الجمهورية العربية السورية
جامعة دمشق
كلية العلوم السياسية
قسم العلاقات الدولية

التهديدات غير التقليدية وتأثيرها على الاستراتيجيات الأمنية للدول: التنافس الصيني - الأمريكي في مجال الأمن السيبراني أنموذجاً

Non – Traditional Threats and their Impact on States' Security Strategies: The Chinese – American Competition in the Field of Cybersecurity as a Case Study

إعداد: محمود حوش

المشرف العلمي: د. نمير عيسى

ملخص:

تسلط هذه الدراسة الضوء على علاقة ظهور التهديدات الأمنية غير التقليدية بوجود تحولات في طبيعة الاستراتيجيات الأمنية المصممة للتعامل مع تلك التهديدات في ظل ما تفرزه من أنماط ومستويات جديدة للتنافس الدولي، كما هو الحال بالنسبة للتهديدات السيبرانية التي أنتجت أنماط مستجدة من الاستجابات الاستراتيجية التي تتبعها الدول في ردع ما يشكل تهديداً أمنياً سيبرانياً، وذلك لكون هذا النمط من التهديدات في علاقات الدول المتبادلة قد فرض حالة من التنافس الدولي مختلفة عن تلك التي تنشأ في ظل التهديدات الأمنية التقليدية، وتجادل هذه الدراسة بأن قيام الصين بتعريف المجال السيبراني باعتباره يمثل مجالاً لإحداث التهديدات الأمنية، وما رافق ذلك من طرحها لمجموعة من الإجراءات والسياسات التي اتخذتها على المستويين الإقليمي والدولي بغاية التعامل مع ما يفرزه هذا المجال من تهديدات، قد أدى إلى تعزيز حالة التنافس الدولي مع الولايات المتحدة الأمريكية، وذلك لأن هذه الإجراءات والسياسات ينظر لها على أنها مصممة بغاية التأثير على بنية النسق الدولي القائم واستبدال المعايير والمؤسسات والقواعد القائم عليها بمجموعة أخرى بديلة تتناسب مع مصالح الصين، وهذا الأمر يدفع بالولايات المتحدة الأمريكية إلى بناء استجابة استراتيجية تؤدي إلى ردع الصين من توظيف التقنيات السيبرانية في إحداث تحولات على مستوى النسق الدولي تؤثر على مكانتها ضمنه، وتستنتج الدراسة بأن طبيعة الإجراءات والسياسات الصينية المرتبطة بتوظيف أدواتها السيبرانية في التأثير على بنية النسق الدولي القائم، قد أدى إلى تنويع خيارات الردع الاستراتيجي الأمريكي واتخاذ مجموعة مستجدة من أنماط الردع تجاه السلوك الصيني في هذا المجال، وهي أنماط تتراوح ما بين "الردع بنزع الشرعية"، "الردع بالعقاب"، و "الردع بالإنكار".

الكلمات المفتاحية: التهديدات غير التقليدية – الاستراتيجيات الأمنية – التنافس الدولي – التهديدات السيبرانية – الصين – الولايات المتحدة الأمريكية – النسق الدولي – الردع.

مقدمة:

تعتبر ظاهرة الأمن من الموضوعات أو الظواهر الأساسية التي تتأسس عليها علاقات الدول وتفاعلاتها المتبادلة، وهي تنطوي في جوهرها على غياب التهديدات التي تتعرض لها الدولة كوحدة مرجعية للأمن تجاه مختلف أنماط المخاطر التي تواجهها أو تحييدها قدر الإمكان، وعلى اعتبار بأن صيغة التهديدات والمخاطر الأمنية التي باتت تواجه المجتمعات والدول أصبحت متنوعة ومتعددة الأبعاد، فإن هذا الأمر قد أفرز جدلاً نظرياً بين عدة تيارات ومدارس أمنية حول كيفية تحديد الظاهرة الأمنية ودراستها، والذي يبدو بأنه تمحور حول ثلاثة أسس عامة، أولاً الجدل حول تحديد الوحدة المرجعية للأمن (فيما إذا كانت الدولة هي الوحدة المعنية بدراسة المخاطر والتهديدات، أم المجتمع أو الفرد)، وثانياً الجدل حول تحديد طبيعة المخاطر والتهديدات (فيما إذا كان البعد العسكري هو البعد الوحيد للأمن أو أن هنالك أبعاداً أخرى غير عسكرية)، وهما ما يعرفان بالجدل الانطولوجي، وثالثاً الجدل حول كيفية دراسة الأمن (فيما إذا كان الأمن يدرس بشكل موضوعي في تحديد المخاطر والتحديات، أم أن الإدراكات والتصورات الذاتية تمارس دوراً مؤثراً في تحديد طبيعة التهديدات التي تواجه مختلف الوحدات المرجعية)، وهو ما يعرف بالجدل الابستمولوجي، وقد كان من نتيجة هذا الجدل أن تعددت الرؤى حول موضوع الأمن، الأمر الذي أفرز معه وجود أنماط مستجدة من التنافس الدولي، وذلك على اعتبار أن التنافس ينشأ بين دولتين أو أكثر في ظل بيئة تتسم بالتهديد المتبادل، فإن تحول صيغة التهديدات الأمنية التي تتعرض لها الدول سينتج عنها وجود تحولات في حالة التنافس الدولي، كما أن تغير صيغة التهديدات الأمنية سينتج عنها وجود أنماط مستجدة من الاستراتيجيات الأمنية، وذلك لأن الاستراتيجيات الأمنية هي الأداة التي تستخدمها الدولة في مواجهة المخاطر الأمنية في ظل بيئة تتسم بالتنافس الدولي.

يمثل المجال السيبراني، بما ينطوي عليه من تقنيات التكنولوجيا المتقدمة وشبكات الاتصالات والانترنت، أحد الصيغ المستجدة غير العسكرية للتهديدات الأمنية التي باتت تواجه الدول، وهو في جوهره ينطوي على مخاطر توظيف هذه التقنيات التي تمتلكها إحدى الدول لإحداث تأثيرات وتهديدات سياسية واقتصادية وعسكرية ومجتمعية لدولة أخرى، وإن توظيف هذا المجال في العلاقات المتبادلة التي تحدث بين دولتين أو أكثر ينتج عنه وجود حالة من التنافس الدولي، وخصوصاً عندما تسعى إحدى الدول من خلال استخدام التقنيات السيبرانية إلى تعزيز مكانتها الدولية على حساب مكانة الدول الأخرى، وهي مكانة تتحدد بشكل أساسي بصياغة وتصميم قواعد ومؤسسات النسق الدولي، وعلى اعتبار بأن تزايد حالة التنافس الدولي الناتجة عن توظيف واستخدام التقنيات السيبرانية تنطوي في جوهرها على التأثير على مكانة الخصوم أو المنافسين، فإن هذا الأمر سيدفع بالدولة أو الدول التي توظف ضدها هذا النمط من التهديدات، إلى صياغة استراتيجية أمنية للتعامل مع المخاطر الناجمة عن استخدام التقنيات السيبرانية، وهي في جوهرها تنطوي على ردع أو منع الخصوم من إمكانية زيادة أو تعزيز نفوذهم الدولي.

إن تحليل صيغة التنافس الأمريكي – الصيني في مجال الأمن السيبراني بوصفه أحد الأنماط المستجدة أو المستحدثة في العلاقات بين الدولتين، يستلزم معه في بداية الأمر تحليل الصيغة التي تدرك بها الصين المجال السيبراني بوصفه قضية تهديد أمني يفرض عليها مجموعة من المخاطر والتحديات، أي بشكل أساسي على الرؤية التي تتبناها النخب والمؤسسات السياسية الصينية لتقنيات التكنولوجيا والاتصال والتي تعمل على تحويل هذا المجال بوصفه يرتبط بإحداث أنماط محددة من التهديدات السياسية والمجتمعية والاقتصادية، وهي رؤية تتحدد بشكل أساسي بالمفاهيم الثقافية التي كونتها الصين عن دور التطورات التكنولوجية في تطوير قوة الدولة وتعزيز مكانتها الدولية، وبالتالي المخاطر المتصورة بالنسبة للصين تنطوي في جوهرها على توظيف تقنيات التكنولوجيا لإحداث تأثيرات على قوتها ومكانتها الدولية، وهذا الأمر نجم عنه اتخاذها لمجموعة من الإجراءات التي تستهدف من خلالها تحييد التهديدات التي يفرضها هذا المجال، ولكن مع توسيع الصين لهذه الإجراءات على المستوى الإقليمي والدولي، والتي ترافقت مع طرح مجموعة من المبادرات والمشاريع مثل إنشاء "منظمة المؤتمر العالمي للأنترنت"، و مبادرة "طريق الحرير الرقمي"، قد أدى إلى وجود صيغة من التناقض مع الولايات المتحدة الأمريكية، وذلك لكون توسيع هذه الصيغة الأمنية تنطوي في جوهرها على بناء معايير وقواعد ومؤسسات للمجال السيبراني، أي لبناء نسق دولي للمجال السيبراني يكون مهيمن عليه من قبل الصين وبعيداً عن مركزية الولايات المتحدة الأمريكية عليه.

