القوة الذكية: التنافس العالمي على قوة الفضاء الإلكتروني والقدرات السيبرانية

Smart Power: The Global Competition for Cyber power and Capabilities

نصيرة صالحي *
جامعة عباس لغرور خنشلة- الجزائر
nasirapolitique@yahoo.fr

تاريخ الإرسال: اليوم / الشهر / السنة * تاريخ المراجعة: اليوم / الشهر / السنة * تاريخ القبول: اليوم / الشهر / السنة

ملخص:

تهدف هذه الدراسة إلى تسليط الضوء على تأثير تكنولوجيا المعلومات والاتصالات في التفاعل بين الفواعل الأساسية في السياسة الدولية (الدول) ، و تأثيره على طبيعة البنية الدولية وتحولات القوة. تدعي هذه الورقة أن استيعاب تكنولوجيا المعلومات والاتصالات في عالم السياسة الدولية أدى إلى ظهور مبادئ ترتيب جديدة للنظام الدولي (الفضاء الإلكتروني)، وأشكال جديدة من القوة بدلاً من القوة المادية (القوة السيبرانية) ونوع جديد من التهديدات (الهجمات غير المبرمجة). يخلص هذا البحث إلى تأكيد فرضيته الأساسية أن تكنولوجيا الاعلام والاتصال والأمن باتا مرتبطان حيث كلما زاد تمكن الدولة من هذه التكنولوجيا كلما تمكنت من زيادة أمنها.

الكلمات المفتاحية: القوة الذكية- الأمن السيبراني- الفضاء الإلكتروني- القوة السيبرانية- الهجمات غير المبرمجة..

Abstract:

This study aims at highlighting the influence of ICT in the interaction between the main actors of international politics (States) , the nature of international structure and the nature of power. This paper claims that the internalization of ICT in the realm of international politics has led to emergence of new ordering principles of the international system (cyberspace) , new forms of power rather than material power (cyper power) and new kind of threats (non Software-based attacks). The research confirms the institutionalist hypothesis: it shows the extent to which the security and ICT become inextricable.

Keywords: smart power, cyber security, cyberspace, cyber power, non-Software-based attacks.

*

مقدمة:

ظلت القوة الصلبة والجانب العسكري تحددان لفترة طويلة طبيعة التفاعلات الحاصلة في العلاقات الدولية وحدود وهيكل النظام العالمي، إلا أن بروز الفضاء الإلكترونى أو السيبرانى Cyberspace وإتساع تأثير العامل التكنولوجي في السياسات الدولية وتحول سمات النزاعات غير تقليدية سواء من حيث الفاعلون والقضايا، أو ديناميات التفاعل في عالمنا الراهن، حيث شكلت القفزات التكنولوجية في مجال الإتصال والمعلومات في أواخر القرن العشرين وبداية القرن الحادي والعشرين سياقات جديدة لنشوب النفوذ السيبراني أو القوة السيبرانيةCyber Powerحول من يملك القدرة على التأثير في مسارات تدفق المعلومات والإتصالات في الفضاء الإلكتروني معيارا لتقدم الدول والمجتمعات، هذا ماساهم في زيادة وعي وإدراك القوى الكبرى بأهمية تأثير العامل التكنولوجي والمعلومات في بنية موازين القوى العالمية والتحول من معيار القوة الصلبة والناعمة نحو القوة الذكية.

كل هذه التحولات التي عرفتها البيئة الرقمية طرحت معها شبكية جديدة من المفاهيم كعقيدة الأمن السيبراني والقوة السيبرانية والحروب السيبرانية، والإرهاب السيبراني العابرة للقارات والدول والجنسيات وتجمعها إيديولوجية واحدة تحت ما يسمى القرصنة الإلكترونية عبر التطور التكنولوجي والمعلومات بنشر أفكارهم لتحقيق أهدافها، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الإفتراضي، ما أدى إلى بروز فضاءات جديدة للصراعات في إطار ما يعرف بالهجمات غير المبرمجة Non Software-based Attacks والتي تشمل هجمات إلكترونية تختلف عن الصراعات التقليدية من حيث الآليات والمستويات ومختصرة حاجز الزمان والمكان في إطار التأثير الشبكي المتزايد وإتساع إستخدام الأفراد والدول للتكنولوجية الحديثة المرتبطة بالفضاء السيبراني.

إشكالية الدراسة:

إلى أي مدى يمكن تحقيق الأمن في ظل تنافس القوى العالمية على إكتساب التطورات التكنولوجية والقدرات السيبرانية؟

فرضيات الدراسة:

زيادة القوة التكنولوجية للدولة يؤدي إلى التنافس العالمي على تحقيق الأمن الوطني القومي.

1. القوة الذكية كمفهوم جديد ضمن التحولات العالمية:

من بين المقاربات المفاهمية التي تم إستدراكها في العلاقات الدولية " القوة الذكية" ، ففي عالم اليوم و مع مطلع القرن الحادي والعشرين أصبح كل شئ ذكي في عالم الثورة المعلوماتية والمعرفية، حيث شاع لفظ "الذكية" لاسيما في مجال التكنولوجية فهناك الحواسيب الذكية والهواتف الذكية، وفي المجال العسكري توجد الأسلحة والقنابل الموجهة بدقة والذخائر الذكية وصولا إلى الحرب الذكية عن بعد.

ومن هنا جاءت خلاصة القول التي انتهت إليها اللجنة التي إشترك في رئاستها ريتشارد أرميتاج نائب وزير الخارجية الأمريكي الأسبق وكان قد شكلها مركز الدراسات الإستراتيجية والدولية وتوصل الفرقاء إلى تسوية تقوم على دمج سياسات القوة الصلبة والقوة الناعمة وجعلها متناغمة في إطار معادلة واحدة تحت إسم " القوة الذكية"، حيث سيجري إستخدام القوة الذكية في الدول الذكية التي تسعي إلى إختصار عمليات كثيرة لمواكبة سرعة التغيير في القرن الحادي والعشرين المتمثلة في التطور التكنولوجي كعنصر مهم لتجنب الحروب (الهرمزي، 2016،ص.52).

