الأمن السيبراني و تأثيراته على هيكل النظام الدولي.

م.م غاردينيا محمد رشيد

جامعة ميسان / كلية التربية الأساسية

mghardynya@gmail.com

المستخلص:

يحظى الأمن والقضاء السيبراني باهتمام العديد من الباحثين خاصة مع ظهور تهديدات قد تصل لحرب إلكترونية. وفي هذا السياق، اهتم علماء السياسة بتفسير هذه القضايا، الأمر الذي خلق ساحة من الجدل والنقاش حول تأثير الأمن السيبراني على شكل النسق الدولي، وما يتضمنه من وحدات ومؤسسات وبنية وتفاعلات وعمليات عالمية تقع في نطاقه. ويقدم هذا البحث استعراضا لأهم القضايا الجدلية المطروحة بين علماء السياسية في هذا الشأن. وينقسم البحث بدوره لأربعة مباحث رئيسة المبحث الأول يتناول الوحدات الدولية الفاعلة في النظام الدولي، أما المبحث الثاني فيناقش تأثير الأمن السيبراني على مجموعة المؤسسات الدولية، في حين أن المبحث الثالث يطرح التغير الذي أحدثه الأمن السيبراني على هيكل النظام الدولي، أما المبحث الرابع يستعرض لأبرز العمليات الدولية الواقعة بداخل الفضاء السيبراني بالنسق الدولي. وتستخدم الورقة اقتراب النسق الدولي (الاقتراب النظمي) للوقوف على هيكل النظام الدولي والفواعل الرئيسية بداخل الفضاء السيبراني وما أحدثه الأمن السيبراني من تغير على القواعد والعمليات بداخل النسق الدولي.

كلمات مفتاحية: الأمن السيبراني، الفضاء السيبراني، الهجمات السيبرانية، النظام الدولي، اقتراب النسق الدولي .

مقدمــة:

ظهر الفضاء السيبراني كبيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية، مكونة من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات والمستخدمين سواء مشغلين أو مستعملين، وزاد الاهتمام بالمفهوم مع زيادة اعتماد العالم على الكمبيوتر والشبكة العنكبوتية وتعبره جامعة هارافارد "الذراع الرابعة للجيوش الحديثة"، وتعود إرهاصاته إلى منتصف الخمسينيات من القرن الماضي مع بداية استخدام الحاسب الألي لمعالجة وحفظ المعلومات. ومع مطلع التسعينيات وظهور الإنترنت وإقبال الكثير من الدول على استخدامها في المجال الأمني والعسكري لتحقيق قفزات نوعية في المجالات الأمنية والسياسية. اهتم علماء السياسة بتفسير هذا السلوك

وظهرت دراسات تتناول هذا التطور التكنولوجي وآثاره السياسية كدراسة المعهد الدولي للدراسات الاستراتيجية بلندن.(عبدالمنعم،٢٠٢٠)

وبدأ الحديث عن قدرة شبكة المعلومات الدولية على إعادة بلورة الأشكال التقليدية وقواعد القوة الدولية والمقدرات الدولية للوحدات الفاعلة في النسق الدولي ، ومع هذا التطور جاء الحديث عن الأمن السيبراني الذي يعني أمن المعلومات وأمن الحاسوب كفرع من فروع التكنولوجيا؛ يهتم بممارسة حماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية وتستهدف عادة الوصول للمعلومات الحساسة، أو تغييرها، أو إتلافها، وابتزاز المال من المستخدمين، وتعطيل العمليات التجارية. ويعرفه "إدوارد أموروسو" صاحب كتاب الأمن السيراني عام ٢٠٠٧؛ بأنه مجموعة الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات. فالأمن السيبراني هو ممارسة الدفاع عن أجهزة الكمبيوتر، والخوادم، والأجهزة المحمولة، والأنظمة الإلكترونية، والشبكات، والبيانات من الهجمات الخبيثة.(المسعودي،٢٠٢١)

ويأتي الاهتمام بالأمن السيبراني مع زيادة الخسائر الناتجه عن الهجمات الألكترونية، وما يعنيه ذلك من تهديدات على الأمن القومي للدول، وبالتبعية على السلم والأمن الدوليين. فمن المتوقع أن تصل الأضرار الناجمة عن جرائم الإنترنت إلى ما يقدر بنحو ١٠.٥ تريليون دولار بحلول عام ٢٠٢٥ وفقا لتقديرهارفارد فيتمثل الهدف الأساسي للأمن السيبراني في تعزيز قدرة الدول على مقاومة التهديدات الكامنة في الفضاء السيبراني، الأمر الذي دفع كثير من دول العالم لوضعه على أجندة عملها، في ظل ظهور الحروب الإلكترونية التي تتعرض لها الكثير من الدول، فانتشار القوة السيبرانية بين عدد كبير من الفاعلين على الساحة الدولية ضرب في قدرة الدول على السيطرة والهيمنة، بل ومنحت فاعلين أصغر قدرة مساحة أكبر لممارسة للعب دور مهم عبر الفضاء السيبراني؛ مما يعني تغير في مقدرات القوى بالنظام الدولي. الأمر الذي غير ماهية بعض التفاعلات بين الوحدات الدولية الفاعلة، كالصراع، والتعاون، والردع والقوة عبر العالم الافتراضي المتشابك (فياض،٢٠٢٠)

من هنا، كان الاهتمام من قبل فرع العلاقات الدولية بدراسة تأثير الأمن السيبراني على النظام الدولي، لتقديم تصور للعلاقات الدولية في كليتها في ظل الفضاء السيبراني، وما يصاحبه من ظواهر جديدة مصاحبة، علاوة على أهمية تفسير سلوك وسياسات الوحدات المكونة للنسق الدولي واهتمامها بقضايا الأمن السيبراني في ظل قدرتها على التأثير على المستوى الدولي. للوقوف على نمط التفاعلات والعلاقات بين الوحدات الأساسية الموجودة بالنسق العالمي، فهل يغلب عليها الصراع أم التعاون، أم التكامل أم خلقت أنماطا مستحدثة من التفاعلات في ظل هذا الفضاء السيبراني.

وتأتي الأهمية العملية بهذه القضية في ضرورة الوقوف على تأثير الأمن السيبراني على شكل النظام العالمي الجديد الذي أخذ في التبلور والتغير، فمن المهم معرفة إلى أي درجة يساعد اهتمام دول العالم بقضايا الأمن السيبراني، وما يصاحبه من آليات وتقنيات حديثة على تغير بنية النظام الدولي، فهل يساعد على خلق تفاعلات

جديدة؟، وهل يعطي مساحة للتعاون والتنمية، أم أنه يغير معايير وتوازنات القوة الأمر الذي قد يهدد السلم والأمن الدوليين؟.(عبدالحميد،٢٠٢١)

واتساقا مع ما تم ذكره، حاول علماء السياسة البحث في جدلية تأثير الأمن السيبراني على النظام الدولي، وانشغلت مراكز الفكر بتلك القضية كالأكاديمية الملكية الايرلندية عام ٢٠١٨، عبر دراسة تأثير الطابع الفوضوي للفضاء السيبراني على الاقتراحات القيمية للحفاظ على المصلحة الوطنية للدولة في المستقبل السيبراني ،وطرح معهد بروكنجز عام ٢٠١٩ قضية تأثير تكنولوجيا الـ G٥ على الامن السيبراني وانعكاساته في التفاعلات بين الوحدات الدولية المختلفة؛ كالحكومات والشركات متعددة الجنسيات واهتم Vladimir Tsakanyan بجامعة الصداقة بين الشعوب في روسيا بقضية دور الأمن السيبراني على السياسات الدولية عام ٢٠١٧، واعتبرت الورقة أن الأمن السيبراني من أهم أدوات الدول لحماية مصلحتها الوطنية، وفرقت بين تلك الاعتبارات الاستقرار العالمي في السياسة الدولية. وفي عام ٢٠١٤ قامت مركز الدراسات الكونية بجامعة بون، ومنظمة فريدريش ناومن للحرية بألمانيا، بدراسة الفضاء السيبراني والعلاقات الدولية النظرية والمأمول والتحديات، وتسعي الدراسة لتوضيح العلاقة بين الفضاء السيبراني والعلاقات الدولية من الناحية المفاهيمية والنظرية، لمناقشة الآثار المترتبة على النظام الدولي، وتقديم مناهج نظرية جديدة ومبتكرة لشرح ديناميكيات هذه العلاقة في مجالات نشاط محددة (مثل الأمن السيبراني والحرب الإلكترونية ونشر المعلومات و المعرفة من خلال الفضاء السيبراني، والترابط بين الأنشطة الاقتصادية والاجتماعية من خلال الفضاء السيبراني وما إلى ذلك) بهدف رفع الوعي بعواقب وتأثيرات وانعكاسات عملية "التحول عبر الإنترنت" لأمن الدول، وتحديد مواقع السلطة وكذلك للجهات الفاعلة الاقتصادية والمدنية التي تتأثر بالمثل بـ "التحول الإلكتروني" (الفتلاوي،٢٠٢١)

وفي عام ٢٠١٨ قامت جامعة لانكستر بدراسة تحمل عنوان الأمننة Securitization، والسياسات العالمية للأمن السيبراني، وتوصلت الدراسة أن الأفراط في التخوف من الأثار الأمنية للتهديدات السيبرانية، والاهتمام الجم بتحقيق الأمان؛ قد تجعلنا نهمل التركيبة المتشابكة للأمن السيبراني في سياقات جيوسياسية واقتصادية مختلفة حول الكوكب. فالكثير من الأحداث السيبرانية تنبثق من الطبيعة المتشابكة للأحداث في القرن الحادي والعشرين، فقد تكون هناك أيضا اتجاهات وتطورات جديدة في طرق استخدام التقنيات الجديدة، وإساءة استخدامها في سياقات مختلفة، أي أن التحديات السيبرانية قد تتأثر باختلاف السياق والتداعيات المحلية، وتؤكد الدراسة على أهمية الاستفادة من تجارب الأخرين، ونقاط الضعف التي يتم تجاهلها في خرائط الجغرافيا السياسية واستكمال البحث العلمي على الصعيد العالمي بتلك القضية محل البحث. ومع هذا الزخم البحثي إلا أنه يلاحظ أن أغلب تلك الدراسات أكدت على أهمية استكمال العمل البحثي في دراسة هذه القضية التي تتطلب مزيدا من البحث والتمحيص، ومن ثم تأتي أهمية هذه الدراسة في استكمال الجدل النظري وتقديمه للمكتبة العربية.(عبدالمنعم،٢٠٢١)

من هذا الإطار، يمكن القول أن هذه الورقة تحاول الإجابة على تساؤل رئيسي يتمثل في ماهية تأثير الأمن السيبراني على النظام الدولي بوحداته، وبنيته وهيكله والتفاعلات بين وحداته، المختلفة والعمليات الدولية، والمؤسسات الدولية والقواعد المنظمة داخل النسق الدولي؟.

