مرتكز تأثير الأمن السيبراني على منظومة الأمن القومي
(المجال الحيوي الخامس)

Fulcrum on the Impact of Cyber Security on National Security Fifth Biosphere

م.د. فراس جمال شاكر محمود الربيعي
Inst. Dr. Firas Jamal Shakir

الملخص

عدُ المرتكز نقطة الـتأثير الجوهرية في محور الكتلة الفيزيائية وهذه اللغة في العلوم التطبيقية، أما العلوم الإنسانية فإن بعد هذا التأثير يخضع لحسابات أكثر دقة لاسيّما إذا كان هذا التأثير يتناسق بشكل عكسي مع منظومة الأمن القومي، ومن هذا المنطلق نؤسس لاطار نظري ومجال تطبيقي وعملي لمحور تأثير البعد الإفتراضي الخامس أو مايسمى الجغرافية الإفتراضية والأمن السيبراني كونه أصبح الجزء الأكثر أهمية نظرا لاعتماد اغلب الدول المتقدمة على التقنيات والقوة الالكترونية التي عدت عصا التحكم في كافة المجالات ذات العلاقة بمنظومة الامن القومي ومن خلال الابعاد السياسية، العسكرية، الاقتصادية، الامنية، الاجتماعية وغيرها من الابعاد ذات الصلة، وعلية فان مرتكز الامن السيبراني اتصف بالحداثة وعد البعد الخامس بعد ابعاد البر والجو والبحر والفضاء ليكون المعادلة الاكثر اهمية في اعادة صياغة السياسات والاستراتيجيات لحماية الامن القومي .

الكلمات المفتاحية: السيبرانية، الانترنت المظلم، المجال الحيوي الخامس، الفضاء السيبراني، الامن القومي، مجتمع مابعد المعلومات.

Abstract:

The fulcrum is the essential point of influence in the axis of the physical mass, and this language is in the applied sciences. As for the human sciences, the dimension of this influence is subject to more accurate calculations, especially if this effect is inversely consistent with the national security system. From this standpoint, we establish a theoretical framework and an applied and practical field for the axis of influence. The fifth virtual dimension, or what is called virtual geography and cyber security, as it has become the most important part due to the reliance of most developed countries on technologies and electronic power, which is considered the control stick in all areas related to the national security system and through the political, military, economic, security, social and other dimensions. Therefore, the pillar of cyber security is characterized by modernity and the promise of the fifth dimension after the dimensions of land, air, sea and space, to be the most important equation in reformulating policies and strategies to protect national security .

Keywords: Cyber, Dark Web, Fifth Biosphere, Cyberspace, National Security, Post-Information Society.

أهمية البحث:

تكمن أهمية البحث في تحديد مرتكز تأثير أبعاد القوة السيبرانية بوصفها نمط للقوة في ساحة التفاعلات الدولية وانعكاسات هذا المتغير على الأمن القومي كونه يتعلق بمجموعة من الأبعاد (السياسية، العسكرية، الأمنية، الاقتصادية، الاجتماعية) ضمن منظومة الأمن المستدام لكيان الدولة ومصالحها القومية فضلاً عن أهمية المجال الحيوي الخامس والمتمثل بنتاجات القوة الإلكترونية واسهاماتها التقنية.

اشكالية البحث:

تتمحور اشكالية البحث في دراسة أبعاد تاثير مرتكز القوة السيبرانية على منظومة الأمن القومي، ومن ذلك تطرح مجموعة أسئلة تمثل أساس اشكالية البحث:

* ما هي السيبرانية وماهي الفواعل الرئيسة في القوة السيبرانية؟
* بماذا تتصف الجغرافية الخامسة أو المجال الحيوي الخامس؟
* ما هو الأنترنت المظلم ومجتمع مابعد المعلومات وتأثر هذه الأنماط على الأمن القومي؟

فرضية البحث :

يسعى البحث لاثبات فرضية مفادها، بما أن أغلب الدول أصبحت تعتمد بشكل كبير على التكنلوجيا والتقنية في المجالات كافة فإن الأمن السيبراني أصبح المرتكز الأكثر أهمية بين المرتكزات الأخرى ذات المساس بالأمن القومي المستدام وعليهه فإن الدول تسعى لتأمين هذا المرتكز بوساطة اتخاذ اجراءات الحماية والدفاع السيبراني وضع سايسات وصياغة استراتيجيات رئيسة وفرعية لتأمين البنية التحتية المعلوماتية والتكنولوجية.

المقدمة

عدُ المرتكز نقطة الـتأثير الجوهرية في محور الكتلة الفيزيائية وهذه اللغة في العلوم التطبيقية، أما العلوم الإنسانية فإن بعد هذا التأثير يخضع لحسابات أكثر دقة لاسيّما إذا كان هذا التأثير يتناسق بشكل عكسي مع منظومة الأمن القومي، ومن هذا المنطلق نؤسس لاطار نظري ومجال تطبيقي وعملي لمحور تأثير البعد الإفتراضي الخامس أو مايسمى الجغرافية الإفتراضية والأمن السيبراني.

منهجية البحث:

تم استخدام المنهج الوصفي التحليلي لاثبات أبعاد الظاهرة وتوضيح نمط القوة السيبرانية باعتبارها الطابع الالكتروني للقوة.

هيكلية البحث:

بالاضافة الى المقدمة تم تقسيم البحث إلى ثلاث مطالب، المطلب الأول تناول مفاهيم ومبادئ الأمن السيبراني، أما الثاني تناول القوة السيبرانية والمجال الحيوي الخامس، والمطلب الثالث تناول الأمن القومي ومرتكز الأمن السيبراني والتهديدات اللامتماثلة، اضافة إلى الخاتمة وقائمة والمصادر.

المطلب الأول: مفاهيم الامن السيبراني ومبادئه

يمكن تناول بعض المفاهيم ذات العلاقة بالأمن السيبراني لتأطيرها بالجانب النظري وكما يأتي:

أولاً: القوة السيبرانية:

إن نشوء القوة السيبرانية كان نتيجة لوجود الفضاء السيبراني، وبالنظر إلى تعريف كـولين غراي Colin S. Gray نجد أن القوة السيبرانية هي من تزيد من

قدرة الوصول إلى الفائدة الاستراتيجية التي قام على أساسها في الفضاء السيبراني، بالإضافة إلى تعريف جين كريستوف نويل Noel Jean - Christophe نجد أنَّه أعتنى بالفواعل الرئيسة للفضاء السيبراني مهما كانت طبيعتهم ومنهم الدولة، ومؤسسة، ومجموعة الأفراد، وقيامهم على استغلال البيانات الرقمية الهائلة المتاحة في الفضاء السيبراني من أجل التأثير على سلوك الفواعل الأخرى على المستوى الدولي بهدف تحقيق مصلحة معينة.

وإلى جانب ما سبق يرى جوزيف ناي والذي يعد من أهم الذين أضافوا القوة الإلكترونية بوصفها شكل جديد إلى القوة التقليدية، فقد رأى أن تلك القوة ترتبط فقط بامتلاك المعرفة التامة بالتكنولوجية والقدرة على الاستعمال من ثم الاندماج في الفضاء الإلكتروني وإتاحة مميزات وأحداث جديدة لأدوات القوة سواء العسكرية، أم الاقتصادية، أم الدبلوماسية، أم المعلوماتية، من ثم فإن تلك القوة تقع ضمن فاعلين محددين فقط وهم الدولة والأفراد وفاعلين غير الدول، إلا جوزيف ناي أكد أن القوة السيبرانية لا تمتلك نفس القدر من المساحة للسيطرة على الفضاء السيبراني بالمقارنة مع قدرة السيطرة على الإقليم البحر أو البري، لذا بدأت الدول جميعها ومنها الكبرى تواجه تحديات في السيطرة على تلك الحدود الرقمية.