تعتبر القوة الذكية من المصطلحات الحديثة في المجال الأكاديمي وفي الخطاب السياسي والإعلامي الأمريكي منذ أن بدأ الباحث السياسي الأمريكي جوزيف ناي Joseph Nye بتوظيف ثنائية الصلب والناعم المستعملة في

تقسيم أجهزة وقطع الكومبيوتر الذي يتألف من أدوات ناعمة وصلبة في سبيل الترويج لمشروعه الاستراتيجي والسياسي والعسكري الذي يقوم على نقل المعركة من الميدان العسكري الصلب إلى الميدان الناعم وأدواته التكنولوجية حيث التفوق لأمريكا وحلفائها. تتلخص القوة الذكية بالجمع بين الصارمة الصلبة المتمثلة بالقوة العسكرية وقوة الجذب الناعمة الاقتصادية لإستثمار المكانة الأمريكية عالميا في التأثير(حسين،ص.62).

وقد أدركت الولايات المتحدة المتحدة كقوة عالمية باحثة عن إستمرار هيمنتها أهمية تأثير العامل التكنولوجي والمعلوماتي في بنية موازين القوى العالمية، إذ وضعت التفوق المعلوماتي كمجال لزيادة قدراتها وحرمان الخصوم منه ضمن استراتيجيتها للأمن القومي للقرن الحادي والعشرين، واتسع هذا الهدف ليشمل مجمل القدرات السيبرانية في مجال الإتصالات والمعلومات مع تزايد التنافس العالمي على حيازة النفوذ في الفضاء الإلكتروني، هذا ما أدى إلى تبلور ظاهرة الصراع السيبراني Cyber Conflict التي إنتشرت بين فواعل من الدول وأنتجت تهديدات واسعة نتيجة نمو إستخدام الأنترنت والهواتف الذكية وتكنولوجية الإتصالات في البيئية الإفتراضية(حنفي على،2017،ص.3).

حيث تنتهج العديد من الدول في العالم إستراتيجية توظيف القوة الذكية في علاقاتها الدولية وسياستها الخارجية بطرق مختلفة وبدرجات متفاوتة، وتعتبر الولايات المتحدة الأمريكية الدولة الأم لإستراتيجية توظيف القوة الذكية التي رسمتها لنفسها بعد الإخفاقات العسكرية وتراجع مكانتها في قمة هرم النظام الدولي، لتجسد التغيرات المستقبلية التي ستطرأ على السياسة الخارجية الأمريكية وسبب في طرح إستراتيجية القوة الذكية بإعتبارها بديل إستراتيجي جديد وتمكين جوزيف ناي من إدخال فكرته إلى مراكز الأبحاث واكتسابها قوة جذب وتأييد واسع.

على ضوء ذلك دعا مركز الدراسات السياسية والإستراتيجية والدولية إلى إجتماعات ومناقشات ضمت أعضاءً من الحزبين الديمقراطي والجمهوري وسفراء وضباط عسكرين، ورؤساء منظمات غير حكومية وقد إجتمعت اللجنة ثلاث مرات سنة 2007 بغية تطوير مخطط تفصيلي لإدارة القيادة الأمريكية وسميت اللجنة في ما بعد بلجنة القوة الذكية التي قدمت توصيات لتقوية مكانة وتأثير الولايات المتحدة الأمريكية عالميا، كما أصدر اللجنة تقريريين أحدهما بعنوان" التوقع العالمي لتحديات الأمن العليا لسنة 2008" والآخر بعنوان" القوة الذكية أمن أكثر لأمريكا(حسين،ص.47).

في ظل ظهور الأنترنت وإستخدامه على نطاق متزايد في أواخر القرن العشرين إتسع المجال العام من المساحات التقليدية لتشمل المواقع الإلكترونية ووسائل التواصل الإجتماعي وشكلت فضاء ممتدا للحوار والنقاش تجاوز حواجز الزمان والمكان ونشأت في ظله مجتمعات إفتراضية مارست أدوارا مؤثرة في القضايا العامة على صعيد داخل الدولة وخارجها(على حسين،2008،ص.11).

وأصبح يعرف المجتمع البشري تطور مطردا في مجال التكنولوجية الرقمية وتطبيقاتها وأصبحت حياة الإنسان أكثر إرتباطا بالأجهزة الإلكترونية والعوالم الإفتراضية، كما جاءت التكنولوجية الرقمية لتلقي بجل تأثيرها على تطور الأنظمة السياسية وتشكيل العلاقات الدولية، ويدعوا المشهد الإلكتروني العالمي في عصر الثورة التقنية والمعلوماتية إلى الوقوف على حدود التفاعل الرقمي القائم بين الفضاء السيبراني والسيادة والأمن القومي للدول العالم، في ظل إنصهار الحدود الجغرافية للدول نتيجة التطورات التكنولوجية التي أتاحت إمكانية الولوج إلى الفضاء الإلكتروني الذي يحوي على العديد من عناصر ومعلومات عن الجوانب الأمنية والسياسية والإقتصادية(بيرم،2019،ص.791).

حيث بات هذا التقدم التكنولوجي ثورة قائمة بذاتها في عالم الإتصالات والعلاقات الدولية وأصبح العالم بفضلها بمثابة قرية كونية، كما أصبح للفضاء الإلكتروني أو السيبراني دور في حركة التفاعلات والتحولات البنيوية كمجال

جديد في العلاقات الدولية وبدأ ينتقل تأثيره من تغييرات هيكلية وتحتية إلى إحداث تغيرات كيفية في النظام العالمي حيث بات العالم يشهد تطورًا في المخاطر الأمنية يرتبط بمراحل النضج التكنولوجي(شلوش،2018،ص.187).

تكمن أهمية الفضاء السيبراني في أنه فسح المجال لنوع جديد من التفاعل بين فواعل دولاتية وغير دولاتية وأدى إلى إنتقال مفهوم القوة ومن يمكن أن يمتلكها، فبعد أن كانت القوة ترتبط حصرا بالدولة كفاعل أساس في السياسات الدولية بات من الممكن أن تمتلك فواعل غير دولاتية القوة في الفضاء السبراني وتشكل تهديد على الفواعل الدولاتية. إنبثقت عبارة Cyberمن أعمال الباحث نوريرت واينر Norbert weiner والتي وصفها بأنها التفاعل بين الإنسان والألة المؤدي إلى خلق بيئة بديلة للإتصال، كما يعرفه المفكر جان بيري بارلو John perry Barlowبأنه مجال إفتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الأنترنت وكم هائل من البيانات والمعلومات(بيرم،ص.793).