إن تحديد سلوك الصين في المجال السيبراني على المستوى الدولي بكونه ينطوي على تعزيز التنافس مع الولايات المتحدة الأمريكية، وذلك لكونه ينطوي على محاولة بناء نسق دولي للمجال السيبراني يكون أكثر تمركزاً حول الصين، نتج عنه وجود استجابة من قبل الولايات المتحدة الأمريكية، وهي في جوهرها تنطوي على بناء استراتيجية أمنية للتعامل مع ما يفرزه السلوك الصيني من مخاطر وتحديات تؤثر على النسق الدولي القائم وعلى مكانة الولايات المتحدة ضمنه، أي لردع الصين ومنعها عن تحقيق أهدافها التي تتبناها، وعلى الرغم من أن تصميم استراتيجية الردع قد اتخذ أساليب مختلفة، وذلك وفقاً لاختلاف أولويات الإدارات الأمريكية المتعاقبة (باراك أوباما – دونالد ترامب – جو بايدن) في التعامل مع ما يمثله السلوك الصيني من مخاطر للولايات المتحدة الأمريكية، إلا أن الردع قد شكل المبدأ العام في الاستجابة الاستراتيجية للولايات المتحدة.

منهج الدراسة:

المنهج الوصفي – التحليلي: الذي يقوم على أساس توصيف مفهوم التهديدات غير التقليدية والأبعاد المرتبطة بها، وتقديم المقاربات النظرية التي تعاملت مع الظواهر الأمنية الجديدة غير العسكرية، وكذلك أيضاً على توصيف مفاهيم التنافس الدولي والاستراتيجيات الأمنية والتحولات التي طرأت عليهما، بالإضافة إلى أنه يقوم على أساس تحليل صيغة العلاقة التي تؤثر من خلالها تحول طبيعة الموضوعات الأمنية على الصيغ المستجدة للتنافس الدولي وللاستراتيجيات الأمنية، وبشكل محدد لتحليل تأثير التهديدات السيبرانية على أنماط التنافس الدولي وتحولات الاستراتيجيات الأمنية للدول.

المنهج التجريبي: الذي يقوم على أساس اختبار مدى قوة العلاقة الارتباطية بين الكيفية التي تدرك من خلالها الصين المجال السيبراني بوصفه قضية تهديد لأمنها القومي وانعكاسات ذلك على سلوكها الإقليمي والدولي المرتبط بطرح مجموعة من السياسات والمبادرات التي تهدف إلى بناء نسق دولي لهذا المجال، وذلك بناءً على افتراضات مدرسة كوبنهاجن للأمن، وأيضاً على أساس اختبار مدى تأثير المخاطر التي تمثلها سياسات الصين الإقليمية والدولية في المجال السيبراني بالنسبة للولايات المتحدة الأمريكية على تبنيها أنماط مستجدة من الردع الاستراتيجي لمنع الصين من تحقيق أهدافها، وذلك وفقاً لافتراضات "الموجة الخامسة من الردع".

تقسيم الدراسة:

تنقسم هذه الدراسة إلى ثلاثة فصول، فضلاً عن مقدمة وخاتمة ونتائج، حيث يتناول الفصل الأول موضوع التنافس والاستراتيجيات الأمنية في ظل التهديدات غير التقليدية: مدخل نظري، وذلك من خلال مبحثين، حيث يتطرق المبحث الأول إلى التهديدات غير التقليدية واتجاهاتها النظرية، وذلك من خلال ثلاثة مطالب، الأول: مفهوم التهديدات الأمنية غير التقليدية، الثاني: الأبعاد الجديدة للأمن، والثالث: الاتجاهات النظرية المفسرة للتهديدات الأمنية الجديدة، أما المبحث الثاني فأنه يعالج تحولات الاستراتيجيات الأمنية وأنماط التنافس الدولي، وذلك من خلال ثلاثة مطالب، الأول: الطبيعة المتغيرة للاستراتيجيات الأمنية، الثاني: أنماط التنافس الدولي في ظل التهديدات الأمنية الجديدة، والثالث: التهديدات السيبرانية والاستراتيجيات الأمنية للدول الكبرى.

