الأمن السيبراني والتحول في النظام الدولي

د. هبه جمال الدين *

مستخلص

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.

Abstract:

A lot of Experts and researchers pay great attention in Cybersecurity & Cyberspace, especially after emergence of new threats that can reach to electronic war. In this prespective, political scientistis try to explain this new issues, which opens debates about the impact of cybersecurity on the international system (its units, intsiutions, structure, interactions & global processes). In this regard, this research tries to review the important debatable issues among political scientisits. The researches consistis of four parts: the first tackle the impact of this new technology on the international units in the international system. The second discusses the

* أستاذ العلوم السياسية المساعد، معهد التخطيط القومى.

Email: hebagamaleldean@inp.edu.eg

impact of cybersecurity on international organizations & instiuttions of international political system. The third reviews the change that happened on structure of international system. While the fourth discusses the prominent international processes in the international political system. The research papers uses political system approach to examinr the chage that happens with cybersescurity on its structure, units, rules and process inside the international political system,

Keywords:**Cybersecurity,Cyberspace,Cyberattacks, International system, Political system approach**

مقدمـــة:

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[١]. وزاد الاهتمام بالمفهوم مع زيادة اعتماد العالم على الكمبيوتر والشبكة العنكبوتية وتعبره جامعة هارافارد "الذراع الرابعة للجيوش الحديثة"[٢]. 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 نوعيةً في المجالات الأمنية والسياسية. اهتم علماء السياسة بتفسير هذا السلوك وظهرت دراسات تتناول هذا التطور التكنولوجي وآثاره السياسية كدراسة المعهد الدولي للدراسات الاستراتيجية بلندن.

وبدأ الحديث عن قدرة شبكة المعلومات الدولية على إعادة بلورة الأشكال التقليدية وقواعد القوة الدولية والمقدرات الدولية للوحدات الفاعلة في النسق الدولي[٣]. 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.[٤] 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 لتقدير EdSurge.[٥]

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.[٦]

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؟.

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 [٧]. وطرح معهد بروكنجز عام ٢٠١٩ قضية تأثير تكنولوجيا الـ 5G على الامن السيبراني وانعكاساته في التفاعلات بين الوحدات الدولية المختلفة؛ كالحكومات والشركات متعددة الجنسيات[٨]. 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.٩ 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".[١٠]

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.[١١] 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.

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؟.

في هذا الصدد، 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 يستعرض التغير الذي أحدثه الأمن السيبراني على هيكل النظام الدولي، أما المبحث الرابع فيطرح أبرز العمليات العالمية الواقعة بداخل الفضاء السيبراني بالنسق 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[١٢]. 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.[١٣]

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.

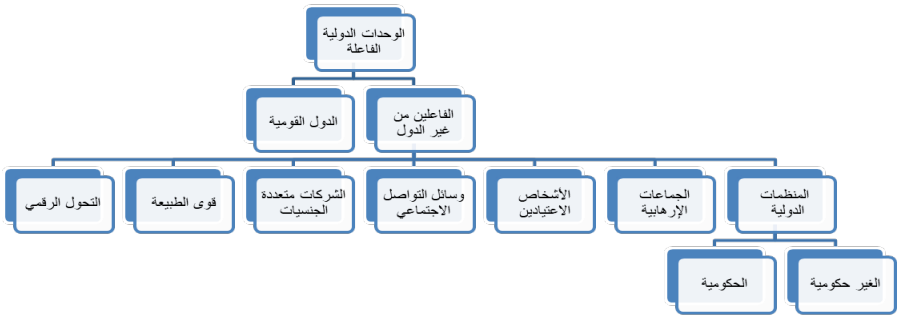
المبحث الأول: الوحدات الدولية الفاعلة في النظام الدولي:

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 و R&D البحث والتطوير في مجال الأمن السيبراني.[١٤]

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



المصدر: الشكل من اعداد الباحثة بتدبر من

Anthony Craig and 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

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.[١٥]

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. [١٦]

أ. الدول القومية "الفاعل التقليدي في العلاقات الدولية": تعتبر الدول بمختلف أحجامها، كبرى أو صغرى فاعل دولى مهما فى النظام العالمى؛ 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 الجغرافى. 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؟[١٧]. وهذا ما سيتم طرحه فيما يلي:

١. 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 (" IP " Internet Protocol)[١٨]، 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. [١٩] وعلى الرغم من ذلك نجد هناك من 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 [٢٠].

٢. 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 من جينسن و فلريانوه و مينيس 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.٢١

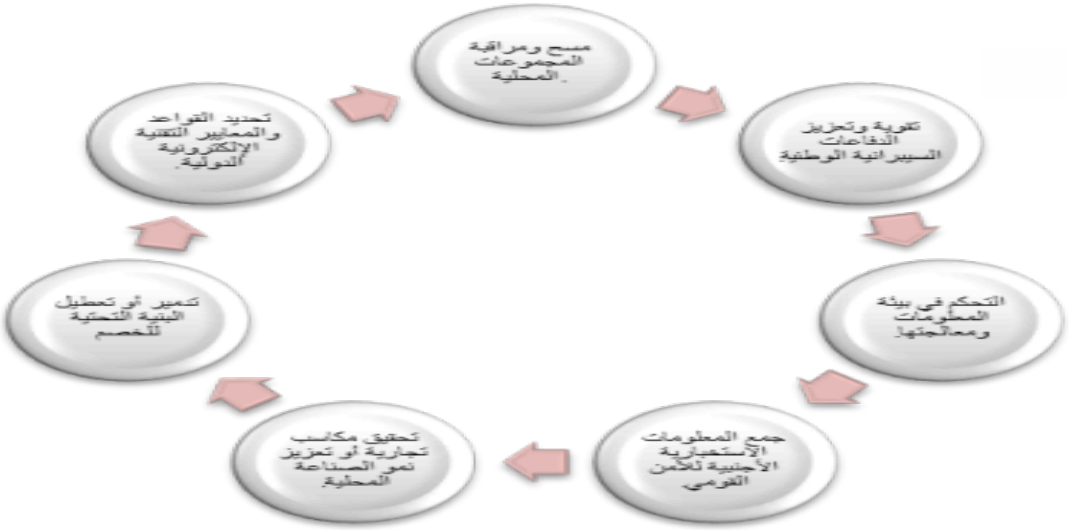
٣. إشكالية التفوق السيبراني للدول مقابل تهديدها للسلم والأمن الدوليين: في إطار ضبابية الفضاء الافتراضي وصعوبة الوقوف على حقائق الإدانة، تدور حول الدول اتهامات بارتكاب أفعال لاختراق السلم والأمن الدوليين بحجة التفوق السيبراني أو الردع الافتراضي، لتحقيق السيادة والنفوذ والأغراض السياسية المحددة والمطروحة. 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.[٢٢] 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. [٢٣] 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. [٢٤]

٤. 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. 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 [٢٥]

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



المصدر: الشكل من اعداد الباحثة بتدبر من

. Julia Voo (& others), National Cyber Power Index 2020 Methodology and Analytical Considerations, China Cyber Policy Initiative, Belfer Center for science and International Affaires, Harvard Kennedy School, Sept 2020, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf, accessed on 09/01/2020

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.

ب.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 أو السلب.

١. التحول الرقمي قوى عالمية: أضحى التحول الرقمي قوى عالمية، [٢٦] 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".٢٧

٢. 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 الحديدية.[٢٨] الأمر 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.

٣. الجماعات الإرهابية : أصغر في مقدراتها من الدول، لها أهدافا تخريبية، إلا أن قدرتهم على القيام بعمليات واسعة النطاق تعوزها مساعدة أجهزة استخبارات دولية، وإن كان من اليسير عليها اختراق المواقع الإلكترونية واستهداف الأنظمة الفاعلة. قد تمارس الضغط لتفعيل تبادل المعلومات الأمنية الرقمية، أو اختراق نظم التأمين وأمن المعلومات.[٢٩] فتستخدم الجماعات الإرهابية هذا الفضاء لسرقة المعلومات، وتسهيل كل ما هو غير مشروع من عينة تجارة البشر والسلاح، مستغلى ما يسمى السوق السوداء أو

المظلمة على الشبكة العنكبوتية. فيعتبر الإرهاب السيبراني تهديدًا رئيسيًا يواجه جميع الدول، وهذا ما يطرحه الواقعيون الجدد.

إلا أن الدول لا تستطع التصدي بفاعلية للهجمات السيبرانية الموجهة إليها كحالة الحروب التقليدية التي تخوضها ضد غيرها من الدول. فبدون امتلاك الدول لسلاح هجومي أو دفاعي مستقر يقومون بالتعدي على سيادتها وزعزعة استقرارها. في ظل صعوبة تتبع الهجمات وتحديد هوية الجاني[٣٠]، فأحد الأسباب الرئيسية وراء تحقيق مجرمي الإنترنت لمثل هذا النجاح في السنوات الأخيرة هو أنهم تمكنوا من تجاوز الحدود الوطنية والعمل على نطاق دولي في ظل نقص التعاون بين الدول المختلفة، الأمر الذي يعيق التحقيقات في جهود الجريمة الافتراضية[٣١]. مما يدفع لدعم التشريعات التي تجرم الهجمات الإلكترونية، وإدماج النشطاء الرقميين والشركات التكنولوجية والرواد التقنين لتعزيز أواصر التعاون الإقليمي والدولي في مجال مكافحة الجريمة الإلكترونية لتشارك المعلومات، وتبادل الخبرات دون تأثير على استقلالية القرار وأولوية المصلحة الوطنية.[٣٢]

٤. الأشخاص الاعتياديين، أسهم الفضاء السيبراني في تمكين الفرد من تغير وتبديل حال العالم، بل وتهديد الأمن السيبراني للقوى العظمى والكبرى في العالم. والمثال على ذلك ما رأيناه في ظاهرة ويكليكس، حيث استطاع مخترق للأمن المعلوماتي الأميركي أن يهدد أكبر دولة في العالم، الولايات المتحدة الأميركية، ويكشف أوراقها وتحالفاتها حول الكرة الأرضية[٣٣] .