أما ويليام جيبسون Gibson William فيرى أن الفضاء الإفتراضي فضاء ثلاثي الأبعاد يتكون من المعلومات فهو العالم الإلكتروني الذي أنشأته شبكات مترابطة لتكنولوجية المعلومات، كما أن الفضاء الإلكتروني ليس ثابتا وإنما هو نظام ديناميكي متطور ومتعدد المستويات للبنية التحية المادية والبرمجيات، حيث أدي ظهور الفضاء السيبراني إلى تغيير محددات تفاعلات السياسات العالمية مع بروز نوع جديد من التهديدات (التهديد السبراني) وإقتضى بذلك ظهور نوع جديد من الأمن وهو الأمن السيبراني وبات الحصول على القوة السيبرانية أحد أهم تجليات البحث عن القوة حيث إنتقل تعظيم القوة Power Maximizing من البحث عن القوة التقليدية بمعناها الواقعي إلى تعظيم القوة السيبرانية وهو ما قد يشكل تطورا مهما في طبيعة الصراع فبعد أن كان الصراع صراعا على الموارد في أرض الواقع سيصبح صراعا على الموارد السيبرانية، كما أن الموقع النسبي للدولية (بالمصطلحات الواقعية) سيتحدد بشكل أكبر من خلال إكتسابها أو عدم إكتسابها للموارد السبرانية ، ولهذا فإن الصراع على القوة السيبرانية كأحد مظاهر القوة يرتبط بالنمو السريع للفضاء السيبراني(شرايطية،2020،ص.398).

وتتوزع القوة وأدوات إدارة الصراعات في الفضاء السيبراني على فاعلين من الدول وغير الدول وكل له هدفه؛ فالدول تسعى من الدخول في هذه الصراعات للحفاظ على مصالحها، تأمين بنيتها التحتية وأمنها القومي من الهجمات الإلكترونية، بينما تتباين أهداف الفاعلين من غير الدول في الصراعات السيبرانية حيث تخدم طبيعة الأنشطة التي يمارسونها على أرض الواقع من أفراد والتنظميات السياسية، شبكات الجريمة المنظمة والمنظمات الإرهابية، والشركات المتعددة الجنسيات، ويمكن تفصيل طبيعة الفاعلين في الصراعات السيبرانية منها:

✓ الدول والحكومات: حيث يتم تنفيذ الهجمات الإلكترونية من قبل الجهات الفاعلة الحكومية لأغراض متعددة أمنية وسياسية، وإيديولوجية ويطرح في هذا السياق جوزيف ناي أربعة تهديدات على الأمن القومي للدول وهي التجسس الاقتصادي، الجريمة الإلكترونية والحرب السيبرانية، والإرهاب الإلكتروني.

✓ الفاعلون من غير الدول: والتي لعبت دورا مهما في وضع قواعد إدارة وحكومة الأنترنت والتي تقوم على الشراكة بين الدول والفاعلين من غير الدول في ظل عدم وجود وضع خاص للدول من قبل الكيانات الرئيسية المسؤولة عن إدارة الأنترنت ومن بين هذه الفواعل نجد الشركات المتعددة الجنسيات التي لها دور في الصراعات السيبرانية، والجماعات المسلحة والتي تسعي لتوظيف الإلكترونية في الفضاء السيبراني، بالإضافة إلى الجماعات الإرهابية التي تستخدم مواقع التواصل الإجتماعي لنشر أفكارها ومعتقداتها، كما توجد جماعات مجهولة تعرف بالأنونيموس منتشرة في الفضاء الإلكتروني تشن هجمات افتراضية لتعبر عن موقفها تجاه قضايا معينة (عبد الصبور،2017،ص.5).

وقد عرف الفضاء السيبراني مجموعة من المفاهيم المتقاربة التي تصب في مجملها في وجود صراع أو هجوم إلكتروني باختلاف الأدوات والوسائل منها:

✓ الحرب السيبرانية: نظام قائم على الرعب المنتشر في الشبكة العنكبوتية(الأنترنت) والتي تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول وإرهاقهم إقتصاديا، وإدخالهم في أزمات نفسية وإجتماعية ناتجة عما يعرف بالإرهاب الصامت(غريب، شرقي،2020،ص.96).

✓ الهجوم السيبراني: يشير إلى إستخدام الخصوم لأكواد الكمبيوتر لأغراض التدخل في وظيفة نظام الكمبيوتر أو الشبكة بما في ذلك وظائف الحكومات والخدمات العسكرية، لتحقيق مزايا استراتيجية وسياسية عن طريق تعطيل تلك الشبكات والأنظمة عن طريق وضعها في حالة عدم الإتصال أو تدميرها بالكامل (قوادرة،2020،ص.521).

✓ الإرهاب السيبراني: بدأ استخدام الإرهاب الإلكترونيCyber Terrorismفي فترة الثمانينيات على يد الباحث باري كولين Barry Collin الذي عرفه بأنه هجمة إلكترونية غرضها تهديد الحكومات لتحقيق أهداف سياسية أو دينية وإيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب(شرقي، غريب،2020،ص.562).

✓ الردع السيبراني: تعود أصول الردع السيبراني إلى عملية عاصفة الصحراء سنة1991 عندما اكتسبت فكرة الثورة في الشؤون العسكرية زخما كبيرا بعد شن الولايات المتحدة حرب معلومات ضد الحكومة العراقية أدت إلى شل شبكة الإتصالات العسكرية العراقية لتبين عن أهمية الردع السيبراني في الحروب المعاصرة(قوادرة،ص.521).

فالردع السيبراني يتعلق بالقدرة على تغيير تصرفات الخصم من خلال تغيير حسابات التكلفة والعائد، فهو يعكس تقييميات ذاتية ونفسية، وحالة ذهنية ناجمة عن وجود تهديد موثوق به برد فعل مضاد غير مقبول، ويمكن أن تنتج عنه ما يسمي الردع بالرفض(Singer, Frledman,2014,p.55).

2- القدرات السيبراني وأثاره على طبيعة الصراعات والتهديدات الأمنية:

إختصر الفضاء السيبراني حاجز الزمان والمكان وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الإفتراضي، ومن ثم برزت فضاءات جديد للصراعات بأدوات مختلفة وأنماط جديد تختلف عن الصراعات التقليدية، وتعود اسباب إهتمام الفاعلين من الدول أو غير الدول لتحقيق الهيمنة من خلال إمتلاكها لعدة سمات منها:

✓ **ساحة صراع إفتراضية:** حيث يتخطى الفضاء السيبراني العديد من الثنائيات التي في الصراعات التقليدية وهو أقل تكلفة من حيث الخسائر المادية وأكثر تحديدا للهدف.

