# الفضاء السيبراني: المفاهيم والأبعاد

**نور الدين حامد علي ابراهيم** *

## ملخص

تتناول الدراسة الفضاء السيبراني وما يحدثه من تغيرات في العلاقات الدولية، وكيفية ظهور الفضاء السيبراني كمفهوم والمراحل تكونية وتطوره، والتأثيرات التي أحدثها في مفهوم الردع وهل يمكن ادخال الفضاء السيبراني ضمن منظومة الردع، والمعوقات التي تواجه ذلك، وتناولت الدراسة كيفية تحقيق تفوق في الفضاء السيبراني وإيجاد نموذج للتفوق لهذا دفاعيًا وهجوميًا للدول، والوسائل اللازم توافرها لتأمين وجود الدولة ومواطنيها وأنشطتها سيبرانيًا، وتجميع أحداث وحالات قرصنة سيبرانية لتصور كيف ستكون الحرب سيبرانية كالهجوم على الأنظمة العسكرية والحكومية، والهجمات المُستهدِفة للبنية التحتية وما تنتج عنه خسائر مادية قد تكون كارثية للدولة المستهَدفة.

وخلصت الدراسة إلي ان الفضاء السيبراني لا يمكن إغفال تأثيره على العلاقات الدولية في تغير طبيعة الردع والحرب، وحتمية اعتماد الفضاء السيبراني بعدًا دفاعيًا جديدًا، وعدم النظر إلي الفضاء السيبرانية والقوة السيبرانية برفاهية وليس ذات تأثير على العلاقات الدولية نظريًا وتطبيقيًا، فإغفال هذا التأثير يحدث خلل في التنظير يترتب عليه خلل في إيجاد نظرية مفسره للتعامل مع الواقع، فالسيطرة على الفضاء السيبراني لا يأتي بالنصر في الحرب بمفرده على سبيل المثال، لكن لا تستطيع أن تفوز بدونه، وأحداث تأثيرات في المجلات الأخرى المرتبطة بالفضاء السيبراني.

**الكلمات المفتاحية:** : الفضاء السيبراني، الردع، الحرب، العلاقات الدولية، القوة السيبرانية.

* طالب ماجستير بقسم العلوم السياسية-كلية التجارة وإدارة الأعمال - جامعة حلوان.

# Cyberspace: Concepts and Dimensions


## Abstract

The study deals with cyberspace and its changes in international relations, how cyberspace appeared as a concept, the stages of its formation and development, the effects it has had on the concept of deterrence and whether cyberspace can be included in the deterrence system, and the obstacles facing it, the study dealt with how to achieve superiority in cyberspace and find a model of superiority for this defensive and offensive such as attacks on military and government systems, targeted attacks on infrastructure and resulting material losses may be Catastrophic for the target state.

The study concluded that cyberspace cannot be overlooked its impact on international relations in changing the nature of deterrence and war, and the inevitability of adopting cyberspace as a new defensive dimension, and not looking at cyberspace and cyber power with luxury and not having an impact on international relations theoretically and practically, the omission of this impact causes a defect in theorizing, which results in a defect in finding an explanatory theory to deal with reality, as controlling cyberspace does not bring victory in war alone, for example, but you cannot win without it, and others related to cyberspace.


**Keywords:** Cyberspace, Deterrence, War, International Relations, CyberPower.

**المقدمة:**

أهمية دراسة الفضاء السيبراني بسبب العلاقة بين الفضاء السيبراني والعلاقات الدولية التي مثلت مرحلة فاصلة للعلاقات الدولية في العقدين الماضيين، لبروز دور الفضاء السيبراني والآلات المتحكم به من تطور الاتصالات والمعلومات وانتشار التكنولوجيا كل هذا أثر على دراسة وتحليل العلاقات الدولية لفهم التفاعلات المستجدة على كافة مستويات الحليل من الكيانات ما فوق الدول إلى مستوي الأفراد، وظهور تفاعلات دولية تعاونية وصراعية في الفضاء السيبراني أدت إلى الحاجة لإعادة التفكير في أنماط التفاعلات والتأثير وطبيعة الأفعال التي يستطيع الفواعل الدولية ممارستها في الفضاء السيبراني، لعقود ظل اهتمام العلاقات الدولية بالتفاعلات البشرية في المجلات البرية والبحرية والجوية والفضائية واعتبرت هذه المجالات ذات خصائص محدودة من الفواعل ومدي كل مجال وحدوده وطبيعة التفاعل فيه، لكن الفضاء السيبراني حول العلاقات الدولية من دراسة التفاعلات بين الدول إلى دراسة حركة التفاعلات بين المجتمعات الدولية على كافة الأصعدة، فأصبح الفضاء السيبراني بعدًا مهمًا في العلوم السياسية وباقي المجالات الاجتماعي والاقتصادي وحتي البعد النفسي[1].

**أولًا: أهمية الدراسة:**

تنبع أهمية الدراسة من الاهتمام المتزايد بالفضاء السيبراني وتأثيرها على التفاعلات بين الفاعلين في مجال العلاقات الدولية، والتأثير على المفاهيم كالحرب والردع، وقدره الفضاء السيبراني الافتراضي على التسبب في خسائر مادية، وما يمكن فعله بالفضاء السيبراني بالتأثير على قوة الدول كالبنية التحتية الحرجة وفى قدرات الدولة العسكرية والاقتصادية.

[1] عادل عبدالصادق، أثر الفضاء الإلكتروني في تغير العلاقات الدولية: دراسة في النظرية والتطبيق، **رسالة دكتوراه**، غير منشورة، كلية الاقتصاد والعلوم السياسية، 2014، ص ص 48-50.

**ثانيًا: إشكالية الدراسة:**

تقوم العلاقات الدولية على دراسة التفاعلات بين الفاعلين الرسميين والغير الرسميين في كافة المجالات، ودراسة أشكال التفاعلات المختلفة الصراعية والتعاونية، هذه التفاعلات تحدث في بيئة طبيعية يسعي الإنسان لاستغلالها للسيطرة على الآخرين، وهذا المنظور التقليدي للعلاقات الدولية يقوم بدراسة التفاعلات بين كيانين أو أكثر في البيئة الطبيعية وينجح في تفسير الظواهر، لكن عند الانتقال لبيئة من صنع الإنسان (الفضاء السيبراني) تتغير طبيعة المفاهيم والتفاعلات ويحدث خلل في التحليل وبالتالي يعجز المنظور التقليدي عن فهم وتفسير التفاعلات في الفضاء السيبراني.

**ثالثًا: تساؤلات الدراسة:**

تنطلق الدراسة من عدة تساؤلات: ما علاقة الفضاء السيبراني بمجال العلاقات الدولية؟ كيف ظهر الفضاء السيبراني وكيفية تطوره؟ تأثير الفضاء السيبراني على مفاهيمي الردع والحرب؟ وكيفية تحقيق تفوق في الفضاء السيبراني وإيجاد نموذج للتفوق لهذا دفاعياً وهجومياً للدول؟

**رابعًا: اقترابات ومناهج الدراسة:**

تعتمد الدراسة على المنهج الوصفي التحليلي لفهم الفضاء السيبراني لتفسير ارتباطه بالعلاقات الدولية، ومن ثم تفسير ظاهرة التفاعلات داخل الفضاء السيبراني، واستخدام المنهج التاريخي لتتبع كيفية ظهور وتطور الفضاء السيبراني.

**خامسًا: تقسيم الدراسة:**

أولاً: الفضاء السيبراني: المفاهيم والتكوين، ثانيًا: الردع السيبراني، ثالثًا: نموذج التفوق في الفضاء السيبراني، رابعًا: الحرب في الفضاء السيبراني، خامسًا: النموذج التطبيقي.

**الفضاء السيبراني: المفاهيم والأبعاد**

ترجع اهمية الفضاء السيبراني إلي عدة عوامل:-

1- أهمية الهجمات السيبرانية في إحداث دمار كبير لتحقيق الإكراه والتأثير في أفعال الآخرين دون وقع إيذاء بدني او تدمير الأصول، لهذا يلجأ العديد من الفاعلين لاستخدم الفضاء السيبراني في الهجوم.

2- الحدود داخل الفضاء السيبرانية محدودة جداً، فيوفر الفضاء السيبراني الإمكانية اللازمة للقيام بهجمات سيبرانية بتكلفة منخفضة بالمقارنة بالبيئات الأخرى المستخدمة في الصراع، بالإضافة إلى القدرة على اكتساب المعرفة اللازمة لتنفيذ هجمات السيبرانية متاحه وسهلة الوصول إليها، وهذا يزيد من الأخطار الأمنية التي تتعرض لها الدول والأفراد.

3- القدرة على التخفي في الفضاء السيبراني من أهم العوامل الجاذبة للمستخدمين له، فمن الصعب تحديد هوية منفذي الهجمات، وفي أحسن الأحوال عدم معرفته على وجهه الدقة، فالتخفي يحدث أزمة في الفضاء السيبراني من حيث وضع استراتيجية للتعامل معه، فيصعب على الدول توجيه الأسلحة السيبرانية ضد منفذ الهجوم لعدم معرفة هويته عكس الأسلحة النووية التي تعطي للفاعلين القدرة على معرفة مصدر الخطر فحيث توازن رعب النووي يؤدي للتفاوض للحد من التسليح.

4- يتسم بعدم وجود قواعد حاكمة لسلوك الفاعلين وبالتالي لا يمكن التنبؤ بما سيحدث وبالتالي عدم القدرة على تحسب رد الفعل، فيمكن لأحد الفاعلين إحداث دمار واسع النطاق دون التقيد بقانون أو ضوابط كالحرب.

5- غياب الحدود والحواجز الجغرافية والزمانية التي تؤدي إلى وجود عقبات جغرافية بين الدول والتي تعوق أو تصعب أي عمل عسكري من دوله ضد اخري، فالحواجز تجعل الطرف الاخر يتحضر للدفاع أو للهجوم أو للقيام بأعمال وقائية.

6 – وجود عدد كبير من الفواعل كالدول، فهناك سباق تسلح على الأسلحة السيبرانية من اجل امتلاك القدرة على شن حرب سيبرانية، وطبيعة الفضاء السيبراني بذاته كبيئة قابلة لتصعيد الصراعات فيها نتيجة لامتلاك عدد كبير من الفاعلين القدرات لتنفيذ الهجمات الإلكترونية[2].

