مجلـة البـاحث للـدراسات الأكـاديـمـيـة
ISSN: 2352-975X ELBAHITH for Academic Studies EISSN: 2588-2368
المجلد: 11 / العدد: 02 / السنة: 2024 / ص ص: 430 - 454

الدبلوماسية السيبرانية وجيوسياسية الفضاء السيبراني: بين مساعي الحوكمة وحسابات التنافس

Cyber Diplomacy and the Geopolitics of Cyberspace: between Governance Efforts and Competitive Calculations

تاريخ الإرسال: 2024/04/01 تاريخ القبول: 2024/05/10

حشاني فاطمة الزهراء* *Fatma Zahra HACHANI*
جامعة المسيلة
University of Msila
Fatmazahra.hachani@univ-msila.dz
توفيق حكيمي *Toufik HAKIMI*
جامعة عنابة
University of Annaba
Toufik.hakimi@univ-annaba.dz

ملخص:

تسترشد هذه الورقة بمفهوم الدبلوماسية السيبرانية وبممارساتها لدراسة فرص بناء عالم سيبراني آمن في عصر يسوده التنافس الجيوسياسي، تمحور التساؤل الرئيسي للورقة على قدرة الدبلوماسية السيبرانية-كلون دبلوماسي جديد أملته ضرورات الاستجابة لمشكلات الفضاء السيبراني- على تخطي القيود الجيوسياسية الشديدة لبلوغ هدفها المتمثّل في حوكمة الفضاء السيبراني الحالي، وعلى ضوء هذا التساؤل، جرى تقسيم هذه الورقة إلى ثلاثة أقسام تعرّض أولها إلى معنى الدبلوماسية السيبرانية والمعالم البارزة في مسارها، ووقف القسم الثاني منها على مشكلات الفضاء السيبراني وأدوار الدبلوماسية السيبرانية، أما القسم الثالث فقد تم تخصيصه لاستعراض القيود التي وضعتها الجيوسياسية الحالية للفضاء السيبراني أمام إمكانات نجاح الدبلوماسية السيبرانية عالميا.

خلصت هذه الورقة إلى تأكيد أهمية الدبلوماسية السيبرانية كأداة حاسمة لحماية مصالح الدول في الفضاء السيبراني بعيدا عن إخفاقات المعالجات التقنية والأمنية، وهي الأهمية التي تعزّزها التحولات العميقة التي أحدثتها الثورة الصناعية الرابعة ومظاهر الـ"عسكرة" المتزايدة لذلك الفضاء، غير أن تلك الأهمية لم تقابلها حتى الآن إنجازات عملية على صعيد التعاون الدولي والالتزام بالقواعد التي تكفل سلمية الفضاء السيبراني، فقد أدى التضارب في مواقف القوى الجيوسياسية الكبرى-التي هي نفسها القوى الأكثر قدرة على رسم معالم المشهد السيبراني العالمي- إلى تقويض

*- المؤلف المُراسل.

جمود الدبلوماسية السيبرانية بفعل تناقض مصالحها الجيوسياسية ومرجعياتها القيمية، وكنتيجة لذلك تحول الفضاء السيبراني إلى ما يشبه مجالا لحرب باردة جديدة بين الشرق والغرب.

الكلمات المفتاحية: الدبلوماسية؛ الفضاء السيبراني؛ الدبلوماسية السيبرانية؛ الجغرافيا السياسية.

Abstract:

This paper is based on the concept of cyber diplomacy and its practices to study the opportunities for building a secure cyber world in an era of geopolitical competition. The main question of the paper revolves around the ability of cyber diplomacy- as a new form of diplomacy- to overcome geopolitical restrictions to achieve its goal of cyber space governance. In light of this question, this paper was divided into three sections, the first of which dealt with the meaning of cyber diplomacy and the prominent milestones in its path. The second section focused on the problems of cyberspace and the roles of cyber diplomacy. The third section was devoted to reviewing the constraints placed by the current geopolitics of cyberspace on the potential for successful cyber diplomacy globally.