✓ **زيادة الإعتماد الإلكتروني:** حيث باتت الدول تربط بنيتها التحتية بالفضاء السيبراني خاصة شبكات الكهرباء والمياه والبنوك والإتصالات وجمع المعلومات.

✓ **صعوبة وضع الحدود:** حيث زادت حالة التأثير الشبكي داخل الدول وخارجها وإتسع إستخدام الأفراد والجماعات والدول للتكنولوجيا الحديثة المرتبطة بالفضاء السيبراني من مواقع التواصل الإجتماعي، هواتف ذكية ومواقع للتعاملات المالية والتجارية(عبد الصبور،2008،ص.5).

وهناك أنماط لإستخدام القوة في الفضاء السيبراني منها:

•يؤثر الفاعل أ على الفاعل ب: هجمات الحرمان من الخدمة وإدخال البرامج الضارة أو حملة المعلومات وتجنيد إعضاء المنظمات الإرهابية.

•**التحكم في الأجندة "قدرة الفاعل أ على إستعادة إستراتيجيات الفاعل ب":** الضغط على الشركات لاستيعاب بعض الأفكار التي تخص البرامج المقبولة.

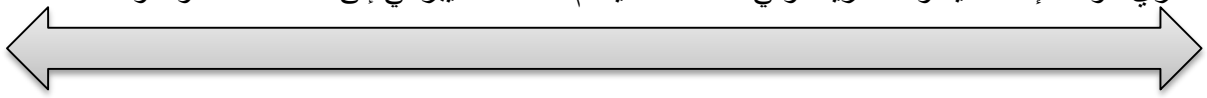
•**قدرة الفاعل أ على إعادة ترتيب أولويات الفاعل ب:** تهديدات بمعاقبة المدونين الذين ينشرون مواد خاضعة للرقابة على مواقع الانترنت.

وبهذا دخل الفضاء السيبراني ضمن المحددات الجديدة للقوة من حيث طبيعتها وأنماط إستخدامها، لتحديد الهدف الإستراتيجي للقوة السيبرانية في خلق ميزة لصناع القرار، وفهم البيئة الإستراتيجية للسلام والحرب وافتقار العدو لهذه الميزة في الوقت نفسه من خلال فهم التحديات والفرص في الفضاء السيبراني(صفاء، خميس مهدي،2020،ص.153).

فقد أصبح للفضاء الإلكتروني دور في حركة التفاعلات والتحولات البنيوية في العلاقات الدولية وبدأ ينتقل تأثيره من تغييرات هيكلية وتحتية إلى إحداث تغييرات كيفية على النظام الدولي، وأصبح يشهد العالم تطور في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي وأصبحت قضية أمن الفضاء الإلكتروني مصدر إهتمام على أجندة القضايا الأمنية الدولية، خاصة بعد أحداث 11 سبتمبر بدأ التركيز على الفضاء الإلكتروني كتهديد أمني جديد وفي سنة 2007 برز بوضوح دور الفضاء الإلكتروني كمجال جديد في العمليات العدائية في الصراع بين إستونيا ورسيا وفي سنة 2008 خلال الحرب بين روسيا وجورجيا(عبد الصادق،2012،ص.2).

وفي عام 2010 أكتشف فيروس إلكتروني مدمر باسم ستكسنيت Stuxnet تمكن من إختراق أكثر من عشرة مواقع صناعية إيرانية فائقة الحساسية منها حواسيب آلية في معامل تخصيب اليورانيوم، كما هو الحال لباقي العمليات السيبرانية خلال سنة2012 اين تعرضت مؤسسات مالية أمريكية ضخمة لهجوم سيبراني أسفر عن محاولة تعطيل المواقع الإلكترونية لبنك أمريكا وكذلك موقع بنك سيتي جروب Citi Group كما تعرضت في نفس السنة شركة أرامكو السعودية التي تعد أكبر شركة نفظ في العالم لهجمات سيبرانية (عثمان،2008،ص.17)، طالت هذه الهجمات أيضا قيادة النقل الأمريكية سنة 2012.

بهذا يصف الجنرال الأمريكي فريزر Fraser الهجوم السيبراني أو الحرب السيبراني بأنها عملية إلكترونية سواء كانت هجومية أو دفاعية تستهدف تدمير البنية التحتية الرقمية الحيوية للولايات المتحدة التي تشكل العمود الفقري لقوتنا الإقتصادية والعسكرية، وفي هذا الصدد يقسم النشاط السيبراني إلى ثلاث فئات للوصول.



هجوم الأنترنت Cyber Attack اضطراب الأنترنت Cyber Disruption الذكاء الرقمي Digital intelligence

الأضرار المادية للممتلكات قطع نظام تدفق المعلومات عمليات الوصول للهدف

كما تعرضت الولايات المتحدة لهجوم إلكتروني خلال سنة 2015 وسرقة للملكية الفكرية مما أدى إلى خسارة مالية كبيرة للشركات الأمريكية(McKenzie,2017 ,p.5).

أصدر أحد أعضاء جهاز المخابرات الأمريكي فرنون كتابا بعنوان" الثلج الأسود: التهديد الخفي للإرهاب المعلوماتي" يشير من خلاله إلى تزايد عدد الهجمات الإلكترونية من ابسط المستويات إلى أكثرها خطورة وقد كانت أكبر الهجمات السيبرانية تلك التي قامت بها كوريا الشمالية على شركة سوني من أكثر الهجمات الإلكترونية التي عملت على تعطيل الآلاف من أجهزة كمبيوتر عن العمل وإختراق المعلومات التجارية السرية للشركة، بالإضافة إلى سرقة آلاف المستندات التي تحتوى على بيانات تتعلق بالشخصيات الشهيرة وموظفي الشركة ورافقت هجماتها الإلكترونية التخويف والتهديد وهو ما عزز من أهمية النقاشات حول التهديد السيبراني وطبيعة الأمن السيبراني(فرحات،2019 ،ص.93).