فمع ذكر أسباب الاهتمام بالفضاء السيبراني نجده يعطي مساحة غير تقليدية تستوعب الكثير من الفواعل الدولية وقدرة على إتاحة كمية غير محدودة من المعلومات وتخطي الحواجز الجغرافية، يري Joseph Nye يجب أن يوجد سعي من الدارسين والمحللين في الأمن القومي لمحاولة فهم الفضاء السيبراني من أجل قضايا الردع والهجوم والدفاع وتأثيره على تفاعلات الفاعلين الدوليين، لكن الطبيعة لهذه البيئة معقدة ومختلفة وصعبة التوقع في ردود الأفعال للفاعلين أو حتي فهمها، فالطبيعة المبهمة للبيئة السيبرانية في التنظير تشبه فترة الأمن النووي في الخمسينات وعدم بلورة مفاهيم كالردع النووي آنذاك، ويضيف Nye أن الفضاء السيبراني أصبح مصدر قوة للفاعلين من غير الدول ووسع دائرة التهديدات الأمنية للدول والناتج عن تقليص الفجوة بين الدول وغير الدول من حيث القدرات في هذه البيئة وامكانية الوصل اليها، ويترتب على ذلك إحداث أضرار وتهديدات مستمرة وللإنصاف لا يعني هذا تساوه قدرات الدول بغيرها كالأفراد إنما حدث تقلص الفحوة بينهم فيستطيع من خلالها الطرف الأضعف تهديد مصالح القوى[3].

وسط هذه التفاعلات في الفضاء السيبراني وتأثيرها على العلاقات الدولية، هناك رؤيا للمدرسة الواقعة التقليدية تري تكنولوجيا المعلومات والفضاء السيبراني أحدث التحديات التي تُحدث تغيرات ثانوية قد تؤثر بشكل محوري على القوة

[2] نوران شفيق علي، الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في ابعاد الأمن الالكتروني، **رسالة ماجستير**، غير منشورة، جامعة القاهرة، كلية الاقتصاد و العلوم السياسية: قسم العلوم السياسية، 2014،ص ص 43 – 45.

[3] Joseph S. Nye, Cyber Power, **Belfer Center for Science and International Affairs**, Harvard Kennedy School, Cambridge,May 2010, p:11.

العسكرية والصراع، أما الواقعية الجديدة تري أن الاعتداءات التي تحدث في الفضاء السيبراني تهدد الدول ويجب مواجهتها بالقوة السيبرانية، لكن لا يزال اعتقادهم أن الصراع على القوة لايزال قائم وحتي مع وجود مصادر جديده للصراع، أما المدرسة الليبرالية تنظر للتطور بشكل إيجابي لزيادة التعاون بين الدول، وأن الاعتماد المتبادل والعولمة تزيد من أهمية الفواعل من غير الدول وإمكانيات التعاون الدولي، وهناك تصور ليبرالي أن الفضاء السيبراني يجب استخدامه كمساحة للتعاون بين الدول لتحقيق نظام دولي حاكم لهذه البيئة، وضرورة وجود قواعد حاكمة له لحماية المستخدمين وحقوق الملكيات الفكرية فيه، لهذا يجب إيجاد تكامل بين الدول لوضع نظام حاكم عالمي لهذا الفضاء[4].

وسط نظرة المدارس الفكرية للفضاء السيبراني، نجد أن الدراسات والنظريات في العلاقات الدولية ركزت منذ منتصف القرن العشرين على أبعاد القوة وكيفية صعود القوة الكبرى وانهيارها والردع وشن الحروب، واغفلت مناهج المعرفة البعد التكنولوجي مثل كمنهج التحليل الكمي للسياسة الدولية، وهذا للاعتقاد أن التطور التكنولوجي يتم بشكل عشوائي وفق التطورات العلمية وما يصدر من اختراعات، فظلت التكنولوجيا تُدرس في سياق هيكل القوة وإعطاء التركيز لتحليل المعلومات، ومع التقدم التكنولوجي في العقد الأخير للقرن العشرين وما تلاه أصبحت العلاقات الدولية تعالج القضايا ذات البعد التكنولوجي منها بشكل من التعقيد والإشكاليات المفروضة الغير القدرة على حل تلك القضايا، فمع تحول العالم إلى قرية صغيرة بالثورة التكنولوجية من الإنترنت والاتصالات فرص هذا تغيرات جزرية ألزمت البحث عن تصورات جذرية بعيداً عن تقسيم العلاقات الدولية مناهج تقليدية وجديدة، فقد فرض الفضاء السيبراني تحديات للمناهج والفرضيات التقليدية في العلوم السياسية[5]،

[4] نوران شفيق علي، "الفضاء الإلكتروني وأنماط التفاعلات الدولية"، مرجع سابق، ص ص 40 – 42.

[5] عادل عبدالصادق، أثر الفضاء الإلكتروني في تغير العلاقات الدولية، مرجع سابق ، ص 64 – 65.

بهذا تحدث فجوة نظرية وتحليلية في تعامل العلاقات الدولية مع الفضاء السيبراني كالاتي:-

1- الفجوة النظرية في تعامل العلاقات الدولية مع الفضاء السيبراني:

أهم التحديات التي واجهت نظريات العلاقات الدولية هو فشلها في التنبؤ أو تفسير انتهاء الحرب الباردة، دفع هذا العديد من المنظرين إلى اعادة تقييم المنطلقات التنظيرية، فالأساس في نجاح أو فشل النظرية مرتبط بقدرتها على التنبؤ بالمستقبل، وليس وقوف دورها على تفسير الماضي والحاضر، ولكي تنجح النظرية يجب أن يكون التركيز على التنبؤ بالتحولات الدولية بدلا من الارتكاز في التنظير على النسق الفكري والعقائدي.

شهدت العلاقات الدولية إشكاليات من حيث قدرة التنظير في تناول موضوعات الفضاء السيبراني والتقدم التكنولوجي، فالدمج بين العلاقات الدولية والفضاء السيبراني يشكل اشكالية كبيرة، لان التركيز التقليدي في نظريات العلاقات الدولية منذ القرن التاسع عشر والعشرين تتعلق بقضايا السلام والحرب والصراع والتعاون والمنافسة بين الوحدات الدولية، وهذا ما جعلها غير مواكبة للتطور والتحديات المفروضة، بتحول العالم من سيطرة الدول بقوتها وسيادتها وشرعيتها، إلى عالم يسيطر علية فواعل متعددة من غير الدول، فالفضاء السيبراني اثر على عدد الوحدات من غير الدول، واستحدث قواعد جديدة تتعلق بسلوك الوحدات الدولية، وانتج فاعلين جدد تأثر في العلاقات الدولية كموقع ويكيليكس ل جوليان أسانج، والجماعات الإرهابية.

2- فجوة التحليل الإمبريقية في تعامل العلاقات الدولية مع الفضاء السيبراني:

فرض الفضاء السيبراني تحديات كبيرة أمام العلاقات الدولية، من حيث طبيعة الفاعلين الدوليين وأولويات ونطاق الموضوعات الناتجة عن العمليات الدولية، انتج هذا فجوة ما بين المعلومات المتواجدة والأنشطة من ناحية، ومدي إمكانية إخضاع

تلك الأنشطة للتحليل الكمي والقياس والملاحظة، خاصتاً مع الدور المتصاعد للتحليل الكمي في العلاقات الدولية، واستخدمه لرصد وتفسير الظواهر والأحداث بشكل كمي إحصائي يساعد في عمليات التفسير والتحليل، فالفجوة تظهر بقوة عند تفسير الأنشطة السيبرانية لإنتاجها كم هائل من المعلومات ويتميز بضخامة غير مسبوقة، وارتباط هذا بحاجة التطور في مجال عمل الأجهزة الاستخباراتية في العالم، وأسهمت تطبيقات الفضاء السيبراني في تجميع وإنتاج المعلومات بشكل غير مسبوق بكميات ضخمة، وظهرت الحاجة إلى إيجاد طريقة سهلة لتحليل المعلومات الضخمة، مثل الإحصائيات ورصد الكلمات المتداولة التي يُتحدث بها، أو المتداولة عبر وسائل التواصل الاجتماعي، فأصبحت المعلومات جزءا مهما في تقدير المواقف ومواجهة الأخطار، وأصبح الفضاء السيبراني عنصراً من عناصر القوة.

3- فجوة التحليل السياسي في تعامل العلاقات الدولية مع الفضاء السيبراني:

أوجد الفضاء السيبراني فجوة بين الممارسة التقليدية لسياسة، والحاجة إلى مناهج وأدوات تحليل جديدة، وهذا يُوجد تحديات أمام علم العلاقات الدولية، لان الطرق التقليدية للتحليل السياسي ارتكزت بشكل كبير حول الدول وتأثيرها، والتحديات والأخطار في الفضاء السيبراني أصبح يحركها فاعلين من غير الدول كالجماعات والافراد والتي لم تكن معروفة قبل ذلك[6].

[6] عادل عبدالصادق، الفضاء الإلكتروني وإشكاليات نظرية العلاقات الدولية، **مجلة السياسة الدولية**، العدد 200، ابريل 2015، المجلد 50، ص ص 128- 129.