This paper concluded by emphasizing the importance of cyber diplomacy as a decisive tool for protecting the interests of states in cyberspace, this importance is reinforced by the profound transformations brought about by the Fourth Industrial Revolution and the increasing manifestations of "militarization" of that space. However, this importance has not yet been matched by practical achievements in terms of international cooperation and adherence to the rules that guarantee peaceful cyberspace. The conflict in the positions of the major geopolitical powers- which are the same powers most capable of shaping the global cyber scene- has undermined the efforts of cyber diplomacy due to the contradiction in their geopolitical interests and value references. As a result, cyberspace has turned into something resembling a field for a new cold war between the East and the West.

reflects the overall research ideas without elaborating on the precise details within 200 words. The researcher focuses on the objective of the research, i.e. the purpose of the research, the methodology used, and the main findings.

The abstract does not contain abbreviations, references, inclusion of an incomplete sentences, use of ambiguous terms or any kind of tables.

Keywords: *Diplomacy; Cyberspace; Cyber Diplomacy; Geopolitics.*

مقدمـة:

أفضى التدفق العشوائي للتكنولوجيات المتطورة التي أفرزتها "الثورة الصناعية الرابعة" إلى إحداث تغيير عميق في الحياة اليومية للأفراد والمجتمعات، ووضع التقدم السريع في مجالي الاتصالات والمعلوماتية كل الدول والمجتمعات ودون استثناء أمام تحديات هائلة لضمان استقرارها وأمنها، سيّما في خضم بروز مصادر وجهات تهديد متعددة وذات أجندات مختلفة وتتميّز بدرجة عالية من الكفاءة التكنولوجية، تتلاعب بالفضاء السيبراني وبالتقنيات المرتبطة به، وبمقدور نشاطاتها الاضرار باستقرار الدول وتهديد السلام العالمي برمّته.

وقد قاد الاستشعار المبكر للعواقب غير المرغوبة لذلك التقدم التكنولوجي من جهة، ولـ"التسيّيس" المتنامي للفضاء السيبراني بسبب تضارب المصالح والقيم والأعراف بين الدول من جهة ثانية، ولتفاقم قضايا التجسس والهجمات السيبرانية ونشاطات القرصنة واختراق الشبكات من جهة ثالثة، إلى تنامي الحاجة إلى تكثيف مظاهر التعاون بين مختلف الفاعلين في المجال السيبراني خارج أطر التعاون التي كانت قائمة بالفعل في الجوانب التقنية البحتة وفي المسائل القضائية، وعلى النحو الذي يدفع باتجاه التأسيس لإطار دبلوماسي يتم استحداثه خصيصا لمعالجة الإشكالات الناشئة عن الاستخدام المتنامي للفضاء السيبراني.

في هذا السياق، كان للولايات المتحدة والدول الغربية الكبرى الدور الأبرز في إرساء التوجه العالمي نحو إدراج المسائل السيبرانية في أجندات السياسات الخارجية للدول، ومن ثم في اعتماد استراتيجيات سيبرانية وتعيين دبلوماسيين "سيبرانيين" لمتابعة تنفيذها، ومع بداية العقد الثاني من القرن الحالي، ورغم الفجوة التكنولوجية الواسعة التي تفصل بينها، سارعت معظم دول العالم للانخراط في الجهود المبذولة لمأسسة التعاون الدولي في المجال السيبراني، وجرى في هذا المنحى التوقيع على عدد من الاتفاقات الإقليمية والدولية، أفضت إلى اعتماد معايير عامة لتحديد "السلوكات

ISSN: 2352-975X ——————————EISSN: 2588-2368

المسؤولة" للدول في الفضاء السيبراني، وتوقف سقف طموحاتها دون بلوغ حد وضع قواعد ملزمة للتصدي للممارسات الخبيثة في هذا الفضاء لاعتبارات سياسية وجيوسياسية عديدة.