كما تعرضت خلال سنة 2015 ثلاث شركات للطاقة في أوكرانيا لهجوم سيبراني لمدة ستة أشهر من خلال إختراق النظام بإستخدام حملة إستهدفت عددا من الموظفين بتثبيت أجهزة التسجيل وسرقة أوراق الإعتماد لمختلف الأنظمة، وتسبب الهجوم في إنقطاع التيار الكهربائي وهذا ما سبب خسائر كبيرة لهذه الشركات(Cyber Terrorism,2017, https://bit.ly/2SbXnwK)

أدى تزايد عدد الهجمات السيبرانية التي شنتها الدول وبعض الفاعلين من غير الدول إلى الإعلان عن شكل جديد من الحروب في العصر الرقمي الذي يهدد أقوى القوى العسكرية وأدت الصراعات السيبرانية إلى دخول الدول في عمليات هجومية ضد دول أخرى دون اشتباك وهذا ما يميز الصراعات السيبرانية في مقابل الاستراتيجية العسكرية الكلاسيكية حيث أن الأفكار الكلاسيكية عن الحرب لم تعد تجدي نفعا في العالم الرقمي أو السيبراني(شنوف، 2020،ص.90).

وتعد روسيا والصين والولايات المتحدة من أكبر القوى في مجال الإستحواذ على القوة الإلكترونية القادرة على توفير أقصى درجات الأمن الإلكتروني Cyber Secuity وهو ما فرض على الدول إتخاذ اجراءات حماية عبر تبني سياسات دفاعية من أجل الدفاع ضد الأخطار المحتملة وحماية نظام المعلومات ومنع تعرضها لعمليات هجومية وتعزيز الأمن الإلكتروني بأبعاده المتعلقة بالبرمجيات والبنية التحية، بالإضافة لتبني سياسات هجومية عبر اتخاذ إجراءات لمهاجمة مصادر التهديد (عبد الصادق،2012،ص.07).

في الوقت الحالي اتسعت قائمة الدول ذات القدرات السيبرانية فلم تعد تقتصر على القوى السيبرانية العظمى Cyber Superpower كالولايات المتحدة والصين وبريطانيا، إذ ظهرت قوى إقليمية سيبرانية كإيران وتركيا وفاعلون من غير الدول يحاولون توظيف القدرات الإلكترونية لتحقيق مآرب إستراتيجية وإقتناص مزايا سياسية وإقتصادية، وإكتساب القدرة على التأثير في بيئة العمليات الإقليمية، إذ برزت إيران كواحدة من أهم الأطراف الإقليمية في تطوير قدرات سيبرانية تضطلع بمهام وأنشطة دفاعية وهجومية، ويعد الفضاء الإلكتروني منصة رئيسية لقوى وأطياف المعارضة الإيرانية لنشر المعلومات، وتنظيم الأنشطة المناهضة للنظام وحشد التعبئة ضد القيود على الحريات والانتهاكات التي يرتكبها النظام.

حيث تم توظيف المعارضة للفضاء السيبراني في تنظيم وحشد التظاهرات التي اندلعت سنة 2009 احتجاجات على ما قال المتظاهرون أنه تزوير للانتخابات لمصلحة الرئيس الإيراني المحافظ محمود أحمدي نجاد وهنا ظهر دور وسائل التواصل الإجتماعي في حشد الشارع ضد النظام، حيث رد النظام الإيراني على هذه الإحتجاجات بشن حملة هجومية سيبرانية من خلال حجب مواقع وغلق منصات إعلامية، وإختراق مواقع عالمية وتم تأسيس الجيش الإلكتروني الإيراني Irans Cyber Army وفي سنة 2010 تأسست وحدة تجسس سيبرانية تعرف بإسم مجلس الباسيج السيبراني Basij Cyberspace Council (عثمان،2017،ص.20).

وبالتالي أولت العقيدة الأمنية الإيرانية إهتماما أكبر بالأمن السيبراني، وبات يدخل ضمن نطاق إستراتيجية الأمن القومي الإيراني والتي بنيت على ركزتين أولها تتمثل بحماية الأمن الوطني الإيراني عن طريق بناء بنية تحية علمية تكنولوجية وإستخبارية تعتمد على إستراتيجية وقائية في أثناء الدفاع وإستراتيجية استباقية في أثناء الهجوم، أما الركيزة الثانية بتطوير العديد من المفاهيم والتقاليد القتالية الخاصة بها، وذلك عن طريق تشكيل شبكة معقدة من الجيوش الإلكترونية القادرة على شن هجمات سيبرانية، إلى جانب تفعيل قدراتها الإستخبارية في نشر المعلومات المضللة، كما تم إنشاء منصب مسؤول التعاون التكنولوجي وتأسيس الرقابة على مشاريع البحوث في مجال تكنولوجية المعلومات لتحقيق مشروع أنترنت وطني تديره وزارة الإستخبارات والأمن الوطني الإيراني(إلياس،2019، https://bit.ly/3mVHiJw)

وعليه أصبحت مختلف الهجمات الإلكترونية كتهديد أمني جديد وفي ظل هذه التغيرات أصبح الأمن السيبراني كتحدي عالمي يهدد الأمن القومي للدول.

3- التحديات التي تفرضها القوة الذكية على الأمن القومي وتحقيق الأمن العالمي:

تحولات براديم الحرب جذريا بإنتقالها من نسق الحرب بين الدول إلى نسق الحروب بين الشعوب والتحول من السعي إلى احتلال الأراضي والاستلاء على الموارد إلى التحكم في إرادة الخصم وخياراته، جعل أهداف الحرب أقل مادية وبات العامل النفسي والدعائي يعلب دورا محوريا فيها، بسبب التغطية الإخبارية المباشرة عبر مواقع الأنترنت والفضائيات.

حيث تزايدت العلاقة بين الأمن والتكنولوجية خاصة مع إمكانية تعرض المصالح الإستراتيجية للدول إلى أخطار وتهديدات الأمر الذي حول الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي وإعادة التفكير في مفهوم الأمن القومي للدولة، وأصبح توفير أمن الفضاء الإلكتروني يتحقق بوجود إجراءات الحماية ضد التعرض للأعمال العدائية، والاستخدام السيئ لتكنولوجية المعلومات وإستخدام الفضاء الإلتكروني، وهو ما جعل الأمن السيبراني يمتد من داخل الدولة إلى النظام الدولي ليشكل نوعا من الأمن الجماعي العالمي، فضلا عن تصاعد مخاطر التهديدات الإلكتروني على البنية التحتية الكونية للمعلومات(عبد الصادق،2017،ص.32).