**أولاً: الفضاء السيبراني: المفاهيم والتكوين:**

**1 – المفاهيم:**

ظهر المصطلح (Cyberspace[1]) من صياغة William Gibson في قصته "الكرم المحترق" عام 1982، فتصور Gibson هذا المصطلح للتعبير عن مكان يُجمع فيه كل البيانات والمعلومات في العالم داخل وعى بلا جسد من خلال أجهزة الكمبيوتر، ووفقا Gibson يتصور هذا الفضاء الأقوياء فيه اللذين يمكنهم التلاعب بالمعلومات لامتلاكهم القدرات الفنية والتقنية لهذا من الأفراد ذو خبرة والمؤسسات والشركات كبرى[2]، واستمرت المفاهيم بالظهور المتعلقة السيبرانية مثل (Cyberpunk) وهو نوع من الخيال العلمي كمفهوم في الثمانينيات لتحليل البيانات والتكنولوجيا الحالية وجعلها تبدو خيالية، وأصبح يستخدم لوصف مواقف الخروج عن القانون أو لتأثير التكنولوجيا والمعلومات على المجتمع، كما ظهر مفهوم آخر متعلق بالفضاء السيبراني وهو شبكات الحاسب ( Networks Computer) وهو عبارة عن شبكه تُعالج فيها أجهزة الكمبيوتر قواعد البيانات لتنتج المعلومات هذه المعلومات يمكن أرسالها واستقبالها من جهاز لآخر أو توفير الوصول إليها عن طريق قواعد تسمي بروتوكولات، فأي كمبيوتر متصل بالأخرين جزء من شبكة، وقد يكون الجهاز جزء من عدة شبكات[3]، وظهر مصطلح Barlowion Cyberspace فضاء بارلوفيان السيبراني : كان مصطلح تخيلي قبل ظهور الإنترنت، فيبين الفضاء السيبراني على انه شبكة من الكمبيوترات التي تنشأ بربط بينهم، فعلي عكس تصور John عن نظرته الخيالية فظهر الفضاء السيبراني على

[1] في حقول الدراسات العربية يستخدم بشكل شائع مصطلح الفضاء الإلكتروني وفي بعض الاحيان الفضاء الافتراضي ، لكن وصف المصطلح بالإلكتروني ليس بالدقيق، لذلك الوصف الافضل للترجمة العربية هو الفضاء السيبراني

[2] William Gibson, **Burning Chrome**, Arbor House Publishing, Pennsylvania, 1986, pp. 248-249.

[3]- Tim Jordan**, Cyberpower: an introduction to the politics of cyberspace**, Routledge, Londan, 1999,pp.20-21.

انه الفضاء الذي يستخدمه الأفراد للتحدث والتواصل ويتطور ليصبح شبكة عالمية تخدم الملايين تكون معقدة التنظيم لا نهائية المدي، فيرجع الفضل هذا في التصور إلى John Barlow لتصوره الفضاء السيبراني فيما يتعلق بشبكات الإنترنت وأصبح هذا الوصف يستخدم لوصف الفضاء السيبراني عكس تصور صاحب المصطلح ذاته[1].

فوفق تقرير الاتحاد الدولي للاتصالات عن الإنترنت والشبكات 2021 أظهر أن 4.9 مليار شخص يستخدم الإنترنت عام 2021 وهذا يعني ان 63% من سكان كوكب الأرض متصلين بنسبة تزيد عن 17 % عن عام 2019 بحجم زيادة 800 مليون شخص، فمع جائحة كورونا كان الإنترنت المصدر الاساسي للبقاء على الاتصال مع العالم فهذه التكنولوجيا كانت السبب الرئيسي في استمرار الانشطة التجارية والتعليمية وحتي في ممارسة الوظائف من المنازل، تعني هذه الأرقام وجود 2.9 مليار شخص لا يزالون خارج الإنترنت ويعيش 96% من هذا الرقم في الدول النامية، وحوالي 390 من هذا الرقم لا تغطيهم شبكات النطاق العرضي لأجهزة المحمول[2]، هذه الأرقام تبين مدي أهمية الإنترنت وهو الجزء الأساسي من الفضاء السيبراني، ويوضح مدي سيطرة الفضاء السيبراني على مجريات الحياة البشرية، وأصبح الإنترنت أثناء الجائحة وما بعدها هو المحرك الرئيسي للتفاعلات الإنسانية بكافة أبعاده الاقتصادية والسياسية والاجتماعية، وأصبح العالم الافتراضي يتجاوز تأثيره ليصبح عامل الرئيسي للتأثير في العالم الواقعي، وبهذا عرفت الأمم المتحدة والاتحاد الدولي للاتصالات الفضاء السيبراني : " التضاريس المادية وغير المادية التي تم إنشائها وتكوينها من بعض أو كل ما

[1] John Perry Barlow," Across the Electronic Frontier", **Electronic Frontier Foundation**, Washington D.C, July 10 1990.

[2] - ITU Report on the Internet and Networks entitled: Digital Development Facts and Figures 2021, link:https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

يلي: أنظمة وأجهزة الكمبيوتر والشبكات، والبرامج وبيانات الكمبيوتر، وبيانات المحتوي وبيانات كلمات المرور للمستخدمين".

هذا التعريف يبين أن الفضاء مكون من ثلاث طبقات مترابطة: الأولي الطبقة البشرية (The Human Layer): تتكون من مستخدمي الأجهزة من الحواسيب والاتصالات، الطبقة الثانية الطبقة المنطقية (The Logical Layer): مكونه من البرامج والبايت، وهذه متحركة بسرعة الضوء وتمثل المعلومات والتعليمات وأصول الفضاء السيبراني من البرمجيات، الطبقة الثالثة المادية: (The Physical Layer) المكونات المادية للشبكات، بما في ذلك الأجهزة والبنية التحتية الثابتة والمتنقلة الموجودة في الارض والبحر والجو في الفضاء.

بينما عرف Joseph Nye **الفضاء السيبراني** بشكل بسيط على أنه: "مجال تشغيلي محكم باستخدام المعلومات عبر الأنظمة المترابطة والنية التحتية المرتبطة بها"، وصوره Nye على أنه عدة طبقات تكون نظام هجين فريد في خصائصها المادية والافتراضية أو المعلوماتية، ولخصها في طبقتين، **فالطبقة المادية:** تتبع القوانين الاقتصادية والسياسية وتخضع للسطلة القضائية والسياسية وتتكون من الانظمة والبنية التحتية المادية للفضاء السيبراني، **والطبقة المعلوماتية أو الافتراضية:** وهي ساحة الإنترنت والبرمجيات والمعلومات ولا يسطره عليه قضائياً، لهذا يمكن شن هجمات من الطبقة الافتراضية ذات التكلفة المنخفضة ضد الطبقة المادية ذات الموارد الشحيحة و المكلفة من المواد المتحكمة في الاتصالات والمعلومات والاجهزة الحاسوبية والبنية التحتية والشبكات والبرمجيات والمهارات البشرية للمستخدمين لهذه البنية، ويقتصر على الاجهزة المتصلة بشبكة الإنترنت ولكن تشمل ايضا الشبكات الخلوية الداخلية وتقنيات الاتصالات الفضائية[1].

1 - Joseph S. Nye, Cyber Power, **Belfer Center for Science and International Affairs**, Harvard Kennedy School, Cambridge, May 2010, p. 3.

كما عرف البيت الأبيض الفضاء السيبراني بأنه الشبكات المترابطة بالبنية التحتية لتكنولوجيا المعلومات وتشمل الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات المدمجة ووحدات التحكم في الصناعات الحرجة، وركز هذا الوصف على المكونات المادية للفضاء السيبراني، ووصف الفضاء السيبراني في الاستراتيجية الوطنية الأمريكية "بالجهاز العصبي للتحكم في الدولة"، ويتكون من مئات الآلاف من أجهزة الكمبيوتر وأجهزة التوجيه ومحولات الإنترنت والخوادم والكابلات الضوئية التي تسمح للبنية التحتية الحيوية بالعمل[1].

**2- مكونات الفضاء السيبراني.**

إن الفضاء السيبراني كان وليد فكرة إنشاء شبكة غير محدودة تنجو من الحرب النووية، فكان التفكير في حالة قيام حرب نووية بوجود نظام الهواتف التقليدي في الخمسينات والستينات القائم بشكله الهرمي فعند تدمير المراكز الرئيسية ستنهار المنظومة وينهار التواصل بين مدن ومناطق الدولة المستهدفة، لهذا صممت "داربا" ( وكالة مشاريع البحوث المتطورة الدفاعية ) شبكة خاصة بنقل البيانات والمعلومات بين الجامعات والمؤسسات وقت الأزمات، فقام Paul Baran عالم الشبكات الأمريكي في منتصف الستينات بالعمل على حل مشكلة الاتصالات في ما بعد الضربة النووية، فوجد الحل في شبكة موزعة بشكل غير هرمي تعمل بشكل تلقائي، فإذا ضربت عدد من المدن وظلت آخري لا تنقطع الاتصالات عن كل ما تبقي حي ويظل متصل بالشبكة فأصبحت هذه التقنية الأساس الإنترنت.

وظهرت شبكة ( أربانت – ARPANET ) وعملت بداية من 1969 حتي اغلقت 1990 وبعد ذلك تم الإعلان عن شبكة الإنترنت العالمية WWW عام

[1] Daniel T. Kuehl, From Cyberspace to Cyber power: Defining the Problem, **National Defense University**, Washington D.C, 2009,pp. 4-2.

1991 لتزويد بخدمات الإنترنت، بحيث يمكن استخدامها من أجهزة الكمبيوترات الشخصية المنزلية، وتطورت الشبكة حتي ظهروها بشكلها المعقد ويمكن الوصول إليها من أي جهاز، وتم إطلاقها عام 1992 على الإنترنت وأصبح معتمد للوصول لأي محتوي على الإنترنت عام 1994 ولتوضيح الفرق بين الانترنت والويب، فالويب ( World Wid Web - WWW ) يمكن لمستخدمين الكمبيوتر النقر بالماوس على الكلمات أو الصور لاستدعاء النص أو الصورة أو الصوت من العديد من مئات قواعد البيانات الموجودة على الإنترنت وهذا يظهر على انه نظام يعمل لربط المستندات ببعضها البعض تعمل فوق الإنترنت لتصبح البيانات قابلة للتنقل بينها من خلال برمجة النصوص الفائقة، والإنترنت عبارة عن شبكة هائلة من الشبكات المرتبطة بأجهزة الكمبيوتر باستخدام الكابلات ، فالإنترنت كان ينمو قبل الويب لكن مع ظهوره أصبح النمو هائل، فالعلاقة بين الأثنين مثل الاختلاف بين الدماغ والعقل، فعند استكشاف الإنترنت تجد الكابلات والأجهزة، وعند استكشاف الويب تجد المعلومات، فسبب هذا تقدم هائل وانخفاض تكلفة الإنترنت وتضاعف أعداد مستخدمي الإنترنت عشرات المرات في الفترة بين 1990–1997 مقارنة بالثمانينات[1].