وهنا ترى الدراسة أن جميع التعريفات التي وردت للقوة السيبرانية تدرس مدى تأثير تلك القوة على فواعل الفضاء السيبراني لتحقيق مصالحها في العالم الافتراضي أو الواقعي، وبالإضافة إلى تحقيق أهداف في مجالات أخرى خارج الفضاء.

ثانياً: الحروب السيبرانية:

تعرف الحروب السيبرانية بأنَّها الحروب الافتراضية التخيلية غير الملموسة تحاكي الواقع على نحو شبه تام، تنحصر بمواجهات الكترونية عبر البرمجيات

التقنية، ولديها جنود تتمثل برامج التخريب المحوسبة مستخدمين طلقات من لوحات المفاتيح ونقرات المبرمجين، بينما يرى البعض أن تلك الحرب تتقابل مع الحرب التقليدية بإحداث وبث الرعب والإرهاب عند الأخرين عبر شبكة الإنترنت مستهدفة الدول، والأفراد، والمؤسسات، والجماعات وتكبدهم الخسائر الاقتصادية لإدخالهم في حالة من الأزمات النفسية والاجتماعية نتيجة تعرضهم لما يعرف بالإرهاب الصامتSilent Terror.

واستناداً الى ما سبق فإن الدول بدأت في إجراء مناورات عسكرية في الفضاء السيبراني بهدف التأكد من جهوزية الأنظمة الدفاعية السيبرانية لديها؛ للتعامل مع أي هجمات سيبرانية مفاجئة وعدم اختراق السيادة الوطنية الرامية الى سرقة معلومات استخباراتية عبر تجنيد العملاء، وأن تلك الحروب القائمة على الاختراقات والقرصنة ونشر الفيروسات ينتج عنها تكبد خسائر كبيرة بحيث أن اكتشاف تلك الهجمات يكون في وقت متأخر قد فات الأوان على التصدي، ومن أكبر المساوئ بأنَّ تلك الحروب لا تستطيع التمييز ما بين المقاتل والمدني، وقد عرفت وزارة الدفاع الأمريكي الحرب السيبرانية" بأنَّها استعمال أجهزة الكمبيوتر والإنترنت وجميع القدرات السيبرانية لإجراء الحرب في الفضاء السيبراني وتحقيق غرض أساسٍ يتمثل في آثار عسكرية داخل الفضاء السيبراني.

ثالثاً: الأمن السيبراني:

يُعرف الأمن السيبراني على أنَّه حماية أنظمة المعلومات (الأجهزة، البرمجيات، البنية التحتية المرتبطة به)، والبيانات المتعلقة بها والخدمات التي تقدمها من الوصول غير المصرح به، أو الأذى أو سوء الاستعمال وهذا يشمل الضرر المتسبب عن عمد من قبل مشغل النظام أو عن طريق الخطأ نتيجة عدم إتباع إجراءات الأمان والحماية.

وكما عرف الأتحاد الدولي للاتصالات (ITU) الأمن السيبراني بأنَّه مجموعة من المفاهيم الأمنية بالإضافة إلى أدوات وسياسات للوصول لضمانات الأمن من ممارسات وتقنيات وأساليب إدارة المخاطر للعمل على حماية البيئة السيبرانية التي تشمل أصول المنظمة والمستخدم، ومن ثم توفر السرية والنزاهة (ITU, 2008).

قدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني بأنَّه " جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث".

وترى الدراسة أن هناك تباين في النظرة إلى الأمن السيبراني بوصفه مفهوم وينبع هذا التباين من التباينات السياسية والتفاوت في القدرات لكل دولة، ما بين القدرات الهجومية والدفاعية، وتقبل هذه الدولة أو تلك لتوظيف الهجمات السيبرانية في تفاعلها على الساحة الدولية، وذلك أن المفهوم هو انعكاس لكيفية فهم وتطبيق كل دولة للأمن السيبراني وموقعه في استراتيجية الأمن القومي المرتبطة بالمصالح العليا للدولة.

رابعاً: أهداف الأمن السيبراني ومبادئه وأهميته:

أصبح الأمن السيبراني من احدى أهم الأولويات التي تعتني بها كافة أطياف المجتمع، في الوقت الذي أصبح فيه الإنترنت أحد الضرورات الحيوية لكل من الأفراد والحكومات والمؤسسات والمنظمات، ومن ثم أصبح هناك أهمية وجود حماية من أي عمليات احتيال عبر الإنترنت أو سرقة الهوية، إلى جانب حماية معلوماتهم المالية التي في حال اختراقها فإنها تؤثر على الوضع المالي لديهم، في الوقت الذي تعاني فيه تلك الجهات من العديد من التحديات منها: محدودية الموارد وضعف في مهارات الأمن السيبراني، من ثم أن العمل على رفع الوعي في آلية استعمال الانترنت وحماية أنظمة الحاسوب يساعد على توفر بيئة آمنة للأنترنت.

يمكن تحديد إحدى أهم أهداف الأمن السيبراني بالآتي:

الهدف الأول: وهو السرية التي تساعد على ضمان الوصول للمعلومات من هم مخولين لذلك لاغير من ثم يمكنهم تلقي أو تغيير أو إدارة المعلومات بحرية.

الهدف الثاني: وهو النزاهة التي تضمن أن من يستطيع الدخول إلى المعلومات ولبوصول إليها هم الأشخاص المصرّح لهم لا غيرهم، من ثم يستطيعون العمل على إجراء أي تغييرات في النظام.

الهدف الثالث: هو توفر النظام والمعلومات التي يديرها النظام ومشغليه مما يضمن أن الكيانات المرخص لها فقط يمكنها الوصول إلى المعلومات أو الموارد المخزنة أو المستعملة في البنية التحتية للمؤسسات.

وتفسيراً إلى ما سبق فإن تلك الأهداف التي قام عليها الأمن السيبراني نابعة من الأهمية القائمة على مدى اعتمادية الحكومات والمؤسسات العسكرية والشركات والمؤسسات المالية والطبية وغيرها على استعمال أجهزة الكومبيوتر والشبكات العنكبوتية في جمع كميات هائلة من البيانات ومعالجتها وتخزينها ولاسيّما إنَّ تلك البيئة تمتاز في حساسية البيانات فيما يتعلق بالملكية الفكرية أو معلومات أمنية أو شخصية أو بيانات مالية، ومن ثم فإنَّ دخول أشخاص غير مخولين إلى تلك المعلومات له عواقب وآثار وخيمة، وقد تزايدت تلك المخاطر بالتزامن مع بدء الشركات والمؤسسات بالاعتماد على استعمال الإنترنت في نقل المعلومات فيما بينها، لذا قد تزايد مدى الحاجة إلى حماية تلك الشركات والمؤسسات لمعلوماتها تزامنا مع ارتفاع خطر الهجمات الإلكترونية، بل أصبحت الهجمات الإلكترونية والتجسس الرقمي يمثلان أكبر تهديد للأمن القومي لأي دولة بل أنه فاق خطر الإرهاب.