يعالج الفصل الثاني موضوع الأمن السيبراني من المنظور الصيني وانعكاساته الإقليمية والدولية، وينقسم إلى مبحثين، حيث يحلل المبحث الأول التهديدات السيبرانية في الرؤية الصينية واستجابتها الأمنية، ويتفرع عنه ثلاثة مطالب، الأول المفاهيم الصينية للمجال السيبراني وتأثيرها على تحديد الرؤية الأمنية، والثاني تصورات الصين للتهديدات السيبرانية وسياقاتها والثالث الأمن السيبراني و" أجندات" السلطة السياسية الصينية، أما المبحث الثاني فأنه مخصص لتحليل الأمن السيبراني الصيني في سياساتها الإقليمية والدولية، وذلك من خلال ثلاثة مطالب، الأول الأمن السيبراني في إطار منظمة شنغهاي للتعاون، والثاني منظمة المؤتمر العالمي للأنترنت وأجندات الأمن السيبراني العالمية، والثالث طريق الحرير الرقمي وانعكاساته على مكانة الصين الدولية.

يحلل الفصل الثالث الاستجابة الاستراتيجية للولايات المتحدة الأمريكية تجاه سلوك الصين في المجال السيبراني، وذلك من خلال مبحثين، حيث يعالج المبحث الأول المنظور الأمريكي للتهديدات السيبرانية الصينية وآليات ردعها، وذلك من خلال ثلاثة مطالب، الأول سياسات الصين السيبرانية وتهديدات النسق الدولي، والثاني تهديدات الصين السيبرانية في المجال العسكري، والثالث أنماط استراتيجيات الردع تجاه سلوك الصين، أما المبحث الثاني فأنه يتطرق إلى بناء التحالفات الأمريكية للمجال السيبراني وتقييد السلوك الصيني، وذلك من خلال ثلاثة مطالب، الأول تحالف "الكواد" وتعديل سلسلة التوريد العالمية لأشباه الموصلات، والثاني التعاون الأمريكي – التايواني – الكوري الجنوبي وزيادة قدرات الولايات المتحدة السيبرانية، والثالث الشراكة الأمريكية – الأوروبية وضوابط التصدير على أشباه الموصلات.

نتائج الدراسة:

١. التحول من مواجهة التهديدات العسكرية إلى التهديدات غير العسكرية ينعكس على تحديد نمط ومستوى التنافس الدولي وعلى السلوك الاستراتيجي للدولة في ردع التهديدات غير التقليدية. إذ أن تنوع صيغة التهديدات التي باتت تواجهها الدول، والتي أصبحت تتخذ أبعاداً سياسية واقتصادية واجتماعية، قد أدى إلى فرض مجموعة من المخاطر والتحديات التي تختلف في جوهرها عن تلك التي تفرضها التهديدات العسكرية، والتي انعكست على وجود تحولات في نمط ومستوى التنافس الدولي، إذ أن التحول من وجود تهديد عسكري إلى وجود تهديد اقتصادي، قد حول نمط التنافس الدولي من النمط الجيوسياسي إلى نمط التنافس الجيو اقتصادي، كما أن وجود التهديدات غير العسكرية للأمن قد حول مستوى التنافس من مستوى النظام الدولي، إلى مستوى النسق الدولي، وذلك لكون هذا النمط من التهديدات مصمم للتأثير على المعايير والقواعد والمؤسسات الدولية، وقد كان من نتيجة هذا الأمر أن تحولت طبيعة الاستراتيجيات الأمنية للدول، إذ أن وجود أنماط وصيغ مستجدة من التهديدات والتنافس الدولي قد أدى إلى وجود استجابات استراتيجية جديدة في التعامل مع المخاطر غير العسكرية، وهذا ما التعبير عنه من خلال تطوير "موجات الردع الاستراتيجي"، التي أوضحت كيفية تحول الاستجابات الاستراتيجية للدول من مواجهة التهديدات العسكرية، إلى مواجهة التهديدات المجتمعية، إلى مواجهة التهديدات الهجينة التي تنطوي على استخدام أبعاد مختلفة للقوة الاقتصادية والمجتمعية والتكنولوجية، وبالتالي فإن الفرضية الأولى **محققة**.

