الحروب السيبرانية دراسة في المفهوم والنشأة ومعدلات النجاح

إعداد الباحثة

جيهان أحمد عبد العال

إشراف

أ.د/ سلوي السعيد فراج **د رشا عطوة عبد الحكيم**

الملخص

إن تكنولوجيا المعلومات والاتصالات تتيح إمكانات هائلة لإنتاجية أفضل في جميع القطاعات وللتواصل عبر القارات حيث تمثل البينية التحتية لهذه التقنيات ارتباطاً بين مصالح متعددة وخدمات مختلفة وبلدان عديدة الأمر الذي يجعل من الأخطار في مجال السيبرانى أخطار عالية تطال الجميع دون استثناء نتيجة لذلك لا يمكن لأي جهة أن تضمن بقائها في منأى من الأخطار فالطبيعة العالمية تستلزم ردا ذا أبعاد عالمية تتجاوز فيه وتتداخل السياسة والاقتصاد، والاجتماع، والتقنية، والقانون .

الكلمات المفتاحية:

الهجمات السيبرانية- الأمن القومي- الفضاء الإلكتروني

abstract

Information and communication technology offers enormous potential for better productivity in all sectors and for communication across continents, as the infrastructure of these technologies represents a link between multiple interests, different services and many countries, which makes the risks in the field of cyber high risks that affect everyone without exception. As a result, no party can It guarantees its survival from dangers. The global nature requires a response of global

dimensions that transcend and overlap politics, economics, social, technology, and law.

المقدمة:

لقد أثرت التطورات السريعة في مجال تكنولوجيا المعلومات على العديد من المجالات، لا سيما في المجالين العسكري والأمني اللذين شهدا طرق جديدة في أسلوب بناء قدرات القوات المسلحة ويرجع ذلك إلى حد ما إلى المستجدات التي طرأت على أنماط التفكير الاستراتيجي بما يتلاءم مع الواقع المتغير.

وتشير العديد من الدراسات والأبحاث القانونية المهتمة بهذا المجال إلى الدور الهام الذي يلعبه الفضاء السيبرانى في الحروب، حيث أوضح **(جون أركويلا JHON ARQUILA-) (وديفيد روزنفيلد) (DAVID RONFELD)** وهما أول من بحثا في موضوع الحروب السيبرانية في كتابهم **(لحروب السيبرانية قادمة) (CYBER WAR IS COMING)**، حيث أشارا فيه إلى أنظمة الاتصال الإلكترونية ودورها في النـزاعات المسلحة مستقبلاً، ومن خلال هذا البحث سيتم تناول ما يلي:

- أولا: مفهوم ونشأة الحروب السيبرانية.
- ثانيا: أنواع الحروب السيبرانية وسماتها
- ثالثا: عناصر الحرب السيبرانية
- رابعا: معدلات نجاح الهجمات السيبرانية

مشكلة الدراسة:

تتمثل مشكلة الدراسة في إلقاء الضوء علي هذا النمط من الحروب والذي يعد الفضاء الاكتروني ميدانة والاسلحة والمعدات المستخدمة فية شكلا جديدا عن الاسلحة

التقليدية وكذلك إيضاح الاضرار التي تلحق بالمرافق والمؤسسات مما يترتب عية خسائر فادحة للدولة والمجتمع وانتظام عمل المؤسسات بمختلف الميادين.

ثانياً: أهداف الدراسة:

تهدف الدراسة الي ما يلي:

- توضيح وتسليط الضوء على ما المقصود بالحروب السيبرانية وأهم أنواعها .
- ايضاح أهم المخاطر والتحديدات التي تواجه النظام السياسي في ظل هذا النوع من الحروب.

تساؤلات الدراسة:

حيث تسعي الدراسة للإجابة عن التساؤلات التالية

١. ما المقصود بالحروب السيبرانية ؟

٢. إلى أي مدى يؤثر الفضاء الإلكتروني فى ظهور أنماط جديدة من الصراعات التي يمكن ان تهدد الأمن القومي؟

٣. ما أهم التحديات التي تواجه صانع القرار فى مواجه هذه الحروب ؟

أولا : مفهوم ونشأة الحروب السيبرانية:

إن لكلمة حرب تعريفان: **التعريف الحرفي** للحرب الذي يستحضر البنادق والدبابات والجيوش المتقدمة، **والتعريف البلاغي** للحرب كما في الحرب على الجريمة، والحرب على الفقر، والحرب على المخدرات، والحرب على الإرهاب ،كما أن مصطلح الحرب الإلكترونية له جوانب من الحرب الواقعية والخطابية، مما يجعله مصطلحًا واسعاً للغاية لاستخدامه عند مناقشة الأمن السيبرانى والهجمات الإلكترونية[١]

١

وعلى الرغم من عدم اتفاق الباحثين المتخصصين حول تعريف محدد لمفهوم الحرب السيبرانية إلا أن أجتهد بعض الباحثين والأكاديميين في تقديم مفهوم يوضح ما هيه هذه الحروب، لذا تتعدد المصطلحات التي ظهرت لتدل على الحروب السيبرانية .

فيعرفه كل من **(ريتشارد كلارك وروبرت كناكي)** بأنها: أعمال تقوم بها دولة ما تحاول من خلالها اختراق أجهزة كمبيوتر لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها[١] .

كما عرفه المفكر العسكري الصيني **(هاف كم جوانج)**، بحرب**(الغرف المغلقة أو حرب المنازل)** ليدل على إمكانية استخدام الشعب بأكمله كشريك في الحرب مع العسكريين.

وأُشير إلى المصطلح أيضا بمصطلح **(دبابات الفكر) (Think tanks)** المكونة من خبراء غير حكوميين مختارين من الصفوة العلمية، يعملون على أجهزة الكمبيوتر الشخصي، ويشتركون في عملية صنع القرار على المستوى الأعلى.

ويُعرف أحيانا بمصطلح **(أولوية الصدمة)** حيث يذكر المحلل العسكري الصيني **(لي يانياف)**: أن أولوية الصدمة" تشكل من خبرا ء كمبيوتر متخصصين يعملون في البحث عن نقاط الضعف والنقاط الحيوية، ويسيطرون على شبكات الكمبيوتر المعادية ومن ثم يقومون بتخريبها[٢].

كما عرفتها **(كليه الشرطة الكندية")** بأنها كل جريمة جنائية تتعلق بجهاز الكمبيوتر باعتباره الهدف من الجريمة أو الأداة المستخدمة لارتكاب العنصر المادي من الجريمة.