الهدف الرابع: وهو الحماية التي تهدف بشكل رئيس إلى الحفاظ على أنظمة التقنيات التشغيلية بكافة الأصعدة ومكوناتها من أجهزة وبرمجيات، من أي اختراقات من جهات خارجية، إلى جانب حماية الخدمات وما تحويه من بيانات.

الهدف الخامس: وهو القدرة على التصدي لأي هجمات أو حوادث تمس أمن المعلومات الهادفة إلى اختراق الأجهزة الحكومية ومؤسسات القطاع العام والخاص.

الهدف السادس: وهو العمل على توفير بيئة آمنة لجميع الفئات المعرضة للهجمات السيبرانية، للوصول لمستوى موثوق من الأمان في إجراء التعاملات في مجتمع المعلومات.

الهدف السابع: وهو رفع جاهزية البنى التحتية للتصدي لأي هجمات الكترونية يحتمل أن تتعرض لها بشكل مفاجئ.

الهدف الثامن: وهو العمل على توفير المتطلبات الأساسية اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستعملين وتقليل أثرها عند التعرض لأي هجمات.

الهدف التاسع: وهو العمل على التخلص من أي نقاط ضعف يمكن أن تكون بمثابة ثغرات في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها، ومن ثم فإن الأمن السيبراني يهدف إلى سد الثغرات في أنظمة أمن المعلومات، إلى جانب مقاومة رفع قدرت الجهات المختلفة على رصد البرمجيات الخبيثة تهدف إلى الحاق أضرار بالغة للمستعملين.

الهدف العاشر: وهو القدرة على اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استعمال الإنترنت

المختلفة، وتدريبهم على آليات مواجهة التحديات المرتبطة باختراق التقنية بقصد الضرر بمعلوماتهم الشخصية أو حتى الإتلاف أو بقصد السرقة.

وبناء على ما سبق ترى الدراسة أن الهدف الرئيس للأمن السيبراني هو صون سيادة الدول من أي هجمات يمكن أن تهدد أمنها أو بناها التحتية، وحقوق الأفراد من انتهاك خصوصيتهم، وضمان بيئة أعمال أمنة للشركات، وتحصين المؤسسات من أي عمليات اختراق قد تمس بسير عملها وتضر بقاعدة بياناتها الخاصة.

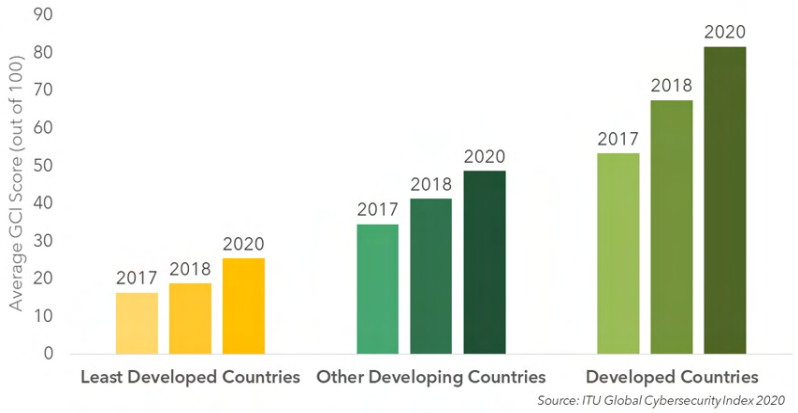
خامساً: مؤشر الأمن السيبراني العالمي GCI

بدأ يزداد عناية الدول المحلي بتنمية قدرتها السيبرانية لما تكبدها الهجمات من خسائر وتهديد للأمن الاقتصادي المحلي والدولي، حيث ساعد مؤشر الأمن السيبراني العالمي (GCI) التابع للإتحاد الدولي للاتصالات على قياس مدى التزام الدولة بالأمن السيبراني ومستوى التطور الذي وصلت إليه، ويقدم توضيح للتدابير القانونية والتقنية والتنظيمية التي تلزم الدولة لبناء قدراتها والتعاون مع الدول الأخرى على النحو الآتي:

- محور الأطر القانونيةlegal: يقيس مدى قانونية التعامل مع الأمن السيبراني والجرائم السيبرانية.
- محور القدرة الفنية:Technical يقيس مدى توافر مؤسسات وأطر فنية للتعامل مع الأمن السيبراني.
- محور تنظيمي:Organizational يقيس مدى توافر سياسات وإستراتيجيات على المستوى الوطني لتنمية الأمن السيبراني وتطويره.

- محور بناء القدرات:Capacity Building يقيس مدى توافر برامج للبحث والتطوير والتعليم والتدريب المرتبط بالأمن السيبراني وتأهيل معتمد لمتخصصين من مؤسسات عامة.
- محور التعاون:Cooperation يقيس مدى توافر شراكات فعالة وأطر للتعاون وشبكات لتبادل المعلومات والخبرات ذات الصلة بالأمن السيبراني.

فعليه يقدّم المؤشر تصنيف لجميع الدول كل دولة على حدى، وفي غالب الأمر يظهر تشارك بعض الدول في نفس الترتيب بما يوضح توازن في مستوى الاستعداد لديهم، إلا أنه أثبت وجود فجوة في قدرة الأمن السيبراني بين الدول الأقل نمواً والدول النامية من حيث الموارد والمهارات والأدوات المستعملة لإدارة مخاطر الأمن السيبراني بشكل استباقي في تلك الدول على مر السنوات، وذلك ما يوضحه الشكل رقم (١) الآتي:



المصدر: GCI, 2020 global cybersecurity index ITU

الشكل رقم (١): مؤشر الأمن السيبراني العالمي

سادساً: مؤشر القوة السيبرانية الوطنية NCBI

يعد مؤشر القوة السيبرانية الوطنية التابع لمركز بلفر للعلوم والشؤون الدولية والذي نشر في عام ٢٠٢٠ عن القدرات الإلكترونية للدول في سياق سبعة أهداف وطنية تسعى الدول لتحقيقها باستعمال الوسائل الإلكترونية هي على النحو الآتي: (Voo, 2020, P 13)

١- مسح المجموعات المحلية ومراقبتها.

٢- التحكم في بيئة المعلومات ومعالجتها.

٣- العمل على جمع معلومات الاستخبارات الأجنبية التي تدعم الأمن القومي.

٤- تقوية الدفاعات السيبرانية الوطنية وتعزيها.

٥- القدرة على تدمير أو تعطيل البنية التحتية للخصم.

٦- الحصول على مكاسب تجارية أو تعزيز نمو الصناعة المحلية.

٧- المشاركة في تحديد القواعد والمعايير التقنية الإلكترونية الدولية.

وبناء على منهجية هذا المقياس التي ترتكز على التمييز بين النية (Intent) والقدرة (Capabilities) في التعامل مع الأمن السيبراني الوطني بناءً على الأهداف أعلاه، فإن الحكومات يمكن أن تملك القدرة دون وجود النية لاستعمال أي وسائل سيبرانية ويمكن حدوث العكس تماماً، لذا تصنف مراكز الثقل السيبرانية للدول بشكل رباعي في إطار هذا المؤشر وهي: دول تمتلك قدرات أعلى ونية أعلى في مجال الأمن السيبراني، دول تمتلك قدرة أقل ونية أعلى، دول تمتلك قدرة أعلى ونية أقل، دول ذات نية أقل وقدرة أعلى.