وسط الشبكة العالمية للإنترنت برزت فكرة الشبكات المغلقة بظهور اتجاه جديد للدول لبناء شبكة للإنترنت والاتصالات داخلية وطنية، من خلال وجود شبكة من المواقع والتطبيقات ووسائل التواصل الاجتماعي ومحركات البحث وبريد إلكتروني وطني، وقد تكون مغلقة أو متصلة بالإنترنت العالمي مع وجود نظم فلاتر لحجب وإغلاق الوصول لألاف المواقع لتجنب التجسس ولأغراض أمنية والسيطرة على الموطنين، هذا الاتجاه دعمته دول لأنشاء شبكات وطنية خشية التجسس على

[1] - Tim Jordan, Cyberpower: an introduction to the politics of cyberspace, op cit ,pp .20-21.

الإنترنت والاتصالات والمعلومات، بعد كشف Edward Snowden العميل السابق في وكالة الأمن القومي الأمريكية بإظهاره تجسس الولايات المتحدة على الهواتف والمراسلات الإلكترونية على مستوي العالم، من ضمنهم قادة وسياسيين للعديد من الدول بحجة مكافحة الارهاب من خلال برنامج PRISM من خلال إعطاء وكالة الأمن القومي الأمريكية صلاحيات واسعة من خلال التشريعات باستخدام شركات التكنولوجيا الأمريكية، سبب هذا أزمة دبلوماسية للولايات المتحدة حتي مع حلفائها المقربين كفرنسا وألمانيا والبرازيل.

فالنموذج المثالي للسيطرة على الإنترنت في الصين لديها شبكة إنترنت خاصة بها بالرغم من ربطها بالإنترنت العالمي، لحمايتها في حالة تعرض للهجمات السيبرانية فيسهل فصل الإنترنت العالمي عنها وتحمي شبكتها من الاختراق وتحافظ على بقاء الشبكة الداخلية تعمل، فالجدوى من الشبكات الوطنية تظهر مع هيمنة الشركات الأمريكية على صناعات الفضاء السيبراني في العالم سواء مكونات Hardware مثل شركة ابل في الأجهزة الإلكترونية، وصناعات معادات الشبكات بالشركة الاولي عالميًا Cisco Systems، و مكونات Software بأنظمة التشغيل المهيمن عليها عالميا مايكروسفت وابل وجوجل، تطبيقات التواصل الاجتماعي مثل فيس بوك وتويتر، ومحركات البحث وحتي أسماء النطاقات (ترخيص أنشاء المواقع) عن طريق منظمة ICANN التابعة لوزارة التجارة الأمريكية، لهذا فإن أصول الإنترنت العالمة متواجدة في الولايات المتحدة الأمريكية ولا يوجد بديل جاهز يقدم الخدمات عنها، لهذا سعت الدول لبناء شبكات إنترنت داخلية سواء تعمل بشكل مستقل أو متصل بشبكة الإنترنت العالمية، فلا ملاذ آمن كما أوضح Snowden أن وكالة الأمن القومي تسطيع التجسس على كافة الشبكات وحتي على أجهزة الاستخبارات المتعاونة مع الولايات المتحدة، وخير دليل اختراق فايروس Stuxnet الشبكة الخاصة بالبرنامج النووي الإيراني وإصابة أجهزة

الطرد المركزي دون اتصالها بالإنترنت، وحتي الأجهزة الغير متصلة فاختراقها CIA باستخدام موجات الراديو مخصصة لاختراق أجهزة الكمبيوتر الغير متصلة ووضع عليها برامج خفية لتسهيل علميات إرسال البيانات في مدي 7 ميل لهذه الموجات، لهذا فالسعي لإنشاء شبكة داخلية مؤمنة لا تعكس إلا الفجوة الكبيرة ما بين الولايات المتحدة الأمريكية والدول الأخرى لعدم تطور قدراتهم وإمكاناتهم السيبرانية لمواجهة التحديات، ففي كل الحالات أصبح التطور السيبراني شيء وجودي وليس رفاهية بنسبة للدول[1].

**ثانيًا: الردع السيبراني:**

الهجمات السيبرانية عبارة عن تقوض لقدرات ووظائف شبكة الكمبيوتر، لغرض قومي أو سياسي من خلال استغلال ثغرة ما تُمكن المهاجم من التلاعب بالنظام الخاصة بالحكومات والمواطنين العاديين والأنظمة الاقتصادية والعسكرية وأنظمة البنية التحتية للدول، وينقلنا هذا لتعريف الردع على انه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء السيبراني"[2]، فالمتطلبات الأساسية لوضع استراتيجية للدرع السيبراني: الوعي العالمي بحال الفضاء السيبراني من حيث التهديديات والفواعل، وجود أنظمة دفاعية سيبرانية فعالة لحماية كل القطاعات المدنية والعسكرية وتكون أولوياتها الدفاع عن البنية التحتية الأساسية، امتلاك مجموعة واسعة من القدرات الهجومية السيبرانية المضادة للتأكيد على قوة الدولة لفرض الردع قبل وأثناء وبعد الأزمات، القيام بعمل شبكة تعاون مع الوكالات الاستخباراتية

[1] - إيهاب خليفة، الدائرة المغلقة: لماذا تتجه الدول لتأسيس شبكات إنترنت وطنية ؟ ، **دورية اتجاهات الأحداث**، مركز المستقبل للأبحاث والدراسات المتقدمة، العدد 7، فبراير 2015 ، ص ص 60 - 64.

[2] - رغد البهي، الردع السيبراني : المفهوم والاشكاليات والمتطلبات، **مجلة العلوم السياسية والقانونية**, العدد الاول، 2017، ص ص 51 – 53.

الحليفة والصديقة، دراسة مناهج وتجارب الردع السيبراني التي تساعد في عملية التخطيط لعمليات الردع المستقبلية[1].

هناك العديد من النظريات للردع لكن المكونات الخاصة لتحقيق الردع السيبراني 8 عناصر:

( الإعلان عن الردع – المصلحة – إجراءات الرفض – إجراءات العقاب – المصداقية – الخوف – الطمأنة – حساب التكلفة والمنفعة ) يستخدم الردع من أجل حماية دولة ما لمصالحها بمنع أعدائها من الهجوم **بإعلان** الردع بشكل علني "لا تفعل هذا إلا سيحدث ذلك"، بحيث أي عمل عدواني تجاه **المصالح** الخاصة بها سيتضمن رد فعل **بإجراءات رفض وعقاب**، ولتحويلة للإعلان ذو مصداقية، فيجب توافر عنصرين، الأول: المصداقية في اتخاذ إجراءات الردع في حال التعرض للهجوم من تدابير عقابية، والثاني الاطمئنان بمعنى **طمأنة** الخصم إذا لم تهاجم مصالحي فلن تتعرض للهجوم أو تتعرض لعقوبات، وهنا نجد الخوف من التعرض للعقاب الشديد في حالة الإقدام على المهاجمة، وتندمج كل هذه العناصر في معادلة حسابية حول التكلفة والعائد أو المنفعة من فعل شيء محدد كالهجوم على مصالح دولة آخري سيبرانياً، فيقوم صانع القرار بحساب تكاليف التكاليف والعائد من الفعل، لكنة يصطدم بإجراءات الخصم الدفاعية والهجومية في حالة الإقدام على الهجوم، فإجراءات **الرفض**: هي إجراءات دفاعية والتي تحرم دولة المهاجمة عن قدراتها على توجيه الهجوم كفصل الشبكات الحساسة داخل الدولة بشكل مؤقت، وإما الإجراءات الهجومية العقابية برد فعل انتقامي ضد الهجوم الأول من الخصم لإلحاق ضرر ساحق به يعجز عن توجيه هجوم ثاني[2].

[1]- Richard L. Kugler, Deterrence of Cyber Attacks, **National Defense University**, Washington, April 2009, p.18.

[2] Will Goodman, Cyber Deterrence Tougher in Theory than in Practice?, **Strategic Studies Quarterly** , Air University (U.S.), v.4, no.3, (Fall 2010), pp. 105 – 107.

هنا تنقسم الآراء حول نظرية الردع ووجود المجال السيبراني كجزء منها، فالرأي الأول يري عدم جدوي الردع السيبراني بحجة طبيعة العمليات السيبرانية والإشكاليات التي تواجه الردع السيبراني من تحديد هوية منفذ الهجوم وعدم وجود قوانين وخطوط فاصلة بين ما يلزم استهدافه ام لا، لهذا في حالة دمج الفضاء السيبراني ضمن نظرية الردع قد يأدي إلى فشل الردع ككل، الرأي الثاني يري إمكانية تلائم الفضاء السيبراني من نظرية الردع لكن بربطة بشروط محددة، كتبني مفهوم واسع للردع والمزج بين القدرات العسكرية والاستخباراتية والاقتصادية والقانونية لتعزيز الأمن المعلوماتي والبنية التحتية لخلق ردع سيبراني وتكامله من نظرية الردع، الرأي الثالث يري أن نظرية الردع جزء أساسي منه الفضاء السيبراني، فعدم وجوده ضمن منظومة الردع يجعل البيانات المتاحة عرضة للسرقة وانتهاك حقوق الملكية وتعطيل الأنظمة الخاصة بالدولة كالأنظمة المالية والأمنية في حالة الهجوم السيبراني، لذلك الفضاء السيبراني جزء لا يتجزأ من استراتيجية الردع للدول[1].

لهذا ظهرت خطوط حمراء في تفاعلات الدولية في الفضاء السيبراني خاصة بعملية الردع السيبرانية، ففي القمة الأمريكية الروسية سلم جو بايدن رئيس الولايات المتحدة الأمريكية قائمة للرئيس الروسي فلاديمير بوتن تضم 16 كياناً للبنية التحتية لا يُمس بهم سيبرانياً، وكشف بأن لديه القدرة السيبرانية كبيرة لكنه لا يريد الدخول في حرب سيبرانية، وسأل عن شعور الرئيس فلاديمير بوتين عن احتمالية تعرض أنابيب النفط والغاز الروسي إذا تعطلت ببرامج الفدية والتي تمثل ثلث إنتاج روسيا القومي وشريان روسيا الاقتصادي، وهذا يمثل أول إعلان للردع سيبرانياً في تاريخ

[1] - رغد البهي، الردع السيبراني، مرجع سابق، ص ص 51 - 52.

العلاقات الدولية، مع إظهار الحدود لهذا الردع والتحذير وطمأنة الخصم وحساب التكلفة، أي توافر شروط الردع السيبراني[1].

