James. "Virtual Defense." Foreign Affairs 80: 3 (May - Jun. 2001): 98-112.
7) Cavelty, Myriam Dunn. "Cybersecurity Research Meets Science and Technology Studies." Politics and Governance 6: 2 (June 2018): 22-30.
8) Da Silva, Joseph. "Cyber security and the Leviathan." Computers & Security 116 (May 2022): 1-17.
9) Denning, Dorothy E. "Rethinking the Cyber Domain and Deterrence." Joint Force Quarterly 77: 2 (April 2015): 8-15.

10) Isnarti, Rika. "A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War." Andalas Journal of International Studies 5: 2 (November 2016): 151-165.
11) Rid, Thomas. “Cyber War Will Not Take Place.” Journal of Strategic Studies 35:1 (February 2012): 5-32.
12) Stadnik, Ilona. “What is an International Cybersecurity Regime and How We Can Achieve It.?” Masaryk University Journal of Law and Technology 11:1 (summer 2017): 129-154.

ثالثاً: الرسائل الجامعية

١) عراجي، أنديرا. "القوة في الفضاء السيبراني: فصل عصري من التحدي والاستجابة". رسالة دبلوم دراسات عليا. الجامعة اللبنانية. ٢٠١٥-٢٠١٦.
2) Akdağ, Yavuz. “Great Power Cyberpolitics: Re-interpreting Offensive Realism and Power Transition Theory for Cyber Deterrence.” PhD Diss. University of South Florida. 2023.
3) Hallows, Richard David. “Securitisation and the Role of the State in Delivering UK Cyber Security in a New-Medieval Cyberspace.” PhD Diss. University of Buckingham. 2020.
4) Poindexter, Zachary A. “Effects of Defend Forward on Security; Stability and U.S. Interest in the Cyber Domain” Master’s Thesis. Naval Postgraduate School. 2022.

رابعاً: شبكة الانترنيت

١) عبد الحي، وليد. نموذج اتخاذ القرار في الحرب السعودية على اليمن. الموقع الإلكتروني لـ (الخليج الجديد). تأريخ النشر: الاثنين ١١ أكتوبر ٢٠٢١. https://thenewkhalij.news/article/245591/ (زيارة الموقع: ٥ شباط ٢٠٢٢).
2) Arquilla, John. “Cyberwar is Already upon Us: But can it be controlled.” Foreign Policy. February 27. 2012. Available at: https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/
3) (Accessed November 2, 2022).
4) Lindly, Dan. Ryan, Schildkraut. “Is War Rational: The Extent of Miscalculation and Misperception as Causes of War.” 2005. Available at: https://www3.nd.edu/~dlindley/IWR/IWR%20Article.htm/ (Accessed June 14, 2023).
5) Petallides, Constantine J. “Cyber Terrorism and IR Theory: Realism; Liberalism; and Constructivism in the New Security Threat.” Inquiries Journal 4:3. (2012). http://www.inquiriesjournal.com/articles/ (Accessed August 17, 2023).