وفيما يلي يقارن جدول رقم (١) ترتيب القوى السيبرانية العالمية لعام ٢٠٢٠ وفقاً لمؤشر القوة السيبراني الوطنية ومؤشر الأمن السيبراني العالمي والتي يسعون الدول إلى تحقيقها بالوسائل الإلكترونية على النحو الآتي:

الترتيب	مؤشر القوة السيبراني الوطنية NCBI	مؤشر الأمن السيبراني العالمي GCI
1	الولايات المتحدة	الولايات المتحدة
2	الصين	السعودية، بريطانيا
3	المملكة المتحدة	إستونيا
4	روسيا	كوريا، سنغافورا، إسبانيا
5	هولندا	الإمارات، روسيا، ماليزيا
6	فرنسا	ليتوانيا
7	ألمانيا	اليابان
8	كندا	كندا
9	اليابان	فرنسا
10	إستراليا	الهند

المصدر: (Voo, 2020) (ITU, 2022)

جدول رقم (١): ترتيب القوى السيبرانية العالمية لعام ٢٠٢٠ وفقاً لمؤشر القوة السيبراني الوطنية ومؤشر الأمن السيبراني العالم.

المطلب الثاني: القوة السيبرانية والمجال الحيوي الخامس

المجال الحيوي الخامس

عدُ الفضاء السيبراني هو المجال الحيوي الخامس الذي يلي كل من المجالات البرية والبحرية والجوية والفضاء الخارجي، وإن كان وجود هذا المكان افتراضياً، إلاّ أن ما يدور فيه من منافسة وصراع وهجمات و حروب مستقبلية جميعها حقيقة، بل أن من المتوقع أن من يتحكم في هذا المكان الافتراضي سيكون له الصدارة في قيادة العالم، لأنَّه يؤثر في جميع جوانب الحياة.

أولاً: الجغرافيا الخامسة:

من الملائم عدّ الفضاء السيبراني (الفضاء الإلكتروني)، نطاق جغرافي خامساً للحرب والسلام والدفاع والاستراتيجية، بعد (البر، البحر، الجو، الفضاء الخارجي). فإنَّه يختلف إختلافاً جوهرياً عن الجغرافيا الأخرى، ذلك يعزى لما يتمتع من مستعملين والآت متخصصة فضلاً عن التفاعلية الإلكترونية وبهذا لا يمكن أن نعدّه مجرد جغرافيا أخرى في المجال (السياسة، والصراع، والاستراتيجية)، بل إنها وحدة فريدة من نوعها. فهنالك بعض المخاطر في التصنيف المناسب للفضاء السيبراني بوصفه خلفية لتسمية جغرافيا.

وهناك بعض المخاطر في التصنيف المناسب للفضاء السيبراني بوصفه خلفية لتسمية الجغرافيا، يمكن أن تحمل أكثر من سرد مهيمن للأسباب والآثار المزعومة، تسعى المناقشة أعلاه إلى تسجيل الادعاءات القائلة بأنَّه: على الرغم من اختلاف الفضاء الإلكتروني اختلافًا جذريًا من الناحية الجيوفيزيائية عن البيئات البرية والبحرية والجوية والأرضية المدارية، فإنهّ لا يزال إلى حد كبير مجالاً جغرافيًا

كآخرين. وأن من الحكمة اعتبار الإنترنت مجال جغرافي آخر (للسياسة، والصراع، والاستراتيجية).

وقد تعمل الاتجاهات الجيوسياسية العالمية على أن تكون حاضرة في البيئة السيبرانية، وبشكل مكثف. فالابتكار الرقمي يتيح للخصوم السياسيين فرصة متزايدة لإيجاد نقاط الضعف التي يمكنها تدمير قدرات القوة الاقتصادية والعسكرية للدولة المعادية.

وتقف الجغرافيا السياسية في مفترق طرق شديد الخطورة عندما يصبح مجال الفضاء الإلكتروني هو خط المواجهة الرئيس. وعلى مدى السنوات القليلة الماضية، بذلت الحكومات والمجموعات غير الحكومية في الشرق الأوسط وشمال أفريقيا جهوداً كبيرة لبناء قدراتها الإلكترونية. وقد يؤدي انتشار الأسلحة الإلكترونية في المنطقة واستعمالها بوصفها أدوات جيوسياسية إلى تصاعد الأزمات الإقليمية وتفاقمها، وإلى زيادة المصالح الغربية في المنطقة.

ثانياً: الطابع الرقمي للجغرافيا السياسية (الجيوبوليتيك):

أصبحت الجغرافيا السياسية تستعمل المهارة السياسية والأصول للحصول على نفوذ في الشؤون الدولية بعيدة بشكل كبير عن الإطار الجغرافي الأصلي لها. ويستضيف الفضاء الإلكتروني (السيبراني) الفضاء الإلكتروني وهو الشبكة العالمية لتكنولوجيا المعلومات المترابطة بما في ذلك الأجهزة والبرمجيات والمعلومات بعض أهم الأسلحة ونقاط الضعف الجيوسياسية للدول على حد سواء. وبما أنَّه لا يمكن التفريق بين التهديدات الإلكترونية والتهديدات الجسدية، فمن المرجح أن تكون "الجيوسياسية الإلكترونية" في طليعة المنافسة الجيوسياسية في المستقبل. وتشمل الأدوات السيبرانية المستخدمة من أجل تحقيق الأهداف الجيوسياسية مجموعة كبيرة

من الأدوات مثل تلك المتعلقة بالمراقبة، والتجسس، والتضليل، أو الهجمات المدمرة او اتلاف البيانات أو تغييرها.

اما الجيوسيبرانية في الفضاء السيبراني، فإنَّها شغلت مكانة كبيرة في الجيوبوليتيك والجغرافيا السياسية، وأن جميع التفاعلات السياسية والاقتصادية والاجتماعية قد أصبحت آلان أغلبها بواسطة الفضاء الإلكتروني، وإنّ رقمية التفاعلات الدولية في الجيوسيبرانية الآن قد بدأت بدورها مزاحمة ثوابت البيئة الاستراتيجية التقليدية، وتزاحمها في قراءة شكل العلاقة وتقديره التي تجمع ما بين المكانة الجيوبوليتيك للدولة مع القدرة التفاعلية الإلكترونية لها، والتطرق إلى الجيل الجديد من الأمن والصراع في هذه البيئة،فضلاً عن ملامح القوى الاستراتيجية للدول الراشدة في هذا المجال.

ثالثاً. المجتمع الخامس (Fifth Society):

ويسمى بـ "مجتمع ما بعد المعلومات"، وقد جاء بعد أربع أجيال رئيسة مرت بها الإنسانية، وهي مجتمعات الصيد، والزراعة، والصناعة، والمعلومات، وأخيراً المجتمع الخامس، أو "مجتمع ما بعد المعلومة" ذلك المجتمع الذي تندمج فيه المعلومة والآلة مع عقل الإنسان، ويعد الإنترنت أو الفضاء السيبراني أو النطاق الخامس، هو العمود الفقري لهذا المجتمع، فبعد الأرض والبحر والجو والفضاء الخارجي أصبح الفضاء السيبراني خامس الميادين التي تسعى البشرية لاستغلالها، وعلى سبيل المثال: بدل استعمال الفرد "خرائط جوجل"، مثلاً للذهاب إلى المكان الذي يريد كما هو الحال في مجتمع المعلومات ستقوم السيارة ذاتية القيادة أو الطائرات المسيرة، من دون طيار وذلك في المجتمع ما "بعد المعلومة"، وبدلاً من أعطاء أوامر للروبوتات للقيام ببعض الوظائف والمهام، فإنَّها سوف تقوم بصورة منفردة بتحليل المعلومات من المجسّات، وأجهزة الاستشعار الموجودة في كل

مكان، وتتخذ القرار بصورة ذاتية، وستقدم تقنيات أنترنيت الأشياء خدمات للبشر تسبق احتياجاتهم وتوقعاتهم، وتصبح نظم الإدارة لا مركزية بصورة كبيرة.