كما عرفت **(معاهدة مجلس أوروبا)** حول الجريمة السيبرانية مصطلح الجريمة السيبرانية على أنها: الجرائم التي تتراوح بين الأشكال والأنماط المختلفة للأنشطة الإجرامية ضد البيانات والمحتوى المعلوماتي وانتهاك حقوق النشر[٣].

ووفقاً لاتفاقية **(شنغهاي للتعاون)** فإن جرائم المعلومات تعني استخدام موارد المعلومات أو التأثير عليها لأغراض غير قانونية[٤] .

أما**(منظمة التعاون الاقتصادي والتنمية) (OECD)** فقد عرفت الحرب السيبرانية على أنها: كل فعل او امتناع من شأنه الاعتداء على الأصول المادية والمعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل في التقنية المعلوماتية.

ووفقاً لتعريف **(مكتب الأمم المتحدة)** فإن الحرب السيبرانية تستخدم لوصف مجموعة واسعة من الجرائم بما في ذلك الجرائم تتمثل في هجمات سيبرانية ضد البيانات وأنظمة الحاسبات مثل القرصنة والتزوير والاحتيال مثل التصيد الاحتيالي والجرائم المتعلقة بالمحتوى مثل مخالفات حقوق الطبع والنشر وكذلك مثل نشر المحتوى الذي تم قرصنته [٥].

وتعرفة **(الجنة الدولية للصليب الأحمر)** بأنها: الأفعال التي يتخذها أطراف نزاع ما لتحقيق ميزة على خصومهم في الفضاء السيبرانى باستخدام أدوات تقنية مختلفة، مثل إتلاف المعلومات أو التجسس السيبرانى[٦].

<u>ومن خلال التعريفات السابقة نجد أن</u> : الحروب السيبرانية هي حروب خفية، أو نزاع ينشأ في الفضاء السيبرانى من خلال اعتداء دولة أو افراد باستخدام التأثير الرقمي الذي تحركه الدوافع السياسية وذلك للإضرار بقدرات دولة أخري ويكون ذلك عن طريق تهديد أنظمة اتصالاتها أو تدمير أو الاضرار بقواعد بياناتها، بهدف إجبار الخصم علي تنفيذ إرادة ضد الدولة القومية من خلال تخريب أو تعطيل الخدمات العامة، وأيضاً من الممكن أن تكون وسيلة قتالية ،حيث تستخدم في الحروب التقليدية من خلال المعلومات التي يتم الحصول عليها مما يساهم في توجيه العمليات العسكرية .

أ. <u>الحروب السـيبرانية في نظريات العلاقات الدوليـة:</u>

لقد أظهرت النظريات التقليدية في العلاقات الدولية (الواقعية والليبرالية) قدرات تفسيرية كبيرة في وصف حالة الصراع بين الشرق والغرب أثناء الحرب الباردة،

وفي ضوء التطورات التي صاحبت نهاية الحرب الباردة؛ بدأت مرحلة جديدة من مراجعة نظريات العلاقات الدولية، تراجعت فيها القضايا التقليدية للأمن التي كانت تشمل القضايا العسكرية، وسباق التسلح، ونظريات الردع وتوازن القوى، لصالح قضايا أخرى ترتبط بمفهوم الأمن غير التقليدي مثل الفقر والمجاعات والأوبئة وقضايا حقوق الإنسان والتدخل الدولي لأغراض إنسانية، كما تصاعد الاهتمام بقضايا التغيرات المناخية وظاهرة الاحتباس الحراري وما لها من تأثير على تغير حدود الدول، واختفاء المدن الساحلية، وتزايد المشكلات الناجمة عن الهجرة وزيادة عدد اللاجئين، فضلًا عن ظهور أبعاد تكنولوجية وإلكترونية جديدة مثل الجرائم والهجمات السيبرانية

ب. الحروب السيبرانية في النظريات الواقعية:

لقد تأسس فكر المدرسة الواقعية على عدة افتراضات؛- كما سبق ذكره- من أهمها أن الدولة هي الفاعل الرئيس المسيطر على العلاقات الدولية، وأنها تتسم بالعقلانية التي تجعلها تحدد مصالحها استجابة لهيكل القوة في النظام الدولي الذي يتسم بدوره بالفوضى، مما يفرض على الدول ضرورة الاعتماد على الذات لتحقيق أمنها القومي من خلال تسخير كل المصادر المادية لقوتها الفعلية والكامنة، خاصة القوة العسكرية التي تعد من وجهة نظر الواقعية البعد الأهم في قوة الدولة، حيث تتحدد أهمية العناصر المادية الأخرى بالقدر الذي يدعم به البعد العسكري.

وبتطبيق مقولات النظرية الواقعية على الظواهر السيبرانية نجد أنها تصلح في تفسير عدد من الأمور المتعلقة بالتهديدات السيبرانية والصراع السيبرانى، والتي منها على سبيل المثال الطبيعة الفوضوية للفضاء الإلكتروني[٧]، فهو نظام لا مركزي ولا توجد سلطة عليه تدير التفاعلات التي تحدث به، لذا يرى "جيمس آدم" – أحد منظِّري الواقعية الجديدة- أن الفضاء الإلكتروني أصبح ساحة القتال الجديدة للدول، وأنه كلما زاد اعتماد الدولة على التطورات التكنولوجية زادت قابليتها للاختراق، وهو ما يفرض على الدول الاعتماد على الذات؛ لتطوير قدراتها السيبرانية أو الدخول في تحالفات مع غيرها من الدول - التي لا يمكن الوثوق بها تمامًا لتدعيم أمنها القومي،

فضلًا عن ضرورة اتجاه الدول للاعتماد على نفسها في تطوير تقنياتها الذكية، وهو جوهر فكر المدرسة الواقعية؛ نظرًا لأن التقنيات التي يتم استيرادها من الغير قد يكون بها ثغرات أو برامج تجسس وأبواب خلفية تسمح بالاختراق وتهديد الأمن.

ومن هنا تظهر عدة إشكاليات تحليلية في الظواهر السيبرانية تقف أمامها النظريات الواقعية عاجزة عن التفسير، ولا تقتصر هذه الإشكاليات على حالة الحرب فقط، بل تشمل أيضًا الفواعل في هذه الحرب والقضايا التي تدور حولها، ويمكن توضيح ذلك في التالي:

- **عدم قدرة النظريات الواقعية على تفسير مراحل أقل حدة من الصراع الدولى:**

إن النظريات الواقعية بمختلف فروعها معنية بحالة الحرب وحالة البقاء، وتعتمد على مصطلحات رئيسة مثل القوة والصراع والحرب والردع، وهي حالات تمثل قمة منحنى الصراع الدولي، وقد تصلح النظريات الواقعية في تفسير الحالات التي تسعى فيها الدولة نحو تدمير خصمها نهائيا للتخلص من "المعضلة الأمنية"، لكن يبقى التساؤل عن قدرة النظريات الواقعية على تفسير حالات أقل حدَة من الصراع غير حالة الحرب والتي تنطبق على حالات الصراع السيبرانى، الذي لا يمكن فيه سحق الخصم أو تدميره نهائيا، ويبقى جليا أنه حتى الآن لم يشهد العالم حالة حرب سيبرانية كاملة أو واضحة يمكن قياسها، بل مستويات أقل من الصراع السيبرانى مثل شن هجمات سيبرانية على الأفراد والبنوك والشركات؛ بهدف الابتزاز أو الحصول على الأموال، وهو ما يضر الاقتصاد القومي للدول في النهاية[٨].