١.مشكلة وتساؤلات الدراسة:

ينطلق البحث من إشكالية رئيسية فحواها ماهية تأثير الأمن السيبراني على النظام الدولي، بوحداته وبنيته وهيكله والتفاعلات بين وحداته المختلفة، والعمليات الدولية، والمؤسسات الدولية والقواعد المنظمة داخل النسق الدولي؟، عبر الإجابة على عدة تساؤلات فرعية:

- ما هى الوحدات الدولية الفاعلة في الفضاء السيبراني والنظام الدولي؟
- ما هى سمات التفاعلات الدولية في النظام الدولي ذات الفضاء السيبراني؟
- ما هو تأثير الامن السيبراني على هيكل النظام الدولي؟
- هل تتأثر بعض المبادئ المنظمة للنظام الدولي والمنظمة الأممية بفعل الأمن السيبراني؟

٢.منهج الدراسة:

يطبق البحث اقتراب النسق الدولي لدراسة تأثير الأمن السيبراني على النظام الدولي بنيانا، ووحدات، ومؤسسات، وعمليات للوقوف على مدى التغير الذي طرحه الأمن السيبراني والفضاء السيبراني على النسق العالمي، للتعرف على ماهية الوحدات الفاعلة والعلاقات والتفاعلات بينها، وشكل بنية النظام وتوزيع مقدرات القوى بين الوحدات الفاعلة، وتأثير ذلك على المبادئ المنظمة للتفاعلات بين الدول ووحداتها الفاعلة،على اعتبار أن النظام الدولي مجموعة من التفاعلات المتداخلة والمعتمدة على بعضها البعض بين الفاعلين الدوليين على الساحة الإقليمية والدولية، من خلال تطبيق مفهوم مورتون كابلن باعتبار النظام الدولي نظاما كليا؛ يتكون من تفاعلات بين الوحدات الدولية التي لا تتسم بالتعاون الكامل، ولا بالصراع الكامل. وذلك للوقوف على السمات الغالبة على التفاعلات بين الوحدات هل يغلب عليها التعاون، أم الصراع أم الحرب، أم سباق التسلح، وما وضع الهجوم، والدفاع في ظل فضاء سيبراني تكثر بداخله الهجمات السيبرانية. وذلك بهدف تفسير قدرة الأمن السيبراني على خلق تفاعلات جديدة بداخل النسق الدولي، وتغير معايير وتوازنات القوى وتحقيق الاستقرار ببنية النظام الدولي(نافعه،٢٠٢٠)

٣.تقسيم الدراسة:

تنقسم الورقة البحثية لأربعة مباحث رئيسة **المبحث الأول** يتناول الوحدات الدولية الفاعلة في النظام الدولي، أما **المبحث الثاني** فيناقش تأثير الأمن السيبراني على مجموعة المؤسسات الدولية، في حين أن **المبحث الثالث**

فيطرح التغير الذي أحدثه الأمن السيبراني على هيكل النظام الدولي، أما **المبحث الرابع** فيطرح أبرز العمليات العالمية الواقعة بداخل الفضاء السيبراني بالنسق الدولي.

المبحث الأول: الوحدات الدولية الفاعلة في النظام الدولي:

جاءت ثورة المعلومات لتتحدي الافتراض الأساسي للمدرسة الواقعية القائل بأن الدول هي أقوى الجهات الفاعلة، وبالتالي أهمها في السياسة الدولية. فتتحدى المعلوماتية أسبقية الدولة، بسبب زيادة مشاركة الجهات الفاعلة غير الحكومية التي تهدد ديناميكيات السلطة التقليدية، وتزداد أهمية الجهات الفاعلة غير الحكومية في العلاقات الدولية وفقا لجوزيف ناي حول انتشار السلطة، ففي المجال السيبراني يمكن للمجرمين من الأفراد والمنظمات والجماعات الإرهابية الاستفادة من إمكانية الوصول للإنترنت لتهديد هيمنة الدولة. كما تلعب الشركات الخاصة دورًا، كمزود للأمن ومصدر للضعف في ذات الوقت. وعلى الرغم من أن الدول لا تزال هي الجهات الفاعلة الأكثر هيمنة عندما يتعلق الأمر بالنزاع السيبراني. تلعب الجهات الفاعلة غير الحكومية والإرهابيون دورًا، لكن تكتيكاتهم كانت عمومًا غير فعالة أو استخدمت كغطاء للدول القومية التي تسعى لإخفاء أفعالها.ويرى جوزيف ناي أن الدول يمكنها على نحو أفضل من غيرها من الفاعلين الدوليين استثمار أدوات الحرب الإلكترونية وتوظيفها لتحقيق أهدافها الوطنية، كما يمكنها رفع قدرات القوى العاملة بالمجال، علاوة على الانفاق على البحث العلمي وR&D البحث والتطوير في مجال الأمن السيبراني.(الفتلاوي،٢٠٢١)

واتساقا مع ما تم ذكره، فقد انشغل علماء السياسة بالوقوف على ماهية الوحدات الفاعلة في ظل النظام العالمي الجديد، الذي يحتل فيه مفهوم الأمن السيبراني ثقل على الصعيد الدولي. فهناك من اعتبر أن التحول الرقمي والأمن السيبراني له تأثير على الفاعلين العاملين بالنسق الدولي، وهناك من اعتبره محفزا لظهور فاعلين جدد، وهناك من اعتبره هو ذاته فاعلا في التنظيم الدولى.

الشكل رقم ١: أبرز الوحدات الدولية الفاعلة في النظام الدولي

يتضح من الشكل السابق تعدد تصنيفات الفاعلين من غير الدول في الفضاء السيبراني؛ ما بين الدول القومية الفاعل التقليدي في العلاقات الدولية، والفاعلين من غير الدول. وقد خلق الفضاء السيبراني فاعلين جدد مستحدثين كقوى التحول الرقمي ووسائل التواصل الاجتماعي، في حين نجد فاعلين أخرين لا يرتبط وجودهم بخصوصية الفضاء السيبراني، وإنما استفادوا مما خلقه من أدوات وآليات ليزداد دورها في الساحة العالمية؛ إيجابا كالشركات متعددة الجنسيات على سبيل المثال، أو سلبا كالجماعات الإرهابية.

ويمكن القول أن ظهور المنظمات الحكومية، كفاعل دولي داخل النسق العالمي يطرح إشكالية بشأن مدى استقلاليتها عن الدول الأعضاء؛ فالسلطة النهائية لاتخاذ قرارات هذه المنظمات وتنفيذها يعتمد على التأييد الذي تمنحه الدول الأعضاء للمنظمات، إلا أن بول ويلكينسون يرى أن درجة استقلاليتها تتفاوت، وبالتبعية تتفاوت درجة تأثيرها في العلاقات الدولية وتعتمد على عوامل عديدة منها طبيعة النظام الدولي، ومدى وجود تهديد خارجي كالهجمات السيبرانية، ومدي التناسق بين أعضائها ودرجة التفاهم على عناصر سياسية للعمل، وكذا قدرة الأمانة العامة لها على بلورة سياسة مستقلة للمنظمة .

وتثار أيضا إشكالية بشأن وسائل التواصل الاجتماعي باعتبارها تعكس توجه الأفراد مما يؤثر على استقلاليتها، إلا أن البروفسور فليب هاورد والباحثة سمانثا برادشو بمعهد اوكسفورد للانترنت يعتبران أن وسائل التواصل الاجتماعي خلقت قوات سيبرانية كونية Global Cyber Troops، يمكنها أن تتلاعب بإرادة الأفراد من قبل فاعلين أخرين. ويرصد تقرير النظام العالمي للمعلومات المضللة The Global Disinformation Order لعام ٢٠١٩ تلاعب وسائل التواصل الاجتماعي بإرادة الشعوب في ٧٠ دولة من قبل الحكومات والاحزاب السياسية منذ عام ٢٠١٧ حتى عام ٢٠١٩.

**الدول القومية "الفاعل التقليدي في العلاقات الدولية": تعتبر الدول بمختلف أحجامها، كبرى أو صغرى فاعل دولي مهما في النظام العالمي؛ بل هو الفاعل الأبرز وفقا للمدرسة الواقعية في العلوم السياسية. وقد انشغل علماء السياسة ومراكز الفكر البحثية بعدة إشكاليات تخص الدولة في النسق الدولي بعد ظهور مفهوم الأمن السيبراني، فطرحت عدة قضايا في هذا السياق كمدى تمتع الدولة بالسيادة في ظل الفضاء السيبراني والإكراه كسمات رئيسة محددة لوجود الدولة وبسط سلطتها ونفوذها بإقليمها ومحيطها الجغرافي. وبالمقابل في النسق الدولي، كذلك الأمر بشأن تفوقها سيبرانيا مقابل تهديدها للسلم والأمن الدوليين. علاوة على ماهية الأهداف الوطنية للدولة المفترض الاطلاع بها، هل تتفق مع تحقيق السلم والأمن الدوليين، وفقا لمبادئ التنظيم العالمي المستندة عليه الأمم المتحدة كالميثاق العالمي للأمم المتحدة وهذا ما سيتم طرحه فيما يلي:

**اشكالية سيادة الدولة في الفضاء السيبراني: أختلف علماء السياسة حول تأثير الأمن السيبراني على سيادة الدولة، فيرى دانيال لامباش أن الفضاء السيبراني ساهم في تعزيز سيادة الدولة عبر دعم "السيادة الإلكترونية"، أو "السيادة على البيانات"، أو ما يسمى بـ"السيادة الرقمية": أي فرض السيادة الوطنية بالفضاء السيبراني، بمعني تشكيل مناطق ذات سيادة وطنية في الفضاء السيبراني، استنادًا إلى نظرية الممارسة والمفاهيم المزدوجة لإعادة التوطين؛ وهو ما يُعرف بـ"الأنطولوجيا الإقليمية"، عبر طرق ووسائل تمارِس من خلالها الجهات الفاعلة (الدول أو غير ذلك) السيطرة على الفضاء السيبراني، كقيام الحكومات بقطع الإنترنت في أوقات الأزمات السياسية، أو التحكم في التعليمات البرمجية والخوارزميات بتقنيات الذكاء الاصطناعي، أو فرض الرقابة الصارمة على المحتوى، وهو ما تفعله تركيا وتايلاند. إضافة إلى اللجوء للقرصنة الوطنية أو فرض قوانين "توطين البيانات"