بالإضافة إلى التحديات التي باتت تواجه الدولة القومية في عصر العولمة، فالدولة القومية تعيش فترة ما بعد الحرب الباردة في ظل تعددية الأقطاب الاقتصادية، وفي ظل شبكة مترابطة من الإعتماد المتبادل وإنتهاء الكتل العسكرية وزيادة تأثير التكنولوجية الحديثة، الأمر الذي وضع تحديات واسعة النطاق أمام سيادة الدولة القومية خاصة مع تزايد دور الفواعل والشركات العابرة القوميات، فلم تعد الدول بمفردها قادرة على مواجهة التحديات التي دخلت فيها الأبعاد التكنولوجية بقوة، وتغيرت طبيعة الصراع على إنتاج المعلومة وإستغلالها وظهرت حرب الأفكار وأهمية الثورة المعلوماتية، وزادت أهمية الفضاء الإلكتروني ودور التكنولوجية في تطوير القوة(عبد الصبور عبد الحي، 2014،ص.73).

كما باتت العلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والإجتماعي والإقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني، خاصة مع تسارع تبني الحكومات الإلكترونية والمدن الذكية في العديد من الدول، وإتساع نطاق وعدد مستخدمي الأنترنت في العالم، حيث تصبح قواعد البيانات القومية في حالة إنكشاف خارجي ولم يعد يقتصر إهتمام الدول على البعد التقني بل تجاوز تأثير الإستخدام السلبي للفضاء الإلكتروني على الرخاء الإقتصادي والإستقرار الإجتماعي للدول، وأصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، وهو ما دفع بالدول إلى إدخال الأمن السيبراني ضمن استراتيجيتها للأمن القومي(زروقة،2019،ص.1025).

وبإدراك أن قدرة الدولة القومية في المجال السيبراني يزيد من قوتها ويعزز مكانتها الدولية فإن الصين منذ المؤتمر الثامن عشر للحزب الشيوعي للصين (2017) تولي أهمية بالغة للإنترنت وعملت على تطوريه وحوكمته ، وقامت بتنسيق القضايا المتعلقة بالإعلام والأمن السيبراني في المجالات السياسية والإقتصادية والإجتماعية والعسكرية، وباتت تمتلك أكبر شبكة واسعة النطاق للألياف البصرية في العالم فكانت الحافز الإستراتيجي لقوة الشبكة الصينية، كما تتبني قوة سيبرانية في القطاع الإقتصادي من خلال بناء إقتصاد رقمي قوي وتعتبر أكبر سوق الكترونية وعززت المجتمع الرقمي لبناء قوة سيبرانية لتحقيق الأمن القومي(شرايطية،ص.401).

ويرتبط الأمن السيبراني بكل الأبعاد العسكرية والإقتصادية والإجتماعية والسياسية التي تتعلق بالأمن القومي، من حيث البعد العسكري فقد تتميز المجتمعات الحديثة بالتغيرات التكنولوجية السريعة التي أثرت على قطاع القوات

المسلحة وعززت من التطبيقات التكنولوجية في الشؤون العسكرية، إدخال الأسلحة الذكية وإعطاء أبعاد جديدة لم تكن معروفة من قبل في فون الحرب، وأصبحت الأنشطة العسكرية تعتمد بشكل متزايد على شبكة الأنترنت، وهذا ما يؤدي إلى زعزعة التوازنات الجيوسياسية وزيادة الهجمات السيبرانية أو الحرب السيبرانية وتعتبر حكومة إستونيا من بين الضحايا الذين تعرضوا للهجوم السيبراني ثم تلتها حكومة جورجيا التي تعرضت لهجوم سيبراني تسببت في تعطيل وتدمير أنظمة الإلكترونية الحكومية والتجارية وعدم إمكانية الوصول إلى المواقع الإعلامية الرسمية والوزارات والهيئات العامة، كما استهدفت المؤسسات المالية والتعليمية وكانت الهجمات السيبرانية منسقة ومباشرة في إطار هجوم بحر/جو وأجبرت القرصنة السيبرانية على إلغاء اقلاع طائرة عسكرية(DARAS,2019,p.41).

وباتت القدرات العسكرية تعتمد على تقنية المعلومات فائقة التطور وعلى توظيف الثورة المعلوماتية واعتبارها نقطة أساسية لسيطرة القوة على مسار الإنتاج العلمي والتقني والتسلح بأسلحة القوة المعرفية والتكنولوجية مما يعطي لها قدرة أكبر على التأثير في الأحداث وهو ما يصدق على الولايات المتحدة الأمريكية، وفي هذا يقول توماس كابلان تخلق المعلومات في المجال الإقتصادي ربحية جديدة للولايات المتحدة الأمريكية فالتوسع والنمو الذي شهدناه هو نتاج ثورة المعلومات والتقنية المزدوجة الإستعمال لها تطبيقات تجارية وعسكرية معنا(حسين،ص.62).

كما نجد العقيدة الروسية الجديدة تكشف أنه تمت إضافة بند جديد يخص تهديدات الأمن السيبراني في المجال العسكري والإقتصادي، فوفقا للعقيدة الروسية الجديدة لأمن المعلومات فإن إحدى التهديدات الرئيسة تتمثل في زيادة عدد الدول الأجنبية التي لديها تأثير على البنية التحتية لمعلومات الأغراض العسكرية في روسيا، ويصف خبير الأمن السيبراني أوليغديميدوف Olegidemov العقيدة في شكلها الحالي على أنها الأفضل لمواجهة التهديدات التي تعتري الأمن العسكري والتكنولوجي في روسيا، ويشير الخبير إلى أن الحكومة الروسية أولت إهتماما خاصا لمواجهة ثورات التوتير الجديدة(زروقة،ص.1026).