٥. الشركات متعددة الجنسيات: سيدعم الأمن السيبراني دور الشركات متعددة الجنسيات في النسق الدولي، فستستخدم الشركات برامج إدارة الحقوق الرقمية والتراخيص المحدودة، وملفات تعريف الارتباط، ومتطلبات التسجيل لإنشاء حدود تسمح بجمع البيانات، ومراقبة المستخدمين، وتحقيق الدخل من الوصول إلى المحتوى الرقمي، ومن ثم سترغب الشركات في إعادة توطين الفضاء الإلكتروني لدعم أنشطتها الريادية. ويفسر دانيال لامباش هذه الميزة إلى موقف العديد من الشركات المتضارب تجاه السياسة والقانون. فمن ناحية، ستمتنع الشركات عادةً عن خرق القانون بشكل صريح لتقليل مخاطر العمل. ومن ناحية أخرى، ستعمل على تحدي الدولة عبر جمع المعلومات الرقمية للمستخدمين، مما يهدد الخصوصية للمستخدمين ويمس الأمن القومي للدول. [٣٤]

٦. 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.[٣٥]

• 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 الممارسات.[٣٦] وتساعد الدول الأعضاء على وضع الخطط والاستراتيجيات لمكافحة الجريمة السيبرانية، وتضم خبراء مكافحة الجريمة السيبرانية من الشرطة وشركات القطاع الخاص والجامعات [٣٧] 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[٣٨]، ومركز ابتكارات الأمن السيبراني في عمان عام ٢٠١٢. كما تولى منظمة الأمم المتحدة للمخدرات والجريمة بمكافحة الجريمة السيبرانية [٣٩]، 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[٤٠].

- 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.[٤١]

- وسائل التواصل الاجتماعي العالمية الكبرى:

أضحت وسائل التواصل الاجتماعي فاعلا رئيسيا في النظام العالمي؛ عبر ما تمتلكه من بيانات وقدرات؛ مثل "فيسبوك" و"جوجل" وتويتر" حيث تمتلك قدرا من المعلومات يسر لها قدرات تفوق في واقع الحال قدرات بعض الدول، فمن خلال تلك المعلومات تستطيع اختراق الأسواق السيبرانية، بل توجه المجتمعات وتشكل الراي العام العالمي. [٤٢]كما سبق الاشارة بشأن الملعلومات المضللة التي تبثها شبكات التواصل الاجتماعي الأمر الذي يسميه غابرييل كوسينتينو بالنظام العالمي لما بعد الحقيقة Post-Truth World Order. [٤٣]

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.

وبعد استعراض القوى الفاعلة على الساحة الدولية كالدول القومية والفاعلين من غير الدول، من المهم التطرق إلى القواعد والإجراءات المنظمة التي تضبط سلوك الفاعلين الدوليين في إطار الأمن السيبراني، وما يطرحه من محددات جديدة على الساحة الدولية والعالمية.

المبحث الثاني: مجموعة المؤسسات الدولية

ناقش 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. [٤٤] 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[٤٥]، 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. [٤٦]

ب. إشكالية التكييف القانوني للهجمات السيبرانية:

يواجه القانون الدولي الإنساني اشكالية أخرى تتعلق بالتكييف القانوني للهجمات السيبرانية وفقا 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.[٤٧]

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 [٤٨]

ث. إشكاليات تثور بشأن كلا من مبدأ سلوكيات الحرب التي تحكم سير العمليات القتالية، ووجوب التمييز بين المدنيين والمقاتلين "العسكريين" والتناسب في استخدام القوة المسلحة:

- تثور معضلة قانونية بشأن توجيه الهجمات السيبرانية ضد أهداف عسكرية، أو مدنية بحجة توافر أسباب مقنعة دفعت بالطرف المحارب لتبنيها؛ كخيار عسكري ضروري. كما جاء فى إعلان سان بترسبورغ عام ١٨٦٨، الذي نص على أن ضرورات الحرب يجب أن تخضع لمتطلبات إنسانية. يضاف إلى الفقرة ٢ /ز من المادة ٢٣ من اتفاقية لاهاي بشان الحرب البرية الصادرة عام ١٩٠٧ بشأن منع تدمير ممتلكات العدو، إلا فى حال وجود ضرورات تقتضي هذا التدمير. كذلك الحال بشأن البروتوكول الإضافي لاتفاقيات جنيف لعام ١٩٧٧ التى قصرت الحرب على استهداف الأهداف العسكرية فقط. علاوة على الفقرة رابعا من المادة ٥١ من البروتوكول الإضافي عام ١٩٧٧ التي تؤكد عدم جواز الهجمات العشوائية. الأمر الذي يمثل بدوره إشكالية كبيرة عند النظر للهجمات السيبرانية التي يصعب خلالها التمييز بين الأهداف العسكرية، والمدنية في الهجمات؛ فمن الممكن استهداف منشآت تقدم خدمة للجهد العسكري وللمدنيين فى ذات الوقت. ويزداد الأمر صعوبة بشأن اتساع وامتداد اثر الهجمات السيبرانية. فعدم تحديد معايير منظمة لاستخدام تكنولوجيا المعلومات للأغراض العسكرية الهجومية ستعنى إمكانية اللجوء لاستخدامها بدعوة الضرورة العسكرية فمبدأ الضرورة العسكرية قد يكون حاضرا بقوة فى أية هجمات سيبرانية متبادلة. [٤٩]
- مبدأ وجوب التمييز بين المقاتلين والمدنيين؛ وفقا للمادة ٤٨ من البروتوكول الإضافي الأول لعام ١٩٧٧ فتعمل اطراف النزاع على التمييز بين السكان المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية. وهو ما نصت عليه الفقرة ٢ من المادة ٥١ من البروتوكول الإضافي لاتفاقيات جنيف، بحظر استهداف المدنيين الأمر الذي يمثل

صعوبة فى التطبيق على الهجمات السيبرانية. فالمهاجم فى أغلب الأحيان سيكون بعيدا عن المكان المستهدف، ومما يصعب التمييز بين المدني والعسكري مما يتطلب جهدا فقهيا بشأن التميز بين سمات المجهولية للهجمات السيبرانية ومبدأ سلوكيات الحرب.[٥٠]

- مبدأ التناسب في استخدام القوة المسلحة؛ كما نصت عليه قواعد تقنين الحرب الجوية في لاهاي عام ١٩٢٢ الفقرة رقم ١ من المادة رقم ٤ التى قصرت مشروعية القصف الجوي على الأهداف العسكرية، وكذا الفقرة 5ب من المادة رقم ٥٧ من البروتوكول الإضافي لاتفاقيات جينيف عام ١٩٧٧؛ التى منعت استهداف الأهداف الغير عسكرية فى الهجوم ومنعت استهداف أرواح المدنيين والأهداف المدنية، الأمر الذي يخلق إشكالية بشأن احترام مبدأ التناسب قبل التخطيط لاستخدام وسائل وطرائق سيبرانية معدة لأغراض هجومية. يضاف إلى إشكالية ضمان مبدأ التناسب في الرد على الهجمات السيبرانية خاصة اذا كانت الأهداف ثنائية المنفعة (أي تجمع بين المنفعة العسكرية والمدنية)[٥١]

وبعد استعراض أبرز الجدل المتعلق بتأثير الأمن السيبراني على القواعد المنظمة للعلاقات بين الفاعلين الدوليين، من المهم التعرض لطرح بعض التغيرات التي تطرأ على التنظيمات الدولية القائمة في سياق الفضاء والأمن السيبراني.

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.

أ.لفوضوية وغياب السلطة الشاملة لمراقبة النظام الدولي يمكننا القول، أننا أمام حالة أشبه بحالة الطبيعة الأولي التي شغلت علماء السياسية والفلسفة الأخلاقية، وتناولتها نظرية العقد الاجتماعي، حيث تتسم حالة الطبيعة الأولي السيبرانية بالصراع وحالة حرب الكل ضد الكل، وانتشار الفوضي.

١) 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؟،[٥٢] وتتشابه حالة حرب الكل ضد الكل مع التهديدات السيبرانية والمخاطر الإلكترونية، بما في ذلك الحرب الإلكترونية، والصراع السيبراني، والإرهاب السيبراني، والجرائم الإلكترونية، والتجسس الإلكتروني.[٥٣] فقد 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.[٥٤]

٢) <u>الفوضى:</u>

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.[٥٥] 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.[٥٦]

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 المؤتمر٥٧. كذلك الحال بشان قمة ميونخ ٥٨٢٠٢٠ التي 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.[٥٩] 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.[٦٠] إلا أنها مجرد بداية تحتاج إلى زخم وإرادة دولية وقدرة على التنفيذ والالتزام[٦١]. 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.