التي تحظر نقل البيانات عبر الحدود كالحالة الروسية والحالة الصينية، الأمر الذي يدعم إظهار قوة الدولة بشكل منتظم. فهناك العديد من الأدوات المتاحة للدول التي تسعى لإعادة إنشاء أراضيها الوطنية في الفضاء السيبراني، كحجب بروتوكول الإنترنت i](IP " Internet Protocol)[IP]، والبحث عن الكلمات الرئيسية لمراقبة المناقشات حول الموضوعات الحساسة، ومنع الوصول إلى مواقع الويب التي تعتبر تخريبية. وهو ما تم تطبيقه في العديد من الدول، كالجدار الناري العظيم في الصين، ونظم الرقابة الحكومية الصارمة على الإنترنت في كوريا الشمالية. وعلى الرغم من ذلك نجد هناكمن اعتبر الأمن السيبراني يحمل في طياته تهديدا لسيادة الدولة، وبسط نفوذها بسبب عمليات الاختراق والهجمات السيبرانية؛ كهجمات وسطاء الظل والثغرات الإلكترونية، واسعة المدى تتعدي حدود الدول الأمر الذي سيتم التعرض إليه بالتفصيل لاحقا (نافعه، و اخرون،٢٠٠٢)

**الاكراه السيبراني: تثير المدرسة الواقعية التساؤل عما إذا كانت القدرات الإلكترونية تمنح الدول سلطة قسرية، في إشارة إلى القدرة على تحفيز الإكراه على إرادة الفرد من خلال إلحاق الضرر بالعدو أو التهديد به. ومع ذلك، هناك شكوكا جدية حول فعالية الإكراه السيبراني، نظرًا لأن التكنولوجيا تفتقر للقدرة التدميرية للعمليات العسكرية التقليدية، ويقل احتمال أن تأخذها الدولة المستهدفة على محمل الجد. يضاف إلى قيود شن حرب إلكترونية على الشبكة المعلوماتية؛ فالأمر يتعلق بالسيطرة على البنية التحتية والعسكرية للخصم والقدرات العسكرية لبلد ما. فالأسلحة السيبرانية لا يمكن أن تكون فعالة إلا عند استخدامها بالتزامن مع العمليات العسكرية التقليدية. وهذا ما يؤكده كل منجينس نوفلريانوهومينيس خلال دراسة فعالية استخدام الأسلحة السيبرانية، حيث قاما بتحليل البيانات المتعلقة بالحوادث الإلكترونية بين الدول المتنافسة، ووجدوا أن الإجراءات الإلكترونية القسرية التي تهدف لتغيير سلوك الهدف غير فعالة بشكل عام مقارنةً بالتعطيل أو التجسس على نطاق أصغر. مما يؤكد أن المفاهيم التقليدية للقوة والحرب لا تترجم بالضرورة بشكل جيد إلى المجال السيبراني، فالقوة السيبرانية لا تحوّل لتوازنات في السياسة الدولية (عبدالفتاح،٢٠١٧)

**إشكالية التفوق السيبراني للدول مقابل تهديدها للسلم والأمن الدوليين: في إطار ضبابية الفضاء الافتراضي وصعوبة الوقوف على حقائق الإدانة، تدور حول الدول اتهامات بارتكاب أفعال لاختراق السلم والأمن الدوليين بحجة التفوق السيبراني أو الردع الافتراضي، لتحقيق السيادة والنفوذ والأغراض السياسية المحددة والمطروحة. ويمكن رصد السمات السياسية لبعض الهجمات السيبرانية حيث تدور الشبهات حول دول بعينها كاختراق مكتب إدارة شؤون الموظفين في الولايات المتحدة عام ٢٠١٤ وتم توجيه الاتهامات من قبل الحكومة الأمريكية إلى الصين، والهجوم السيبراني على أوكرانيا عام ٢٠١٥ وأسفر عن قطع الكهرباء على ربع مليون أوكراني الذي اتهمت خلاله روسيا. فعلى الرغم من سرية وعدم القدرة على إثبات تورط الدول المذكورة في تلك الاعتداءات والجرائم، ولكنها تعكس لجوء الدول للساحة السيبرانية لاستكمال صراعاتها، وبسط نفوذها سواء بالتورط في الهجوم أو حتى بالزعم بتورط الدولة المعادية لها سواء صح الزعم من عدمه. فالفضاء السيبراني أضحى ساحة للاتهام والتشويه والهجوم والتعدي. فمن الصعب رؤية خط واضح بين المكان الذي تبدأ فيه الدولة وأين تنتهي،

بشان الاختراق الإلكتروني. ففي هذا السياق، تستخدم تقنية "الأعلام المزيفة False Flags"، حيث تسمح للمهاجم بإخفاء هويته وترك الأدلة التي تشير إلى شخص آخر، وفي هذا السياق قامت بعض الدول المعتدية بتضليل أجهزة المخابرات لنسبة العمليات إلى الدولة التي تعارضها. وفي ظل ضبابية المشهد لا يُعرف الكثير علنًا عن القدرات الإلكترونية لغالبية الدول باستثناء الاختراقات المشتبه بها التي تم إطلاقها بالفعل، وذلك لأن هذه القدرات عادةً ما تكون سرية للغاية. بمجرد إطلاق أداة إلكترونية، يفقد مرتكب الجريمة ميزتها الاستراتيجية. (مازار و اخرون،٢٠١٦)،

**الأهداف السيبرانية الوطنية للدولة:قدم مركز بلفر سبعة أهداف رئيسة كأهداف وطنية تطلع بها الدول لحماية أمنها السيبراني تمثل في بعضها خرقا لحقوق الإنسان، بل وقد ترتقي إلى حد تهديد ركائز النظام الدولي فبدل أن تتسم بالرشادة لدعم السلم والأمن الدوليين أضحت تهدد السلم العالمي. يتمثل الهدف الأول في مسح ومراقبة المجموعات المحلية من خلال قيام الدولة، من منطلق حماية أمنها القومي بالمراقبة الإلكترونية لرصد واكتشاف وجمع المعلومات الاستخبارية عن التهديدات المحلية والجهات الفاعلة داخل حدودها. أم الهدف الثاني هو تقوية وتعزيز الدفاعات السيبرانية الوطنية: أي تعزيز الدولة لدفاعاتها الوطنية لحماية عن الأصول والأنظمة الحكومية والوطنية، وتحسين السيبرانية الوطنية والنظافة والمرونة. والهدف الثالث يقوم على التحكم في بيئة المعلومات ومعالجتها: أي ازدواجية ضوابط المعلومات، وتحكم الدول في المعلومات عبر استخدام الوسائل الإلكترونية وتغيير الروايات في الداخل والخارج وحاولت حماية خصوصية الإنترنت وحرية التعبير لمواطنيها. وبشأن الهدف الرابع يدور حول جمع المعلومات الاستخبارية من دول أخرى لحماية الأمن القومي: من خلال قيام دولة ما بانتزاع أسرارًا وطنية من خصم أجنبي كالمعلومات السرية عن الاتفاقيات، والخطط العسكرية السرية وسرقة الملفات والوصول إلى اتصالات كبار الشخصيات الحكومية مثل أعضاء البرلمان. (الفتلاوي،٢٠٢١)

**والهدف الخامس يسعى لتحقيق مكاسب تجارية أو تعزيز نمو الصناعة المحلية؛ فيمكن للدولة من خلال نشاطها السيبراني تنمية صناعة التكنولوجيا المحلية الخاصة بدولة ما أو استخدام الوسائل التكنولوجية لتطوير صناعات محلية أخرى، عبر وسائل قانونية مشروعة أو غير مشروعة كالتجسس الصناعي ضد الشركات الأجنبية لتيسير نقل التكنولوجيا.أما الهدف السادس فيسعى لتدمير أو تعطيل البنية التحتية للخصم وقدراته كاستخدام دولة ما تقنيات وتكتيكات وإجراءات إلكترونية مدمرة؛ لردع أو تآكل أو إضعاف قدرة الخصم على القتال في المجالات الإلكترونية أو التقليدية. كشكل من أشكال الدفاع الشرعي عن النفس. وأخيرا الهدف السابع يتمثل في تحديد القواعد والمعايير التقنية الإلكترونية الدولية؛ أي مشاركة الدولة بنشاط في المناقشات القانونية والسياسية والفنية الدولية حول المعايير الإلكترونية. ويمكن اعتباره أكثر الأهداف مثالية لدعم ركائز النظام العالمي، ودعم السلم والأمن الدوليين. كما تظهر في الشكل رقم ٢ (زايد،٢٠٢٠)

الشكل رقم ٢: الأهداف الوطنية للدول وفقا للمؤشر العالمي للقوى السيبرانية الوطنية

يتضح من الطرح السابق للمؤشر العالمي للقوى السيبرانية الوطنية أن بعض هذه الأهداف منها المشروع والمثالي كالهدف السابع، ومنها الذي يغلب عليه عدم المشروعية، بل والشرعية مما يهدد السلم والأمن الدوليين. من هنا ينبغي التساؤل حول ما إذا كان من الممكن اعتبار هذه الأهداف بداية ردة على التنظيم الدولي الذي قامت مبادئه على عدم شرعية التدخل في الشأن الداخلي، وعدم التهديد باستخدام القوة، وعدم شرعية تهديد السلم والأمن الدوليين فهذه الأهداف والمقومات، تتسم بالتعدي على أمن وسيادة وخصوصية الدول الأخرى والفاعلين الدوليين. كما إنها تمثل خرقا للإعلان العالمي لحقوق الإنسان الذي يكفل حماية الخصوصية الأفراد.

من هنا يتضح أبرز الإشكاليات التي تدور حول الدول القومية كفاعل تقليدي في العلاقات الدولية خلال الفضاء السيبراني، الأمر الذي يطرح تساؤلا حول ماهية الفاعلين من غير الدول في الفضاء السيبراني.