- **صعوبة تقدير قوة الدولة السيبرانية فى مواجهة غيرها من الدول وإشكالية امتلاك القوة:**

تركزت القوة في المدارس الواقعية على المفهوم المادي الصلب لها، متمثلا في القوة العسكرية، والتي يمكن قياسها وتقديرها بناء على عدد الجنود والأسلحة

وغيرها من العناصر المادية، في حين أن القوة السيبرانية هي قوة هجينة، تتكون من عناصر مادية وعناصر أخرى ناعمة، ولكلا منها تأثيره في العلاقات الدولية.

من ناحية أخرى، ترى الواقعية أنه من الضروري قياس قوة الدولة لمعرفة موقف الدول الأخرى منها، بما يحقق في النهاية توازن القوى، لكن يعتبر تقدير قوة الدولة السيبرانية أمرا صعب القياس؛ لأنها غير ملموسة أو مرصودة، ولا تعلن الدول عن قدراتها السيبرانية الهجومية.

كما أن تقدير قوة الدولة السيبرانية لا يتوقف فقط على حجم القدرات الهجومية أو الدفاعية التي تمتلكها الدولة، ولكن يتوقف أيضا عن الأهداف الحيوية والاستراتيجية المرتبطة بالفضاء السيبرانى فيها، فمثلا دولة مثل كوريا الشمالية، لديها قدرات متقدمة هجوميا في مجال الحرب السيبرانية، لكن لا توجد بداخلها بنية تحتية تعتمد على الفضاء السيبرانى يمكن إصابتها في حالة الحرب[٩].

- **<u>رغم محورية مفهوم الردع عند الواقعيين فإن تحققه أمر صعب في ظل الصراع السيبرانى :</u>**

إن الردع عند الواقعيين هو تعظيم قوة الدولة لمنع الدول الأخرى من الاعتداء عليها بما يحافظ على أمنها القومي، وهو ما يصعب تحققه بصورة كبيرة في الفضاء الإلكتروني، نظرا لعدة إشكاليات، منها: القدرة على تقدير القوة السيبرانية للخصم كما تم توضيحه في النقطة السابقة، ومن ناحية أخرى قد تتعرض إحدى الدول إلى هجمات سيبرانية من قِبل عدو لها، ومن ثَمَّ فقد تقوم بشنِّ هجوم سيبرأني انتقامي عليه بهدف تحقيق الردع، لكن هذا الهجوم يكون غير مؤثر، وفي هذه الحالة يفشل تحقيق الردع بالإضافة إلى النقطة الأهم، ألا وهي القدرة على التتبع ومعرفة مصدر الهجمات الحقيقي، وهذه إحدى إشكاليات الهجمات السيبرانية، والتي تتمثل في صعوبة معرفة الطرف المُعتدي حتى يمكن الانتقام منه أو ردعه وبالتالي لا تستطيع النظرية الواقعية تفسير حالة الردع في الصراعات السيبرانية.

- **دخول فواعل من غير الدول في الصراع السيبرانى:**

إذا كانت النظريات الواقعية تعلي من دور الدولة في الصراع الدولي، وينظر إليها التقليديون على أنها الفاعل الوحيد في العلاقات الدولية، فإن الأمر ليس كذلك في الصراع السيبرانى؛ فعلى الرغم من محورية دور الدولة فيه، فإن هناك فواعل غير الدول لهم دور كبير في الصراع السيبرانى، مثل الحركات الإرهابية التي تستخدم الإرهاب السيبرانى لتحقيق أهدافها[١٠]، ومجموعة القرصنة الإجرامية المنظمة، فضلا عن دور شركات التكنولوجيا العملاقة التي تقوم بتصنيع هذه التقنيات وإدارتها، وكذلك بعض المنظمات الدولية المعنية بإدارة الإنترنت مثل الاتحاد الدولي للاتصالات.

ج. الحرب السيبرانية في النظرية الليبرالية:

ترى النظرية الليبرالية أن الدولة ليست هي الفاعل الوحيد في العلاقات الدولية، بل إن هناك فواعل أخرى غير الدول تلعب دورا مهما في العلاقات الدولية، مثل الجماعات الإرهابية والشركات متعددة الجنسيات والمنظمات غير الحكومية، مع الاعتراف بأن الدولة هي الأكثر تأثيرًا في مجمل العلاقات، وتؤكد الليبرالية أهمية الأمن الجماعي، باعتباره وسيلة لتعزيز الأمن الدولي، من خلال إقامة مؤسسات للأمن الجماعي توفر آلية أكثر فاعلية لعملية التوازن إزاء طرف معتد، وذلك من خلال إيجاد قوة ضاربة توفر الردع، أو اتخاذ إجراءات أكثر صرامة في حال فشل الردع [١١].

ويمكن الاستفادة من النظريات الليبرالية في تحليل بعض المتغيرات الخاصة بطبيعة الفضاء الإلكتروني وطبيعة الصراع السيبرانى في الاهتمام مثلا بالأبعاد غير العسكرية للقوة، وإدخال دور الفواعل من غير الدول في تحليل العلاقات الدولية، والتأكيد على فكرة الأمن الجماعي الضرورية؛ لمواجهة التهديدات السيبرانية العابرة بطبيعتها للدول، والتي تحتاج إلى تعاون دولي مؤسسي للتغلب عليها من خلال مشاركة البيانات والمعلومات[١٢]، وتمثيل مفهوم الاعتماد المتبادلين الدول والجماعات الإنسانية، والذي هو مفهوم أساسي في الليبرالية وأحد مظاهر الحالة السيبرانية، فضلا عن فتح الفضاء السيبرانى لمساحات تفاعل غير تقليدية تحد من سيادة الدول وهو ما

تتفق معه الليبرالية، وبالرغم من ذلك فإن هناك بعض الإشكاليات التي ما زالت تحتاج إلى مزيد من التفسير، والتي منها:

- **إشكالية العلاقة بين الدولة وغيرها من الفاعلين من غير الدول:**

إن النظريات الليبرالية لا تقدم فهماً واضحا للعلاقة بين الدولة وغيرها من الفاعلين من غير الدول التي أعطت لها هذه النظريات اهتماما كبيرا. فقد أصبحت الشركات التكنولوجية العملاقة أحد عناصر إدارة الصراع الدولي بما تمتلكه من تقنيات وتكنولوجيا وخدمات، وبما تمتلكه أيضًا من معلومات؛ حيث تمتلك شركات مثل ميكروسوفت وفيس بوك وجوجل وأبل وغيرها العديدَ من المعلومات الاستراتيجية التي يوجد حولها العديد من التساؤلات عما إذا كانت هذه الشركات تشارك هذه المعلومات مع بعض الدول أم لا فإذا قامت مثلا بإعطاء هذه المعلومات إلى حكومة ما، فإن ذلك سيعطي تلك الدول هامش مناورة أكبر ومركز قوة أفضل في علاقاتها الدولية على حساب الدول الأخرى التي لم تشارك هذه الشركات المعلومات معها، وهو ما لم تفسره النظريات الليبرالية.

- **عدم قدرة المنظمات الدولية على التخلص من حالة الفوضى في الفضاء السيبرانى:**

تعتمد النظريات الليبرالية على دور المؤسسات الدولية في التخلص من حالة الفوضى في العلاقات الدولية، لكن الواقع يشير إلى عكس ذلك، وبصورة خاصة حالة الفوضى في الفضاء السيبرانى؛ فالمنظمات الدولية المعنية بإدارة الإنترنت مثل منظمة **(الأيكان ICANN)** الخاصة بإدارة عناوين ونطاقات الإنترنت وكذلك الاتحاد الدولي للاتصالات، لا تستطيع التغلب على حالة الفوضى في الفضاء السيبرانى، فالهجمات السيبرانية غير معروف مصدرها أو من يقف خلفها، ويصعب حتى إثبات ذلك، والأسلحة السيبرانية يتم تطويرها واستخدامها حتى دون أن يعلم الخصم أنه تم اختراقه من الأساس، ويصعب معرفة مَن يقوم بشن هذه الهجمات أهم دولٌ؟ أم فواعل من غير الدول؟

ومن الأمثلة على ذلك ما كشفته تسريبات **(إدوارد سنودن)** عام ٢٠١٣ عن تجسس وكالة الأمن القومي الأمريكية عبر الإنترنت على زعماء وسياسيين أوروبيين بارزين في ألمانيا والسويد والنرويج وفرنسا وذلك بين ٢٠١٢ و٢٠١٤، واستطاعت الوكالة الأمريكية الاطلاع على رسائل نصية ومكالمات هاتفية وسجل الإنترنت لعدد من الشخصيات السياسية الأوروبية من بينهم المستشارة الألمانية **(أنجيلا ميركل)**، ووزير الخارجية الألماني السابق **(فرانك فالتر شتاينماير)**.

- **صعوبة تفسير حالة الأمن الجماعى فى الصراعات السيبرانية:**

لم توفر الليبرالية إطارا يمكن من خلاله فهم الأمن الجماعي السيبرانى في ظل الإشكاليات التي يثيرها من صعوبة فنية في معرفة الطرف المعتدي من الأساس وأيضًا صعوبات تعريف نوعه وجنسه، عما إذا كان فاعلًا من الدول أو من غير الدول، ولم توضح أيضًا آلية يمكن من خلالها تحقيق الأمن الجماعي لمواجهة الصراعات السيبرانية في ظل وجود حالة من التكتم على الأسرار التقنية بين الدول؛ للحفاظ على قوتها النسبية في مواجهة غيرها[١٣].

- **العلاقة الجدلية بين الأمن والخصوصية الفردية:**

إن الليبرالية لم تحسم العلاقة الجدلية بين الأمن والخصوصية، فهل يحق للدولة التجسس على الأفراد بداخلها وتسجيل مكالماتهم واتصالاتهم عبر الإنترنت لدواعي الحفاظ على الأمن وهل يحق للشركات التكنولوجية الكبرى العابرة للحدود أن تجمع المعلومات الشخصية عن الأفراد من مختلف دول العالم، متخطية في ذلك جميع الحدود الوطنية والإقليمية بداعي أنها تسعى نحو تحسين الخدمة التي تقدمها، أو تحسين جودة الإعلانات التي تظهر لعملائها؟ أسئلة عديدة تفرض البحث عن أطر جديدة تفسر هذه الإشكاليات.

د. الحرب السيبرانية في النظرية النقدية

إذا كانت المنظورات التقليدية للعلاقات الدولية قد تعاني قصورا في الإلمام بجميع أبعاد الأمن السيبرانى، وذلك لأنها تغفل البعد القيمي، فإن النظريات النقدية التي تأخذ الأبعاد المعيارية في الاعتبار تظهر أهميتها في ضوء تزايد ارتباط العالم بثورة المعلومات، وتغير منظومة القيم في المجتمعات، كما حذرت النظرية النقدية من مخاطر الخصوصية غير المقيدة والروابط الحصرية التي تقود إلى غربة بين المجتمعات وإلى احتمال نشوب حرب أو إقصاء اجتماعي.

أضف إلي ذلك أن النظرية النقدية اهتماما كبيرا للأبعاد القيمية، حيث ترى أن سلوك الدول وتفاعلاتها في العلاقات الدولية تتبع الطريقة التي تفكر بها، وأن بنية النظام الدولي ليست بنية مادية لوحدات هذا النظام، وإنما هي نتاج للتفاعلات الاجتماعية بين وحداته، وضمن هذا البناء الاجتماعي للنظرية النقدية، تكون التوزيعات المادية محددة بشكل كبير لسلوكيات الدول، لكنها ليست وحدها فهناك عنصر المعرفة بين الدول وخبرة التعاطي مع حالات التفاعل وعملية الإدراك المشترك، وهي كلها عوامل تفيد في تشكيل بنية النظام الدولي ومساراته التفاعلية. فالتهديدات السيبرانية بصورتها العسكرية لا تكون إلا بين أعداء تقليديين بينهم معارك قائمة، سواء سياسية أو عسكرية، مثل الصراع الصيني الأمريكي أو الروسي الأمريكي، لكن تقل حدتها بين غيرهم من الدول، فمثلًا نادرا جدا ما يتم الحديث عن هجمات سيبرانية متبادلة بين الصين وكندا على سبيل المثال.