أ. الجهود الدولية للتصدي للهجمات السيبرانية:

على الرغم من غياب سلطة عليا تنظم التفاعلات بالفضاء السيبراني كما سبق الذكر، ولكن هناك جهود دولية تمت وتتم تستهدف ضبط التفاعلات وسلوك الوحدات الدولية الفاعلة في الفضاء السيبراني في إطار التنظيمات الدولية القائمة ومنها ما أسفر عن اتفاقات دولية على الصعيد الإقليمي أو الثنائي بين الوحدات الدولية وبعضها البعض. منها ما يدور حول المساعدة في وضع وصياغة الخطط والاستراتيجيات الوطنية ومنها ما يسعى لتقديم الدعم التقني والفني، ومنها ما يقدم القوي البشرية ويستهدف لتدريب الكوادر، ومنها ما يساعد في تفعيل آلية الحساب والعقاب كالمنظمة الدولية للشرطة الجنائية "الإنتربول، [٦٢] ويمكن تصنيف أبرز تلك الجهود على مستويات أممية، وإقليمية وثنائية تم خلالها محاولات لمأسسة الجهود الدولية بداخل التنظيمات الدولية القائمة، ويمكن طرح أبرزها فيما يلى:

٣) <u>المستوى الأممي:</u> قامت الأمم المتحدة بعدد من الجهود لمأسسة وتنظيم والتصدي للهجمات والجرائم السيبرانية تنوعت بين وضع قواعد موضوعية واجرائية ومؤتمرات وقمم دولية وجهود لبعض الهيئات والاجهزة التابعة لها، ويمكن طرح ابرز تلك الجهود:

- <u>وضعت الأمم المتحدة مجموعة من القواعد الموضوعية و إجرائية لمواجهة الجرائم السيبرانية</u>. فتتضمن القواعد الموضوعية : النص على قائمة الحد الادنى للأفعال المتعين تجريمها و اعتبارها من قبيل الإجرام السيبراني و تحديثها دورياً و المتضمنة: جريمة الاحتيال أو الغش المرتبط بالكمبيوتر، وجريمة التزوير التى تطال برامج الكمبيوتر أو التزوير المعلوماتي وجريمة تخريب و اتلاف الكمبيوتر: و جريمة الدخول غير المصرح به، وجريمة الاعتراض غير المصرح به. أما القواعد الإجرائية فتتضمن بعض الأسس الواجب أخذها في الاعتبار من أبرزها؛ كوجوب تحديد السلطة المعنية بإجراء التفتيش والضبط في بيءة تكنولوجيا المعومات، ووجوب التعاون الفعال بما يتيح التنسيق والتعاون للأغراض القضائية في حل الجرائم، والسماح للسلطات العامة باعتراض الاتصالات داخل البيئة المعلوماتية مه استخدام الأدلة التى يمكن ان يتحصل عليها. وادخال بعض التعديلات التشريعية في حالة الضرورة بما يتماشى مع طبيعة الإجرام

السيبراني داخل القانون الوطني و كذلك القواعد القائمة في مجال الإثبات الالكتروني من حيث مصداقية الأدلة و ما يمكن أن تثيره من مشاكل عند تطبيقها. [٦٣]

- مؤتمرات وقمم دولية: فقد توصلت منظمة الأمم المتحدة في مؤتمرها الثامن المنعقد بهافانا ١٩٩٠ حول منع الجريمة و معاملة إلى اصدار قانون خاص بالجرائم المتعلقة بالحاسوب. [٦٤]
- بعض جهود اللجان والهيئات والأجهزة التابعة للامم المتحدة:
  - قامت لجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية في أبريل 2010 في دورتها الثانية عشرة بصياغة مجموعة من الإعلانات تضمنت إنشأ فريق خبراء حكومي دولي لبحث مشكلة الجريمة السيبرانية والاستجابات الدولية لها.[٦٥]
  - افتتح المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة دورته لعام 2010 بجلسة إعلامية عن التحديات التي يطرحها الأمن السيبراني، فضلاً عن التهديدات والفرص التي يتيحها استخدام الإنترنت الآخذ في الاتساع. أعلن المشاركون في المناقشة أنه يتعين على الأمم المتحدة أن "توحد أداءها" بشأن هذه القضية. وحذّروا من أن النطاق الدولي لحرب سيبرانية فعلية وعواقبها الوخيمة سوف تقضي استجابة منسقة؛ ولا تكفي الآن استراتيجيات اعتماد حلول على أساس مخصص وتقوية الدفاع.

– أهتمت الأمم المتحدة بالبناء المؤسسي فقانت بإنشاء بعض الكيانات مثل الشراكة التعددية ضد التهديدات السيبرانية Impact عام ٢٠٠٩ كأول منظمة تدعمها الأمم المتحدة للتحالف لدعم الأمن السيبراني[٦٦]

٤) المستوى الإقليمي: يطرح هذا الجزء الجهود التى تمت على مستوى إقليمى منها ما تمخض عنها انشأ لجان أو إدارات داخل بعض المنظمات الإقليمية للتصدي للهجمات السيبرانية، ومنها ما أسفر عن اتفاق قانونى لمواجهة تلك الجرائم والهجمات، ويمكن طرح أبرز تلك الجهود في:

- منظمة حلف شمال الأطلسي (الناتو) ومحاولات إقليمية لمأسسة الجهود: أنشأ الحلف هيئة معنية بإدارة الدفاع السيبراني، وفريقاً للاستجابة للحوادث الحاسوبية يكفل إرسال فرق الدعم السريع إلى فرادى البلدان الأعضاء، ومركزاً للتميز من أجل الدفاع السيبراني التعاوني.[٦٧] ويضم هذا المركز الذي يوجد مقره في إستونيا خبراء يضطلعون بالبحث والتدريب في مجال الأمن السيبراني. وتضم البلدان التي ترعى هذا المركز: إستونيا ولاتفيا وليتوانيا وألمانيا وإيطاليا والجمهورية السلوفاكية وإسبانيا.[٦٨]
- المجلس الأوروبي – اتفاقية بودابست بشأن الجرائم السيبرانية: تعالج اتفاقية المجلس الأوروبي بشأن الجرائم السيبرانية بعض الجرائم السيبرانية من خلال توفير أحكام قانونية نموذجية يمكن أن تعتمدها البلدان وتكيفها مع احتياجاتها الخاصة. وعلى الرغم من أن الاتفاقية تقدم بعض الحلول القانونية للجرائم من قبيل النفاذ غير القانوني (القرصنة) واعتراض الاتصالات، فإنها لا تعالج بعض أنواع عمليات الهجوم السيبراني الأكثر تهديداً مثل التجسس للحصول على البيانات وأعمال التخريب. وعلى الرغم من أن الاتفاقية تساعد على تعزيز التعاون الدولي من خلال تجريم التهديدات السيبرانية

الأساسية، فإن قوتها الإلزامية محدودة بسبب محاولة الجهة التي قامت بصياغتها عدم مخالفة تشريعات وطنية أخرى يحتمل أن تتعارض معها.وقد صدقت ثلاثون بلداً فقط على هذه المعاهدة منذ فتح باب التوقيع في نوفمبر 2001، مع بلد واحد منها من خارج أوروبا.[٦٩]

- الاتحاد الدولي للاتصالات: بهدف معالجة مسألة الأمن السيبراني عبر الشبكات الذكية تحديداً. فقام الاتحاد الدولي للاتصالات بإنشاء فريق متخصص معني بالشبكات الذكية من أجل جمع وتوثيق المعلومات والمفاهيم التي ستكون مفيدة من أجل إعداد توصيات لدعم الشبكات الذكية من منظور الاتصالات لدعم الأمن السيبراني وزيادة فاعلية التصدي للهجمات السيبرانية.[٧٠]

١) التعاون الثنائي: سعت بعض الدول بشكل ثنائي مع مثيلتها من الدول الأخرى التعاون في مجل الأمن السيبرانى ومنها الذي تخطى مذكرات تفاهم لمأسسة التعاون فى كيانات تنظيمية تنظم التفاعلات بينها وبين بعضه البعض كصندوق الصين إسرائيل بين شنغهاي وهونج كونج وتل أبيب GEOC، تم تأسيسه عام ٢٠١٣ للاستثمار فى شركات التكنولوجيا الثقيلة، في مجالات علوم الحياة والطابعات ثلاثية الأبعاد، الأمن السيبراني، والذكاء الاصطناعي وأنترنت الأشياء.[٧١]

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.

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.

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.

مقدرات القوى السيبرانية:

تثار إشكالية السرية ونقص المعلومات عند الحديث عن القوة السيبرانية؛ فيغلب عليها السرية عن الإعلان والمكاشفة نظرا لارتباطها بمقدرات الأمن القومي للدول؛ فهناك نقصا في البيانات المتاحة للجمهور. علاوة على سرية بعض البيانات المهمة مثل عدد العسكريين العاملين في الفضاء السيبراني، أو عدد الأشخاص داخل المخابرات المختصين إلكترونيا. يضاف إلى وجود نقصا في المعلومات الأقل حساسية قد يكون لوجود مشكلة بقواعد البيانات بالدول المختلفة؛ كعدد العمالة الماهرة في مجال التكنولوجيا. هذا علاوة على تعمد بعض الدول إخفاء بيانات محددة لحماية نواياها، وقدراتها كشكل من أشكال الحروب، لامتلاك عنصر المباغتة والمفاجأة أضافة للتنصل من المسؤولية والمحاسبة، والتورط في الجرائم المخططة. يضاف إلى الطبيعة الخفية أيضا عند الحديث عن العملات المشفرة يزيد الأمر صعوبة في ظل المنع والحظر ببعض الدول لاستخدامها. مما يشكل ضبابية للوقوف على القوة السيبرانية الواقعية لكل دولة وفاعل دولي بالنظام العالمي.[٧٢] وفهم كيفية استباق التهديدات، والتواصل بشكل فعال عبر الفرق المختلفة، وإدارة المشروعات.٧٣

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.[٧٤] 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.[٧٥] 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 الاجماع، 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.[٧٦]