وحينها تكتسح "الثورة الذكية" كل المفاهيم والطرق التقليدية التي عرفتها البشرية منذ بدء الخليقة، وسيعجز العالم عن مواجهة التوسونامس التكنلوجي الذي بدأ، في التحرك بالفعل، من أجل ظهور عصر جديد يتخيّله بعضهم إن الآلة تكون هي السيد والإنسان يكون هو العبد، ولذا يتطلب وجود رؤية شاملة بوصفها استراتيجية لما ستكون عليه الأفراد في السنوات القادمة، وكيف يمكن التعامل مع التهديدات والتحديات التي تقودها الثورة الذكية، كما ينبغي تحديد الاحتياجات منها وكيفية حمايتها، حتى لا يقع الإنسان ضحية انجازات التكنولوجيا.

وقد يرى البعض أن التطور التكنلوجي يحتاج إلى عقود من الزمن، فإنَّ ثمانية أعوام فقط تفصل بين اعلان شركة ابل عن الأي فون الأول لها في عام (٢٠٠٧) وبين انتشار أكثر من ملياري جهاز هاتف ذكي حول العالم بحلول نهاية عام (٢٠١٥)، فإن سرعة التطور التكنلوجي تسير بسرعة كبيرة جداً، وإن هذه السرعة في كل عام تتضاعف أكثر وأكبر، وليس فقط من حيث الكم بل حيث الكيف وطريقة الانتاج التي ستجعل أغلب المنتجات التي تكون غالية الثمن حالياً، ستكون منخفضة الكلفة مستقبلاً مثل السيارات ذاتية القيادة، بل ومن الممكن أن تكون بأسعار تنافسية، وسوف تؤثر أكثر فأكثر هذه التكنولوجيا على الهويات والثقافات، وذلك بفعل أثر العولمة التي أفرزتها هذه التطورات التكنلوجية.

إنَّ هذا التغيير الذي تحدثه التكنولوجيا بشكل كبير، في حالة حركة مستمرة، لذلك هو في طريقه إلى المزيد من التطور التكنلوجي الهائل، حتى نجد أنفسنا في قلب مجتمع ما بعد المعلومات، أو ما يسميه بعضهم مجتمع الذكاء الفائق، وهو مدفوع بمجموعة من محركات القوى، مثل: Driving Forces التكنلوجية، وتأتي

في مقدمتها مواقع التواصل الاجتماعية، وتطبيقات الموبايل الأخرى، والطائرات بدون طيار(Drones)، وإنترنيت الأشياء (Internet O Things)، والذكاء الصناعي (Artificial Intelligence)، والحوسبة السحابية (Cloud Computing)، والسيارات ذات القيادة(Self-Drive Cars)، والروبوتات، والعملات الافتراضية أو الرقمية، وتقنيات الواقع الافتراضي التي من الممكن أن تدفع بقوة نحو إنشاء حياة جديدة تسيطر فيها التكنولوجيا على شكل الحياة البشرية، وتعيد صياغة كافة التفاعلات الشخصية والدولية.

المطلب الثالث: الأمن القومي ومرتكز الأمن السيبراني والتهديدات اللامتماثلة

أولاً: تهديدات الأمن القومي

إنَّ الربط ما بين الأمن والأمن السيبراني أدى الى ظهور ما يسمى بـ "رقمنة الأمن" القائم على الربط ما بين الأمننة والتسييس التي تجبر الدول على اتخاذ بعض القرارات العاجلة والتدابير الاحترازية والاستثنائية للتصدي لأي تهديد عبر تكوين جيش دفاع وطني إلكتروني، ومن ثم تبرز علاقة ما بين المعضلة الأمنية والمكنة الادائية، فكلما ازدادت المعضلة الأمنية ازدادت التهديدات، وكلما ازدادت التهديدات ازدادت الحاجة لرفع الإمكانيات الادائية لمواجهة التهديد وتحجيمه.

ومن ثم فإن التهديدات السيبرانية التي ظهرت نتيجة المعضلة الأمنية المعاصرة أحدثت تحولاً في اعتبارات الأمن القومي الذي تجاوز المفهوم التقليدي في العقود الأخيرة، وأن تلك التهديدات والمخاطر لم تعد بالضرورة ذات طابع العسكري لتمس الأمن القومي، بل أصبحت متنوعة ومتعددة على النحو الآتي

١. تهديدات القطاع الاقتصادي:

يرتبط الأمن السيبراني ارتباطاً وثيقاً بالقطاع الاقتصادي، وتحديداً بعد أن ساد ما يعرف بـ "عصر المال الإلكتروني"، والذي يقوم على استعمال المحفظة الالكترونية التي ساعدت على تزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي، ونتيجة ذلك أصبحت القطاعات الاقتصادية الأكثر تعرض للتهديدات السيبرانية من أي قطاعات أخرى، وبحسب البنك الدولي فإن قطاع الخدمات المالية يتعرض لهجمات سيبرانية أكثر من القطاعات الأخرى بنسبة ٦٥٪، على الرغم أن التقنيات الرقمية التي تستعمل في القطاع الاقتصادي ذا كفاءة عالية.

ومن جانب أثر الهجمات السيبرانية الموجهة نحو القطاع الاقتصادي على الأمن القومي، فإنَّه عند استهداف المؤسسات والبنوك المالية العالمية الكبرى في ظل الترابط بين بينها، يصبح تعرض إحداها لأي نوع من الهجمات قد يمتد أثره إلى شبكات المال والأعمال في العالم، ويؤدي إلى حالة من الفوضى المالية، وربما تؤدي إلى انهيار البورصات والأسواق المالية، مما يحدث خسائر مالية باهظة للدول، والتشكيك في منظومتها الأمنية، خاصة إذا طالت هذه الهجمات الودائع والمدفوعات الخاصة بالأفراد، الذين قد يسرعون إلى استرداد أموالهم أو إلغاء حساباتهم البنكية.

ومن ثم فإن الأمن القومي الاقتصادي الذي يعتمد على قدرة الدولة على حماية الأهداف والمصالح الاقتصادية وتعزيها على نحو مستدام، وبما يحقق قدرتها على مواجهة الظروف التي تهدد أو تعيق هذه الأهداف، قد تلاشى نسبة لحجم الهجمات السيبرانية المستمرة، وقد توقع خبراء الأمن السيبراني أنَّ الجرائم السيبرانية سوف تكلف العالم ١٠،٥ تريليونات دولار سنويًا بحلول عام ٢٠٢٥، وهذا يمثل أكبر تحويل للثروة الاقتصادية في التاريخ.

وهنا تلاحظ الدراسة، أن موضوع الأمن السيبراني والهجمات السيبرانية يشكل تهديداً أمنياً متعاظماً للأمن الدولي واقتصاده وذلك بسبب اعتماد الأخير على البنية التحتية المعلوماتية بوساطة التعاملات والتبادلات التجارية في منظومة الاقتصاد الدولي وتسعى الدول والمؤسسات الاقتصادية تدعيم برامج الحماية والدفاع والردع السيبراني لتقليل مخاطر وآثار الهجمات السيبرانية وتحصين البيئة السيبرانية.