**.الفاعلين من غير الدول:تتنوع التصنيفات الفرعية للفاعلين الدوليين من غير الدول؛ فهناك فاعلين مستحدثين بفعل الفضاء السيبراني كقوى التحول الرقمي، وهناك فاعلين استخدموا الأليات الجديدة المتعلقة بالأمن السيبراني بالإيجاب أوالسلب.

**التحول الرقمي قوى عالمية: أضحى التحول الرقمي قوى عالمية، مؤثرة سياسيا بشكل ايجابي عبر الثورة المعلوماتية، وبشكل سلبي كالهجمات السيبرانية والتجسس والإرهاب السيبراني. وينظر كل من مركز بلفر وكلية هارفارد كيندي، إليه باعتباره طاقة إلكترونية عالمية تتطلب وجود استراتيجية لتوطين الأنترنت لحماية المصالح التجارية لحماية الصناعة والتجارة، بل ومختلف مجالات الأمن القومي للدول. فالقوة السيبرانية تعتبر "دولة من الطراز العالمي" في حماية الصحة الإلكترونية للمواطنين والشركات والمؤسسات. لديه الأنظمة القانونية والأخلاقية والتنظيمية لتعزيز ثقة الجمهور؛ والقدرة على إبراز القوة الإلكترونية لتعطيل أو إنكار أو إضعاف الخصوم"(JuliaVoo , National Cyber 2020)

**الطبيعة فاعل للهجمات السيبرانية: قد تتسبب الطبيعة في هجمات سيبرانية مما يسمى بالزلزال السيبراني cyberquake، فقد تنقطع الكهرباء بفعل قوى الطبيعة وبالتبعية يتأثر كل من الفضاء والأمن السيبراني سلباً. كما حدث في مقاطعة كيبيك الكندية في عام ١٩٨٩ بسبب التوهجات الشمسية. فقد أضرت هذه التيارات الجيومغناطيسية بشكل متقطع بالمحولات الضخمة، وشبكات الطاقة مما دفع البعض في البداية للحكم بأن ما تم هو هجوما سيبرانيا. إلا أن التحقيقات قد أثبتت خلاف ذلك. فقد أظهرت الدراسات أن التيارات الجيومغناطيسية الناجمة عن التوهج الشمسي أو ما اسمها باتريك باولاك بروسيلس" المسئول التنفيذي بمعهد الاتحاد الأوروبي للدراسات الأمنية، بالعاصفة المغناطيسية الأرضية التي تعد من أبرز الأعطال التي تمت بل أنها من أبرز أسباب الصدمات العالمية المحتملة في المستقبل بسبب قدرتها على تعطيل شبكات التوصيل، مثل شبكات نقل الطاقة الكهربائية، وأنابيب النفط والغاز، وكابلات الاتصالات تحت البحر، وشبكات التلغراف والسكك الحديديةالأمر الذي قد يدفع بعض الدول إذا تسرعت في الحكم بإلقاء اللوم على الدول المنافسة لها، أو التي

تصنفها في دائرة العداء مما يسهم بدوره في توتر العلاقات بين الدول وبعضها البعض وبدوره قد يسفر عن تهديد للسلم والأمن الدوليين.(عبدالفتاح،٢٠٢٠)

**المنظمات الدولية: "الحكومية والغير حكومية: تلعب المنظمات الدولية الحكومية وغير الحكومية دور في الفضاء السيبراني لتحقيق الأمن السيبراني كفاعلين من غير الدول وفقا لبول ويلكينسون كما سبق الإشارة.

١-المنظمات الدولية الحكومية: تهدف لتضافر الجهود الحكومية لمواجهة الهجمات والتهديدات السيبرانية، وتتنوع دورها ما بين تبادل الخبرات والمعلومات وتوفير الكوادر المدربة، والمساعدة في وضع الخطط والاستراتيجيات لمكافحة الجريمة السيبرانية، دعم الجهود الدولية للتصدي للهجمات السيبرانية. كالمنظمة الدولية للشرطة الجنائية "الإنتربول"، حيث تقدم ساحة من أجل التواصل بين أجهزة الشرطة وسائر الجهات المعنية في مجال مكافحة الجريمة السيبرية لتبادل الخبرات والمعلومات وأفضل الممارساتوتساعد الدول الأعضاء على وضع الخطط والاستراتيجيات لمكافحة الجريمة السيبرانية، وتضم خبراء مكافحة الجريمة السيبرانية من الشرطة وشركات القطاع الخاص والجامعات وأهتمت الأمم المتحدة بالبناء المؤسسي في هذا السياق؛ فبدأت بأنشاء بعض الكيانات مثل الشراكة التعددية ضد التهديدات السيبرانية Impact عام ٢٠٠٩ كأول منظمة تدعمها الأمم المتحدة للتحالف لدعم الأمن السيبراني[ومركز ابتكارات الأمن السيبراني في عمان عام ٢٠١٢. كما تولى منظمة الأمم المتحدة للمخدرات والجريمة بمكافحة الجريمة السيبرانية ، وعلى صعيد إقليمي أنشا الاتحاد الأوروبي المجلس الأوروبي ضد الجريمة السيبرانية، والذي نجح في التوصل لاتفاقية بودابست للجريمة السيبرانية وأسفر عنها تأسيس مكتب برنامج الجريمة السيبرانية للتصدي من التحديات (مازار، و اخرون،٢٠١٦)

٢- المنظمات الدولية غير الحكومية: كما تلعب المنظمات الحكومية غير الحكومية دورا بارزا في مجال مكافحة الجريمة السيبرانية؛ عبر عدة صور كوضع معايير لتطوير العمل في مجال المكافحة كمجموعة عمل مكافحة التصيد عبر تطوير معايير البيانات، أو عبر مكافحة الاعتداء على الطفولة، بسبب تلك الهجمات كالمنظمة الأوروبية غير الحكومية للتحالف من أجل أمان الطفل أونلاين Enacso. فتوفر ساحة لجمعيات حماية الطفل عبر أوروبا من خلال مشاركة الخبرة وافضل السياسات في مجال حماية الطفل أونلاين. ومرصد مراقبة الأنترنت IWF توجد في بريطانيا تقوم بإزالة أية مشاهد جنسية للاعتداء على الطفل (فارس قرة،٢٠٢٠)

من هنا يتضح، أن الأمن السيبراني والتقدم التكنولوجي قد أثر على تحديد ماهية الوحدات الدولية الفاعلة، بل أضحى نفسه فاعلا على الساحة الدولية، ويسر لفاعلين قائمين بالفعل على زيادة فاعليتهم لتحقيق أهدافهم بطرق مشروعة وغير مشروعة تؤثر بدورها على السياسة الدولية.

المبحث الثاني: مجموعة المؤسسات الدولية

سيناقش هذا المبحث تاثير الأمن السيبراني على القواعد والإجراءات الرسمية التي تضبط سلوك الفاعليين الدوليين، بما في ذلك القواعد المستقرة في العلاقات الدولية والتنظيمات الدولية. فينقسم هذا المبحث لقسمين رئيسين الأول يناقش القواعد والإجراءات الرسمية المنظمة وما طرأ عليها من تغير، والثاني يقدم طرحا للتغيرات التي طرأت على التنظيم الدولي كنسق يتواجد في إطاره سلطة عليا تنتظم خلالها سلوك الوحدات الدولية.

١.تأثير السيبرانية على القواعد المستقرة في علاقات الدول:

أدي تطور العلاقات الدولية إلى مجموعة من الأعراف والتقاليد الدبلوماسية التي اتضحت معالمها في شكل مبادئ عامة بميثاق الأمم المتحدة. وتعززت في مجموعة من الإعلانات والتوصيات والقرارات الصادرة عن الأمم المتحدة. علاوة على عدد من الاتفاقيات الدولية المنظمة كاتفاقيات جينيف الأربعة تنظم اتفاقيات لاهاي لعام ١٨٩٩ و١٩٠٧ واتفاقيات جينيف الأربعة لعام ١٩٤٩ والبروتوكولان الإضافيان لعام ١٩٧٧[إلا أنها جميعا لم تتناول الفضاء السيبراني وما يتم خلاله من هجمات سيبرانية قد تمتد لحرب سيبرانية واسعة النطاق الأمر الذي يطرح اشكاليات قانونية أمام فقهاء القانون الدولي والقانون الدولي الإنساني لتنظيم سلوك الوحدات الدولية بالفضاء السيبراني؛ ويمكن طرح أبرز تلك الإشكاليات القانونية فيما يلي:

أ. مدى اختصاص القانون الدولي الإنساني بالهجمات السيبرانية:

يقف القانون الدولي الإنساني أمام معضلة تتعلق بمدى اختصاصه القانوني بالتصدي للهجمات السيبرانية؛ فلم تنظم اتفاقيات لاهاي لعام ١٨٩٩ و١٩٠٧ واتفاقيات جينيف الأربعة لعام ١٩٤٩ والبروتوكولان الإضافيان لعام ١٩٧٧ الهجمات السيبرانية فظهورها لاحق لها. خاصة في ظل عدم القدرة على إثبات الدليل المادي للهجمات السيبرانية، وكذا الإقرار المادي الملموس المباشر أو الغير مباشر عقب الهجمات السيبرانية كالدمار أو التعطيل الجزئي أو الكلي للأهداف المدنية أو العسكرية، كذلك الحال بشان القتل أو الجرح الذي يصيب العسكريين أو المدنيين مما يصب في عدم قدرة تصدي القانون الدولي للهجمات السيبرانية بالأساس. (فياض،٢٠٢١)

ب.إشكالية التكييف القانوني للهجمات السيبرانية:

يواجه القانون الدولي الإنساني اشكالية أخرى تتعلق بالتكييف القانوني للهجمات السيبرانيةوفقا للضرر الناتج عنها؛ فقد عرّف البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف الأربعة لعام ١٩٤٩ في الفقرة ١ من المادة ٤٩ بأن: «الهجوم هو أعمال العنف الهجومية أو الدفاعية ضد الخصم». الأمر الذي يمثل تحديا بشأن طبيعة الهجمات فالعمليات السيبرانية معقّدة كونها قد تفي بالغاية العسكرية المطلوبة من دون التسبب بآثارٍ مدمرة أو ضارة أحيانًا. الأمر الذي انقسم بشأنه فقهاء القانون الدولي الإنساني فمنهم من اعتمد على المعني العام للنص باعتبار الهجمات تقتصر على العمليات العسكرية التي يسفر عنها ضرر مادي أو إصابات، ومنهم من نظر للهجمات بغض النظر عن أثارها الغير مدمرة أو الغير ضارة. وهناك من نظر للضرر الواقع بالبنية