إذا يمكن القول إن النظريات النقدية على اختلاف فروعها وأشكالها ترى أن لفرد في حد ذاته قد يصبح هو مستوى التحليل، وليس الدولة كما في حالة الواقعية، أو النظام الدولي كما في حالة الليبرالية. والنماذج التي توضح ذلك عديدة، منها نموذج(**جوليان أسانج**)، ونموذج (**إدوارد سنودن**)، حيث استطاع كل منهما أن يؤثر ليس فقط في الأمن القومي للولايات المتحدة الأمريكية من خلال نشر العديد من الوثائق السرية الحكومية، أو من خلال تسريب برامج التجسس السرية التي تقوم بها أجهزة الأمن

القومي الأمريكي، بل استطاع أيضا أن يؤثر في النظام الدولي كله، وتسبب ذلك في توتر العلاقات بين الولايات المتحدة وأشد حلفائها مثل ألمانيا وفرنسا[١٤].

ثانيا: أنواع الحروب السيبرانية وسماتها :

لقد غيرت النظم المعلوماتية من طبيعة الصراعات والحروب، وأدخلت أساليب جديدة ومختلفة وهي مفاهيم بحاجة الى تقييم وصياغة، ومنها الحروب الموجهة وحرب الشبكة والحرب التجسسية والحرب الفضائية والحرب النفسية والاعلامية، وهذا ما سيتم التطرق اليه كالتالي:

أ. **<u>الحروب الموجهة</u>**

وتعتمد هذه الحروب على استهداف معلومات معينة التي تستطيع من خلالها التحكم عن بعد بالأسلحة سواء كانت برية أو بحرية أو جوية، مثل القنابل الذكية التي استخدمت في حرب الخليج الثانية عام١٩٩١، وكذلك القنابل التي استخدمت في الحرب الامريكية على العراق عام ٢٠٠٣، وذلك من خلال اعتماد الولايات المتحدة على إستراتيجية **(الصدمة والترويع)**، التي تقوم على قدرة تكنولوجية متطورة ومنظومات تسليحية متكاملة وقادرة على تطبيق التأثير المستهدف من أجل التأثير في إرادة الخصم وإدراكه، وتتطلب هذه الاستراتيجية عدة عناصر لنجاحها المعرفة الكاملة بالعمليات الذهنية والمنظومات التقنية لقادة الخصم، كما تعتمد على السرعة في جميع مراحل العمل العسكري سواء في المناورات او التحركات داخل الميدان وضمان السيطرة على العمليات سواء على الارض او في مجال الاشارات اللاسلكية والبنية الاساسية للاتصالات بما يضطر الخصم الى الاستسلام خوفا من تعرضه لدمار واسع.

كما تعد الطائرات بدون طيار **(drones)** من الأمثلة الحديثة في منظومة الأسلحة التي يتم التحكم بها عن بعد، فهي تمتلك إمكانيات تتفوق بها على إمكانيات الطائرات التقليدية، حيث إنها لا تحتاج إلى مطارات مجهزة للإقلاع وللهبوط، كما إنها تطير بسرعة فائقة ولمسافات أطول.

ب. **الحروب الشبكية: "الفيروسية "**

وهو شكل جديد من أشكال الحروب التي تمكن من التأثير على نشاطات وأعمال الخصم وخصوصاً اذا كان مجتمع الخصم متطوراً ويعتمد بدرجة كبيرة على وسائل المواصلات والاتصالات وذلك من خلال مهاجمة لشبكات الاتصال بواسطة فيروسات معلوماتية متنوعة، أما اذا كان الخصم أقل تطورا في اعتماده التقنيات الحديثة فان اساليب حروب الشبكات كالفعاليات التقنية والتشويش لن يكون مؤثراً بالدرجة المطلوبة، ومن ثم سيتم الاعتماد على الاسلحة التقليدية المعروفة والتي تعتمد على الدقة في الاصابة والسرعة في الاستجابة، لذا فان حروب الشبكة موجهة بشكل اساس نحو تحجيم العدو، ومن ثم هي تختلف عن الحرب الموجهة التي تكون نحو شل قدرة العدو العسكرية[١٥].

ج. **الحروب التجسسية**

إن التقدم التقني اصبح واحد من أهم مفاتيح المستقبل وعامل حاسم للسيطرة في النظام العالمي الجديد، لذا أصبحت المنافسة شديدة في الميدان التكنولوجي والسياسي والاستراتيجي، لان من سيحصل على التكنولوجيا فانه سيسيطر في المجالات الأخرى، لذا يرى بان جزء كبير من الاتصالات العالمية تسيطر عليها اجهزة الامن والاجهزة المخابراتية، إذ ان هذه الاجهزة تراقب كل شيء تقريبا وينتشر وكلاء متخصصون في كل بلدان العالم مدعومون بأقمار صناعية تجسسيه لجمع المعلومات والعمل مع الالاف من الاذاعات والقنوات، وكل ذلك يتجه لهدف واحد الا وهو التجسس على العالم، فالوكالات الامنية تنتشر في كل بلدان العالم وتسعى وتتنافس وبكل الطرق للحصول على المعلومات، مستخدمة كل الوسائل المتاحة بعملية تصارع اشبه بالحرب ذاتها من هنا انطلقت حرب التجسس هذه، فالدول تسعى لانفاق ثروتها على قواعدها التنصتية ونصب وسائل ذات تقنية عالية الكفاءة للتجسس على العالم[١٦].

د. **الحرب الفضائية**

فمنذ عام(١٩٨٣) سعت الولايات المتحدة الامريكية لتطوير برنامج حرب النجوم او منظومة الدفاع الاستراتيجي وامتلاك القدرة المطلقة على صد اي هجوم صاروخي،

ومنذ ذلك الوقت طور الفضاء العمليات العسكرية الارضية في مجال المراقبة والاتصالات والملاحة والرصد الجوي بحيث عمقت التكنولوجيا مفهوماً جديداً يخص الميدان والجبهة على كل الابعاد يدعى بالجبهة متعددة الابعاد.

وبالتالي يمكن للحروب السيبرانية أن تتخذ مسارات مختلفة ويتم توظيفها اقتصادياً وسياسياً وعسكرياً ونفسياً للتأثير على تفكير واتجاهات العدو كقدرته على إدارة الصراع أو الحرب بمفهومها الشامل ، ومن أهم هذه المسارات والحروب كما أشار اليها **(مارتن ليبيسكي)** :

أ. حرب القيادة والسيطرة: وهي الاستخدام غير الشرعي للمعلومات بهدف السيطرة على مقدرات أنظمة معلومات القيادة والسيطرة التابعة للعدو.

ب. حرب السيبرانية النفسية: تعنى حرب المعلومات النفسية بمحاولة طمس الحقائق عن مجتمع وتغليفها بالأكاذيب بهدف تشكيك افراده بعدالة القضية التي يقاتلون من أجلها وزعزعة ثقتهم بقدراتهم، بالإضافة إلى بث الفرقة بين صفوفهم، أو بهدف التأثير على الخصم من أجل ان يقوم بعمليات عدوانية .