وفي ذات الوقت بسبب سرية المعلومات المتبادلة خلال سلاسل الكتل يمكن استخدامها في الجرائم الإلكترونية، وغسيل الأموال والإرهاب[٧٧]. 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 [٧٨]. 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.[٧٩]

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.[٨٠]

وكان للربط الالكتروني والاقتصاد الرقمي أثره على تهديد الأمن السيبراني للدول وغيرها من الوحدات الدولية الفاعلة، ومقدراتها الاقتصادية ضاعفت عدد الهجمات السيبرانية على مستوى العالم، ثلاث مرات على مدار العقد الماضي، ونظراً لاعتماد الصناعة المالية والمصرفية في أغلب العالم على تكنولوجيا تقنية المعلومات والاتصالات، فإن أي هجمة سيبرانية ناجحة على مؤسسة مالية كبرى أو نظام أساسي أو خدمة يستخدمها الكثيرون يمكن أن تنتشر تداعياتها سريعاً في النظام المالي بأسره، وما يصاحب ذلك من اضطراب واسع الانتشار وفقدان الثقة في تلك القطاعات [٨١]

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 السيبرانية 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. 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 IP لأجهزة 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.[٨٢] 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.[٨٣]

ت. الطبيعة بيئة محفزة لزيادة الهجمات السيبرانية بهيكل النظام الدولي: "الكورونا وزيادة معدلات الهجمات السيبرانية"

ساهم انتشار فيروس كورونا عالميًا في زيادة سرعة تحديث كثير من المجتمعات تكنولوجيا، وزيادة الاعتمادية علي التكنولوجيا في هذا الصدد، ولكن مع زيادة الاعتمادية زادات معها الهجمات السيبرانية. ففي إطار زيادة عدد الأجهزة المرتبطة بشبكة الأنترنت في إطار أنترنت الأشياء، مع زيادة المحفزات السياسية والاقتصادية لاستغلال شبكة المعلومات الدولية، خاصة وقت الجائحة تزداد مخاطر الأمن السيبراني والتهديدات المتضمنة بزيادة معدلات الاختراق.[٨٤] ويوضح الشكل رقم ٣ إحصائية ببعض الهجمات السيبرانية خلال فيروس الكورونا.

الشكل رقم ٣: إحصائيات عن بعض الهجمات السيبرانية بالعالم خلال جائحة الكورونا

المصدر: Fintech News, The 2020 Cybersecurity stats you need to know, August 20, 2020,

https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need -to-know, accessed on 10/06/2021/

يتضح من الشكل السابق أن العالم أصبح العالم يواجه نوعين من الفيروسات فيروس حيوي وأخر افتراضي؛ فيروس كورونا Corona Virus، وفيروسات الكمبيوتر Computer Virus، أو ما يمكن اعتباره C&C Virus أي فيروسات الكمبيوتر التى تستغل أزمة كورونا لتحقيق أهداف شخصية. ويمكن تفسير زيادة الهجمات السيبرانية خلال انتشار جائحة الكورونا، بأنها نتيجة عدة أسباب أبرزها زيادة العمل عن بعد فى ظل ضعف ثقافة الأمن السيبراني لدي الكثيرين نظرا لاستخدام برامج غير أصلية، وغير محدثة تسهل عملية الاختراق. مع صعوبة تأمين بيئة الأعمال السيبرانية، وزيادة الاعتماد على تطبيقات التواصل الاجتماعي، مما يزيد من احتمالية التعرض لهجمات سيبرانية. يضاف لاستغلال المخاوف والقلق البشري بسبب الكورونا. فقد زادت مواقع النصب والاحتيال المدعية تقديمها لمعلومات وقائية بشأن الفيروس؛ فأصدرت شركة الأمن السيبراني (Check Point)تقريرًا أشارت فيه إلى أنه منذ بداية هذا العام، تم إنشاء أكثر من

٤٠٠٠ موقع إلكترونى خاص بكورونا أو (كوفيد-١٩)، وبحسب الشركة فإن ٣% من هذه المواقع ضارة، و٥% مواقع مثيرة للريبة والشك.[٨٥] .

في هذا الصدد، يمكن القول أن هناك حاجة لاستكمال النقاش الدائر بين علماء السياسة حول الملامح المميزة للنظام العالمي في ظل الفضاء السيبراني، خاصة بشأن عدد من القضايا الجدلية كفاعلية سلاح الردع في الساحة السيبرانية الأمر الذي يحتاج مزيدا من الوقت والجهد والتنظير للوقوف على عدد من المحددات؛ كتأثير سباقات التسلح السيبراني على العلاقات بين الدول، وتوزيع القدرات الإلكترونية بين الجهات الحكومية وغير الحكومية، وكذا أسباب ضبط النفس بالرغم من المنافسة الأمنية الشديدة.[٨٦]

وبعد استعراض التغير الذي طرأ على هيكل النسق الدولي وما يصاحبه من ترتيب مغاير لمقدرات الوحدات الدولية داخله. وما أحدثه الأمن السيبراني من محاولات لوضع مقومات مغايرة تتحدد على أساسها مقومات القوى الفاعلة، من المهم النظر لتأثير الأمن السيبراني على الفاعل الرئيسي في العلاقات الدولية، ألا وهو الدول فرغم عضوية الدول في المنظمات الدولية التي يتزايد دورها على الصعيد الدولي يمكنها أن تعارض أو ترفض تصرفات تلك المنظمات كما أنها يمكنها منع بعض الشركات العابرة للقوميات، وكذلك المنظمات الدولية غير الحكومية من العمل بأراضيها، بالإضافة لعملها على التصدي للجماعات الإرهابية والإجرامية. باعتبار الدول مازالت الفاعل الرئيسي في العلاقات الدولية. وهذا ما سيتم تناوله فيما يلي.

ث. <u>تأثير الأمن السيبراني على ترتيب الدول بالنسق الدولي:</u>

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 للبقاء٨٧. 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.[٨٨] 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.[٨٩] والسياسات الدفاعية والهجومية في ذات السياق.

وقد انشغل علماء السياسية والمراكز البحثية بتطوير مفاهيم القوة والتأثير في ضوء الفضاء السيبراني كمركز بلفر للعلوم والشؤون الدولية، وجامعة كيندي هارفارد. فاعتبرا كلا 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 أنه يمكن احتساب الخبرة والقدرات التقنية: عبر قياس جودة وكمية مبادرات التخطيط الحكومية (مثل الاستراتيجيات الوطنية للأمن السيبراني وخطط الأزمات وغيرها، وكذا وثائق التخطيط الحكومية ذات الصلة).

الشكل رقم ٤ :تقسيم الدول وفقا لمركز بلفر

المصدر: الشكل من اعداد الباحثة بتدبر من

Julia Voo (& Others), National Cyber Power Index 2020 Methodology and Analytical Considerations, China Cyber Policy Initiative, Belfer Center for science and Internatioanl Affaires, Harvard Kennedy School, Sept 2020, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf, accessed on 09/01/2020

وفي هذا السياق، من المهم التمييز بين النية والقدرة فالحكومة قد تكون لديها القدرات لتحقيق هدف باستخدام الوسائل السيبرانية، ولكن ليس لديها النية للقيام بذلك. وقد ترغب في السعي لتحقيق هدف من خلال الوسائل الإلكترونية، لكنها تفتقر إلى القدرة أو الموارد المطلوبة للقيام بذلك بالفعل.٩٠ وتوصلا كل منهما إلى تصنيف الدول وفقا لمعيار القدرة والنية وتتدرج بين القوى السبرانية العظمي والكبرى وفقا لأربعة تصنيفات رئيسة.

فالمجموعة الأولى تتمثل في دول تمتلك قدرة أعلى ونية أعلى: تأتي في هذه المجموعة كل من الولايات المتحدة والمملكة المتحدة والصين وفرنسا وألمانيا فجميعهم يمتلكون قدرة أعلى ونية أعلى. فتأتي النية الأعلى متمثلة في الهجمات الإلكترونية التي ينون استخدامها سيبرانيا لتحقيق أهداف السياسة الخارجية للدولة ويتمتعون بامتلاك القدرات اللازمة لتحقيقها. ***أما المجموعة الثانية هى دول تمتلك قدرة أقل ونية أعلى:*** حيث دول تحاول اتباع سياسة الردع ولكنها لا تمتلك القدرات التي تمكنها من أن تصبح قوة إلكترونية شاملة فتنشر علانية خطط مستقبلية، وتعلن عن نيتها لخوض هجمات سيبرانية واسعة النطاق وموجهة خاصة للجهات السيبرانية التخريبية وتقع في هذه المجموعة كل من روسيا، إيران، إسرائيل، هولندا، فعلى سبيل المثال أعلنت هولندا في استراتيجيتها الوطنية السيبرانية لعام ٢٠١٨ عن نيتها "لاستخدام... قدرات هجومية واستجابة أوسع في المجال السيبراني"، خاصة ضد الجهات الفاعلة السيبرانية التخريبية. وتقع أيران في هذه المجموعة ويُنسب إليها – وفقا لتقرير بلفر لعام ٢٠٢٠– شن هجمات إلكترونية متعددة مما يشير إلى أنها كانت تسعى بقوة لتحقيق بعض الأهداف من خلال الفضاء الإلكتروني. ومع ذلك، كانت واحدة من أقل الدول تسجيلًا حول قدراتها المحيطة بالمعايير والدفاعات الإلكترونية والتجارية والكسب والتحكم في المعلومات الخارجية. ويتسم نهج الدول بهذه المجموعة بمحاولات الردع اللفظي فتقوم هذه الدول بإبلاغ الدول الأخرى بنشاط تنوي القيام به، ولكن قدراتها المعلنة أقل مما تنتوي القيام به وهنا قد يفسر الأمر أما أنها لم تكشف عن قدراتها الحقيقية بشكل معلن أو أن قدراتها المتاحة أقل لتحقيق أهدافها السيبرانية ومن ثم فما تمارسه فقط ردع لفظي أو ما يمكن تسميته "ظاهرة صوتية" لخلق حالة من الرهبة والمهابة والنفوذ في قلب الأعداء ودول الجوار. ***أما المجموعة الثالثة: دول تمتلك قدرة أعلى، ونية أقل:*** وتأتي في هذه المجموعة دول مثل كوريا الجنوبية وسنغافورة وتتسم هذه الدول بتوافر القدرات العالية لتصبح قوة إلكترونية، ولكنها ليس لديها نية معلنة لشن هجمات أو تحقيق لأهداف محددة، ويفسر ذلك أما برغبة الدولة في إثارة الخلافات واتسامها بالردع السلمي فقط أو بأنها تعتزم استخدام القدرات السيبرانية لإنجاز مهمة محددة، ولكن دون المكاشفة عنه من أجل المباغتة والمفاجأة وعدم التورط والاتهام. ***أما المجموعة الرابعة تندرج في إطارها دولا ذات نيية أقل وقدرة أقل:*** تندرج في هذه المجموعة كل من مصر وليتوانيا، وتتسم هذه المجموعة بسمة خاصة، فإما لا تعمل بنشاط على تطوير قدرتها الإلكترونية، وكذا لا تعلن عن نيتها لبلوغ أهداف خارجية محددة لإبراز القوة في الفضاء الإلكتروني، أو أنها لم تنشر قدرًا كافيًا من المعلومات عن استراتيجيتها الإلكترونية أوما تقوم به من شن هجمات إلكترونية تنسب إليها أو ما تستخدمه من قدرات. ورغم تصنيف التقرير للمقدرات الدولية لكل دولة وفقا للنية والقدرة، ولكنه يوصي صناع القرار بعدم الارتكاز على القدرة والنية معا فعليهم