السيبرانية الناتج عن الهجمات. وهناك من وجد أهمية الوقوف على الهدف من وراء استخدام تلك الهجمات السيبرانية حتي يمكن تحديد ماهيتها كأسلوب حرب أو وسيلة للقتال(فياض،٢٠٢١)

ت.مبدأ الامتناع عن استخدام القوة أو التهديد باستخدام القوة في العلاقات الدولية مقابل الحرب السيبرانية بالوكالة:

تنص الفقرة ٤ من المادة ٢ من ميثاق الأمم المتحدة بامتناع أعضاء الجماعة الدولية جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة، أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه أخر لا يتفق ومقاصد الأمم المتحدة. فالأصل في القانون الدولي هو عدم التدخل في شئون الدول، ولكن قد تميل الدول لإخفاء نشاطها لتوجيه ضربة سيبرانية توقع أضرار بالدولة العدو لها عبر تعهيد تلك الهجمات لفاعلين من غير الدول لتجتب المسؤولية الدولية ضدها كشكل من أشكال الدعم لحروب الوكالة (يوسف، ٢٠٢٠)

٢.التنظيمات الدولية:

يبحث هذا الجزء في دراسة تأثير الأمن السيبراني للوحدات الفاعلة في النسق الدولي على التنظيمات الدولية، فعلى الرغم من اهتمام المنظمات الأممية والدولية بالأمن السيبراني، ومحاولة التعاون للتصدي للهجمات السيبرانية المهددة للسلم والأمن الدوليين، يطرح الأمن السيبراني إشكالية كبيرة بشأن مراقبة التفاعلات بين الفاعلين الدوليين والفاعلين من غير الدول، الأمر الذي خلق بدوره حالة أقرب لحالة الطبيعة الأولي التي تغيب خلالها السلطة الشاملة لمراقبة النظام الدولي، وصراع حرب الكل ضد الكل. وبالرغم من ذلك هناك أيضا جهود وإن كانت لا ترقي لحد إنشاء منظمات أممية لمواجهة التهديدات السيبرانية ولكنها تتم على الصعيد الأممي والإقليمي والثنائي من المهم الوقوف عليها عند الحديث عن التنظيم الدولي للتصدي للهجمات السيبرانية بداخل النسق العالمي. (تورية،٢٠٢٠)

أ-الصراع وحالة "حرب الكل ضد الكل":

يتوافق الوضع الراهن بالفضاء السيبراني لما وصفه توماس هوبز بشان أسباب الصدام لتحقيق المنفعة الذاتية للإنسان، حيث ساد الصراع في حالة الطبيعة الأولي؛ بناء على ثلاثة أسباب للصدام والصراع تتوافق ما الوضع الحالي بالفضاء السيبراني:

- أولا المنافسة، حيث يتنافس الأفراد من أجل الكسب ويكون العنف هو الوسيلة لتحقيق ذلك.

- ثانيا عدم الثقة: كمحرك للدفاع عن النفس حيث ترفع التمييز بين الظالم والمظلوم فكلاهما يبرران سلوكهما الهجومي والاحترازي، باسم الدفاع عن النفس لتجعل الفراد، أمام ضرورة اتخاذ جميع الإجراءات ومن أهمها الهجوم قبل الدفاع لأنه ينظر للأخر بصفقته عدو يجب مواجهته.

- ثالثا المجد: مقصد للسمعة الأخلاقية- أو الردع وفقا للمدرسة الواقعية- والسيطرة على الأخر.

الأمر الذي يصل لمرحلة "حرب الكل ضد الكل" فالكل يتسلح ليحمي نفسه، ويغلق خزانته لحماية ممتلكاته ويسيج أرضه لمواجهة من يقتحم ممتلكاته. ففي حالة الحرب لا معني للظلم أو القانون أو الخطأ أو الصواب، فيكون ملك كل إنسان ما يستطع الحصول عليه طالما قادر على الاحتفاظ به؟،وتتشابه حالة حرب الكل ضد الكل مع التهديدات السيبرانية والمخاطر الإلكترونية، بما في ذلك الحرب الإلكترونية، والصراع السيبراني، والإرهاب السيبراني، والجرائم الإلكترونية، والتجسس الإلكترونيفقد أصبح الأمن السيبراني مصدر قلق رئيسي لواضعي السياسات، ومصدر اهتمام كبير لعلماء العلاقات الدولية بسبب الخسائر المالية للشركات من خلال الجريمة الإلكترونية، أو سرقة البيانات الحكومية السرية، أو استهداف البنية التحتية الحيوية، حيث يشكل الأمن السيبراني تحديًا كبيرًا للأمن الاقتصادي والوطني للبلدان على مستوى العالم. يعتبر الفضاء الإلكتروني الآن المجال الخامس للحرب بعد الأرض والبحر والجو والفضاء . (سعود، ٢٠٢٠)

ب-الفوضى:

سادت حالة ما قبل الدولة "الطبيعة الأولى" الفوضى العارمة التي كانت تطرح إشكالية العلاقة بين القوة والحق ومبررات الملكية والحرية الفردية. وتظهر الفوضى بسبب انعدام الثقة الأمر الذي طرحه هوبز كما سبق الذكر، حيث يشبه المجال السيبراني عالمًا واقعيًا بطبيعته الفوضوية، والافتقار إلى الحوكمة المؤسسية، حيث تخشى الدول بعضها البعض وتطور قدراتها استجابةً لذلك ففي ساحة المعركة الإلكترونية، يستطيع أي شخص تنظيم هجوما سيبرانيا. وفي ظل عدم إمكانية إنكار امتلاك الدول المزيد من الموارد المالية والتكنولوجية، إلا أن الفضاء السيبراني فرض واقعا مهما مكن الشركات، ومجموعات المصالح الخاصة، والمنظمات الإرهابية، والأفراد من إحداث الضرر بشكل متساوٍ في ظل درجة معينة من الذكاء الحاسوبي، الأمر الذي يتم دون وجود قواعد أو ضوابط فلا يمكن تفسيره أو ضبطه أو التنبؤ به وبتبعاته وحدوده بل وأطرافه والفاعلين والمتسببين مما يزيد من حالة الضبابية والفوضى. (مازار، و اخرون ،٢٠١٦)

وعلى الرغم من هذه الطبيعة الفوضوية، ولكن الجماعة الدولية تسعى لمحاولة الاتفاق على قواعد منظمة لاستخدام الفضاء السيبراني، عبر طرح القضية في العديد من المحافل الدولية كمؤتمر دافوس الاقتصادي لعام ٢٠٢١، حيث احتلت القضية صدارة أجندة المؤتمركذلك الحال بشان قمة ميونخ ٢٠٢٠التي أكدت على أهمية الدور الذي تلعبه الحكومات في مجال الأمن السيبراني، وقمة العشرين التي عقدت في فبراير ٢٠٢٠ وتوصلت إلى الحاجة إلى وجود السياسات الملائمة لتخفيف أثر الهجمات السيبرانية، ومواجهة التحديات عبر سياسات منسجمة وموحدة، تتضمن ايضا المنشآت الصغيرة والمتوسطة التي تحتاج إلى مساعدة. فاتفقت جميعها على إثارة القضية لتعكس اهتمام الجماعة الدولية الذي اسفر من قبل على اتفاقية بودابست لمكافحة الجرائم المعلوماتية في ٢٣ نوفمبر عام ٢٠٠١؛ التي وقعتها الدول الأعضاء في المجلس الأوروبي. إلا أنها مجرد بداية تحتاج إلى زخم وإرادة دولية وقدرة على التنفيذ والالتزام ورغم ذلك تظل الإشكالية قائمة في ظل غياب هوية

الفاعل في الفضاء السيبراني، تصبح إرادة الدول للالتزام ببنود أي اتفاق قد يوقع مستقبلا محل شك وتظل الفوضى صفة مصاحبة للتفاعلات في النسق الدولي. (الفتلاوي،٢٠٢٠)

وانطلاقا مما سبق، على الرغم من الجهود الدولية المبذولة في هذا الشأن لكن على الجماعة الدولية بذل مزيد من الجهد لوضع القواعد والإجراءات الرسمية التي تضبط سلوك الفاعليين الدوليين بالنسق الدولي.

وبعد استعراض تاثير الأمن السيبراني على القواعد والإجراءات الرسمية التي تضبط سلوك الفاعليين الدوليين، والتنظيمات الدولية من المهم التطرق لبنية النسق الدولي وما قد يطرأ عليها من تغيرات بفعل الأمن السيبراني.

المبحث الثالث: الأمن السيبراني وهيكل النظام الدولي:

يتناول هذا المبحث هيكل النسق الدولي؛ أي دراسة تكوين القوة والنفوذ، التي تنتظم على أثرها وحدات النظام الدولي في علاقات معينة تتضمن خاصية التدرج التي تتحدد من خلال كيفية توزيع المقدرات بين الوحدات الدولية. والمقصود بالمقدرات أي نمط توزيع الموارد الاقتصادية والعسكرية ونمط تويع الاتجاهات والقيم السياسية بين مختلف وحدات النظام الدولي.

وإذا نظرنا للأمن السيبراني وتأثيره على هيكل النسق الدولي نجد أننا أمام عدة إشكاليات في هذا الشأن كسرية مقدرات القوى السيبرانية أي عدم أفصاح بعض الدول عن واقع ما تمتلكه من قدرات سيبرانية حقيقية، والطبيعة ودورها فى التاثير على سلوك الفاعلين الدوليين كبيئة محفزة لزيادة الهجمات السيبرانية التي ترتكبها الوحدات الدولية الفاعلة، وتهديد القوى

العسكرية بفعل القدرات السيبرانية، الأمر الذي يؤثر على بنية وقيادة النظام الدولي ككل. (عبدالمنعم،٢٠٢٠)

وتفرض تلك الإشكاليات النظر للتغير الذي طرأ على ترتيب الدول في هيكل النظام الدولي وفقا للأمن السيبراني، وما يطرحه من إشكاليات مصاحبة، باعتبارها الفاعل الرئيسي في العلاقات الدولية الذي يمكنه منع عمل بعض الفاعلين الدوليين في مجال سيادته، أو الاعتراض على بعض قرارات المنظمات الحكومية الدولية، أو رفض استخدام بعض التقنيات الحديثة في المعاملات على الساحة الداخلية، أو بمعاملته على الصعيد الدولي كالتخوف من تقنين استخدام العملات المشفرة على سبيل المثال لا الحصر.(الشوابكه،٢٠١٨)

في هذا الصدد، سينقسم هذا الجزء بدوره إلى قسمين رئيسين الأول يتناول الإشكاليات المصاحبة للتغير في هيكل النظام الدولي بفعل الأمن السيبراني، والثاني سيناقش تأثير الأمن السيبراني على ترتيب الدول في هيكل النظام الدولي.