في هذه الحالة تحسب تكاليف الاعتداء السيبراني من ناحية والخسائر من خلال تقدير إجراءات الرفض والعقاب، فإجراءات الرفض السيبرانية هي تجنب الرد السيبراني والاكتفاء بحصر الأهداف السيبرانية التي قد تتعرض للهجوم ووضعها في حالة عدم الاتصال لجعلها آمنة، أو بجعل الهجمات السيبرانية للخصم دون جدوي من خلال استنفار أنظمة الحماية وأفراد الحماية السيبرانية، مع ذلك فإجراءات الرفض لا تستطيع الوقوف وحيدة في مواجه الهجمات السيبرانية فلا تكفي هذه الإجراءات للردع السيبراني لان في حالة فشل الهجوم سيواصل الخصم المهاجمة حتي يحقق اختراق ناجح.

بالمقارنة مع الردع النووي فتستطيع الدولة تنفيذ هجوم مضاد ساحق وفوري أما الردع السيبراني فيختلف، فرد الفعل السيبراني وتحقيق عقاب سيبراني ساحق، يجب أولا التعرف على الجهة المنفذة، من خلال فحص الشبكات والأجهزة المستهدفة، ثم اختيار الأهداف المراد تحقيقها اختراقها أو تدمرها (الاهداف السيبرانية) من أجل تحقيق انتقام ساحق ودقيق، عكس المجال المادي من المعتمد على شبكة من الرادارات وأنظمة الإنذار المبكر تحدد له مصدر الهجوم، وفى حالة نجاح الهجوم السيبراني بإمكان المهاجم تعطيل شبكات القيادة والسيطرة للقوات المسلحة، لهذا تلجأ بعض الدول لإزالة ارتباط المنظومات العسكرية بالفضاء السيبراني فقد يحدث تعطيل مسبق للأسلحة السيبرانية من قبل العدو قبل بدء الهجوم الساحق، والجزء المشترك بين الردع التقليدي والسيبراني وجوب تعادل ميزان القوة للدول المتصارعة من الناحية الجيوسياسية، عن حالة التفاوت في القدرات وحدوث هجوم إذا كانت

[1]- Alyza Sebenius, "Biden’s Cyber Red Line Is Prime for Putin Challenge", **Bloomberg**, 2021-06-18 , link: https://www.bloomberg.com/news/articles/2021-06-18/biden-s-cyber-red-line-is-prime-for-putin-challenge-experts-say

الدولة الضحية غير قادرة على تحمل عواقب سلسلة من الأفعال الانتقامية السيبرانية فيجب أن تتخلي عن الانتقام في المقام الاول، فوجود توازن سيبراني بين أطراف الصراع يكون امتداداً للمجال المادي، لكن في حالة **حدوث طمأنة متبادلة** بين الجانبين ينجح الردع، لكن لم تتوقف الدول عن البحث في الشبكات والأنظمة والأجهزة لإيجاد ثغرات سيبرانية لاستغلالها وقت نشوب حرب[1].

لكن مع تطبيق قواعد الردع التقليدي على الدرع السيبراني على أرض الواقع نجد إشكالية في كيفية التعامل في الفضاء السيبراني، لذلك ظهرت الحاجة إلى المزيد من الوسائل والطرق الجديدة للرد على الهجمات السيبرانية ضمن عناصر الردع السيبراني كالاتي:

**الخيار الاول** للردع يتمثل في عدم الرد على الهجوم مع الاعتراف بأن الإجراءات الأمنة السيبرانية ليست كافية، والقيام بتطوير الأنظمة بشكل مستمر لسد الثغرات السيبرانية، لكن هذا الردع السلبي يرفع من كفاءة الأمن السيبراني ويزيد من صعوبة وتكلفة أي هجوم آخر في المستقبل، فيمثل هذا النوع من الردع زيادة النشاط السيبراني بشكل واسع، **الخيار الثاني** الاحتجاج الدبلوماسي بطرد مسؤولين الدولة المتهمة في الهجمات السيبرانية، فمن شأن هذا الإضرار بسمعة الدولة على الصعيد الدولي لكنه في المقابل لا يشكل رد كافي لردعها عن شن الهجمات في المستقبل، **الخيار الثالث** العقوبات الاقتصادية بإيقاع عقوبات اقتصادية على الجهة المنفذة للهجوم في الفضاء السيبراني، كما حدث مع تعزيز الولايات المتحدة الأمريكية ضد كوريا الشمالية عندما نفذت كوريا هجمات سيبرانية ضد شركة سوني، لكن هذا النوع من الرد لا يغير توجه الدولة المنفذة للهجوم، إلا بطرح الدولة المنفذة للعقوبات مبدأ تغير السلوك مقابل تخفيض أو التخلص من العقوبات، لكن الدولة

[1]- Will Goodman, Cyber Deterrence Tougher in Theory than in Practice? , op.cit., pp. 108 - 109.

المنفذة للعقوبات قد تتعرض لأضرار اقتصادية في حالة الاعتماد المتبادل في علاقات اقتصادية بينهم وتكون خسائرها ضخمة، **الخيار الرابع** الانتقام السيبراني هو اساس الردع فمع استهداف النية التحتية أو سرقة ونشر المعلومات، يرد بالمثل على الدولة المهاجمة لكن هذا الخيار يزيد من خطر التصعيد لحالة الحرب السيبرانية، ويلزم امتلاك القدرات والإمكانيات الدفاعية القوية والهجومية لتنفيذ هذا الخيار، **الخيار الخامس** الرد العسكري خيار غير منطقي ولا عقلاني للرد على الهجمة السيبرانية، لكن هذا الخيار قد تلجأ إليه الدولة في حال التسبب بكارثة سيبرانية في بنيتها التحتية والتي تشمل أنظمة القيادة والسيطرة للقوات المسلحة، فمثل هذه الهجمات في حالات التوتر العسكري بين الدول قد تكون تمهيد للحرب الشاملة، لهذا يكون الرد بهجوم عسكري انتقامي للمجال السيبراني ووقائي على ارض الواقع.

هذه الخيارات من ردود الأفعال من أبسطها إلى أكثرها تطرفاً تعكس الخيارات المتاحة والمرنة في الردع السيبراني ففي حالات الخطر قد تلجأ الدول إلى التهديد بالهجوم العسكري أو استهداف أهداف مناظرة، فلكل فعل رد فعل سيبراني قد يصل لشن حرب سيبرانية شاملة، فعصر المعلومات يختلف عن عصر الحرب الباردة فالردع النووي ليس فيه إلا خيار واحد التدمير النووي المتبادل، فلا مرونة فيه وعدد الدول الممتلكة لهذه القدرات ضئيل في العالم، لكن في الفضاء السيبراني وعملية الردع مرونة في رد الفعل، فتمتلك الكثير من الدول القدرات السيبرانية وتعمل على تطويرها وبلغ عددهم 140 دولة وأدخلت 30 دولة منهم الوحدات السيبرانية في جيوشها، هذه المرونة في الاستراتيجية السيبرانية جعلت الدول تلجأ لخيارين في التعامل مع الهجمات السيبرانية، الأول الأنظمة البديلة: فاستخدام منظومة سيبرانية واحدة لإدارة البنية التحتية يمثل خطر في حالة نجاح الاختراق، لهذا يمكن للدول إنشاء أنظمة بديلة أو طارئة في حالة تدمير النظام الأساسي لاستعادة السيطرة

سريعاً، الثاني إعادة التشغيل فتتغلب الدول على الهجمات بشكل سريع بإعادة تشغيل الأنظمة أو من خلال حجب الخدمة عن الجميع فعلي الرغم من فاعلية هذا الخيار لكن مكلف اقتصادياً وقانونياً[1].

على الرغم من التحديات الاستراتيجية للردع السيبراني لعدم معرفة المرتكب للهجمات، لكن حالات إستونيا 2007 وجورجيا 2008 مع نفي روسيا الهجمات السيبرانية لكنها كانت متزامنة مع عبور القوات الروسية الحدود الجورجية، لهذا تحدث الحرب السيبرانية كجزء من الحرب الواقعية وبالتالي يمكن توجيه هجوم مضاد كما في الواقع في الفضاء السيبراني، فالردع السيبراني أصعب نظرياً من الممارسة لعدم وضوح قواعد نظرية حاكمة لهذا النوع من الردع، على غرار الدرع النووي فكانت الخمسينات من القرن لماضي بالنسبة للردع النووي كحال السيبراني الآن، فالتفاعلات بين الدول النووية أبرزت قواعد تنظم وتحكم الردع النووي، كأزمة الصواريخ الكوبية في الستينات، لهذا الردع السيبراني صعب وليس مستحيل فبالرغم من حقيقة الحرب السيبرانية وظهور استراتيجيات سيبرانية للدول، لا يزال الردع السيبراني مرتبط كجزء من الردع ككل، فيحدث عندما تنشب حرب على ارض الواقع ولا يحدث منفرداً.

**ثالثًا: نموذج التفوق في الفضاء السيبراني.**

فمن أجل تحقيق تفوق في الفضاء السيبراني وإيجاد نموذج للتفوق لهذا دفاعياً وهجومياً يجب مراعاة خصائص هذه البيئة المميزة عن البيئات الأخرى كالاتي: –

**1-** الجغرافيا: ففي الواقع لا يكمن تحريك الجبال والمحيطات لكن في الفضاء السيبراني صنيعة الإنسان تتشكل جغرافيا الفضاء السيبراني وفق تفاعلات المتحكم فيه الإنسان باستخدام الأجهزة والبرمجيات، فيمكن إيقاف أو تشغيل

[1] - رغد البهي، الردع السيبراني، مرجع سابق، ص ص 59 - 61.

جزء من الفضاء السيبراني بضغطة زر أو نقله أو إنشاؤه أو نسخه أو كبح الوصول إلى هذا الجزء.

**2-** وصول المقاتلين: كما الحال في المجال الجوي والبحري يتطلب إرسال مقاتلين توفير معدات كالطائرات والسفن ووجود قواعد من الطائرات والموانئ وإنفاق هائل متاح فقط للدول، في المقابل فسفن ومطارات الفضاء السيبراني متاحة من أقرب موزع خدمة انترنت، ووسيلته للهجوم جهاز كمبيوتر محمول بسيط يشتري ببضعة مئات من الدولارات.