ورغم التقدم الحاصل على صعيد الاهتمام بالبعد السيبراني في أجندات السياسات الخارجية، ظلت الفجوة قائمة بين الممارسة والنظرية، وتأخر تبلور مفهوم الدبلوماسية السيبرانية عن ظهور المصطلح ذاته، كما لم يبذل باحثو الدبلوماسية والعلاقات الدولية إلى وقت قريب سوى جهد محدود في وضع تصور متكامل لمفهوم الدبلوماسية السيبرانية، وعلى ضوء هذا الواقع، تتطلع هذه الورقة لدراسة مفهوم الدبلوماسية السيبرانية والوقوف على واقع ممارساتها واشكالات تحقيق أهدافها، ومن ثم نحو معالجة دورها المفترض في حوكمة الفضاء السيبراني العالمي انطلاقا من التساؤل التالي: **باعتبارها مجالا دبلوماسيا جديدا أملته مشكلات الفضاء السيبراني المتفاقمة، فإلى أي مدى بلغ نجاح الدبلوماسية السيبرانية في تخطي الحواجز الجيوسياسية نحو بناء عالم سيبراني آمن؟**

تنطلق هذه الورقة من إطار مفاهيمي نستعرض من خلاله الإشكالات المفاهيمية لهذا النوع المستحدث من الدبلوماسية، كما تضمن ذلك احاطة تاريخية بالمسار الذي سلكته الدبلوماسية السيبرانية حتى الآن، وتخوض الورقة في جزئها الثاني في مشكلات الفضاء السيبراني وفي الأدوار التي اضطلعت بها الدبلوماسية السيبرانية في إطار البحث عن علاجات لها، ووقفت الورقة في قسمها الأخير على الاعتبارات الجيوسياسية التي حالت دون تحقيق غايات الدبلوماسية السيبرانية في حوكمة الفضاء السيبراني وخلق عالم سيبراني آمن.

المحور الأول: في مفهوم الدبلوماسية السيبرانية وتبلور ممارساتها

يربط التصور المعاصر مفهوم الدبلوماسية بمسارات التفاوض والتفاعل السلمي بين ممثلي الدول والمنظمات الدولية والجهات الفاعلة غير الحكومية، ولكونها أداة

EISSN: 2588-2368 ——————— ISSN: 2352-975X

رئيسية لتنفيذ السياسات الخارجية للدول، تسعى الفواعل الدولية من خلال عمل دبلوماسيتها إلى تأمين مصالحها الوطنية بالعمل على احلال السلام والتعاون ومعالجة مختلف القضايا والمشكلات عبر التفاوض، ورغم التحولات العديدة التي عرفها النظام الدولي منذ ثمانينيات القرن الماضي، والتي أدّت في عمومها إلى تعدّد الجهات الفاعلة وتشعّب قضايا العمل الدبلوماسي، الّا أن الوظائف الرئيسية للدبلوماسية لم يطرأ عليها تغيير جوهري حتى اليوم.

وقد كان من نتائج النفاذ السريع والمتزايد إلى عالم الانترنت والتكنولوجيات الرقمية الحديثة مطلع القرن الحالي تنامي مخاطر الحوادث السيبرانية بأنواعها الكثيرة والمعقدة، ومن ذلك تعريض سلامة وسرّية البيانات الشبكية، وتعطيل عمليات وأداءات البنى التحتية الحيوية، وكذا تعريض أمن وسلامة الناس والشركات والقطاعات الاقتصادية وحتى بلدان بأكملها للخطر، ونجم عن ادراك تلك المخاطر ادراج ملفات الأمن السيبراني ضمن أولويات السياسة الخارجية للدول، وهنا برزت أهمية الدبلوماسية مجددا ليس فقط في تأمين المصالح الوطنية في الفضاء السيبراني المتعاظم تأثيره فحسب، بل أيضًا في العمل على بناء الثقة ومعالجة أشكال جديدة من الخلافات التي تنشأ ضمن ذلك الفضاء مع الفواعل الأخرى.