١.الإشكاليات المصاحبة للتغير في هيكل النظام الدولي:

يطرح هذا الجزء لأبرز الإشكاليات التي فرضها الفضاء السيبراني على بنيان النظام الدولي وخلقت حالة من الجدل بشأن توزيع المقدرات وترتيب الوحدات الدولية الفاعلة بداخل النسق الدولي.

أ.الأمن السيبراني وإشكالية توزيع المقدرات الاقتصادية للوحدات الدولية الفاعلة:

إن الحديث عن توزيع المقدرات الاقتصادية في الفضاء السيبراني، أمرا يرتبط بتدفقات البيانات كأساس الاقتصاد العالمي. ومع التسارع الحالي لرقمنة المؤسسات العالمية، مدعومًا بالاعتماد السريع للتقنيات المتطورة مثل تلك الخاصة بالحوسبة السحابية وتحليلات البيانات، زادت أهمية البيانات كمدخل للصناعات، وهذا ليس فقط لصناعات المعلومات، ولكن أيضًا للصناعات التحويلية والتقليدية الأخرى. فيرتبط توزيع المقدرات الاقتصادية على الساحة الدولية بامتلاك البيانات. هذا ويرتبط استخدام الإنترنت ارتباطًا وثيقًا بالتنمية الاقتصادية، فارتفاع معدل انتشار الإنترنت إلى حد كبير يرجع إلى مجموعة من مقاييس النجاح الاقتصادي، فتحقيق الوصول الشامل لا يتطلب إصلاحات في قطاع الاتصالات فحسب، بل يتطلب أيضًا سياسات لمساعدة الأفراد والشركات على تحقيق أقصى استفادة من الإنترنت. ومن ثم فهناك علاقة بين شبكة المعلومات الدولية والتنمية الاقتصادية فالاقتصاد الرقمي قد يكون مدخلا لبناء قوى اقتصادية كبيرة لبعض الكيانات الدولية الفاعلة؛ كالدول، والشركات متعددة الجنسيات، والمنظمات الدولية الحكومية وغير الحكومية، في ظل بنية معلوماتية تستند عليها بنية الاقتصادات الرقمية. وفي المقابل هي ساحة لزيادة القدرات الاقتصادية لوسطاء الظل والجماعات الإرهابية عبر الأنترنت المظلم وفي ظل سرية المقدرات السيبرانية، لا يمكن الوقوف على التوزيع الكلي للموارد الاقتصادية للفاعلين على مستوى النظام الدولي. فيوفر الفضاء السيبراني منصات وفرص اقتصادية ممتازة لتنمية اقتصاديات الوحدات الفاعلة في النظام الدولي عبر ساحة الاقتصاد الرقمي، وما يوفره من سد الفجوات في التنقل والتجارة والابتكارات والتمكين الاقتصادي، والحد من الفقر. وساعدت تقنية سلاسل الكتل على مزيد من الموثقية، وحماية المعاملات المالية. وتستخدم أيضا في تعزيز التجارة الدولية بين الوحدات الفاعلة بشكل مشروع دول وشركات وأفراد ومنظمات، نظرا لما توفره من تخزينًا آمنًا وقويًا وموثقًا ومقاومًا للتعديل، فضلاً عن طبيعتها اللامركزية القائمة على البنية التحتية المحايدة، من حيث عدم وجود جهة فاعلة واحدة لديها سيطرة كاملة عليها، فهي تخضع لقواعد الإجماع، بمعنى أن التحكم في البنية التحتية التقنية يتم تقاسمه بين أصحاب المصلحة، وهذا يعتبر مناسباً بشكل خاص للأنظمة البيئية التي يحتاج المشاركون فيها إلى التعاون، مع الاحتفاظ بالمصالح المتضاربة أو المتنافسة والتي يمثله واقع التجارة الدولية. (مازار، و اخرون،٢٠١٦)

وفي ذات الوقت بسبب سرية المعلومات المتبادلة خلال سلاسل الكتل يمكن استخدامها في الجرائم الإلكترونية، وغسيل الأموال والإرهاب ، وفي المقابل نجد أن الهجمات السيبرانية تؤثر سلبا على المصالح الاقتصادية عبر الممارسات الاحتيالية الالكترونية، وجرائم الاستغلال والسطو، والتخريب الاقتصادي والقرصنة الإلكترونية، وسرقة الاصول الفكرية، وغسل الأموال والجرائم المالية عبر الأنترنت وفقًا للتقرير السنوي الرسمي لجرائم الإنترنت لعام ٢٠١٩ الصادر عنCybersecurity Ventures، فإن الجرائم الإلكترونية هي أكبر تهديدا لكل شركة وفاعل دولي في العالم، وواحدة من أكبر المشكلات التي تواجه البشرية. فتتوقع مشاريع الأمن السيبراني أن تكلف الجريمة الإلكترونية العالم ما يزيد عن ٦ تريليونات دولار سنويًا مع نهاية عام ٢٠٢١، مقارنة بـ ٣

تريليونات دولار في عام ٢٠١٥. ويضيف التقرير أيضًا أن هذا يمثل أكبر تحويل للثروة الاقتصادية في التاريخ ؛ تهدد الجرائم الإلكترونية حوافز الابتكار والاستثمار، علاوة على زيادة أرباح تجارة المخدرات والعقاقير غير المشروعة.(لامباش،٢٠٢٠)

ناهيلك عن استخدام العملات المشفرة وما تحمله من مخاطر اقتصادية كامنة للدول التي لا تمتلك نظما متقدمة تكنولوجية وأيضا خروج ودخول الأموال دون رقابة البنوك المركزية للدول وغيرها من الأثار السلبية التي قد تظهر جراء التعامل وتداول هذه العملات الرقمية.

(أمين،٢٠٢٠)

في هذا السياق يمكن القول أن توزيع المقدرات الاقتصادية في ظل الأمن السيبراني، أمر غير متكافؤ، ولا يمكن الوقوف على هيكل توزيع المقدرات الاقتصادية بين الوحدات الدولية الفاعلة.

ب. القوة السيرانية مهددة لمقدرات توزيع القوى العسكرية:

يساعد الفضاء السيبراني على دعم تغير بنية النظام الدولي، عبر تغير هيكل توزيع القوى بمعناها التقليدي، فبالنظر للنظام الدولي الحالي الذي تهيمن عليه الولايات المتحدة الأمريكية كقوى عظمى وحيدة في العالم، يمكن القول أنها لم تعد قادرة على القيادة داخل الفضاء السيبراني رغم ما تمتلكه من مقدرات عسكرية هائلة. فتتعرض الولايات المتحدة الأمريكية إلى هجمات سيبرانية متكررة تمثل تهديدا لأمنها القومي، بل وتحديا كبيرا أمام صانع القرار الأمريكي. ففي ظل اهتمام الإدارات الأمريكية المتلاحقة بالتسليح والاهتمام بالتفوق العسكري، كان الأمن السيبراني محل جدلا فيري آدامز أن "التفوق العسكري الساحق والميزة الرائدة في تكنولوجيا المعلومات، جعلت الولايات المتحدة الدولة الأكثر عرضة للهجمات الإلكترونية"، فمن غير المرجح أن تتفوق أية دولة على الولايات المتحدة في القوة العسكرية التقليدية في المستقبل القريب. (مشوش،٢٠٢٠)

لذا ستبدأ الدول المعادية في إنفاق الموارد لتطوير أسلحة إلكترونية تمنحها ميزة غير متكافئة، وربما تهزم الولايات المتحدة دون إطلاق طلقة واحدة، مما شكل صعوبة في الوقاية من هذه الهجمات. فمن فترة لأخرى تستخدم مجموعة من المتسللين أدوات كمبيوتر متطورة لاختراق مئات قواعد بيانات الحكومة الأمريكية، بما في ذلك ناسا والبنتاغون ووكالات أخرى. كالهجوم الذي تعرضت له الولايات المتحدة الأمريكي عام ١٩٩٨ فقد تعرضت لسرقة الأف المستندات السرية والعقود والتشفير والمواد الحساسة، ولم تسفر التحقيقات التي امتدت على مدار خمسة سنوات إلا عن تحديد عناوين بروتوكول الانترنت IPلأجهزة الحاسوب التي قامت بالهجمة، وتم تحديد هويتها الروسية، ولكن دون إمكانية إدانة الدولة الروسية فمن غير الواضح ما إذا كانت هذه الهجمات ترعاها الدولة، لكن الحكومة الأمريكية لم تستطع التأكد من براءة روسيا، مما أدى إلى مزيد من عدم الثقة والشك، وفي ١٣ ديسمبر ٢٠٢٠ تعرضت ما لا يقل عن ٦ وكالات حكومية أمريكية للاختراق بفعل برنامج خبيث أصاب آلاف الشركات فيما يبدو أنها واحدة من أكبر عمليات الاختراق التي تم الكشف عنها، حيث

استطاع متسللين النفاذ إلى البريد الإلكتروني الخاص بوزارتي الخزانة، والتجارة الأمريكيتين مما سبب مشاكل كثيرة تخطت حدود الدولة الامريكية ذاتها (خليفه،٢٠٢٠)

ث. تأثير الأمن السيبراني على ترتيب الدول بالنسق الدولي:

ظهرت الحاجة للأمن مع تطور الحضارات للتحرر من الخوف والشعور بالأمان والاستقرار، وجاء اقتران الأمن بالقومي ليعني اقتران التحرر من الخوف بكيان الدولة، باعتبار الدولة ظاهرة قانونية وسياسية تسعى للبقاء فالدولة القومية هي الإطار السياسي والقانوني لمفهوم الأمن والسيادة؛ فهي السند الشرعي الذي يستند عليه مفهوم الأمن القومي، وحماية المصالح من خلال بناء قوة الدولة. الأمر الذي يرتبط بالبعد الوظيفي الاستراتيجي للدولة الذي تلعب خلاله القوات المسلحة دورا كبيرا سواء على مستوى الردع، أو دورها في مسرح العمليات، وما يصاحب ذلك من دور وثقل بالنظام الدولي. بمعنى أخر إن الأمن القومي بالمعني التقليدي للنظرية الواقعية مرادفة لمعني السياسة الدفاعية والهجومية التي تتحدد بحماية القيم والمصالح الحيوية للدولة، التي تشكل جوهر سياسة أمنها القومي، ويأتي الردع هنا ليحتل مكانة مميزة فالقوة العسكرية للدولة تحميها من كافة الأخطار التي تهددها وتحقق أهدافها وأغراضها ومن ثم تدعم مكانتها بالساحة الدولية. إلا أن مع ظهور الفضاء السيبراني وما صاحبه من تهديدات أوجبت على الدول النظر إلى حماية مقدرتها سيبرانيا عن طريق آليات الأمن السيبراني، واختلفت الموازين وانشغل علماء السياسية في إعادة النظر لمراكز الثقل ومفهوم وأليات القدرات العسكرية للدولة في ذات الشأن. فيطرح علماء السياسية إشكالية العلاقة بين امتلاك القدرات التكنولوجية والسيبرانية، وتعديل ميزان القوى في النظام الدولي، فهناك من يعتبر أنه نظرًا للتكلفة المنخفضة نسبيًا للدخول إلى مجال الحرب السيبرانية، فإن الدول الأضعف تقليديًا تتحدى الدول الأقوى وتعيد تكوين توزيع المقدرات بداخل النظام الدولي. فعلى سبيل المثال، تم إيلاء الكثير من الاهتمام لتدريب كوريا الشمالية لآلاف المتسللين، والوحدة ٦١٣٩٨ الصينية، المتهمين بحملات التجسس السيبراني المستمرة ضد الولايات المتحدة، والتطور المتزايد في تكتيكات الحرب الإلكترونية الإيرانية. كما يتم تقويض ديناميكيات القوة التقليدية بسبب الفكرة المتناقضة القائلة بأن البلدان الأكثر تقدمًا من الناحية التكنولوجية، هي أيضًا الأكثر اعتمادًا على البنية التحتية الرقمية وبالتالي فهي الأكثر عرضة لهجوم سيبراني معوق. وعلى الجانب الآخر يعتبر Lindsay أن القوى التكنولوجية العظمى فقط هي التي تمتلك القدرة على تطوير الأسلحة السيبرانية الأكثر تطورًا، مما يشير إلى أن الطبيعة غير المتكافئة للمجال السيبراني قد تكون مبالغًا فيها فهى ستظل ملكا للقوى العظمي. والسياسات الدفاعية والهجومية في ذات السياق (تورية،٢٠٢٠) .

بعد التعرض لبنية النسق الدولي في ضوء التغيرات التي أحدثها الأمن السيبراني؛ من المهم التطرق لأبرز العمليات العالمية التي تتم بين الوحدات الفاعلة في النسق الدولي والوقوف على أبرز السمات الغالبة على التفاعلات بينها.

المبحث الرابع: مجموعة العمليات العالمية: الصراع، الردع، والتعاون

يناقش هذا المبحث مجموعة العمليات العالمية التي تتم داخل النسق الدولي، أي التفاعلات الدولية التي تتم بين الوحدات الفاعلة؛ عبر الوقوف على أبرز السمات المميزة للتفاعلات بين الوحدات الدولية المختلفة، فهل يغلب عليها سمة التعاون أو الصراع أم الردع.

اختلف علماء السياسية حول تحديد النمط الغالب على التفاعلات في النظام العالمي؛ فهناك من اعتبر الأمن السيبراني محركا لمزيد من الصراع والتصعيد. وهناك من اعتبر أن الردع هو النهج الغالب، في حين نجد فريق ثالث اعتبر أن نمط التعاون الدولي هو السلوك الأكثر شيوعا وانتشارا لتحديد شكل التفاعلات في النظام العالمي..

أ. الصراع الدولي:

أصبح الفضاء السيبراني ساحة جديدة للتنافس بين الفاعليين الدوليين والفاعلين من غير الدول، الأمر الذي شغل علماء السياسية فهل تخطي الأمر لحد تصاعد الصدام والحرب، أم أن الأمر يقف فقط لحد سباقات التسلح السيبراني والحديث عن عسكرة الفضاء السيبراني وشن هجمات متباعدة بين فترة وأخرى. فتعتبر المدرسة الواقعية أن بالرغم من سباق التسلح لكن شن الحرب السيبرانية أمرا مستبعدا وفي هذا الصدد. وتثير الواقعية أسئلة مثيرة للاهتمام حول القوة الإلكترونية، من يمتلكها، ومدى ارتباطها بالاستقرار الدولي. وفيما يتعلق بما إذا كانت القوة الإلكترونية ستحول ديناميكيات القوة التقليدية، لصالح أشكال أقل تدميراً من التفاعلات السيبرانية. فالجريمة السيبرانية ليست سهلة كما يُفترض غالبًا وفي الواقع أننا لم نشهد الكثير من النزاعات الإلكترونية. كما أن استيراد فكرة الردع من العصر النووي هو حكم خاطئ ولا معنى له في سياق واقع الأسلحة السيبرانية. (فياض،٢٠٢١)

وهناك من يعتبر أن التنافس السيبراني قد يصل لدرجة الصراع؛ فيمكن للهجمات السيبرانية أن تؤدي لتراجع النظم الالكترونية والكهربائية والهجمات يمكنها أن تغير أسعار البورصة وتقرع جرس خدمات الطوارئ وتضعف من الاستجابة العسكرية وتزعج الاقتصاد. ويعتبر هذا الاتجاه أن تحول الصراع السيبراني للحرب يتوقف على ثلاثة محددات رئيسة:

- البناء العقلي mindset: التطورات الكبيرة في تكنولوجيا المعلومات والاتصالات لها تأثير غير متوقع على المجتمع وطريقة التفكير ومن ثم اتخاذ القرار.
- التكنولوجيا: تمثل محددات مهمة للحياة العامة كالهواء والطريق والتحكم في السكك الحديد.
- استمرار غياب التشريعات الرادعة: وغياب القوانين المنظمة لاستخدام الأسلحة السيبرانية.

وعلى الرغم من أن ردود الفعل السائدة بشأن الهجمات تدعو لحتمية التعاون، وأهمية الإفصاح والتشارك؛ لكن عقبات السياسة والتصارع ستقف حتمًا عائقًا أمام ذلك الاتجاه، مما يؤكد أهمية الضغوط المجتمعية من أجل

حث الحكومات على تجاوز حواجز الصراع بما يحد من هجمات تُنبئ أغلب المؤشرات على أنها في طريقها إلى الازدياد

وفي هذا السياق، قد سنت الولايات المتحدة وحدها ٣٤ قانوناً جديداً و٥ أوامر تنفيذية لتنظيم التفاعلات السيبرانية ودعم محددات الأمن السيبراني، بما في ذلك تعزيز معايير البنية التحتية، وتبادل المعلومات عن التهديدات السيبرانية، ووضع عقوبات لمعاقبة وردع العناصر المهاجمة. وعلى الرغم من الجهود المبذولة لتحسين الأمن السيبراني، يشتد الصراع السيبراني العالمي ليصل لدرجة النزاعات بين الدول وبعضها البعض، حيث تستخدم دول مثل روسيا وإيران وكوريا الشمالية الهجمات الإلكترونية لزيادة مجال نفوذهم. (الفتلاوي،٢٠٢٠)

ب. الردع السيبراني:

في ظل ضبابية الفضاء السيبراني وضعف القدرة على تحديد الجاني والتطور السريع للاسلحة السيبرانية، تأتي قضية الردع لتثير إشكالية بين علماء السياسة، فاتفقوا على الاهتمام بالتسليح السيبراني لمنع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي، والأصول التي تدعم العمليات الفضائية ولكنهم اختلفوا في فاعلية الردع من عدمه.

فنجد أنصار المدرسة الواقعية يعتبرون أن اكتساب القدرات العسكرية أمرًا أساسيًا لردع العدوان من الدول الأخرى والحفاظ على الأمن القومي، حيث يهدف الردع إلى تثبيط الهجمات من خلال إظهار القدرة العسكرية للفرد واستعداده للرد بالمثل. وهنا يأتي ميرشايمار معتبرا أن الردع يؤثر على السياسة الالكترونية، ويضرب الامثلة بالاستراتيجية الوطنية للأمن السيبراني، التي أصدرتها الحكومة الأمريكية حيث تهدف لإقناع الخصم القائم والمحتمل بأنه سيتكبد خسائر غير ممكنة إذا شن هجوما على الدولة، الأمر ذاته أثارته حكومة المملكة المتحدة عن الحاجة إلى الرد على الحوادث السيبرانية ذات الاجراءات الهجومية. فنظرًا لعدم اليقين المحيط باستخدام التكنولوجيا الإلكترونية كسلاحا هجوميا، يجب على الدول المضي بحذر في المجال السيبراني والتركيز على إنشاء دفاعات مرنة. في الواقع، من خلال الامتناع عن الحرب الإلكترونية الصريحة، ظلت العديد من الدول حكيمة إلى حد ما في سلوكها في الفضاء الإلكتروني حتى الآن، وهذه نتيجة يجدها المنظرون الواقعيون جذابة ومجالًا لمزيد من التفصيل النظريهذا وقد استخدمت عدة دول تقنيات وتكتيكات وإجراءات إلكترونية مدمرة؛ لردع أو تآكل أو إضعاف قدرة الخصم على القتال. في المجالات الإلكترونية أو التقليدية. ويشمل ذلك الهجمات الإلكترونية على البنية التحتية الحيوية، وهجمات DDOS على شبكات الاتصالات الحكومية. ويشمل أيضًا الهجمات الإلكترونية لإثبات النية والقدرة على ردع الخصم عن التصرف (مازار ، و اخرون،٢٠١٦)

ت.التعاون السيبراني مدخلا للتوازن بالنظام العالمي الجديد:

الأمن السيبراني ليس فقط ساحة للتصعيد والردع، فيرى سين أوكيفي أنها قد تكون مدخلا لدعم الاستقرار في بيئة النظام العالمي. فيضع على الولايات المتحدة كقوى عظمي بالعالم عبء بذل الجهد لتعزيز التعاون مع الحلفاء في الفضاء العسكري، والاستفادة من القدرات الناشئة لغيرها من الدول حتى القوى المناوئة لها كالصين وروسيا. كأهمية توجيه أمريكا دعوة للصين للالتحاق بفريق الدول المستكشفة للفضاء في ظل القدرات المتطورة التي أظهرتها الصين في هذا المجال والمهم الاستفادة منها. وعليها أيضا تنحية خلافاتها جانبا مع روسيا لاستمرار التنسيق بينهما بشأن العمليات في الفضاء السيبراني، للحفاظ على استدامة هذه الأنشطة المشتركة في ظل اعتماد الولايات المتحدة على نظام الدفع الروسي"RD-180"، والذي تحتاجه في مركبات الإطلاق للفضاء "أطلس. ومن ثم قد يكون ذلك دافعا لوضع مدونة لقواعد دولية للفضاء السيبراني مما ييسر القدرة على الإنفاذ عبر الوصول إلى مجموعة عملية من البروتوكولات من خلال اتفاق ثنائي أولاً، على أن يتم محاكاته على الآخرين. (الفتلاوي ، ٢٠٢١)

الخاتمة:

وأخيرا لا أخراً، يمكن القول أن ظهور الفضاء والأمن السيبراني خلق ساحة جديدة من النقاش الدائر بين علماء السياسة، والمدارس الفكرية المختلفة حول ملامح وسمات النظام العالمي وماهية الوحدات الفاعلة على الساحة الدولية، والتفاعلات بينها والعمليات الدولية بداخل النسق الدولي وهيكل هذا النسق الدولي. ففي ظل فضاء سيبراني أشبه بحالة الطبيعة الأولى لما قبل ظهور السلطة يتسم بالفوضى والتحارب مازال الجهد البحثي يحتاج لمراجعة وتدقيق. ورغم ذلك فقد تم التوصل لعدد من النتائج التي تجيب على التساؤل الرئيسي للدراسة وما نتج عنه من تساؤلات فرعية والوقوف على مدى صحة فروض الدراسة:

- ساهم الأمن السيبراني في ظهور فاعلين جدد بالنظام الدولي بل وعزز من دور بعض القوى القائمة وزودها بأدوات جديدة للتأثير وتحقيق مبتغاها وخلق تحديات جديدة أمام بعض الفاعلين الرئيسين على الساحة الدولية كالدول التي مازالت هي الفاعل الأبرز على الساحة الدولية، التي أضحت تنافسها قوى جديدة كالتحول الرقمي ذاته، وقوى والطبيعة، ووسائل التواصل الاجتماعي العالمية والكبرى، علاوة على الفاعلين من غير الدول كالاشخاص الاعتياديين، والجماعات الإرهابية علاوة على الشركات المتعددة من غير الجنسيات والمنظمات الدولية الحكومية وغير الحكومية.

- يسود التنظيم الدولي الفوضوية في ظل غياب السلطة الشاملة لمراقبة النظام الدولي التي هي أشبه بحالة الطبيعة الأولي التي عالجتها نظريات العقد الاجتماعي. فكان سباق التسلح السيبراني أشبه بحرب الكل ضد الكل، فالكل يتسلح ليحمي نفسه ويغلق خزانته لحماية ممتلكاته ويسيج أرضه لمواجهة من يقتحم ممتلكاته، وتتشابه حالة حرب الكل ضد الكل مع التهديدات السيبرانية والمخاطر الإلكترونية، بما في ذلك الحرب الإلكترونية، والصراع السيبراني، والإرهاب السيبراني، والجرائم الإلكترونية، والتجسس الإلكتروني.

- مع ظهور الأمن السيبراني تثور عدة إشكاليات بشأن التكييف القانوني للهجمات السيبرانية والحروب السيبرانية؛ كاختصاص القانون الدولي الإنساني بالنظر للهجمات السيبرانية، ضرورة الضربة العسكرية السيبرانية، واشكالية التخطيط والتناسب عند شن تلك الهجمات، يضاف إلى التمييز بين المقاتلين والمدنين خلال الهجمة السيبرانية.

- قد انشغل علماء السياسية والمراكز البحثية بتطوير مفاهيم القوة والتأثير في ضوء الفضاء السيبراني كمركز بلفر للعلوم والشؤون الدولية وجامعة كيندي هارفارد. فاعتبرا كل منهما أن القدرة هي قياسات لنوعية وكمية ما تمتلكه الدولة من أهداف إلكترونية لناتج واحد، أو أكثر من هذه الأهداف كعدد براءات الاختراع المودعة سنويًا، وعدد أكبر شركات الأمن العالمية، وعدد العمال المهرة. وتوصلا لإمكانية احتساب الخبرة والقدرات التقنية: عبر قياس جودة وكمية مبادرات التخطيط الحكومية كمحددات للقوى السيبرانية.

- تتعدد مراكز الثقل للدول وفقا لمعياري النية والقدرة إلىدول تمتلك قدرة اعلى ونية أعلى، ودول تمتلك قدرة أعلى ونية أقل، ودول تمتلك قدرة أقل ونية أعلى، ودول تمتلك نية أقل وقدرة أقل

- القوى السيبرانية لا يمكن الارتكاز عليها كمحدد وحيد للقوى الدولية المؤثرة ولكن تقف جنبا إلى جنب وتتكامل مع المقدرات التقليدية كالقوى العسكرية والحضارية والسياسية والاقتصادية والوطنية للدول.

المراجع :

١- ايهاب خليفة، الأمن السيبراني: لماذا تصاعدت القرصنة الإلكترونية مع انتشار "كورونا"؟، الإثنين، ٠٦ أبريل، ٢٠٢٠

٢- اميل امين، الأمن السيبراني العالمي... حروب خلفية ومساحات إرهابية، ١٢ فبراير ٢٠٢٠،

٣-أحمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل: كلية القانون، العدد الرابع، ٢٠١٦، https://iasj.net/iasj/download/3f12bd1a72924acd، متوفرة بتاريخ ٢٠٢١/٠٨/٠٢

٤-اسماعيلي علوي يوسف، حالة الطبيعة من الأساس الفرضي-التاريخي إلى بعده الإجرائي، منظمة انفاس، ١٩ يونيو ٢٠١٧، https://www.anfasse.org/2010-12-30-16-04-13/2010-12-05-17--29-12/7480

٥-باتريك باولاك بروسيلس وناثالي فان ريمدونك، ماذا لو قادت "الشمس" إلى حروب سيبرانية؟، ١٩ فبراير ٢٠١٩،

٦-حمدون إ. توريه، البحث عن السلام السيبراني، الأمين العام للاتحاد الدولي للاتصالات، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، يناير ٢٠١١

٧-حمدون إ. توريه، البحث عن السلام السيبراني، الأمين العام للاتحاد الدولي للاتصالات، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، يناير ٢٠١١

٨-حسن فياض، "الهجمات السيبرانية من منظور القانون الدولي الإنساني"، مجلة الدفاع الوطني اللبناني، تشرين الأول ٢٠٢٠، العدد ١١٤

٩-حسن نافعة (وآخرون)، مقدمة في علم السياسة: الأيديولوجيات والأفكار والنظم السياسية "الجزء الأول "، الجيزة: دار الجامعة للطباعة والنشر، ٢٠٠١-٢٠٠٢، ص ٤١

١٠- دانيال لامباش، السيادة الإلكترونية: اتجاهات تشكيل مناطق سيبرانية تحت سيطرة الدول والشركات، هدير أبو زيد، ٢٣ سبتمبر ٢٠٢٠

١١-فاطمة الزهراء عبد الفتاح، قراصنة " الويندوز": كيف كشفت هجمات "الفدية الخبيثة" ثغرات الأمن السيبراني،، ١٤ مايو ٢٠١٧

١٢-فارس قرة، الأمن السيبراني – Cyber Security، الموسوعة السياسية،٣٠ يونيو ٢٠٢١

١٣-فتح الرحمن يوسف، ولي العهد السعودي يطلق مبادرتين للأمن السيبراني، الشرق الاوسط، ٠٥ فبراير ٢٠٢٠، العدد رقم (١٥٠٤٤)

١٤-عماد الدين عبد الحميد، "استراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي (٢): دراسة في العملات الرقمية للبنوك المركزية "الحلقة الثانية""، مجلة الاقتصاد الإسلامي، ١٠ أبريل ٢٠٢١،

١٥- عيسي المسعودي، احذروا الاستثمار في العملات الرقمية، الشبيبة، ٢٥ فبراير ٢٠٢١

١٦-سليم زايد، تفاصيل الهجوم السيبراني الأخطر على المؤسسات الأمريكية، مصر اليوم، ٢٠ ديسمبر ٢٠٢٠

١٧-مراد مشوش، "الجهود الدولية لمكافحة الإجرام السيبراني"، مجلة الواحات للبحوث والدراسات، العدد ٢، ٢٠١٩، المجلد رقم ١٢

١٨-مراد الشوابكة، ماذا تعني IP، مركز الدراسات الاستراتيجية والدولية CSIS موضوع، ٣ ديسمبر ٢٠١٨

١٩-مايكل جيه مازار (وأخرون)، فهم النظام الدولي الحالي، بناء نظام دولي مستدام: أحد مشروعات RAND لاستكشاف إستراتيجية الولايات المتحدة في عالم متغير، مركز راند، ٢٠١٦، ص٧

٢٠-نهلة عبد المنعم، جدية مخرجات مؤتمر «ميونخ ٢٠٢٠» في اختبار جديد، المرجع، ١٣ فبراير ٢٠٢٠، https://www.almarjie-paris.com/13900، متوافرة بتاريخ ٦ فبراير ٢٠٢١.

٢١-يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، ٢٠٢١

22-Racing to protect the most important network of the 21st century, Brookings Institute, September 3, 2019, https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/, accessed on 06/02/2021

23-Vladimir Tsakanyan, The role of cybersecurity in world politics, Vestink Rund International Relations, Peoples' Friendship University of Russia, 2017 Vol. 17 No. 2 339—348, http://journals.rud n.ru/internatio nal relations, accessed on 06/02/2021

24- Anthony Craig & Brandon Valeriano, Realism and Cyber Conflict: Security in] the Digital Age, Feb 3, 2018, https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/, accessed on 09/01/2021