**3-** كسب الحرب: السيطرة على الفضاء السيبراني لا يأتي بالنصر في الحرب بمفرده، لكن لا تستطيع أن تفوز بدونه، فيتم التلاعب بأنظمة المعلومات الخاصة بالعدو، وأحداث تأثيرات في المجلات الأخرى المرتبطة بالفضاء السيبراني كتعطيل أنظمة الدعم اللوجستي لتقليل دعم للقوات المعادية وخفض فاعليتها، والتحكم في أنظمة توليد الكهرباء.

**4-** عدم التنسيق بين الأسلحة السيبرانية: من أبرز خصائص الفضاء السيبراني عدم التنسيق بين الأسلحة الدفاعية والهجومية، فالأنظمة السيبرانية الدفاعية والهجومية ليست متشابهة وليست قابلة لتبادل الأدوار، هذا التناقض يشابه إلى حد كبير القوات الجوية فتكوينها من أنظمة دفاع جوي ومقاتلات متعددة المهام، فلا تستطيع الدفاعات الجوية أداء مهام القاذفات والعكس، على النقيض القوات البحرية التي تستطيع مدمرة أداء مهام دفاعية وهجومية.

فالأسلحة السيبرانية كالسيف الزجاجي يمكن أن تكون حادة تقتل، وقد تنكسر في أول ارتطام لها، وهذا يرجع إلى طبيعة المهمة ففي حالات الأسلحة الدفاعية يستطيع المهاجمين استخدام الثغرات غير المعروفة من أجل تعطيل هذه الأنظمة، في المقابل الأسلحة الهجومية عند الاكتشاف المبكر للثغرات يمكن المدافعين من معالجتها وإغلاق الثغرة وإيقاف المزيد من الهجمات، فالأسلحة خاصتاً الهجومية

ذات استعمال واحد، تستخدم ثغرة أو عيب غير معروف يمكن استغلاله عند بداية الهجوم يسمي (Zero Day) لأن المؤقت الخاص بالثغرة هو الصفر عند حدوث الاختراق، ثم يتدافع المبرمجين لسد الثغرة وتصحيحها[1].

**1- نموذج التفوق السيبراني لديه 4 عناصر أساسية:-**

**العنصر الاول الوسائل السيبرانية لتحقيق هجمات سيبرانية:** باستخدام الهندسة الاجتماعية للتلاعب بالمدافعين والتركيز على أساليب خداعية لم يشملها التدريب الذي خضعوا له، لأن خطأ واحد منهم يكفي لفتح ثغرة، وتطوير برامج "حصن طروادة"، والإخلال بسلسلة الإمدادات المعادية بأحداث اختراق في الانظمة المستهدفة تمكن المهاجمين من التحكم في الأنظمة التشغيلية، استخدام عمليات رفض الخدمة بإغراق النظام ملايين من الطلبات الزائفة لتشكيل ضغط، تفكيك الأنظمة مادياً باستخدام الذخائر، كتدميرها بالمقاتلات أو بتفجر مراكز الخوادم باستخدام متفجرات C4 يزرعها عملاء، هذا ينتج تأثير متبادل ما بين العالم المادي والفضاء السيبراني، العثور على عيوب في أنظمة التشغيل SCADA وهذا يمثل درة التاج لأي مهاجم يمتلك ترسانة هجومية تسمح بتطوير برمجيات وإدخالها عن طريق الثغرات، استهداف الشبكات والأجهزة غير المتصلة بالإنترنت بأجهزة لاسلكية، **العنصر الثاني الدفاعات السيبرانية:** يمكن استخدام العديد من الأساليب للحماية من الهجمات السيبرانية عن طريق تثبيت جدران حماية، اكتشاف المتسللين، وضع أنظمة المصادقة بوضع كلمات مرور واسم مستخدم للوصول للبيانات، إغلاق الثغرات الأمنية المعروفة، ومنع وفصل الأنظمة الحساسة من التوصيل بشبكة الإنترنت وعدم توصيلها بشبكات لاسلكية مفتوحه، الاعتماد على تشفير المعلومات، إنشاء كلمات مرور صعبة الفك، عمل أنظمة وخوادم لتخزين المعلومات

[1] William D. Bryant , Cyberspace Superiority: A Conceptual Model, **Air & Space Power Journal**, Vo.27, No.6, November-December 2013, pp. 30 – 31.

احتياطياً في حالة تعرض الأنظمة الأساسية للتدمير أو للحذف، وتدريب العاملين على أساليب الخداع السيبرانية، **العنصر الثالث الطرق المتاحة بالإنترنت:** غالباً العمليات السيبرانية من قبل الدول أثناء حالات السلم تهدف إلى جمع المعلومات الاستخباراتية والتجسس السيبراني، وفي النزاعات التسلل واختراق الأنظمة المعادية بهدف معرفة خطط العدو أو جاهزية القوات وقدراتها الفعلية، العمل على إحداث خلل في أنظمة التوجيه كإرسال الإمدادات إلى أماكن خطأ على سيبيل المثال أو تغيير المعلومات المخزنة أو الجداول الزمنية، أو تقييد وصول العدو إلى المعلومات وبالتالي التقليل من فاعليتها، وتوفير الدعم لكافة القوات كخداع أنظمة الدفاعات الجوية المعادية أو التشويش على الأنظمة الفضائية، **العنصر الرابع الهجوم:** استخدام أخطاء المستخدمين لأنظمة المستهدفة لعمل هجمات سيبرانية ناجحة، عمل هجمات غير مستندة إلى الإنترنت باستخدام الشبكات اللاسلكية أو تركيب مودم لاسلكي في الشبكة أو الأجهزة المستهدف اخترقها، إضافة برمجيات خبيثة تربك أنظمة الحماية السيبرانية، كسر كلمة مرور واسم المستخدم واحد، يُمكّن من فك التشفير النظام بأكمله، والضغط ينفذ الهجمات متزامنة لاختراق الأنظمة الاساسية والنسخ الاحتياطية لتدمير الأنظمة والمعلومات[1].

**رابعًا: الحرب في الفضاء السيبراني.**

كما العادة تستعين المجالات الدراسات الناشئة بمصطلحات تستخدمها قد لا تتشارك المعني مع المصطلح الأصلي لكنها تستخدم لوصف حالة ناشئة، فاستخدام مصطلح الحرب مع الفضاء السيبراني لا يقل خطورة في الوصف عن حرب حقيقة تقتل الأف وملايين البشر، فهجمات سيبرانية في دولة ما قد تتسبب بكارثة مع تعرض البنية التحتية للهجوم، لهذا هناك العديد من التعريفات كالاتي:

[1] Ibid., pp. 33-38.

**أ-** تعريف منظمة شنغهاي للتعاون: "مواجهة بين دولتين أو أكثر في فضاء المعلومات تهدف إلى تقويض الأنظمة السياسية والاقتصادية والاجتماعية أو غسل الادمغة نفسياً لزعزعة استقرار المجتمع والدولة".

**ب-** يعرف الجيش الأمريكي: "الاستخدام المتعمد للأنشطة التخريبية أو التهديد بها، ضد أجهزة الكمبيوتر والشبكات، بقصد التسبب في ضرر أو تحقيق أهداف اجتماعية أو أيديولوجية أو دينية أو سياسية أو ما شابه ذلك، أو لتخويف أي شخص من أجل تحقيق هذه الأهداف ".

**ج-** بموجب القانون الدولي: استخدام القدرات القائمة على الشبكة لدولة ما لتعطيل أو إنكار أو إضعاف أو معالجة أو تدمير المعلومات المقيمة في أجهزة الكمبيوتر وشبكات الكمبيوتر، أو أجهزة الكمبيوتر والشبكات نفسها، في دولة أخرى[1].

فالحرب قد تحدث بين دولتين أو أكثر، وتطور استخدام الأسلحة من السيوف والرماح إلى القنابل النووية والصواريخ العابرة للقارات، لكن المعضلة عدم القدرة على تصور الحرب السيبرانية منفرده أو ضمن الحرب التقليدية كيف ستكون، لهذا بعض التفاعلات السيبرانية بين الدول أظهرت إلينا تصور عن كيفية الحرب السيبرانية إذا حدثت بشكل موسع، فوجود العديد من نقاط الضعف في الشبكات المحلية للدول نتيجة للكم الهائل من الأجهزة المتصلة بالفضاء السيبراني المهددة بالاختراق والهجمات السيبرانية، بسبب نقاط الضعف في البنية الهندسية للشبكات وبروتوكولات الإنترنت الخاصة بتوصيل الأجهزة في الفضاء السيبراني، وأبرز ثلاث أنواع من التهديد تتعرض لها الشبكات المحلية للدول:-

- هجمات الحرمان من الخدمة: بالهجوم لغرض حرمان الجهة المستهدفة من استخدام الإنترنت، وأشهر ثلاث حالات بالهجوم السيبراني على دول بغرض

[1]- Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?", Springer, Heidelberg , Berlin, link: https://link.springer.com/chapter/10.1007/978-3-642-37481-4_2#aboutcontent

الحرمان من الخدمة اُتهمت فيها روسيا، الأولي ضد إستونيا 2007 عندما أزالت الحكومة تماثيل ورموز خاصة للحقبة السوفيتية من العاصمة، قام القراصنة الروس بإغراق الفضاء السيبراني لإستونيا بملايين الطلبات والأوامر على مواقع الإلكترونية واستهدفت عناوين البروتوكولات الخاص بشركات الاتصالات والبنوك، الحالة الثانية جورجيا 2008 عندما اندلعت اشتباكات بين روسيا وجورجيا تزامن معها هجمات سيبرانية باستخدام شبكات البوت نت للإطاحة بالحكومة الجورجية في الفضاء السيبراني وتعطيل المواقع الإخبارية وتقطع الإنترنت عن البلاد بعمل حزمة خانقة على مستخدمي الانترنت داخل جورجيا وعدم قدرتهم على التواصل مع العالم، ووصل سيطرتهم لإشارات المرور والتلاعب بحركة السير، الحالة الثالثة في قرغيزستان بتعطيل الإنترنت لأكثر من اسبوع بواسطة روسيا للضغط على الحكومة لإغلاق قاعدة ماناس الأمريكية على أراضيها وقد اتي ثماره وأغلقت القاعدة.