النظر لكل منهم بشكل منفصل نظرا لصعوبة وسرية جمع المعلومات.٩١

وفي إطار تطبيق تلك المعايير تمثل الولايات المتحدة والصين القوى الرائدة في العالم، حيث حدد التقرير اكثر القوى السيبرانية شمولا على مستوى العالم في عشرة دول، ورغم أنها تخلو من الدول العربية كما هو موضح في الجدول رقم ١ ولكن تحتل كل من السعودية ومصر وإيران مكانة ضمن القوى السيبرانية المؤثرة في العام، وفقا لمقدرات القوى الوطنية للأمن السيبراني وفقا لعام ٢٠٢٠

الجدول رقم ١: ترتيب القوى السبرانية العالمية العشرة خلال أعوام ٢٠٢٠ و٢٠١٨ و ٢٠١١ وفقا للمؤشر العالمي للقوى السيبرانية القومية

م	القوى السيبرانية العالمية وفقا لمؤشر عام ٢٠٢٠	القوى السيرانية العالمية وفقا لمؤشر لعام ٢٠١٨	القوى السيبرانية العالمية وفقا لمؤشر عام ٢٠١١
١	الولايات المتحدة	المملكة المتحدة	المملكة المتحدة
٢	الصين	الولايات المتحدة	الولايات المتحدة
٣	المملكة المتحدة	فرنسا	استراليا
٤	روسيا	لتوانيا	المانيا
٥	هولندا	استونيا	كندا
٦	فرنسا	سنغافورة	فرنسا
٧	المانيا	اسبانيا	كوريا الجنوبية
٨	كندا	ماليزيا	اليابان
٩	اليابان	كندا	ايطاليا
١٠	استراليا	النرويج	البرازيل

المصدر: Julia Voo, Op.cit (& others),

يتضح من الجدول السابق أن الولايات المتحدة الأمريكية قد أحدثت تقدما في التصنيف العالمي كقوى عظمى عالمية تلاها الصين وتراجعت المملكة المتحدة لتصبح قوى كبرى وليست عظمي في مجال الأمن السيبراني، وقد يفسر ذلك بسبب المشاكل الاقتصادية التي مرت بها بسبب أزمة البريكست وانسحاب المملكة المتحدة من الاتحاد الأوروبي. وتحتل روسيا المرتبة الرابعة عالميا وقد حققت طفرة خلال هذا العام فلم تكن مدرجة من قبل خلال مؤشري ٢٠١٨ و٢٠١١، وعلى خلاف المتوقع تأتي ألمانيا في المرتبة الرابعة متراجعة عن المرتبة الرابعة التي كانت تحتلها مع عام ٢٠١١ أما اليابان فكانت تحتل المرتبة التاسعة متراجعة مرتبة عن عام ٢٠١١. ويلاحظ أن كل من اليابان وألمانيا لم يحتلا مكانة ضمن الدول العشرة الأكثر تأثير مع مؤشر عام ٢٠١٨، وفي المرتبة الثامنة تأتي كندا متقدمة مرتبة عن عام ٢٠١٨ ومتراجعة ثلاثة مراكز بالنسبة لمؤشر عام ٢٠١١. وتأتي استراليا في المرتبة العاشرة محققة طفرة عن عام ٢٠١٨ وتراجعا عن مؤشر عام ٢٠١١ حيث كانت تحتل المرتبة الثالثة خلال هذا العام، وخرجت

سنغافورة من الدول العشرة الرائدة خلال عام ٢٠٢٠. ورغم وجود مصر في مرتبة متقدمة كدولة ذات تأثير في مجال الأمن السيبراني، ولكن مع سرعة الربط الإلكتروني الذي لا تتواكب مع الأمن السيبراني والمتوقع اكتمالها مع عام ٢٠٣٠ وفقا لرؤية مصر للتنمية المستدامة، قد تتراجع مكانة مصر مما يتطلب المواكبة بين الربط الإلكتروني والأمن السيبراني.٩٢

ورغم ما تم ذكره ولكن ستظل مراكز الثقل في النظام العالمي متكاملة بين المقدرات السيبرانية، والمقدرات العسكرية والسياسية والحضارية، والاقتصادية والوطنية للدول، خاصة في ظل سرية القدرات السيبرانية لكل دولة وعدم المكاشفة بها بشكل واضح لاعتبارات الأمن القومي.

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 السيبرانى 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.٩٣ .

أ. الصراع الدولي:

أصبح الفضاء السيبرانى 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 وفى هذا الصدد. وتثير الواقعية أسئلة مثيرة للاهتمام حول القوة الإلكترونية، من يمتلكها، ومدى ارتباطها بالاستقرار الدولى. 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 وفى 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 السيبرانية٩٤ .

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: ٩٥

- *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 فى طريقها إلى الازدياد [٩٦]

وفي هذا السياق، قد سنت الولايات المتحدة وحدها ٣٤ قانوناً جديداً و٥ أوامر تنفيذية لتنظيم التفاعلات السيبرانية ودعم محددات الأمن السيبرانى، بما فى 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 وايران وكوريا الشمالية الهجمات الإلكترونية لزيادة مجال نفوذهم. ٩٧

مما يتطلب مزيدا من البحث والدراسة حول الفضاء السيبرانى، ودرجة تحول التنافس لصراع، بل وإمكانية تطوره لدرجة الحرب وإن كان الأمر مستبعدا وفقا للمقدرات والإمكانات الحالية بدول العالم المختلفة.

ب. الردع السيبراني:

فى ظل ضبابية الفضاء السيبرانى وضعف القدرة على تحديد الجانى والتطور السريع للاسلحة السيبرانية، تأتي قضية الردع لتثير إشكالية بين علماء السياسة، فاتفقوا على الاهتمام بالتسليح السيبرانى لمنع الأعمال الضارة ضد الأصول الوطنية فى الفضاء الرقمي، والأصول التي تدعم العمليات الفضائية.٩٨ 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. .٩٩ فنظرًا لعدم اليقين المحيط باستخدام التكنولوجيا الإلكترونية كسلاحا هجوميا، يجب على الدول المضى بحذر فى المجال السيبرانى والتركيز على إنشاء دفاعات مرنة. في الواقع، من خلال الامتناع عن الحرب الإلكترونية الصريحة، ظلت العديد من الدول حكيمة إلى حد ما فى سلوكها فى الفضاء الإلكترونى حتى الآن، وهذه نتيجة يجدها المنظرون الواقعيون جذابة ومجالًا لمزيد من التفصيل النظري .١٠٠هذا وقد استخدمت عدة دول تقنيات وتكتيكات واجراءات 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[١٠١].

وعلى الصعيد الأخر، نجد أن هناك من يقلل من فاعلية سلاح الردع في الفضاء السيبراني مثل Sternstein ويعتبرون أنه قد يبدو خيارًا جذابًا نظرًا لصعوبة الدفاع كما تمت مناقشته سابقًا، إلا أن هناك العديد من المشكلات التي تقوض الردع السيبراني. .[١٠٢]

- *أولاً: لا يمكن إثبات قدرة الدولة على الانتقام ماديًا بسبب الطبيعة الافتراضية للأسلحة السيبرانية، والسرية التي تحتفظ بها الدول عليها.*
- *ثانيًا: على عكس الأسلحة النووية، لا تتمتع الأسلحة السيبرانية بنفس القدرة التدميرية، و لكي يكون لها تأثيرا رادعا كافٍ، يجب استخدامها بشكل متكرر وبتأثير كبير. مما يعد أمرًا صعبًا، لأن كل سلاح إلكتروني مصمما لثغرة أمنية محددة يمكن تصحيحها لاحقًا.*
- *ثالثًا: قد يكون من الصعب تحديد مصدر الحوادث الإلكترونية وغالبًا ما ينكر الجناة التورط. فلا يمكن للدولة أن تكون متأكدة ممن تقوم بالرد عليهم.*

تشير هذه الحجج إلى أن ردع العدوان من خلال الوسائل الإلكترونية هو سياسة غير قابلة للتطبيق في الممارسة العملية. ومن النقاط المثيرة للقلق أيضًا أنه في حين تقدر الصعوبات الكامنة في حماية الشبكات، قد لا تعطي الحكومات الأولوية للتدابير الدفاعية، أو تعتمد على التكنولوجيا القديمة. فيعتمد الردع كنظرية على قدرة الدولة المستهدفة على النجاة من الضربة الأولى، وتضيع هذه الفروق الدقيقة فى المناقشات حول الردع الإلكتروني.