٢. تزايد حجم التهديدات السيبرانية في العلاقات المتبادلة بين الدول الكبرى يؤدي إلى تعزيز التنافس الدولي حول تحديد بنية النسق الدولي ويدفع نحو بناء استراتيجيات أمنية. إذ أن اعتبار المجال السيبراني بما ينطوي عليه من تقنيات تكنولوجيا واتصال باعتباره قضية تهديد أمني تواجه الدولة، أي أن إسقاط المعاني والدلالات على هذا المجال من قبل الفواعل والنخب السياسية في الدولة باعتباره ينطوي على إحداث مخاطر أمنية محددة، ينعكس على وجود سلوكيات محددة من قبل مؤسسات السلطة السياسية بغاية التعامل مع ما يفرضه المجال السيبراني من تحديات ومخاطر مختلفة، وينعكس على سلوكها الإقليمي والدولي بغاية وضع المعايير والقواعد وصياغة المؤسسات التي يجب أن تحكم سلوك الدول، أي بغاية بناء نسق دولي لهذا المجال، وهذا ما ينتج عنه وجود تصادم في المصالح مع الدول التي ترفض صيغة النسق الدولي التي طرحته الدولة الساعية لبنائه، وبالتالي ينشأ تنافس دولي حول تحديد بنية النسق الدولي لهذا المجال، وهذا ما يدفع بالدولة التي ترى بسلوك الدولة المنافسة بهدد لها مصالحها، إلى صياغة استجابة استراتيجية تنطوي في جوهرها على ردع المنافسين من توظيف التقنيات السيبرانية لبناء وتصميم نسق دولي يتعارض مع مصالحها، وبالتالي فإن الفرضية الثانية **محققة**.

٣. إضفاء الصين للطابع الأمني على المجال السيبراني بوصفه يرتبط بإحداث تهديدات سياسية ومجتمعية واقتصادية ينعكس على طبيعة سلوكها الإقليمي والدولي في تحديد بنية النسق الدولي لهذا المجال. حيث أن الصيغة التي تصغى من خلالها النخب والمؤسسات السياسية الصينية الصيغة الأمنية على تقنيات التكنولوجيا والاتصال، والتي تم "ترجمتها" من خلال مفاهيمها الثقافية التي تتبناها حول المجال السيبراني، وهي "السيادة السيبرانية"، و "القوة السيبرانية الكبرى"، قد أدت إلى تعريف المجال السيبراني إلى كونه ينطوي على إحداث التهديدات السياسية والمجتمعية، وتهديدات للبنية التحتية الحرجة للدولة، وتهديدات التنافس مع الدول التي تمنعها من تحقيق موقع القوة السيبرانية الكبرى، وتحديدها لأن التقنيات السيبرانية تنطوي على هذه المخاطر، قد نتج عنه وجود سلوكيات محددة للتعامل مع تهديدات المجال السيبراني، والتي تجسدت في "الاستراتيجية الوطنية للأمن السيبراني"، و "استراتيجية تنمية الاقتصاد الرقمي"، و "استراتيجية الاندماج العسكري – المدني"، وقد أدت إلى وجود سلوكيات إقليمية ودولية لتحديد المعايير الأمنية التي تعكس لها تصوراتها للمجال السيبراني، وبناء القواعد والمؤسسات الدولية التي تحكم هذا المجال، وهو ما تجسد في إطار "منظمة شنغهاي للتعاون"، و "منظمة المؤتمر العالمي للأنترنت"، و "مبادرة طريق الحرير الرقمي"، وهي جميعها مصممة لتحديد بنية نسق دولي للمجال السيبراني ويعكس لها هيمنتها على هذا المجال، وبالتالي فإن الفرضية الثالثة **محققة**.