- الهجمات على العمليات العسكرية والحكومية: باستهداف الأنظمة بهجمات بشكل يومي جزء أساسي منها للتجسس، إما للحصول على تصاميم الأسلحة وإما للحصول على معلومات سرية، أو لفهم كيف يفكر العدو أثناء نشوب حرب أو معرفة الخطط العسكرية وتمركز القوات، لهذا أي شبكة متصلة بالإنترنت عرضة للهجوم وحتي غير المتصلة، فتعتمد الحكومات والجيوش على هذه الشبكات في أوقات السلم، لا يعني الاعتماد عليها في حالة نشوب حرب، أو في المجال المادي فتنقلب ميزة التسليح عالي التكنولوجيا للجيوش الحديثة إلى كارثة في حال تعطلها أثر هجمات سيبرانية.
- الهجمات على البنية التحتية: فقد تبدو هجمات الحرمان من الخدمة ضئيلة الضرر نسبياً في الفضاء السيبراني للدول لكنها تحمل تكاليف وخسائر مادية كبيرة إذا استمر قطع الخدمة إلى أسبوع واحد، وإذا حدث الهجوم على البنية

التحتية تكون الخسائر فادحة على ارض الواقع باستهداف العمليات الصناعية والأنظمة الإدارية المتعلقة بها، فمجموعة من الهاكرز يمكنهم التلاعب بالأنظمة الخاصة بالطاقة كأنابيب نقل النفط والغاز ومصانع إنتاج الوقود ومحطات توليد الكهرباء، ففي تجربة عام 2009 نفذ مختبر أيداهو الوطني التابع لإدارة الطاقة الأمريكية استهداف مولد كهرباء بهجمة سيبرانية بغرض تدميره في نظام محاكاة، بعد النجاح في اخترق نظام التحكم في المولد تم عطائه أوامر تشغيلية مربكة أدت إلى ارتجاجه ثم انفجار المولد من تلقاء نفسه، وهذا النوع من المولدات لا تنتجه كل الدول ومن تنتجه يصنع المولد الواحد في 6 أشهر حسب الطلب[1].

في حالة فقدان التيار الكهربي لا تنهار أو تتوقف مراكز الإنترنت الرئيسية بشكل مباشر لان المراكز تحتوي على مصادر طاقة احتياطية تضمن تشغيلها لعدة أيام، لهذا تعتبر شبكة الكهرباء بالغة الأهمية في مجتمعاتنا الحالية، هي المحرك الاساسي للحياة البشرية، فبالنظر لتكوين شبكة الكهرباء على الرغم من كونها تنمو وتتغير بشكل مستمر، وتكوينها معقد كشبكة الإنترنت، لكنها تصنف باعتبارها شبكة عشوائية منتظمة فلا يوجد بها محاور متصلة مباشرة بعدد كبير من العقد ومعظم العقد لديها أكثر من ارتباط لتكوينها من محطات لتوليد ومحطات الجهد المختلفة ومحطات التوزيع، لهذا يسيطر على الشبكة عدد قليل من المحطات المركزية، فآلية عمل الشبكة الكهربائية بأن تولد الطاقة وتتدفق في الشبكة من خلال مسارات ذات مقاومة اقل وإذا تم قطع مسار واحد يحول التيار تلقائيا إلى الروابط المتبقية للوصول إلى الأجزاء الفاقدة للتيار الكهربي، وعند تحميل الروابط مزيد من الضغط

[1] ريتشارد كلارك، **حماية الفضاء الإلكتروني في دول مجلس التعاون الدول الخليج العربي**، مركز الامارات للدراسات و البحوث الاستراتيجية، ابوظبي، 2011، ص ص 11 – 14.

نتيجة أعطال الروابط الأخرى يتسبب هذا بارتفاع درجة الحرارة ويتم إغلاق التيار تلقائيا أو بتدخل بشري للحفاظ على الشبكة من التلف.

بمعرفة آلية العمل نجد ان مشغلو الشبكة يوزعون الأحمال على الروابط بالتبديل بينهم لاستمرار تشغيل الشبكة، أي فشل في عملية توزيع الأحمال تتوقف الشبكة أو تدمر أجزاء منها، والفشل في برامج التشغيل أو مشكلة في الحماية يحدث انقطاع في الشبكة وقد تكون كارثة كما حدث في 14 اغسطس 2003 الساعة 4:10 مساء بخلل في أنظمة التشغيل لشبكة الكهرباء فقطع التيار عن شمال شرق الولايات المتحدة ووصل إلى مقاطعة أونتاريو في كندا وفقد 50 مليون شخص الطاقة لفترة طويلة، كشفت التحقيقات بعد ذلك أن أعطال في البرامج أحدثت خلل في الإجراءات التشغيلية، فكانت البداية مع اتصال شجرة مع أحد خطوط الضغط العالي في كيلفلاند الواقعة في ولاية أوهايو الأمريكية ومع درجات الحرارة العالية استشعرت أنظمة السلامة خطر فقامت بتفعيل صمامات الأمان تلقائياً لتجنب المزيد من الأضرار المادية وبوجود أخطاء برمجية وتشغيلية في انظمة سكادا حدث الخلل، فالمستفاد من هذا أن على الرغم من سبب انقطاع الكهرباء بسبب خلل برمجي في الأنظمة المتحكمة بالشبكة وليس هجوم سيبراني إلا أن الشبكة الكهربائية تعتمد في تشغيلها على الفضاء السيبراني من تجميع معلومات والتشغيل والتواصل بين مراكز التحكم وإصرار الأوامر بأنظمة اسكادا، فالعلاقة بينهم اعتماد كتبادل وهذا يشكل قلق لخبراء الأمن السيبراني من الناحية النظرية والعملية يمكن تعطيل الطاقة بهجمة سيبرانية وتنهار القدرات السيبرانية معها[1].

عدم التعطل الطاقة الكهربائية بسبب هجمات سيبرانية في المثال السابق لا يعني عدم تعرض أنظمة التحكم والمراقبة الصناعية SCAD، المختصة بالتحكم

[1] William D. O'Neil, Cyberspace and Infrastructure, op.cit., pp. 6 - 10.

والإشراف وتحصيل البيانات الخاصة بالبنية التحتية والعلميات الصناعية المعقدة للهجوم السيبراني، أبرز الحالات كالاتي:-

- في مارس 2000 Queensland أستراليا تسبب هجوم سيبراني على أنظمة التحكم في المياه في المدينة أطلاق ملايين الجالونات من المياه الصرف الغير معالجه في شبكة المياه العامة، وكان الهجوم من Robert Stringfellow المهندس في شركة الصرف الصحي لفشلة الحصول منصب رشح له فانتقم من الشركة، حالة اخري في أغسطس 2008 وقع الانفجار في خط الأنابيب التركي باكو- جيهان نتيجة هجوم سيراني استخدم القراصنة أنظمة كاميرات المراقبة وضعف برامجها أمنياً للدخول إلى الشبكة والتحكم في خط الأنابيب.
- واهم حالات هجمات الطاقة، عام 2010 استهدف قطاع النفط والطاقة وشركات البتروكيماويات داخل الولايات المتحدة الأمريكية باستخدام برامج خبيثة سيمت بالتنين الليلي Night Dragon، ادعت شركة الأمن السيبراني مكافى أن مصدر الهجمات الصين، 15 أغسطس 2012 هاجمت برنامج خبيث مدمر لأنظمة الكمبيوتر الخاصة بشركة أرامكو السعودية وشركة الغاز القطرية سمي ( شمعون – Shamoon )، في 2010 ظهر البرنامج الضار (ستوكسنت – **Stuxnet** ) كأول سلاح رقمي معروف عالميا استهدف شبكات نظام التحكم الصناعي في منشاة نطنز الإيرانية لتخصيب اليورانيوم لإتلاف أجهزة الطرد المركزي بالتلاعب في إعدادات التشغيل.
- هجوم سد نيويورك عام 2013 استطاع قراصنة إيرانيين اختراق نظام التحكم الخاص بسد صغير في مدينة Rye Brook في ولاية نيويورك اعلنت عنه الجهات الرسمية ولم تُعلن نتائج هذا الاختراق، 1 ديسمبر 2014 أصدر مكتب العدل الاتحادي الألماني تقرير عن تعرض مصنع لأعمال الحديد والصلب ذو خبرة لم يحدد هويته إلى هجوم سيبراني عن طريق اختراق شبكة المصنع

وصولاً لأنظمة الإنتاج، تسببت الهجمة في نهاية المطاف بعدم إغلاق "الفرن العالي" (الفرن يستخدم لصهر خامات الحديد) وتشغيله بطاقته الكاملة مما أدي إلى خسائر مادية فادحة للمصنع، في 17 ديسمبر 2016 تعرضت شبكة تعرضت شبكة الكهرباء الأوكرانية لهجة سيبرانية على محطات التشغيل المركزية أدت إلى إعماء مركز التحكم للشبكة، مما أدي إلى توقف 30 محطة فرعية وانقطاع الكهرباء عن الملايين[1].

مما سبق ظهرت نقاط ضعف في الأنظمة التشغيلية للبنية التحتية بمختلف أنواعها، فأهم نقاط الخلل التي تعرض أمن البنية التحتية للخطر كالاتي:

- **حدود الأنظمة:** بمعني عدم القدوة على كشف النشاط الغير مصرح به في الأنظمة الحرجة، وضعف الحدود بين شبكات البنية التحتية والمؤسسات المسؤولة عنها.
- **العالمين:** الافتقار لآلية تتبع للحسابات وكلمات المرور الخاصة بالعاملين في المؤسسات، التهديدات المحتمل من الموظفين السابقين، اختراق الحسابات ذات الصلاحيات الواسعة.
- **تخصيص الموارد:** عدم وجود موظف احتياطي أو بديل في الحالات الحرجة، فقدان المعرفة التنقية اللازمة من قبل العاملين في المواقف الحرجة.
- **التحكم في الوصول المادي عبر الانترنت:** بالتحكم عبر الإنترنت في المعدات والمواقع الميدانية بشكل كامل، يزيد فرصة الاختراق لعمل تعديل أو حذف البيانات، أو إضافة البرامج الخبيثة أو الوصول إلى شبكة البنية التحتية الحرجة، وتخريب وسرقة الأصول السيبرانية، وإضافة برمجيات خبيثة لالتقاط كلمات المرور.