وعلى خلاف ما تم ذكره، هناك من يطرح استراتيجية جديدة مثل "كيلو" الذي قدم استراتيجية " الردع المتقطع" لمعالجة فاعلية الردع في الفضاء السيبراني عبر التصدي لسلسلة من الإجراءات تراكمية الآثار " أي تعزيز الردع من خلال جعل استجابة الضحايا أكثر احتمالية، وأكثر جوهرية وإعطاء الضحايا مزيدًا من التحكم في وقت الاستجابة، بدلاً من طلب الرد بعد وقت قصير من أي هجوم. لكن فى الوقت نفسه، قد تؤدي هذه الفوائد المزعومة إلى مشاكل قانونية. فالمسافة الزمنية بين الهجوم الإلكتروني ورد الضحية قد تتعارض مع الحظر القانوني المفروض على الإجراءات العقابية البحتة. وإذا اتخذت

الإجراء شكل تدابير مضادة فيمكن تصنيفها كإجراءات من شأنها أن تنتهك القانون الدولى ولكن بالنسبة للفعل غير المشروع. ويجعل التأخير من الصعب على الدولة المجيبة أن تفي بمتطلبات اتخاذ التدابير المضادة لحمل الدولة المخالفة على الامتثال لها.[١٠٣] ومن ثم يصعب الارتكاز عليه نظريا وعمليا في ذات الوقت.

وفى هذا السياق، ظهر مفهوم الدفاع المرن لمجابهة المخاطر السيبرانية، عبر إنشاء دفاعات مرنة ففي ظل عدم اليقين المحاط بالفضاء الإلكتروني على الدول التدقيق خلال استخدامها للتكنولوجيا الإلكترونية كسلاح هجومى، والمضى باعتدال وحصافة فى ظل توزيع القدرات الإلكترونية والصريحة بين الجهات الفاعلة الحكومية وغير الحكومية ١٠٤.

ت.التعاون السيبراني مدخلا للتوازن بالنظام العالمي الجديد:

الأمن السيبرانى ليس فقط ساحة للتصعيد والردع، فيرى سين أوكيفى أنها قد تكون مدخلا لدعم الاستقرار في بيئة النظام العالمي. فيضع على الولايات المتحدة كقوى عظمي بالعالم عبء بذل الجهد لتعزيز التعاون مع الحلفاء فى 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 فى 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 الروسى"RD-180"، والذي تحتاجه فى 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 ثنائى أولاً، على أن يتم محاكاته على الآخرين. [١٠٥]

ومن ثم يتضح أن التفاعلات الدولية فى الفضاء السيبرانى بداخل النسق الدولى تجمع بين الصراع والردع والتعاون وإن كان التعاون هو السمت الغالب خاصة في ظل الزخم الدولى للاهتمام بالأمن السيبرانى لدعم السلم والأمن الدوليين سواء فى مجال الحماية أو الردع، فمن المتوقع أن يتجاوز الإنفاق على الأمن السيبراني 170 مليار دولار بحلول عام ٢٠٢٢.[١٠٦]

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.
- كان للأمن السيبراني الدور في إضفاء بعض السمات على التفاعلات الدولية بين الفاعلين بالنسق الدولي يمكن طرحها في الاتي: القوة السيبرانية أضحت ساحة للتغلب على القوى العظمى كبديل للقوة التقليدية العسكرية، في ظل العسكرة المتزايدة للفضاء الإلكتروني، وغياب الإنذار المبكر في الصراعات السيبرانية، إضافة للصبغة الهجومية السيبرانية للتفاعلات الدولية التي أضحت خلالها الدول مرتكبا الهجمات السيبرانية. هذا علاوة على سباق التسلح السيبراني بين القوى الفاعلة بالنظام الدولي، في ظل نظام عالمي يجمع بين ملامح الصراع والردع السيبراني مقابل التعاون بالمجالات السيبرانية كمدخل لإعادة التوازن بين مقدرات القوى بالنظام العالمي الجديد، في ظل غلبة الطابع السري على مقدرات القوى السيبرانية. يضاف إلى أن الأمن السيبراني قد أضحى ضمن مجالات التعاون الثنائي لتعزيز العلاقات الدولية. وزيادة الانفاق العالمي في الفضاء السيبراني مقابل نقص الكوادر المدربة بالعالم. مع تأثير القوى الطبيعية على الأمن السيبراني وبدوره على العلاقات الدولية، فأضحت الطبيعة فاعلا ومرتكبا للهجمات السيبرانية، كما أنها بيئة محفزة لزيادة الهجمات السيبرانية: كما حدث خلال جائحة الكورونا.
- 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 إلى دول 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.**

هوامش الدراسة

[١] **هارفارد بزنس ريفيو**، ما معني الأمن السيبراني؟، سكول ببليشنغ، ٢٠٢٠، https://hbrarabic.com/%D8%A7%D9%84%D9%85%D9%81%D8%A7%D9%87%D9%8A%D9%85-%D8%A7%D9%84%D8%A5%D8%AF%D8%A7%D8%B1%D9%8A%D8%A9/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A٢٠٢٠ ديسمبر ١٥ متوفرة بتاريخ /،

[٢] **المرجع نفسه**

[٣] فارس قرة، **الأمن السيبراني – Cyber Security**، الموسوعة السياسية، https://political-encyclopedia.org/dictionary/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A، متوفرة بتاريخ ٣٠ يونيو ٢٠٢١

[٤] **موسوعة أراجيك مجتمع**، ما هو الأمن السيبراني وما هي فوائده، ٢٠٢٠، https://www.arageek.com/l/%D9%85%D8%A7-%D9%87%D9%88-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A٢٠٢٠ ديسمبر ١٥ متوفرة بتاريخ ،

[5] Amy Borrett and Georges Corbineau, **Cybersecurity rankings reveal leading global cyber powers,** TECHMOINITOR, Nov. 27, 2020, https://translate.google.com/translate?sl=auto&tl=ar&u=https://techmonitor.ai/cybersecurity/cybersecurity-rankings-reveal-leading-global-cyber-powers, ACCESSED ON 09/11/2021

[٦] فارس قرة، **مرجع سابق.**

[7] Cairtriona Heinl, **Cyber Dynamics and World Order: Enhancing International Cyber Stability**, Irish Studies in International Affairs, 2018, Vol. 29, pp. 53-72, https://www.jstor.org/stable/10.3318/isia.2018.29.18?seq=1, p. 53

[8] Tom Wheeler and David Simpson, **Why 5G requires new approaches to cybersecurity**
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

[9] 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

[10] Jan-Frederik Kremer & Benedikt Müller (eds), **Cyberspace and International Relations :Theory, Prospects and Challenges**, Berline: Center for Global Studies (CGS) & Friedrich Naumann Foundation for Freedom, Springer-Verlag Berlin Heidelberg, 2014, https://link.springer.com/content/pdf/bfm%3A978-3-642-37481-4%2F1.pdf, accessed on 30 June 2021

[11] Marck Lacy & Daniel Prince, **Securitization and the Global Politics of Cybersecurity**, 2018, https://eprints.lancs.ac.uk/id/eprint/89179/2/securitizationcyber21.pdf, accessed on 30 June 2021

[١٢] 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، https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1598/RAND_RR1598z1.arabic.pdf، متوفر بتاريخ ٣٠ يونيه ٢٠٢١

[13] Dinsh, **Study of International Politics (Systems Approach),** Your Article Library, https://www.yourarticlelibrary.com/international-politics/study-of-international-politics-systems-approach/48476, accessed on 06/02/2021

[14] 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

[١٥] **لمزيد من التفاصيل انظر:** بول ويلكينسون، **العلاقات الدولية: مقدمة قصيرة جدا**، لبني عماد تركي (ترجمة)، ٢٠١٣، مؤسسة هنداوي، https://www.hindawi.org/books/93705863/3/، متوفرة بتاريخ ٢ أغسطس ٢٠٢١

[16]**For more information please visit:**

Philip N. Howard & Samantha Bradshaw, **The Global Disinformation Order2019 Global Inventory of Organised Social Media Manipulation,** Computational Propaganda Research Project, Oxford Internet Institute, London: University of Oxford, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf, accessed on 2/08/2021

[17]**For more information please visit:**

Official website of United Nations, The Charter of the United Nations, 24 October 1945, https://www.un.org/en/sections/un-charter/introductory-note/index.html, accessed on 06/02/2021

[١٨] مراد الشوابكة، **ماذا تعني IP**، موضوع، ٣ ديسمبر ٢٠١٨، https://mawdoo3.com/%D9%85%D8%A7%D8%B0%D8%A7_%D8%AA%D8%B9%D9%86%D9%8A_IP، متوفر بتاريخ ٠٢ أغسطس ٢٠٢١