ج. حرب المعلومات الاقتصادية: نتيجة لإعتماد المؤسسات المالية على قاعدة معلوماتية تقنية متطورة لا مركزية، يعتمد بعضها على بعض، معتمدة على الفضاء الالكترونى لذلك، فإن توقف اجهزة الصرف الآلي، وبطاقات الائتمان، قد يعني أن الحركة الاقتصادية قد توقفت .

ومن ثم ان هناك أشكال مختلفة للحروب السيبرانية :

- السياسي: الذي يهدف إلى التأثير على عقول القادة ومتخذي القرار.
- العسكري :الذي يهدف إلى تدمير المعلومات ونظمها العسكرية واستغلالها أو الحرمان من استخدامها او توظيفها ضد العدو.
- الاقتصادي: الذي يهدف إلى سرقة الأسرار التجارية للشركات وخاصة المنافسة واستثمارها او تدمير سمعتها.

- الشخصي :الذي يهدف إلى اغتيال السمعة الشخصية للأفراد والجماعات[١٧] .

ه. سمات الحروب السيبرانية:

تتسم الحروب الإلكترونية بأنها غير محددة المجال وقد تكون غامضة الأهداف هذا إلى جانب قدرتها التدميرية الكبيرة، وقد يتضمن التجسس والنسف لكن لا دخان ولا أنقاض ولا غبار، ويتميز أطرافه بعدم الوضوح، ولكن تداعياته خطيرة، سواء عن طريق تدمير البنية التحتية للمنشأت الحيوية عن طريق قصفها بالعديد من الفيروسات، أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة للنيل من تلك المواقع، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت، ومن ثم فأن أهم سمات هذه الحروب كالتالي :

- ساحة صراع افتراضية: حيث تخطت المساحات الجغرافية، ويشارك في الحروب السيبرانية مدنيون وعسكريون .
- الاعتماد على الفضاء الإلكتروني: حيث إن الدول الحديثة تربط بنيتها التحتية بالفضاء السيبرانى ومنها شبكات المياه والكهرباء والبنوك .
- صعوبة الردع الإلكتروني، بما أن الفضاء السيبرانى يعد ساحة افتراضية، فبالتالي يصعب على الدول وضع حدود لسياتها عليها، ومع ضعف القوانين الدولية للسيطرة على هذا الفضاء السيبرانى أصبح عملية الردع صعبة ومعقدة .
- حروب لا تناظرية : فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن حروب يعني أنه ليس هناك حاجة لدولة معينة او منظمة ما لقدرات ضخمة لتشكل تهديدا خطيرا وحقيقيا على دولة مثل الولايات المتحدة الأمريكية.
- غياب الشفافية الإلكترونية ، نتيجة لعدم القدرة على معرفة القائمين على الهجمات الإلكترونية ، ظهرت مشكلة غياب الشفافية[١٨] .

ثالثاً: عناصر الحرب السيبرانية

لأنها حرب فلابد لها من طراف متحاربين، من ثم فهي تتضمن ثلاثة عناصر: المهاجم والمدافع ولمعلومات، ومن هنا يمكن التمييز بين عدة أنماط للحرب السيبرانية، من حيث درجة الشدة، وإمكانية التنبؤ بالأزمات الناجمة عنها:

أ. **النمط الأول**: أزمات الحرب السيبرانية الباردة منخفضة الشدة **LOW (INTENSITY)**، وتعبر عن صراع مستمر بين الفاعلين المتنازعين، وقد تكون ذات طبيعة ممتدة ذات بعد تاريخي وديني وايدلوجي ممتد، كأن تكون امتدادا أو جزءا من الصراعات التقليدية الممتدة مثل(الصراع العربي- الإسرائيلي، الصراع الهندي الباكستاني، الصراع بين الكوريتين) وخلالها عادة ما يتم اللجوء إلى القوة الناعمة التي تجمع بين الجيلين الرابع والخامس للحرب، حيث تشمل وسائل عدة، مثل الحروب النفسية وحرب الأفكار والتجسس وسرقة المعلومات[١٩].

ب. **النمط الثاني**: أزمات الحرب السيبرانية متوسطة الشدة **(MEDIUM) INTENSITY**، وتظهر عند تحول الصراع عبر الفضاء إلى ساحة موازية لحرب تقليدية دائرة على الأرض، وينجم عن العمليات مجموعة متداخلة من الأزمات التقليدية، وهي ليست في حاجة إلى سيناريوهات أو بدائل كما في الأزمات السياسية، الأمر يتوقف على القدرات السيبرانية، وامتلاك برامج قادرة على الردع الإيجابي أو الهجوم المحدود أو الشامل، وينجم عنها بعض الأزمات نتيجة عدم القدرة والسيطرة على إدارة الشبكات، ومنها اختراق المواقع الإلكترونية، وسرقة المعلومات وتخريبها، وعرقلة شبكات الطاقة الكهربائية أو شبكات الطرق والمواصلات البرية والسكك الحديدية والطيران، وشبكات البنوك، وإدارة المفاعلات النووية[٢٠].

ج. **النمط الثالث**: أزمات الحرب السيبرانية مرتفعة الشدة وأزماتها الكارثية **(HIGH INTENSITY)**، ويعبر ذلك النمط عن نشوء حروب في الفضاء الإلكتروني منفردة، وهي غير متوازية مع الأعمال العسكرية التقليدية، ولم يشهد العالم هذا

النوع من الحروب، وإن كانت احتمالات حدوثها واردة في المستقبل مع تطور القدرات التكنولوجية وزيادة الاعتماد عليها، وينطوي هذا النمط من الحروب على سيطرة البعد التكنولوجي على إدارة العمليات العسكرية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، والاستحواذ على القوة الإلكترونية، والهدف من وراء ذلك تحقيق "الهيمنة الإلكترونية الواسعة" بشكل أسرع، ويعتقد بعض الخبراء ان شن إسرائيل هجمات فيروس **(ستاكس نت)** ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة ، يعد نموذجاً تقريبيا لمثل هذا النمط من العمليات.

وتتوقف قوة آثار هذه الهجمات والبرامج في مجملها على ثلاث عوامل، هي: أهمية الخدمة المقدمة، والاحتياطات المسبقة، وقوة الهجمة. ومن صور الأزمات التي تتعرض لها البنية التحتية المعلوماتية، على سبيل المثال، ضعف الخدمة جزئياً، مثل انقطاع التيار الكهربائي، وتوقف الخدمة كلياً ،مثل توقف كامل لبث القنوات الفضائية، وتقديم خدمات مزيفة من جهات وهمية ،مثل العبث بنظام عمل البنوك.