٤. تؤدي مساعي الصين التنافسية في المجال السيبراني مع الولايات المتحدة الأمريكية في التأثير على بنية النسق الدولي القائم إلى صياغة أنماط مستجدة من سلوك الردع الاستراتيجي الأمريكي. إذ أن طرح الصين لمبادراتها حول المجال السيبراني، التي تنطوي على محاولة بناء وتعميم نسق دولي للمجال السيبراني، قد نتج عنه وجود تنافس في المصالح مع الولايات المتحدة الأمريكية، وذلك لكونها ترى بأن هذه المساعي تنطوي على مخاطر تعديل النسق الدولي الليبرالي القائم والذي يعكس لها مصالحها، وهذا ما استلزم معه وجود استجابة استراتيجية أمريكية للتعامل ما يفرزه السلوك الصيني من مخاطر وتحديات، وهي استجابة تقوم بشكل أساسي على أساس ردع الصين ومنعها من تعديل النسق الدولي القائم، وقد اتضح سلوك الردع الذي اتبعته الولايات المتحدة الأمريكية، من خلال الاستراتيجيات المتبعة من قبل الإدارات الأمريكية المتتالية، بدءً من "الردع بنزع الشرعية" المتبع من قبل إدارة الرئيس باراك أوباما، و "الردع بالعقاب" من قبل إدارة الرئيس دونالد ترامب، و "الردع بالإنكار" المتبع من قبل إدارة الرئيس جو بايدين، وبالتالي فإن الفرضية الرابعة **محققة**.

الخاتمة:

أعطى السلوك الصيني في المجال السيبراني، من ناحية كيفية تفاعلها مع هذا المجال كقضية تهديد أمني يفرض عليها، وانعكاساته على سلوكها الإقليمي والدولي، تطبيقاً واضحاً لافتراضات مدرسة كوبنهاجن بمقاربتها "حول الأمننة وترجمة الأمن"، و "المجمعات الأمنية الإقليمية"، إذ أن المعاني والدلالات التي تسقطها النخب والمؤسسات السياسية الصينية تجاه المجال السيبراني قد عملت على تحويله من مجرد قضية عادية إلى قضية تهديد أمني تواجه الصين من خلال ثلاثة جوانب، وهي التهديدات السياسية والمجتمعية المرتبطة بالمجال السيبراني، والتهديدات الاقتصادية المرتبطة بالمخاطر التي تواجهها في مجال التصنيع التكنولوجي، ومخاطر التنافس الدولي، وإن الكيفية التي تمت من خلالها "ترجمة المجال السيبراني" بكونه يرتبط بهذه الصيغة من التهديدات، فأنها ارتبطت بالمفاهيم الثقافية الصينية التي كونتها حول الفضاء السيبراني، وهي مفاهيم "السيادة السيبرانية" و "القوة السيبرانية الكبرى". وتحديد المجال السيبراني بكونه ينطوي على تهديدات أمنية قد أنتج صيغة معينة من السلوكيات الأمنية للصين للتعامل ما يفرزه هذا المجال من مخاطر، وهذا ما كان واضحاً من خلال الاستراتيجيات التي طرحتها مثل "الاستراتيجية الوطنية للأمن السيبراني"، و "استراتيجية "تنمية الاقتصاد الرقمي"، و "استراتيجية الاندماج العسكري – المدني"، أما على المستوى الإقليمي والدولي فأن السلوك الذي انتهجته الصين فهو ينطوي في جوهره على "توسيع صيغة الأمننة" التي طرحتها حول هذا المجال والذي يهدف إلى بناء نسق دولي للمجال السيبراني يعكس لها مصالحها وتؤدي دوراً مركزياً ضمنه، وهذا ما كان واضحاً من خلال مبادراتها التي طرحتها، وهي "الأمن السيبراني في إطار منظمة شنغهاي"، و "منظمة المؤتمر العالمي للأنترنت"، و "مبادرة طريق الحرير الرقمي".