وعليه يمكن القول بأن القوة السيبرانية ترتكز على وجود نظام متماسك فيه تناغم بين القدرات التكنولوجية والإقتصاد والقوة العسكرية وإدارة الدولة وغيره من العوامل التي تسهم في دعم إمكانيات الدولة على ممارسة الإكراه والإقناع أو التأثير على الدول الأخرى من خلال السيطرة على الفضاء الإلكتروني، فضلا عن أن تكلفة الحصول على القوة أصبحت مرهونة بثورة المعرفة والتطور التكنولوجي الذي مكن من ادراج فواعل جديدة في السياسات الدولية، و هو ما زاد من حالة الإنكشاف الأمني للدولة وذلك بإعتمادها المتزايد على الفضاء الإلكتروني كالبرامج الحكومة الإلكترونية التي أصبحت عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات وهو ما جعل المعضلة الأمنية التي كانت تعاني منها الدول في السابق تبرز بشكل جديد (شلوش،2018،ص.199) ، لنكون بذلك أمام معضلة أمنية سيبرانية A cyber security dilemma .

الخاتمة:

ساهمت الثورة التكنولوجية والاعتماد على التقنيات المتطورة في كافة مناحي الحياة في تغيير العديد من المفاهيم التقليدية في العلاقات الدولية بدءً بوحدات التفاعل في العلاقات الدولية أين بات واضحا أن الدولة لم تعد

الفاعل الوحيد والأساس في هذه التفاعلات في ظل قدرات فواعل أخرى سواء ما تحت أو ما فوق دولاتية على إكتساب تكتولوجيات الاعلام والاتصال والتحكم فيها بصورة أفضل في بعض الأحيان من الدولة حد ذاتها.

أدى هذا التطور إلى خلق مساحات جديدة للصراع أدت إلى إنحسار مجالات الصراع الواقعية لصالح مجالات صراع سيبرانية، وباتت معها الحروب حروبا سيبرانية (الجيل الخامس من الحروب)، وهو ما رسم إدراكا متزايدا لدى صانعي القرار خاصة في الدول الكبرى أن المعركة لم تعد تقتصر على تعظيم القوة والحصول على الموارد كما كان من قبل، بل باتت مرهونة بمدى قدرة الدولة على التحكم في المجال السيبراني وتعزيز أمنها السيبراني أمام التهديدات السيبرانية التي باتت تهدد الدول من قبل فواعل دولاتية وغير دولاتية ، وهو ما يفسر التغير الذي بات يعتري وبشكل كبير المشاريع الاستراتيجية للأمن القومي للدول الكبرى، فالمشروع الأمريكي للأمن القومي بات أكثر إدراكا لأهمية المزاوجة بين ثنائية الصلب والناعم للحفاظ على هيمنتها على النظام العالمي وذلك من خلال توظيف القوة السيبرانية و محاولة إستغلال تفوقها التكنولوجي للتسويق لصورتها كقوة عظمى لا يستقيم حال النظام العالمي ولا توازنه إلا من خلالها وباتت تستخدم في ذلك العديد من الوسائل التي تدخل ضمن الدبلوماسية العامة والرقمية ، أما روسيا في إستراتيجيتها للأمن القومي فهي تتوجس من إمكانية إمتلاك فواعل أخرى سواء دولاتية أو غير دولاتية للقوة السيبرانية وهو ما يشكل خطرا عليها وباتت تستخدم تفوقها في مجال الهجمات السيبرانية لمناكفة قوة الولايات المتحدة من خلال التأثير على نتائج الانتخابات الامريكية، أما الصين فإن إستراتجيتها باتت تركز بشكل أكبر على التفوق في مجال النطاق العريض للألياف البصرية للجيل الخامس.

توفر هذه الصورة نموذجا مختصرا عن طبيعة الصراع في المرحلة القادمة وعن كنه وطبيعة توازن القوة في مرحلة القوة الذكية، التي غيرت مفهوم القوة والأمن وأدت إلى بحث الدولة عن تعظيم قوتها السبرانية A cyber power maximazing ذات التأثير على مختلف الأبعاد العسكرية والإقتصادية والإجتماعية والسياسية .

قائمة المراجع:

أولا: قائمة المراجع بالعربية:

●الكتب:

1. عبد الصبور عبد الحي، سماح. (2014). القوة الذكية في السياسة الخارجية دراسة في أدوات السياسة الخارجية الإيرانية تجاه لبنان 2005-2013، مصر: دار البشير للثقافة والعلوم.
2. الهرمزي، سيف. (2016). مقتربات القوة الذكية الأمريكية كآلية من آليات التغيير الدولي الولايات المتحدة الأمريكية أنموذجا، بيروت: المركز العربي للأبحاث ودراسة السياسات.

●الدوريات العلمية:

1. بيرم، فاطمة.(2019). السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجا، المجلة الجزائرية للأمن الإنساني، العدد الأول، المجلد05.
2. تغريد، صفاء، خميس مهدي، لبني.(2020).أثر السيبرانية في تطوير القوة، مجلة حمو رابي للدراسات، العدد33.
3. حسين، إبتسام على.(2017). فرص وقيود الأطراف المتنازعة على المجال العام السيبراني، مجلة السياسة الدولية، العدد208.
4. حسين، أزهار عبد الله. إستراتيجية توظيف القوة الذكية في السياسة الخارجية الأمريكية بعد عام 2008 دراسة تحليلية ، مجلة تكريت للعلوم السياسية، العدد التاسع، المجلد3.
5. زروقة، إسماعيل.(2019). الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، العدد الأول.
6. شرايطية، سميرة.(2020). السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي، المجلة الجزائرية للأمن والتنمية، العدد 16.

7. شرقي، صبرينة، غريب، حكيم.(2020). الإرهاب الإلكترونية والتحول في مفهوم القوة، مجلة الباحث للدراسات الأكاديمية، العدد الثاني، المجلد07.
8. شلوش، نورة.(2018). القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدولة، مجلة مركز بابل لدراسات الإنسانية، العدد الثاني، المجلد8.
9. شنوف، زينب.(2020). الحرب السيبرانية في العصر الرقمي: حروب مابعد كلاوزوفيتش، المجلة الجزائرية للأمن والتنمية، العدد الثاني، المجلد التاسع.
10. عبد الصادق، عادل.(2012). القوة الإلكترونية: أسلحة الإنتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، العدد 188.
11. عبد الصادق، عادل.(2017). أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، مجلة السياسة الدولية، العدد208.
12. عبد الصبور، سماح.(2017). الصراع السيبراني طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية، العدد 208.
13. عثمان، أحمد زكي.(2017). تأثيرات القدرات السيبرانية في الصراعات الإقليمية، مجلة السياسة الدولية، العدد 208.
14. على، خالد حنفي.(2017). إشكالية تداخل الصراعات السيبرانية والتقليدية، مجلة السياسة الدولية، العدد 208، المجلد 52.