رابعاً: معدلات نجاح الهجمات السيبرانية :

أوضحت التقريرات التي اوردتها شركة **(Imperra)** وهي شركة تقدم برمجيات وخدمات للأمن السيبرانى وذلك في تقريرها السنوي الخاص بالدفاع ضد التهديدات السيبرانية التي تعرضت لها المؤسسات المشاركة في الاستطلاع وذلك من ٧٠.٥% في عام ٢٠١٥ الى ٧٨%في عام ٢٠١٩، والجدير بالذكر الى ان أكبر خمس دول من حيث نسب تعرض المؤسسات فيها لهجمات سيبرانية ناجحة كانت كلا من أسبانيا والسعودية، وكولومبيا، وتركيا، واليابان .

وقد وصفت وزارة العدل الأمريكية هجمات الفدية **(Ransomware)** بالنموذج الأكثر انتشارا من الجرائم السيبرانية بل اظهرت بعض التقريرات انها مثلت حول ٥١% من الجرائم السيبرانية خلال عام ٢٠١٨ وتعتبر هجمات الفدية **(Ransomware)** هي مجموعة من البرامج الضارة التي تصيب أجهزة الكمبيوتر

الخاصة بالأشخاص والمؤسسات وتتحكم في الملفات الأساسية ومن ثم تقيد وصول المستخدم الأساسي لتلك الملفات والتهديد بإتلافها وتدميرها تماما في حال عدم دفع الفدية التي يفرضها الهاكرز.

ومثال ذلك تلك البرامج :

- هجوم **(WannaCry)**: والذي أثر على ما يقارب ١٥٠ دولة[٢١]، وقدر مكتب التحقيقات الفيدرالي **(FBI)** ان المبلغ الاجمالي لمدفوعات الفدية يبلغ حوالي مليار دولار سنويا كما ان الخسائر المترتبة على تلك الجرائم تجاوزت ال ٥ مليار دولار في عام ٢٠١٧ ومن المتوقع ان يصل الرقم الى ١١.٥ مليار دولار في عام ٢٠١٩ و٢٠ مليار دولار في عام ٢٠٢١ اي ان معدل الخسارة من المتوقع يتجاوز ٧٤% [٢٢].
- هجوم**(Petya)**: والذى يعد مجرد جزء من أجزاء البرامج الضارة عندما بدأ تداوله عبر البريد العشوائي المتصيد في ٢٠١٦، وكان من بين اهم اسباب شهرته انه قام بتشفير سجل التشغيل الرئيسي في الأجهزة المخترقة، وهو ما ساعد على منع المستخدمين من الوصول الى الملفات الخاصة بهم بعد ذلك، وبشكل مفاجئ في يونيو ٢٠١٧ ، بدأ انتشار نسخة اكثر خبثا من البرنامج الضار وكان مختلفا عن البرنامج الأصلي الذي تم تجاهله **(Not Petya)** ، ظهر في الأساس عبر أحد برامج المحاسبة الأوكرانية المخترقة، وانتشر عبر أداة استغلال الثغرات **(Eternal Blue)** ذاتها والتي استخدمها هجو**(WannaCry)** ، ومن المتوقع أن **(not Petya)** هو هجوم إلكتروني شنته روسيا ضد أوكرانيا، رغم أن روسيا قد أنكرت ذلك، وهو ما يفتح الباب أمام عصر محتمل من البلدان التي تستخدم البرامج الضارة كسلاح لها.
- هجوم **(Ethereum)**: هي عملة مشفرة مثل عملة البيتكوين، وفي شهر يوليو تمت سرقة مبلغ قدره ٧.٤ ملايين دولارات أمريكية بعملة **(Ether)** وذلك في غضون بضع دقائق وبعد ذلك، وبعد بضعة أسابيع فقط تمت سرقة ٣٢ مليون دولارًا أمريكيًا وقد أثارت الحادثة بكاملها الأسئلة بخصوص أمن العملات القائمة على تكنولوجيا البلوك تشين **(blockchain)**.

- **طرق التهديد**
- تتعدد وتتنوع طرق التهديدات والمخاطر والجرائم ، فهي تتنوع نسبة الى مستوياتها من جهة التقنية مثلاً من جهة كأخطاء أو ثغرة في النظام كما يمكن ان تصدر عن سوء استخدام قصدي أو غير قصدي أو عن هجوم أو اختراق داخلي او خارجي كما تضاف إلى الجرائم والتهديدات والمخاطر نقاط الضعف والعنصر البشري.
- وهناك مصادر أخرى وهي بين الاعتداءات الصادرة عن الأفراد وتلك الصادرة عن الدول بعيداً عن الصراعات العسكرية وخارج عمليات التجسس يقوم افراد وعصابات باعتداءات على إدارات حكومية وطنية أو أجنبية، ولكن هذه الاعتداءات لا ترقى أبدا الى خطورة تلك التي تقوم بها الدول، ونتيجة لفشل التعاون بين البلدان المختلفة تحولت عمليات التجسس والجرائم السيبرانية من قبل الدول إلى ممارسات يومية على الشبكة العالمية للمعلومات ويبقى خطر اندلاع حروب كنتيجة لها ونتيجة حسابات خاطئة لنتائج هذه الاعمال ومدى تأثيرها.
- ونتيجة لهذه الأعمال لا يمكن تجنب ردات الفعل الإنتقامية على هذه الاعمال او التهديد بها لردع الجهة المعتدية وذلك سواء ضمن إطار الصراع او خارجه فالطريقة الأمثل تجديد النتائج العملية للاعتداءات الموجهة والمقصودة، ولبيان المستويات المختلفة من تلك الجرائم في الفضاء السيبرانى لا بد من تصنيف الجرائم السيبرانية وهو ما يسمح بالتمييز بينها وفقاً لدرجة شدتها ومستوى انتشارها وايضاً الاثار المترتبة عليها.