٢. التهديدات السياسية

تتفاقم التهديدات غير التقليدية على الأمن القومي سياسياً نتيجة استعمال الفضاء السيبراني من قبل المنظمات الإرهابية التي من شأنها إلحاق الشلل بجميع أنظمة السلطة والعمل على قطع الاتصالات والسيطرة عليها ما بين جميع الوحدات المركزية، إلى جانب القدرة على تعطيل أنظمة الدفاع الجوي و تهديد أمن الدولة، ولا سيّما العمل على تهديد شخصيات سياسية مهمة و تدمير بعض شبكات المعلومات والأنظمة الالكترونية في المنشآت الوطنية لسرقة معلومات مهمة واختراقها لرؤساء الدول كبار الشخصيات السياسية لتهديدهم بها واستعمالها في العمليات الإرهابية.

بالإضافة إلى ما سبق، يمكن أن تثير الهجمات السيبرانية الفتن في الدولة عبر شحن الشعب ضد السلطة الحاكمة و اقناعهم بوجود العديد من الاحتياجات والحقوق التي لم توفرها لهم الدولة وذلك عبر استعمال وسائل التواصل الاجتماعي في بث تلك الأفكار التي يمكن أن تتطور وتؤدي إلى الخروج بمظاهرات غير سلمية تدمر الدولة، ومثال على ذلك: ثورات الربيع العربي التي قامت عام ٢٠١١ التي استطاعت إسقاط العديد من أنظمة الحكم ومنها بعض الدول لم تستطع العودة إلى حالة من الاستقرار حتى يومنا هذا وأصبحت بيئة خصبة للتنظيمات الإرهابية.

وترى الدراسة أنَّ المجال السياسي الرقمي الذي يتضمن جميع المعلومات الحساسة التي تتعلق بأجهزة الدولة كافة قادرة على خلق حالة من عدم الاستقرار في الدولة، بشن هجمات سيبرانية عبر إقامة حملات الفتن على وسائل التواصل الاجتماعي من أفراد هواة، وبذلك يتم تدمير الدولة نتيجة الجهل وبأقل التكاليف لمجرد استطاعة بعض الأفراد من التعامل مع بعض البرامج القرصنة الإلكترونية.

٣. التهديدات الاجتماعية والثقافة

يتشكل التهديد في هذا الشأن بعده ذروة الإنتاج الفكري وشموله على معلومات ذات طابع جماعي وفردي، مما يعرض الأمن القومي في بعض الحالات إلى تهديدات خطيرة مثل المظهر المادي لاستقرار المواطنين، والذي يرتبط بصورة مباشرة بالهواجس الأمنية للدولة، لذا فإنَّه يلعب دوراً مهماً في حماية الأمن القومي ويمكن أن يكبدها خسائر اجتماعية كبيرة.

وذلك عند المساس في الحياة الاجتماعية والثقافية ورفاهية الأفراد بتوجيه رسائل إعلامية ودعائية تثير الرعب ما بينهم، والتي تهدف إلى القيام بحملات نفسية ضد الدول المستهدفة، ومنها العمل على اختراق احدى صفحات الإلكترونية لمستشفى والعبث بأنظمة العلاج بهدف الإضرار بالمرضى، والدخول إلى أنظمة مصانع غداء الأطفال والتلاعب في مستويات ونسب المواد الغذائية التي من شأنَّها قتل الأطفال، أو حتى العمل على نشر المهمل للمعلومات بوساطة الوسائط الاجتماعية التي من طبيعتها أقل حماية من المواقع الأخرى، وما يزيدها خطورة أنَّها تحتوي على برامج متعددة المهام ومنها النصية و تشغيل وتحميل الملفات والوسائط والتطبيقات عبر الإنترنت.

ويمكن أن يعرض تكرار الهجمات السيبرانية المجتمع إلى حالة من تقويض الشعور بالأمان، والنظر بأنَّ العالم بأسره مهدد مما يزيد الدعم للسياسات المتشددة،

عبر المطالبة باتخاذ أشد الإجراءات والقرارات العسكرية التي من شأنّها مواجهة الجماعات الإرهابية، في حين أن افتقار الأفراد الى المعرفة الكافية الإلمام بالتعامل مع الفضاء السيبراني تؤدي الى إثارة مشاعر الرعب وعدم الثقة في السلطة وذلك بما يسمى بـ "العجز المكتسب" حيث يتم تعزيز اللامبالاة بمجرد أن الافراد لا يستطيعون تقدير الهجمات السيبرانية والحماية منها.

٤. تهديدات قطاع الصناعة

أدى التحول الرقمي في خطوط الإنتاج والأنشطة الهندسية وعمليات الصيانة إلى التطور في التهديدات السيبرانية على الأنظمة الصناعية، وقد أشارت بعض الدراسات أن غالبية الحكومات على الرغم ادراكهم لتلك التهديدات إلاّ أنّهم ليسوا مستعدين لمواجهتها، وفي المقابل بدأت تزداد اعداد هجمات الفدية التي تستهدف شبكات الأنظمة الصناعية ومؤسسات الطاقة ومنها: النفط والغاز، والمطالبة بدفع مبالغ مالية لإعادتها بما نسبته ٥٪ ما بين عامي ٢٠١٨- ٢٠٢٠، وما يزيد الأمر تعقيداً أن تلك الهجمات السيبرانية تقوم بتغيير أنشطتها باستمرار لتحقيق أهدافها بطرق مختلفة.

ومن جانب آخر، فإنَّ تعرض شركة "كولونيال بايب لاين" والتي تعد من أكبر مشغلي خطوط الأنابيب في الولايات المتحدة الأمريكية إلى هجمات سيبرانية عام ٢٠٢١ تسببت في اغلاق أنابيب البترول وانعدام وصوله إلى مناطق كبيرة في الولايات المتحدة نتيجة عدم القدرة على تشخيص الضرر واحتوائه، كان قد أثار المستهلكين وعزز حالة من عدم الرضا حتى تعالت أصواتهم، وبدأوا بالمطالبة باتخاذ إجراءات صارمة تجاه تلك القضية وحلها، وبذلك ليس من الضروري أن يكون هدف الهجمات دوافع مالية، فإنّها في بعض الأحيان ذات دوافع مختلفة ومنها أيديولوجية وسياسية مهددة بجميع الحالات للأمن القومي بتلك الدولة.

وقد صدر تنبيه من مصدر حكومي إلى مزودي البنية التحتية في عام ٢٠٢٠ يحذر من الدول القومية التي تعمل على توسع التهديدات للمرافق، وبروز المزيد من الجهات الفاعلة المتطورة التي تضع قطاع الطاقة بوصفه جزءاً من حملاتهم الأوسع، وقد ورد بالتنبيه ما يأتي: "الحذر من الدول القادرة، على الأقل على تنفيذ هجمات ذات آثار تخريبية مؤقتة ضد البنية التحتية الحيوية بوصفها إجراءاً رادعاً أو انتقامياً للتطورات الجيوسياسية الأخرى"، ويزداد هذا التحدي في المناطق النامية ومواقع الإنتاج ذات الأثر الكبير والعائد المنخفض للطاقة، منها مزارع الطاقة الشمسية، حيث وجد أن تكلفة تأمين موقع البنية التحتية الإلكترونية وتشغيلها والمراقبة الإضافية يمكن أن تتجاوز أي إيرادات تتحقق من عمليات الموقع.