15. غريب، حكيم، شرقي، صبرينة.(2020).تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران(فيروس ستكنست)، مجلة دفاتر السياسة والقانون، العدد الثاني، المجلد12.
16. فرحات، علاء الدين.(2019). الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، العدد الثالث.
17. قوادرة، حسين.(2020).الردع السيبراني بين النظرية والتطبيق، المجلة الجزائرية للأمن والتنمية، العدد16،المجلد09.

•المواقع الالكترونية

1. فراس، إلياس، عقيدة الأمن السيبراني في إيران ومعادلات المواجهة مع أمريكا،2019 ، https://bit.ly/3mVHiJw، تاريخ التصفح2019/08/14 .

ثانيا: قائمة المراجع بالأجنبية:

•Books :

1- DARAS, Nicholas J.(2019) Cyber-Security and information warfare, Nova Science Publishers: :New York.

2- McKenzie, Timothy M. (2017) , Perspectives on Cyber Power Is Cyber Deterrence Possible?, Air University :Air Force Research Institute .

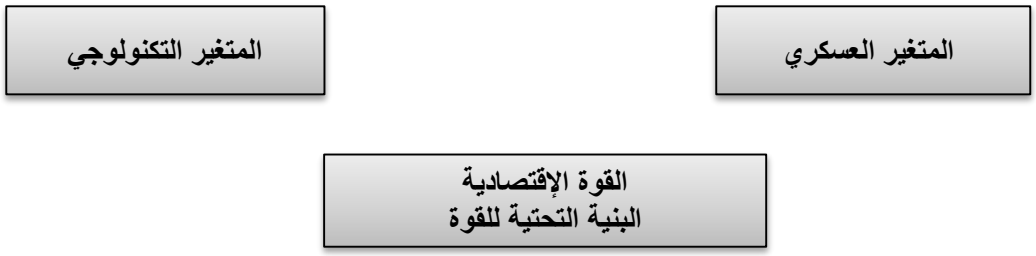
3- Singer, P. W., Friedman, Allan.(2014), Cyber Security And Cyber War, Oxford University Press, New York.

•Electronic resources:

1- Terrorism Cyber. (2017): Assessment Of The Threat To Insurance, Cambridge Centre for Risk Studies Cambridge Risk Framework, https://bit.ly/2SbXnwK ,14/06/2020.

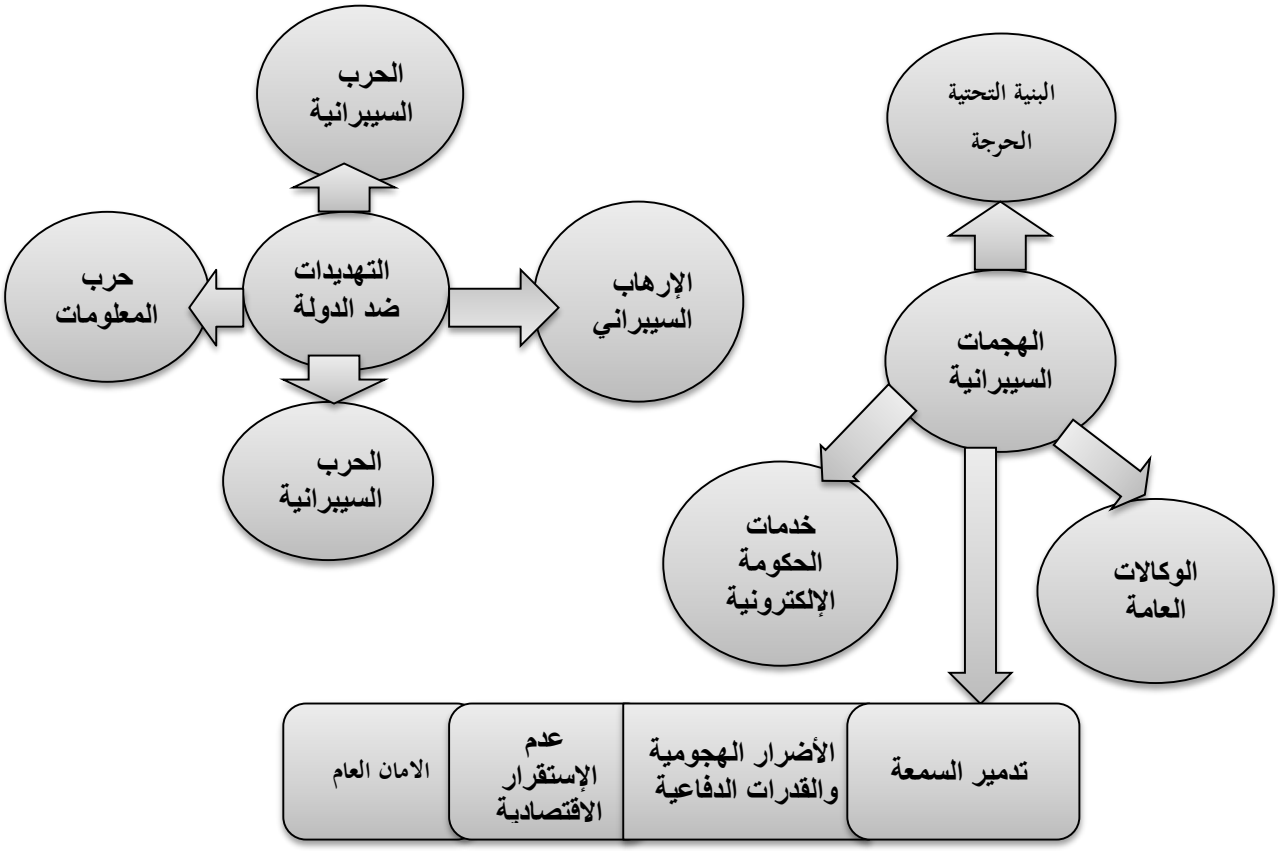
ملاحق:

الشكل (01): مثلث القوة في إطار تكامل المتغيرات



المصدر: الهرمزي ،ص.42.

الشكل (02): التهديدات السيبرانية للدول



المصدر: عبد الصبور،ص.5.