[١٩] دانيال لامباش، **السيادة الإلكترونية: اتجاهات تشكيل مناطق سيبرانية تحت سيطرة الدول والشركات**، هدير أبو زيد، ٢٣ سبتمبر ٢٠٢٠، https://futureuae.com/arE/Mainpage/Item/5818/%D8%A7%D9%84%D8%B3%D9%8A%D8%A7%D8%AF%D8%A9D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D8%A7%D8%AA%D8%AC%D8%A7%D9%87%D8%A7%D8%AA-%D8%AA%D8%B4%D9%83%D9%8A%D9%84-%D9%85%D9%86%D8%A7%D8%B7%D9%82-%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D8%AA%D8%AD%D8%AA-%D8%B3%D9%8A%D8%B7%D8%B1%D8%A9-%D8%A7%D9%84%D8%AF%D9%88%D9%84-%D9%88%D8%A7%D9%84%D8%B4%D8%B1%D9%83%D8%A7%D8%AA ، متوفرة بتاريخ ٢٠ يونيه ٢٠٢١

[٢٠] فاطمة الزهراء عبد الفتاح، **قراصنة " الويندوز:" كيف كشفت هجمات "الفدية الخبيثة" ثغرات الأمن السيبراني**،، ١٤ مايو ٢٠١٧، https://futureuae.com/ar-AE/Mainpage/Item/2793/%D9%82%D8%B1%D8%A7%D8%B5%D9%86%D8%A9-%D8%A7%D9%84%D9%88%D9%8A%D9%86%D8%AF%D9%88%D8%B2-%D9%83%D9%8A%D9%81-%D9%83%D8%B4%D9%81%D8%AA-

%D9%87%D8%AC%D9%85%D8%A7%D8%AA-
%D8%A7%D9%84%D9%81%D8%AF%D9%8A%D8%A9-
%D8%A7%D9%84%D8%AE%D8%A8%D9%8A%D8%AB%D8%A9-
%D8%AB%D8%BA%D8%B1%D8%A7%D8%AA-
%D8%A7%D9%84%D8%A3%D9%85%D9%86-
%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A ، متوفرة بتاريخ ٢٠ يونيه ٢٠٢١

[٢١] Brandon Valeriano, **Op.cit** & Anthony Craig

[٢٢] لمزيد **من التفاصيل حول شبهات الاعتداءات السيبرانية من قبل الدول انظر:**
Shannon Vavra, **The world's top cyber powers**, Axios, Aug 13, 2017 https://www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276-a2bf-4a84b4986fe9.html, accessed on 22/05/2021

[٢٣] باتريك باولاك بروسيلس وناثالي فان ريمدونك، **ماذا لو قادت "الشمس" إلى حروب سيبرانية؟**، ١٩ فبراير ٢٠١٩،

https://futureuae.com/ar-AE/Mainpage/Item/4552/%D9%85%D8%AE%D8%A7%D8%B7%D8%B1-%D8%BA%D9%8A%D8%B1-%D9%85%D8%AA%D9%88%D9%82%D8%B9%D8%A9-%D9%85%D8%A7%D8%B0%D8%A7-%D9%84%D9%88-%D9%82%D8%A7%D8%AF%D8%AA-%D8%A7%D9%84%D8%B4%D9%85%D8%B3-%D8%A5%D9%84%D9%89-%D8%AD%D8%B1%D9%88%D8%A8-%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9 ، متوفرة بتاريخ ٢٠ يونيه ٢٠٢١

[24] Shannon Vavra**, Op.cit.**

[25] . Julia Voo (&Others) , **Op.cit**

[26] Amy Borrett and Georges Corbineau, **Op.cit**

[27] . Julia Voo (& others), **Op.cit**

[٢٨] باتريك باولاك بروسيلس وناثالي فان ريمدونك، **ماذا لو قادت "الشمس" إلى حروب سيبرانية؟**، ١٩ فبراير ٢٠١٩،،

https://futureuae.com/ar-AE/Mainpage/Item/4552/%D9%85%D8%AE%D8%A7%D8%B7%D8%B1-%D8%BA%D9%8A%D8%B1-%D9%85%D8%AA%D9%88%D9%82%D8%B9%D8%A9-%D9%85%D8%A7%D8%B0%D8%A7-%D9%84%D9%88-%D9%82%D8%A7%D8%AF%D8%AA-%D8%A7%D9%84%D8%B4%D9%85%D8%B3-%D8%A5%D9%84%D9%89-%D8%AD%D8%B1%D9%88%D8%A8-%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9 متوفرة، بتاريخ ٢٢ يونيه ٢٠٢١

[٢٩] فاطمة الزهراء عبد الفتاح، **مرجع سابق.**

[٣٠] Constantine J. Petallides, "**Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat"**, Inquiries, 2012, VOL. 4 NO. 03, http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-

ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat, accessed on 16/12/2020

[31] Noah Gamer, **The intersection of politics and cyber secure**, September 28, 2015, https://blog.trendmicro.com/the-intersection-of-politics-and-cyber-security/, accessed on 07/02/2021

[٣٢] فاطمة الزهراء عبد الفتاح، **مرجع سابق.**

[٣٣] اميل امين، **الأمن السيبراني العالمي... حروب خلفية ومساحات إرهابية**، ١٢ فبراير ٢٠٢٠، https://www.independentarabia.com/node/93586/%D8%B3%D9%8A%D8%A7%D8%B3%D8%A9/%D8%AA%D9%82%D8%A7%D8%B1%D9%8A%D8%B1/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%85%D9%8A-%D8%AD%D8%B1%D9%88%D8%A8-%D8%AE%D9%84%D9%81%D9%8A%D8%A9-%D9%88%D9%85%D8%B3%D8%A7%D8%AD%D8%A7%D8%AA-%D8%A5%D8%B1%D9%87%D8%A7%D8%A8%D9%8A%D8%A9 ، متوفرة بتاريخ ٩ ياير ٢٠٢١

[٣٤] دانيال لامباش، **مرجع سابق.**

[٣٥] بول ويلكينسون، **مرجع سابق**

[٣٦] **الموقع الرسمي للمنظمة الدولية للشرطة الجنائية** "**الأنتربول**"، خدمات التعاون في مجال مكافحة الجريمة السيبرية، https://www.interpol.int/ar/4/6/6، متوفر بتاريخ ٢١ يونيو ٢٠٢١

[٣٧] **المرجع نفسه**

[38] **International Multilateral Partnership Against Cyber Threats (**IMPACT), https://en.wikipedia.org/wiki/International_Multilateral_Partnership_Against_Cyber_Threats,

[39] International telecommunication Union, ITU-IMPACT establishes first Cybersecurity Innovation Centre for Arab region, Connect World, 19 December 2012, https://connect-world.com/, accessed on 22/06/2021

[40] **Georgetown University Law Library**, International and Foreign Cyberspace Law Research Guide, https://guides.ll.georgetown.edu/cyberspace, accessed on 22/06/2021

[41] **Ibid**

[٤٢] اميل امين، **مرجع سابق.**

[43] Gabriele Cosentino, **Social Media and the Post-Truth World Order: the Global Dynamics of Disinformation**, Cham: Palgrave Pivot imprint, 2020, https://link.springer.com/content/pdf/10.1007%2F978-3-030-43005-4.pdf?error=cookies_not_supported&code=9e97165f-ba74-4ce0-a377-12433038459f, accessed on 02/08/2021

[44] Official Website of United Nations, **Op.cit.**

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

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

[٤٧] حسن فياض، "**الهجمات السيبرانية من منظور القانون الدولي الإنساني**"، مجلة الدفاع الوطني اللبناني، تشرين الأول ٢٠٢٠، العدد ١١٤،

https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A ، متوفر بتاريخ 02/ 08/2021

[٤٨] يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، https://jlaw.journals.ekb.eg/article_45192_52d735c1a23cca2bf7dbbe56c4eb6846.pdf، متوفر بتاريخ 2/08/2021

[٤٩] يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، https://jlaw.journals.ekb.eg/article_45192_52d735c1a23cca2bf7dbbe56c4eb6846.pdf، متوفر بتاريخ 2/08/2021

[٥٠] 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

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

[٥٢] 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-%d8%ad%d8%a7%d9%84%d8%a9-%d8%a7%d9%84%d8%b7%d8%a8%d9%8a%d8%b9%d8%a9-%d9%85%d9%86-%d8%a7%d9%84%d8%a3%d8%b3%d8%a7%d8%b3-%d8%a7%d9%84%d9%81%d8%b1%d8%b6%d9%8a-%d8%a7%d9%84%d8%aa%d8%a7%d8%b1%d9%8a%d8%ae%d9%8a-%d8%a5%d9%84%d9%89-%d8%a8%d8%b9%d8%af%d9%87-%d8%a7%d9%84%d8%a5%d8%ac%d8%b1%d8%a7%d8%a6%d9%8a-%d9%80-%d8%a7%d8%b3%d9%85%d8%a7%d8%b9%d9%8a%d9%84%d9%8a-%d8%b9%d9%84%d9%88%d9%8a-%d9%8a%d9%88%d8%b3%d9%81، متوفرة بتاريخ ١٩ يناير ٢٠٢١

[53] TIM MAURE & HANNES EBERT, **International Relations and Cyber Security: Carnegie Contribution to Oxford Bibliographies**, Carnegie Endowment for International Peace, OXFORD UNIVERSITY PRESS, JANUARY 11, 2017, https://carnegieendowment.org/2017/01/11/international-relations-and-cyber-security-carnegie-contribution-to-oxford-bibliographies-pub-67672, accessed on 16/12/2020

[54] Anthony Craig & Brandon Valeriano**, Op.cit**

[55] **Ibid**

[56] Tim Maurer, & Hannes Ebert, **Op.cit**

[٥٧] **لمزيد من التفاصيل انظر:**

Algirde Pipikaite (& Others), **These are the top cybersecurity challenges of 2021**, World Economic Forum, 21 Jan 2021,

https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/, accessed on 06/02/2021

[٥٨] 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.