ثانياً: دور الردع في مواجهة التهديدات اللامتماثلة:

عدت هذه العلاقة الجديدة بين تاثير التهديدات اللامتماثلة وأدوات كبحها ووسائلها والحد منها والتي تعرف بوسائل الردع وأدواتها محط عناية أغلب الباحثين والمختصين بالشأن السياسي والأمني لعدة اعتبارات أهمها صعوبة تحديد ملامح التهديدات اللامتماثلة على نحو يؤمن الوصف الدقيق لها وماهي حدودها وأبعادها كونها وليدة مجموعة من المتغيرات التي أسست لتكتيكات اختلفت بشكل جذري عن التهديدات التقليدية، فالتهديدات اللامتماثلة تتضمن مجموعة كاملة من الوسائط المختلفة من الحرب بما في ذلك القدرات النظامية والتكتيكات غير النظامية والأعمال الإرهابية، بما في ذلك العنف العشوائي والإكراه والإجرام". في مستوى أعلى من التهديد يشار في الكثير من الدراسات إلى "الحرب اللاتماثلية" Asymmetric War، وهو النمط الغالب في حروب اليوم لذلك تسمى بـ"حروب العصر"، بحيث تكون الأطراف المتحاربة غير متساوية ومتفاوتة في القوى والوسائل والتنظيم، و تتخذ عدة أشكال، ويمكن قراءتها على ثلاثة

مستويات، فهناك المستوى الميداني يتميز بـ (كثرة العمليات السرية، والمفاجأة، والغدر والحيل و ما إلى ذلك) والمستوى الإستراتيجي العسكري ويتضمن (حرب العصابات، والحرب الخاطفة، وغيرها)، والمستوى الإستراتيجي السياسي (حرب ذات معطى ثقافي وأخلاقي وديني) لذلك، يمكن وصف النهج اللاتماثلي بـ (سلاح الضعيف) الذي هو سمة فاعلين لا يملكون إلا وسائل محدودة جداً لكن قدرتهم على الإضرار كبيرة، ومنها استعمال طائرات النقل المدني مثلا، في مهاجمة أهداف مدنية وعسكرية، فإنَّه من المعقد تقدير التهديد وهذه الصعوبة مردها سببان: - العقبة الأولى: وتتمثل في تقويم التهديد تتمثل في تحديد الدرجة الكافية للتهديد التي بموجبها يمكن أن يلحق هذا التهديد ضرراً بنقطة حيوية بالنسبة للدولة. أما العقبة الثانية: مرتبطة بعدم ثبات الإدراك وسرعة تغيره بين الذاتي أو الموضوعي، وهذا يقود إلى أمرين، استحالة معرفة إنَّ كان كيان ما يشكل تهديداً أولاً، أضف إلى ذلك أن إدراك التهديد إذا كان مغطى بالخوف فإنَّه يقوّض القدرات العقلانية لمختلف الفواعل، ويشل كل محاولة لوضع سياسات أمنية مناسبة، ومن هنا فأنَّ الردع في التهديدات اللامتماثلة سيكون أقل تاثيراً من الردع في التهديدات التقليدية، وبذلك فأن مضامين الردع قد تغيرت مع التهديدات اللامتماثلة ومن نواحي عدة أبرزها قد ارتبط بجوهرية تلك التهديدات وتشعبها وغموضها فموازين القوى التقليدية ذات ملامح محددة، أما اللاتماثل فذو كينونة تختلف من ناحية الفواعل ومستوياتها التي تؤثر في البيئة الدولية وأهمها (الدول، والمنظمات، والمؤسسات الاقتصادية، والأفراد) فضلاً عن تعدد الأدوات المستعملة في التهديدات اللامتماثلة وفي مقدمتها جانب المعلوماتية والتكنولوجيا والأسلحة السيبرانية.

عند التطرق إلى وصف البيئة الأمنية بعد انتهاء الحرب الباردة وبعد توسيع مفهوم الأمن ما هو إلاّ نتيجة لظهور مخاطر وتهديدات جديدة على الساحة الدولية

تتجاوز التهديدات العسكرية، أي انتقال التهديد من تهديد تقليدي إلى تهديد غير تقليدي بعبارة أخرى غير واضح المعالم، وهي لا تصدر من وحدات سياسية (الدول) بل هي تهديدات مجهولة المصدر وغير معروفة، تعرف هذه التهديدات بالتهديدات اللاتماثلية أو اللاتناظرية أو غير المتكافئة وتكون بين فاعلين غير متكافئين. كما سبق ذكره والاختلاف أو عدم المساواة يكمن في القوة وعادة ما يكون هذا النمط من التهديدات، وسيلة للتعويض عن نقص في الموارد للطرف الضعيف الذي يستعمل التهديدات بوساطة الاعتماد على أساليب ووسائل متعددة يستهدف بوساطتها المساس بنقاط الضعف للطرف الأقوى، وتتميز التهديدات اللاتماثلية بمجموعة من الخصائص هي:

أ. إنّها من طبيعة غير عسكرية، وشهدت صعوداً في مرحلة ما بعد الحرب الباردة، حيث شملت الدول الكبرى صناعياً التي لا تزال تعاني من خطر الحرب التقليدية بين الدول بعضها ضد بعض الآخر.

ب. إنَّها بنسبة كبيرة تصدر من فواعل غير دولية والرجعيات (الدول والأقاليم والمجتمعات والأفراد).

إنَّها تؤثر على أمن جميع الفواعل وجميع الخصائص المناسبة للدول وتعاملاتهم مع بعضهما.

ج. تأخذ عادة شكل الخطر قبل أن تصبح تهديداً فإن كان نوع التهديد عادة معرّفاً ويلحق ضرراً مباشراً، فإن التهديد أو الخطر على خلافه غير قابل للقياس ومشكوك فيه.

د. يعد الأمن السيبراني أحد أشكال اللاتماثل في التهديد هو حزمة من الاجراءات التي تأخذ بنظر الاعتبار تأمين حماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم والتلف أو السرقة أو الوصول غير المصرح به

للخوادم والبيانات فضلاً عن التعطيل أو عرقلة الخدمات التي تقدمها لذلك فأنَّ إدارة المخاطر المعلوماتية يمكن استعمالها في حماية البيئة السيبرانية التي ترتبط بها الموارد البشرية والمادية للدولة

ثالثاً: أوجه الردع وبذلك يتضح أن الردع يتكون من جزئين:

الأول (مادي): وهو يشمل كل أنواع القوة وأدواتها ما يكفي لإنزال العقاب بالخصم.

الثاني (معنوي أو نفسي): يهدف إلى التأثير النفسي على الخصم بوساطة إقناعه بجدوى الرضوخ للرادع وعدم الرضوخ يعني ارتفاع ثمن العند والتشبث بالمواقف بشكل لا يستطيع تحمله.

رابعاً: الردع وتوازن التهديد

انطلاقاً من نظرية توازن القوى التي شكلت محوراً أساسياً في تفسير ظاهرة العلاقات الدولية والتي تروم فيها الدول إلى خلق حالة من التوازن النسبي الذي يحقق لها مكاسب متعادلة في جانبها الأغلب، وفي خضم التقدم والسعي الحثيث للدول لتبني سلوكيات وسياسات تحقق لها المصلحة العليا لأهدافها تغوّ ت الاتجاهات وزادت حجم التهديدات ونوعيتها في بيئة النظام الدولي، ومن هذا المنطلق سلط الباحثون في الشأن السياسي والدولي على وضع أُطر نظرية تفسر وقائع الأحداث والتي أسفرت عن ظهور مايعرف بـ(نظرية توازن التهديد).