إن الاستجابة الأمريكية التي نشأت في مواجهة السلوك الصيني في المجال السيبراني، تتجسد بشكل أساسي ضمن افتراضات "موجة الردع الخامسة"، مع إضافة الردع بنزع الشرعية لها، إذ أن السياسات الصينية المطروحة على المستوى الدولي، والتي تهدف إلى بناء نسق دولي للمجال السيبراني، فإن هذا الأمر يعني بالنسبة للولايات المتحدة الأمريكية بأن هذه المساعي مصممة للتأثير على بنية النسق الدولي القائم، والذي قامت بنبائه منذ نهاية الحرب الباردة، وهذا ما يستلزم معه وجود استجابة استراتيجية أمريكية تعمل على منع الصين من تحقيق أهدافها، والتي تجسدت بخيار "الردع الاستراتيجي"، والتي تبدو بأنها موجهة بشكل أساسي بغاية منع الصين من الوصول إلى تقنيات التكنولوجيا المتقدمة (أشباه الموصلات)، إذ أن ردع الصين عن تحقيق مشاريعها التي تستند إلى توظيف التقنيات السيبرانية في إحداث تحولات في بنية النسق الدولي، فإن هذا الأمر يستلزم معه منعها من الوصول إلى التقنيات الأساسية لصناعتها التكنولوجية، وهنا يتضح مدى قدرة الموجة الخامسة من الردع على تفسير الاستجابة الأمريكية والتي قامت على أساس ثلاثة أنماط، وهي "الردع بنزع الشرعية" التي اتبعتها إدارة الرئيس الأمريكي (باراك أوباما)، والتي تعني التوجه لإلزام الصين بمجموعة من الاتفاقيات والقواعد بالشكل الذي يردعها عن تعميم معايير ها التي تتبناها حول المجال السيبراني، و "الردع بالعقاب" الذي تم اتباعه من قبل إدارة الرئيس (دونالد ترامب)، وهي تستهدف فرض عقوبات على شركات التكنولوجيا الصينية بالشكل الذي يمنعها من الوصول إلى تقنيات أشباه الموصلات العالمية، و "الردع بالإنكار" الذي يتبع من قبل إدارة الرئيس الأمريكي (جو بايدين)، والذي قام على أساس التوجه لعقد تحالفات مع مجموعة من الدول التي تؤدي دوراً هاماً ضمن سلسلة التوريد العالمية لأشباه الموصلات، وذلك لحرمان الصين ومنعها من الوصول إلى هذه التقنيات، وهو ما يؤدي إلى ردعها عن تحقيق أهدافها في تعديل النسق الدولي.

المراجع:

1. Berling, T, Gad, U, Petersen, K, Waever, O. (2022). **Translation of Security: A Framework for The Study of Unwanted Future**. 1st ed. London: The UK. Routledge. P:221.
2. Buzan, B, Hansen, L. (2009). **The Evolution of International Security Studies**. 1st ed. Cambridge: The UK. Cambridge University Press. P:384.
3. Buzan, B. Waever, O, Wilde, J. (1998). **Security: A New Framework for Analysis**. 1st ed. London: The UK. Lynne Rienner Publisher. P: 237.
4. Buzan, B. Waever, O. (2003). **Regions and Power: The Structure of International Security**. 1st ed. Cambridge: The UK. Cambridge University Press. P:564.
5. Cavelty, M. (2013). From Cyber – Bombs to Political Fallout: Threats Representations with an Impact in The Cyber Security Discourse, **International Studies Review**. No:15. P – P:105 – 122. London: The UK. Oxford University Press.
6. Chihong, C. (2015). Cybersecurity in the Chinese Context: Changing Concepts, Vital Interest, and Prospect for Cooperation. **China Quarterly of International Strategic Studies**. Vol:1, No: 3. P – P:471 – 486. Singapore: Singapore. World Scientific Publishing.
7. Hansen, L, Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and The Copenhagen School. **International Studies Quarterly**. No:53. P – P:1155 – 1175. London: The UK. Oxford University Press.
8. Monghan, S. (2020). **Hybrid Threats: Toward a Fifth Wave of Deterrence Theory and Practice.** Study to The European Centre of Excellence for Hybrid Threats. Helsinki: Finland. P:16 – 19. P:49.
9. Eriksson, J, & Giacomell, G. (2007). Introduction: Closing the Gap Between International Relations Theory and Studies of Digital – Age Security. 1st ed. P – P:1 – 28. Edited by: Johan Eriksson, & Giampiero Giacomello. **International Relations and Security in the Digital Age**. New York: The USA. Routledge.
10. Hollis, D. (2017). **China and U.S. Strategic Construction of Cybernorms: The Process is The Product**. Hoover Working Group on National Security, Technology, and Law. Washington DC: The USA. P:24