النتائج:

إن التهديدات والأخطار السيبرانية قد تصدر عن أعمال قصدية كالاختراقات والاعتداءات وأعمال غير قصدية كالإهمال وقلة الوعي والادراك، ويمكن توزيع التهديدات والاخطار في الفضاء السيبرانى من اهدافها منها ما يطال الدول ومنها ما يطال الأشخاص وممتلكاتهم وأموالهم وقد جاء التصدي لهذه المخاطر السيبرانية من

خلال إرادة سياسية تطلع إلى وضع وتنفيذ استراتيجية لتنمية البنية الاساسية والخدمات الرقمية قابلة للتنفيذ بجانب توفير مستوى كاف من أمن الأنظمة حتى لا يمكن تهديد أداء المؤسسات حيث أن الأمن السيبرانى يهدف إلى مساعدة الأفراد والدول والمنظمات المختلفة على حماية أصولها ومواردها من النواحي التنظيمية والبشرية والمالية والتقنية والمعلوماتية بحيث تتمكن من الاستمرار بأداء مهماتها، والهدف النهائي هو ضمان عدم تضررها بشكل دائم لدى حدوث أي اعتداء أو حادث وهذا ما يعرف بالمرونة السيبرانية اتى تعتبر أحد أهم المسائل والتحديات التي لابد من مواجهتها في مسيرة بناء الثقة في الفضاء السيبرانى

هذا إلى جانب أن هناك أنماطاً اخرى من الجرائم مثل الارهاب السيبرانى والتصيد الاحتيالي **(Cyber laundering)** والخداع السيبرانى **(Phishing)**، فمع التوسع في استخدام الانترنت ووسائل تكنولوجيا المعلومات والاتصالات زادت حجم التعرض للجرائم السيبرانية وكذلك حجم الخسائر المترتبة عليها ومما يزيد من فداحتها " الارهاب السيبرانى "الذي يعد أحد أشكال الجرائم السيبرانية والذي يعمد إلى توظيف مجموعات متنوعة من أشكال الجرائم السيبرانية لتحقيق أهدافه، كما أنه توجد سلطة عليه تدير التفاعلات التي تحدث به، لذا يرى **(جيمس آدم)** – أحد منظِّري الواقعية الجديدة- أن الفضاء الإلكتروني أصبح ساحة القتال الجديدة للدول، وأنه كلما زاد اعتماد الدولة على التطورات التكنولوجية زادت قابليتها للاختراق، وهو ما يفرض على الدول الاعتماد على الذات؛ لتطوير قدراتها السيبرانية أو الدخول في تحالفات مع غيرها من الدول - التي لا يمكن الوثوق بها تمامًا لتدعيم أمنها القومي، فضلًا عن ضرورة اتجاه الدول للاعتماد على نفسها في تطوير تقنياتها الذكية.

[1] Richard K. Betts, Conflict after the Cold War: Arguments on Causes of War and Peace, Longman, New York 2002, P.548.

[٢] محمد عبد العظيم، الحرب المعلوماتية دراسة حالة للويكيليكس، مرجع سابق، ص ١٦٥ .

[3] p.sai Sheela, et al, cyber-crime- Definition, challenges and the cost, international journal of computer & Mathematical sciences (JCMS), vol.3, no.2,(April 2014), p.34

[4] United Nations Office on Drugs and Crime, comprehensive study on cybercrime, New York, February 2013, p.12

[5]United Nation office on Drugs and Crime, Global program on cybercrime, New York, Accessed AT:
https://www.unodc.org/unodc/En/cybercrime/Global-programme-cybercrime.Html

[٦] بن تغرى موسى، الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد ١٢، الجزائر، ابريل ٢٠٢٠، ص ٤.

[7] Anthony Craig and Brandon Valeriano, Realism and Cyber Conflict: Security in the Digital Age, E-International Relations, London School of Economics, London, 2018, Accessed At:
https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

[8]Constantine J Petalites, Cyber Terrorism, and IR Theory; Realism, Liberalism, and Constructivism in the New Security Theart, inquiries, journal, VOL. 4 NO. 03, 2012, Accessed At:
http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat

[9] Lucas Kello, the meaning of the Cyber Revolution, Quarterly Journal: International Security, 2013, Accessed At:
https://www.belfercenter.org/publication/meaning-cyber-revolution-perils-theory-and-statecraft

[10]Constantine J, Petalites, Cyber Terrorism and IR Theory: Realism, Liberalism and Constructivism in the New Security Threat. inquiries journal, VOL 4 No.03.2012 Accessed At:
http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat

[١١] إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، مركز المعلومات ودعم اتخاذ القرار، مجلس الوزراء ، القاهرة، ديسمبر ٢٠٢١، ، تاريخ الاطلاع: يناير ٢٠٢٢، متاح على الرابط:
https://idsc.gov.eg/DocumentLibrary/View/6486

[12] Johan Eriksson, G. Giacomello, The Information Revolution, Security, and International Relations: (IR)relevant Theory, Sage Publications, Vol.27, No.2, 2006, p.221.244, Accessed At:
https://www.semanticscholar.org/paper/The-Information-Revolution%2C-Security%2C-and-Theory-Eriksson-Giacomello/8036b71792f4101e966fc2ea3464c583e73fac50

[١٣]إيهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، مركز المستقبل للدراسات والأبحاث المتقدمة، أبو ظبي، ٢٠٢١، ص ٤.

[14] RYAN C. MANESS, BRANDON VALERIANO, Cyber spillover conflicts: transitions from cyber conflict to conventional foreign policy disputes? Routledge Publisher, New York, 2016, pp.45-64.

[١٥] عادل عبد الصادق، أثر الإرهاب الإلكتروني على مبدأ استخدام القوة في العلاقات الدولية ، رسالة ماجستير، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، ٢٠٠٩ ، ص ١٥٢.

[١٦]قاسم خضير، عباس العزاوي، ديناميكيات الحروب الالكترونية وأثرها في الصراع الدولي، المركز الديمقراطي العربي، برلين، فبراير ٢٠٢١، متاح على الرابط :
https://democraticac.de/?p=73151

[١٧] محمد العظيم، مرجع سابق ، ص ١٧٤ .

[١٨] هبة هاشم، برنامج مقترح قائم على جغرافية الحروب السيبرانية لتنمية الوعي بمخاطرها وتعزيز قيم المواطنة الرقمية للطلاب العلمين بكلية التربية، دار المنظومة، مجلة كلية التربية، جامعة عين شمس، العدد ٤٤، الجزء الثالث، القاهرة ،٢٠٢٠، ص ٢٠ .

[١٩] عبد الغفار الدويك، الازمات والحروب السيبرانية تهديدات تتجاوز الفضاء الإليكتروني، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، فبراير ٢٠١٩، متاح على الرابط:
https://acpss.ahram.org.eg/News/16843.aspx

[٢٠] هبة هاشم محمد ، مرجع سابق، ص ٩٩ .

[21] Reuters, Cyber expert credited with stopping "WannaCry attack admits malware charges, April 2019, Accessed At:
https://www.nccgroup.com/media/4xrla5rm/ncc-group_-the-guide-to-incident-response-planning.pdf

[22] Cybersecurity Ventures, 2019 official Annual Cybercrime Report", Herjavec Group, Washington,2019,p.7.