[٥٩] فتح الرحمن يوسف، **ولي العهد السعودي يطلق مبادرتين للأمن السيبراني**، الشرق الاوسط، ٠٥ فبراير ٢٠٢٠، العدد رقم (١٥٠٤٤)، https://aawsat.com/home/article/2115901/%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%B9%D9%87%D8%AF-%D8%A7%D9%84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A-%D9%8A%D8%B7%D9%84%D9%82-%D9%85%D8%A8%D8%A7%D8%AF%D8%B1%D8%AA%D9%8A%D9%86-%D9%84%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A٢٠٢١ ، متوفرة بتاريخ ٦ فبراير

[٦٠] **اتفاقية بودابست لمكافحة الجرائم المعلوماتية**، شبكة قوانين الشرق، ١١ فبراير ٢٠١٠، https://eastlaws.blogspot.com/2010/02/blog-post_11.html، متوفرة بتاريخ ٠٦فبراير ٢٠٢١

[٦١] **لمزيد من المعلومات انظر:**

Ben Bain, **Cybersecurity's new world order**, Apr 25, 2008, https://fcw.com/articles/2008/04/25/cybersecurity146s-new-world-order.aspx, accessed on 10/1/2021

[٦٢] **الموقع الرسمي للمنظمة الدولية للشرطة الجنائية** "**الأنتربول**"، خدمات التعاون في مجال مكافحة الجريمة السيبرية، https://www.interpol.int/ar/4/6/6، متوفر بتاريخ ٢١ يونيو ٢٠٢١

[٦٣] مراد مشوش، "**الجهود الدولية لمكافحة الإجرام السيبراني**"، مجلة الواحات للبحوث والدراسات، العدد ٢، ٢٠١٩، المجلد رقم ١٢، https://www.asjp.cerist.dz/en/PresentationRevue/2، متوفرة بتاريخ 02/08/2021

[٦٤] مراد مشوش، **مرجع سابق**

[٦٥] **المرجع نفسه**

[66] **International Multilateral Partnership Against Cyber Threats (**IMPACT), https://en.wikipedia.org/wiki/International_Multilateral_Partnership_Against_Cyber_Threats, accessed on 11/05/2021

[67] "NATO 2020", www.nato.int/cps/en/natolive/official_texts_63654.htm?selectedLocale=en.

[٦٨] مراد مشوش، **مرجع سابق**

[٦٩] **المرجع نفسه**

[70]**Telecommunication Standardization Sector (ITU-T)**, Focus Group on Smart Grid (FG Smart), www.itu.int/ITU-T/focusgroups/smart/, accessed on 30/07/2021

[71] **GEOC: GoCapital & Eoc official website**, What is GEOC, www.gocapitalgp.com/strategy, accessed on 21/01/2021

[72] . Julia Voo (& Others**), Op.cit**

[73] Joanne Cheng, **Op,cit**

[74] Kristen Eichenseh, **Op.cit**

[٧٥] **مستشارية الأمن الوطني: أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات**، استراتيجية الأمن السيبراني العراقي،

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf، متوفرة بتاريخ ٢٩ يونيو ٢٠٢١

[٧٦] 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، https://www.aliqtisadalislami.net/%d8%a7%d8%b3%d8%aa%d8%b1%d8%a7%d8%aa%d9%8a%d8%ac%d9%8a%d8%a9-%d8%aa%d8%b9%d8%b2%d9%8a%d8%b2-%d8%a7%d9%84%d8%a3%d9%85%d9%86-%d8%a7%d9%84%d8%b3%d9%8a%d8%a8%d8%b1%d8%a7%d9%86%d9%8a-%d9%84%d9%84%d8%a7-2/، متوفرة بتاريخ ٢٩ يونيو ٢٠٢١

[٧٧] مستشارية الامن الوطني، **مرجع سابق**

[78] Ravikumar Ramachandran, **Cybersecurity and its Critical Role in Global Economy**, ISACA Now Blog, 23 January 2019, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/cybersecurity-and-its-critical-role-in-global-economy, accessed on 29 June 2021

[79] **Ibid**

[٨٠] عيسي المسعودي، **احذروا الاستثمار في العملات الرقمية**، الشبيبة، ٢٥ فبراير ٢٠٢١، https://shabiba.com/article/id/153333، متوفرة بتاريخ ٢٠ يونيو ٢٠٢١

[٨١] عماد الدين عبد الحميد، **مرجع سابق**

[82] Tim Maurer & Hannes Ebert, **Op,cit**

[٨٣] سليم زايد، **تفاصيل الهجوم السيبراني الأخطر على المؤسسات الأمريكية**، مصر اليوم، ٢٠ ديسمبر ٢٠٢٠، https://www.masralyoum.net/ksa/7582395/%D8%AA%D9%81%D8%A7%D8%B5%D9%8A%D9%84-%D8%A7%D9%84%D9%87%D8%AC%D9%88%D9%85-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A7%D9%84%D8%A3%D8%AE%D8%B7%D8%B1-%D8%B9%D9%84%D9%89-%D8%A7%D9%84%D9%85%D8%A4%D8%B3%D8%B3%D8%A7%D8%AA-%D8%A7%D9%84%D8%A3%D9%85%D8%B1%D9%8A%D9%83%D9%8A%D8%A9، متوفرة بتاريخ ١٩ يناير ٢٠٢١

[84] Tim Maurer, **Op.cit**

[85] **لماذا تصاعدت القرصنة الإلكترونية مع انتشار "كورونا"؟**، الإثنين، ٠٦ : ايهاب خليفة، **الأمن السيبراني**، أبريل ٢٠٢٠، https://futureuae.com/ar-AE/Mainpage/Item/5477/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%84%D9%85%D8%A7%D8%B0%D8%A7-%D8%AA%D8%B5%D8%A7%D8%B9%D8%AF%D8%AA-%D8%A7%D9%84%D9%82%D8%B1%D8%B5%D9%86%D8%A9-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%85%D8%B9-%D8%A7%D9%86%D8%AA%D8%B4%D8%A7%D8%B1-%D9%83%D9%88%D8%B1%D9%88%D9%86%D8%A7، متوفر بتاريخ ٢٠ يونيه ٢٠٢١

[86] Anthony Craig and Brandon Valeriano, **Op.cit**

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

[٨٨] **المرجع نفسه**، ص ٤٤

[89] Anthony Craig and Brandon Valeriano, **Op.cit**
[90] . Julia Voo (& others) ,**Op.cit**
[91] . **Ibid**
[٩٢] **فاعليات الورشة المنظمة بمعهد التخطيط القومي حول الأمن السيبراني وموقف الدولة المصرية**، القاهرة، ٣ فبراير ٢٠٢١
[93] Julia Voo (& others), **Op.cit**
[94] Anthony Craig and Brandon Valeriano, **Op.cit**
[95] **Cyber Security Intelligence**, Cyber Warfare Is The New Frontier NATO treaty warfare army hackers, https://www.cybersecurityintelligence.com/, 15/12/2020
[٩٦] فاطمة الزهراء عبد الفتاح، **مرجع سابق.**
[٩٧] **مركز الدراسات الاستراتيجية والدولية CSIS**، تحديات عالمية ٢٠١٦: عسكرة الفضاء، الحروب السيبرانية، أمن الطاقة، ١ يناير ٢٠١٦،
https://futureuae.com/ar-AE/Mainpage/Item/659/%D8%AA%D8%AD%D8%AF%D9%8A%D8%A7%D8%AA-%D8%B9%D8%A7%D9%84%D9%85%D9%8A%D8%A9-2016-%D8%B9%D8%B3%D9%83%D8%B1%D8%A9-%D8%A7%D9%84%D9%81%D8%B6%D8%A7%D8%A1%D8%8C-%D8%A7%D9%84%D8%AD%D8%B1%D9%88%D8%A8-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9%D8%8C-%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B7%D8%A7%D9%82%D8%A9٢٠٢١ ، متوفرة بتاريخ ١يونيه
[٩٨] هارفارد بزنس ريفيو،، **مرجع سابق**
[99] Anthony Craig and Brandon Valeriano, **Op.cit.**
[100] **Ibid**
[101] . Julia Voo (&others), **Op.cit**
[102] Anthony Craig and Brandon Valeriano, **Op.cit**.
[103] Joanne Cheng, **Can Edtech Close the Talent and Workforce Gap in Cybersecurity**?, Edsurge, Jan 14, 2021, https://www.edsurge.com/news/2021-01-14-can-edtech-close-the-talent-and-workforce-gap-in-cybersecurity, accessed on 21/01/2021 .& Kristen Eichenseh, **Today's Revolution: Cybersecurity and the International Order**, Lawfare, February 8, 2018,, https://www.lawfareblog.com/todays-revolution-cybersecurity-and-international-order. Accessed on 09/01/2021
[104] Anthony Craig and Brandon Valeriano, **Op.cit**
[١٠٥] **مركز الدراسات الاستراتيجية والدولية CSIS**، مرجع سابق.
[106] Joanne Cheng**, Can Edtech Close the Talent and Workforce Gap in Cybersecurity**?, Edsurge, Jan 14, 2021, https://www.edsurge.com/news/2021-01-14-can-edtech-close-the-talent-and-workforce-gap-in-cybersecurity, accessed on 21/01/2021
Kristen Eichenseh, **Today's Revolution: Cybersecurity and the International Order,** Lawfare, February 8, 2018,, https://www.lawfareblog.com/todays-revolution-cybersecurity-and-international-order. Accessed on 09/01/2021