[1] - Kevin E. Hemsley and Dr. Ronald E. Fisher, **History of Industrial Control System Cyber Incidents**, Idaho National Laboratory, December 2018, pp. 4 - 22.

- **إدارة الحسابات:** اختراق كلمات المرور يؤدي إلى الوصول غير المصرح به إلى الأنظمة، وخاصية التشغيل الذاتي للأنظمة تجعل القراصنة يتلاعبون بالأنظمة، كعمل خلل يجبر النظام على التوقف ذاتياً[1].

مما سبق هناك عدة نقاط لتقوية وزيادة السلامة السيبرانية لأنظمة البنية التحتية، فمن أجل حل المشكلات والثغرات السيبرانية بأن يضع المشغلين أنفسهم مكان الخصم أو المخترق الذي يتمثل هدفه في إلاف أو تدمير البنية التحتية، ويوضع في الاعتبار التوصيات التالية:

- وجود أنظمة سكادا فرعية للتحكم ولتشخيص الأعطال والصيانة للبنية التحتية وعدم الاعتماد على نظام واحد متحكم في الشبكة ككل.
- ضمان وجود موظفين مدربين ومحترفين لتشغيل البنية التحتية.
- التقييم المستمر والتحديث لأنظمة البنية التحتية وللمعدات.
- في مرحلة تصميم الأنظمة يتم اختبارها ضد الهجمات السيبرانية بعمل محاكاة لهجمات، لاكتشاف الثغرات الأمنية و إغلاقها.
- فحص مراكز التحكم الرئيسية للبنية التحتية، ورصد أي تغيرات مفاجأة كالاهتزازات غير الثابتة وعدد دوان الآلات على سبيل المثال[2].

**خامسًا: النموذج التطبيقي:**

بالتطبيق علي ما سبق فيما يخص الردع والحرب السيبرانية نجد أن الصين قامت بتحديث جيشها من أجل الحروب القادمة التي قد تخوضنها، لهذا قامت العقيدة الصينية منذ التسعينات علي استخدام العمليات السيبرانية لأغراض مختلفة: (جمع

[1] Ibid., pp. 24.
[2] S.A. Timashev, Cyber Reliability, Resilience, and Safety of Physical Infrastructures, **IOP Conference Series Materials Science and Engineering**, March 2019, pp.12-13. pp.12-13.

المعلومات الاقتصادية والعمليات استخبارات الدولة وللتجسس والتحكم في تدفق المعلومات)، وتدعم العمليات السيبرانية جهود الصين لمراقبة الحكومات الأجنبية والأنشطة خارج الصين والتي يعتبرها الحزب الشيوعي الصيني تهديدًا، وأصبحت العمليات السيبرانية جزء أساسي من التخطيط العسكري الصيني، لان تفسير الصين للأمن الإقليمي يعني أن الدول الأخرى مجبرة على رضوخ لمطالب الصين في بحر الصين الجنوبي والشرقي وضم تايوان، يُحدث هذا اصطدام مع الولايات المتحدة، لهذا يركز جيش التحرير الصيني علي استخدام القوة السيبرانية لتعطيل القدرات السيبرانية والتكنولوجية الأمريكية من أجهزة الاستطلاع والأقمار الصناعية بالقرب من ساحل الصين، ولإعاقة وصول القوات الأمريكية إلى المنطقة وحرمان القوات البحرية والجوية الأمريكية من القدرة على العمل بحرية في نطاق 1700 كيلومتر من البر الرئيسي، هذا جزء مما يسميه جيش الصيني استراتيجية "التدخل المضاد"، وتطورت الخطط الصينية بعد ذلك للقدرة على تدمير الأقمار الصناعية الأمريكية وأصول المراقبة يمكن أن يساعدها في منع الجيش الأمريكي من العمل أثناء التدخل في أي صراع في غرب المحيط الهادئ، بهذا أصبحت الحرب السيبرانية عنصر اساسي في تخطيط العمليات العسكرية الصينية، وطور جيش التحرير الشعبي قدرات متكاملة في الحرب السيبرانية تمكنه من الدفاع عن شبكات الكمبيوتر العسكرية والمدنية، مع الاستيلاء و السيطرة على أنظمة معلومات الخصم[1].

[1] Larry Wortzel, The Chinese Way of (Cyber) War**, Defense Dossier**, Issue 4, August 2012, p1.

## الخاتمة

نجد أن الفضاء السيبراني ليس كما هو متصور يتكون من منظومة غير مادية، على العكس من ذلك فالفضاء السيبراني قام على أساس البنية التحتية للاتصالات الهواتف ثم تطور يتكون من طبقات تشغيلية عديدة مادية وغير مادية، وتوسع عن طريق توسعات جغرافية لتغطية الشبكة من المناطق إلي المدن ثم ليتشمل المساحة الجغرافية للدولة ومن ثم تترابط شبكات هذه الدول فيما بينها وتكون الفضاء السيبراني، والاعتماد على شبكة الفضاء السيبراني في تشغيل البنية التحتية للدول شكل خطر كبير على مدي التأثير المتبادل بين هو افتراضي وما هو واقعي، وبالتالي شكل الفضاء السيبراني خطرًا على سيادة الدول في كيفية حماية أصولها سيبرانيًا، وظهرت القدرة على تهديد البنية التحتية وخاصة الطاقة بجميع ابعادها بدايتًا من منشآت توليد الطاقة كمفاعلات نووية وسدود والمحطات التقليدية لتوليد الكهرباء وصولاً لمحطات توزيع الكهرباء، والقدرة على تخريب منظومات الإمداد من النفط والغاز والقدرة تعطيلها، فيما يخص الفاعلين فلا تزال الدولة تحتل مكانه في تفاعلات الفضاء السيبراني بما تمتلكه من التحكم في الاصول للشبكة وتوافر القدرات الازمة للقيام بعلميات سيبرانية، وظهرت الشركات كلاعب مهم إما لتحقيق أمنها السيبراني، أما استخدام الفضاء السيبراني لتحقيق ميزة تفوق على الاخرين بالتجسس، لكن الجديد هنا أن سيادة الدول في هذا الفضاء تأكلت بشكل كبير لقدرة الأفراد على ممارسه القوة في الفضاء السيبراني بشكل غير مسبوق، فظهرت جماعات وأفراد بامتلاك بعض الامكانيات المعلوماتية والمادية مكنهم التأثير في سيادة الدول وأمن المؤسسات المالية والشركات سيبرانياً.

## قائمة المراجع

### باللغة العربية:


1- إيهاب خليفة، الدائرة المغلقة: لماذا تتجه الدول لتأسيس شبكات إنترنت وطنية؟ ، **دورية اتجاهات الأحداث**، مركز المستقبل للأبحاث والدراسات المتقدمة، العدد 7، فبراير 2015.

2- رغد البهي، الردع السيبراني: المفهوم والاشكاليات والمتطلبات، **مجلة العلوم السياسية والقانونية**، العدد الاول، 2017.

3- ريتشارد كلارك، **حماية الفضاء الإلكتروني في دول مجلس التعاون الدول الخليج العربي**، مركز الامارات للدراسات والبحوث الاستراتيجية، ابوظبي، 2011.

4- عادل عبد الصادق، الفضاء الإلكتروني وإشكاليات نظرية العلاقات الدولية، مجلة السياسة الدولية، العدد 200، ابريل 2015، المجلد 50.

5- عادل عبدالصادق، أثر الفضاء الإلكتروني في تغير العلاقات الدولية: دراسة في النظرية والتطبيق، **رسالة دكتوراه**، غير منشورة، كلية الاقتصاد والعلوم السياسية، 2014.

6- نوران شفيق علي، الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في ابعاد الأمن الالكتروني، **رسالة ماجستير**، غير منشورة، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية: قسم العلوم السياسية، 2014.


### باللغة الإنجليزية:


1- Alyza Sebenius, Biden’s Cyber Red Line Is Prime for Putin Challenge, Bloomberg, 2021-06-18 , link: https://www.bloomberg.com/news/articles/2021-06-18/biden-s-cyber-red-line-is-prime-for-putin-challenge-experts-say.

2- Craig B. Greathouse, Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?, Springer, Heidelberg , Berlin, link: https://link.springer.com/chapter/10.1007/978-3-642-37481-4_2#aboutcontent.

3- Daniel T. Kuehl, From Cyberspace to Cyber power: Defining the Problem, **National Defense University**, Washington D.C, 2009.

4- Daniel T. Kuehl, From Cyberspace to Cyber power: Defining the Problem, **National Defense University**, Washington D.C, 2009.

5- ITU Report on the Internet and Networks entitled: Digital Development Facts and Figures 2021, link:https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf.

**6-** John Perry Barlow," Across the Electronic Frontier", **Electronic Frontier Foundation**, Washington D.C, July 10 1990.

**7-** Joseph S. Nye, Cyber Power, **Belfer Center for Science and International Affairs**, Harvard Kennedy School, Cambridge, May 2010.

**8-** Joseph S. Nye, Cyber Power, **Belfer Center for Science and International Affairs**, Harvard Kennedy School, Cambridge, May 2010.

**9-** Kevin E. Hemsley and Dr. Ronald E. Fisher, **History of Industrial Control System Cyber Incidents**, Idaho National Laboratory, December 2018.

**10-** Larry Wortzel, The Chinese Way of (Cyber) War**, Defense Dossier**, Issue 4, August 2012

**11-** Richard L. Kugler, Deterrence of Cyber Attacks, **National Defense University**, Washington, April 2009.

**12-** S.A. Timashev, Cyber Reliability, Resilience, and Safety of Physical Infrastructures, **IOP Conference Series Materials Science and Engineering**, March 2019.

**13-** S.A. Timashev, Cyber Reliability, Resilience, and Safety of Physical Infrastructures, **IOP Conference Series Materials Science and Engineering**, March 2019.

**14-** Tim Jordan**, Cyberpower: an introduction to the politics of cyberspace**, Routledge, Londan, 1999.

**15-** Will Goodman, Cyber Deterrence Tougher in Theory than in Practice?, **Strategic Studies Quarterly**, Air University (U.S.), v.4, no.3, (Fall 2010).

**16-** William D. Bryant , Cyberspace Superiority: A Conceptual Model, **Air & Space Power Journal**, Vo.27, No.6, November-December 2013.

**17-** William Gibson, **Burning Chrome**, Arbor House Publishing, Pennsylvania, 1986.