ترتكز نظرية توزان التهديد على قوام اكتساب القوة وتعظيمها من أجل التهديد وليس الدفاع والمعيار بين نظريتي توازن القوى وتوازن التهديد هو الرغبة في امتلاك القوة والمقسمة بين القوة الهجومية والدفاعية، ويمكن بيان تفسير دلالات القوتين تبعاً للغايات التي تتوخاها، فالقوة الهجومية تكون هدفها توزان التهديد،

أما الدفاعية فإنَّها تسعى لتحقيق مبدأ توازن القوى، وعلى نحو أكثر دقة فأنَّ المخرجات الناتجة والناشئة عن اختلال توازن القوى يمكن أن تؤسس الى تبني اتجاهات نظرية توازن التهديد كون الأخير يعد توازناً قسرياً وأمراً حتمياً يعطي انطباعات بأنَّ التهديدات إذا لم تصل حد التوزان فأنَّها ستكون مخاطر أمنية تمس الأمن القومي للدول.

تعد المرحلة الأولى من توازن التهديد حرجة جداً كونها تتعلق بعملية ادراك التهديد وتشخيصه على نحو الدقة وهذا يؤسس لترتيبات لاحقة كونه الادراك واحداً من أبرز متغيرات نظرية توزان التهديد وهذه المرحلة تتطلب القيام بعملية احاطة شاملة لماهية التهديدات في البيئة المحيطة وفق نماذج تحليلية تحدد حجم التهديد ومستواه ودرجة الحراجة والتأثير والمدة الزمنية المتوقعة لتحول التهديد إلى خطر يمس منظومة الأمن القومي للدولة، وبهذا المجال فأن النظرة الموحدة لتشخيص التهديد يمكن أن تضع رؤية واضحة وشاملة لتوافر قدرات وامكانيات تشكل حالة من التهديد المقابل وهنا تتحق نظرية توزان التهديد، بذلك سيكون الردع أحد أشكال توازن التهديد أو قد يجعلنا أمام هذه الحالة لعدة اعبتارات، فعندما تمتلك الدولة قدرات وموارد القوة وموارها وعواملها ومقوماتها سينتج عن ذلك تبني سلوكيات دولية تسعى إلى تحقيق جملة من الأهداف قد تشكل جزءاً كبيراً منها تهديداً لمصالح دولٍ تملك هذا من جانب، من جانب آخر فإنَّ عملية الإذعان والمسايرة وتجنب رفع مستوى التهديد والإجراءات الاستفزازية ستكون عنصراً داعماً لنظرية توازن التهديد.

الخاتمة

يتضح بأن الأمن السيبراني عد بعداً خامساً يتصف بالحداثة والأهمية كونه ارتبط ارتباطاً وثيقاً بكل المجالات نظراً لأهمية التكنولوجيا وعالم التقنية وظهور مايعرف بالذكاء الاصطناعي، ومن هذا المنطلق فإن تاثير مرتكز الأمن السيبراني كان الوقع الأكثر أهمية وتاثيراً على منظومة الأمن القومي فعالم الاقتصاد والسياسية والتواصل الاجتماعي الإلكتروني شكّل محور عمل الأمن السيبراني وبدون تأمين هذا البعد تكون منظومة الأمن القومي الأكثر خطراً من تهديدات القوة السيبرانية وهنا نعني بأن القوة السيبرانية تتمثل بالجانب المسمى بـ Hardwareو Soft ware والذي يقصد بها الأنظمة والبرامجيات والتطبيقات الرقمية التي تبحث عن الثغرات في البرامج والشبكات وتعمل على تأمينها من الاختراق والتجسس الرقمي، فضلاً عن الأجهزة التي تعمل في مراكز SOCوالتي تؤمن السيطرة الرقمية على قواعد البيانات وسلسلة العمليات المعلوماتية وضمان سلامة تدفق المعلومات ومنع الدخول غير المصرّح به على الأجهزة والشبكات والحواسيب الرقمية،ومن جانب آخر فقد اشتملت أبعاد التهديدات اللامتماثلة على جملة من المتغيرات التي تختلف عن التهديدات بين الأطراف المتعادلة، فالفواعل التي تنفذ التهديدات غير متكافئة فضلاً عن عدم القدرة في معرفة حدودها وآليات الحد من خطورتها وردعها، ومن هنا كانت تلك التهديدات في مرمى نظريات الردع بيّد أن الأخير قد اكتسب معنىً آخر فرضته بيئة التهديدات اللامتماثلة، مما أدى إلى تبني استراتيجيات ردع غير تقليدية وتتسم بقدرتها على الحد بشكل كبير من خطورة التهديدات اللامتماثلة، ومن جانب آخر كانت نظرية توازن التهديد أحد أبرز الطروحات الفكرية في ميدان الدراسات الدولية والاستراتيجية والتي تأطرت بممارسات عملية من الدول الفواعل وبوساطة المستويات كافة (أفراداً، أومؤسسات، أومنظمات، أو شركات، أو دول،أو تحالفات) لتحقق شكلاً ونمطاً

جديداً من ممارسة الردع إزاء التهديدات اللامتماثلة، وستكون هذه الممارسات فاعلة لتحقيق الأهداف المتوخاة من الردع إضافة إلى ذلك فان الاستراتيجيات المستعملة في الردع ستعتمد على تكتيكات خاصة تنسجم مع طبيعة وأثر التهديدات اللامتماثلة وفي مقدمتها تهديدات الأمن السيبراني.

المصادر العربية

١-رمضان، شريف (٢٠٢١)، الحرب السيبرانية ومدى وملاءمتها مع القانون الإنساني، مجلة كلية الشريعة والقانون بتفهنا الأشراف- دقهلية، المجلد ٤، العدد ٢٣.

٢- ممدوح، إيناس (٢٠٢٢)، دور الأمن السيبراني في مواجهة الإرهاب الإلكتروني، مجلة العلوم القانونية والاقتصادية، المجلد ٦٤، العدد ١.

٣- شنوف، زينب (٢٠٢٠)، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، المجلة الجزائرية للأمن والتنمية، العدد ٢، المجلد ٩.

٤- الصابري، بهاء (٢٠١٧)، الحروب الالكترونية: اللاتماثل في التهديد، مجلة الأزمات والبحوث السياسية، العدد ٢ .

٥-أوراغ، كريم (٢٠٢١)، الاختراق الالكتروني في الفضاء السيبراني وأفضل الطرق للحماية منه، مجلة التطوير العلمي للدراسات والبحوث، العدد ٤، المجلد ٢.

المصادر الأجنبية

1. Rashid, Awais (2019). **The Cyber Security Body of Knowledge, University of Bristol**. United Kingdom**.**
2. International Telecommunications Union (ITU), (2008). **Overview of cyber security. Data Networks, Open System Communications and Security – Telecommunication Security.**
3. Pawlicka ،A. ،Choras M. & Pawli (2021) ،**The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good, Vol 25.**
4. Christen, M., Gordijn, B., Loi, M. (2020), **The Ethics of Cybersecurity,** The International Library of Ethics, Law and Technology, vol 21.