أولا- في معنى الدبلوماسية السيبرانية:

تأسيسا على ما سبق، يتم النظر إلى الدبلوماسية السيبرانية من زاوية إطار العمل الهادف إلى حل القضايا الناجمة عن الاستخدام الدولي للفضاء السيبراني اعتمادا على تطبيق الأدوات والمهارات الدبلوماسية[1]، وبتعبير آخر، يستخدم مصطلح الدبلوماسية السيبرانية للإشارة إلى "أسلوب محدّد تنتهجه الفواعل الدولية في تعاملها مع المشكلات المختلفة التي تنشأ في الفضاء السيبراني، والتي تتراوح ما بين قضايا إدارة الإنترنت ومعالجة الجرائم السيبرانية، إلى حماية البنية التحتية الحيوية، إلى قضايا التجسس السيبراني والصراع السيبراني، بالإضافة إلى سلوك الدولة

ISSN: 2352-975X ——————————EISSN: 2588-2368

المسؤول في الفضاء السيبراني"[2]، وبعبارات أدق، "إذا كان البعد السيبراني سببا أساسيا لـ[وجود] دبلوماسية، فمعنى ذلك هو أننا بصدد الدبلوماسية السيبرانية".[3]

يقود التصور أعلاه إلى اعتبار الدبلوماسية السيبرانية مجالًا جديدًا نسبيا، ذلك لأن الفضاء السيبراني ظل تقليديا مجالا بعيدا عن أدوار الجهات الحكومية، وانحصر نطاق الفاعلين السيبرانيين على المهندسين والتقنيين من الموظفين العاديين، لكن التهديدات المتزايدة للأمن السيبراني، وطبيعتها المتخطية للحدود، كانت بمثابة "دعوة مفتوحة" لمختلف الفاعلين الحكوميين للتعامل بشكل جدِّي مع القضايا السيبرانية من خلال الوسائل الدبلوماسية، وترتب عن انخراط الفاعلين الرئيسيين في ذلك المسار ظهور الدبلوماسية السيبرانية كأداة مستحدثة لتنفيذ السياسات الخارجية للدول في المجال السيبراني، وفي معالجة المسائل الأمنية المرتبطة به.

مع ذلك، لا يحصل الاجماع على معنى الدبلوماسية السيبرانية بتلك البساطة، وبشكل أكثر تفصيلا، أفرزت موجة التحولات التي عرفها مجال تكنولوجيا الاتصالات والمعلوماتية ممارسات ومفاهيم دبلوماسية متعددة لا يتم التمييز بينها بشكل سليم، وفي كثير من الأحيان يجري التعامل مع مفاهيم "الدبلوماسية الرقمية" *Digital Diplomacy* والدبلوماسية الإلكترونية *E-Diplomacy* و"الدبلوماسية الافتراضية" *Virtual Diplomacy* و"دبلوماسية تويتر" *Twiplomacy* كمرادفات لمفهوم الدبلوماسية السيبرانية، وقد كان هذا الحال صحيحا مع البدايات الاولى لظهور مصطلح الدبلوماسية السيبرانية، وهو الواقع الذي تغيّر مع تبلور المفهوم لاحقا كما سيأتي تبيانه.

من حيث المبدأ، يجري التمييز بين مفهوم الدبلوماسية السيبرانية ومفاهيم الدبلوماسية الإلكترونية والرقمية والافتراضية من خلال النظر إلى هذه الأخيرة من زاوية الوسائل التي يستخدمها الدبلوماسيون في القيام بوظائفهم الدبلوماسية، أي

إلى استخدام الأدوات والأساليب الرقمية أو الإلكترونية (تقنيات الاتصال الحديثة، منصات التواصل الاجتماعي، التجمعات الافتراضية...) من قبل الدبلوماسيين في تفاعلهم مع الكيانات الرسمية وغير الرسمية، وبحسب توم فليشر Tom Fletcher (أكاديمي ودبلوماسي بريطاني سابق)، يعتبر هذا الشكل من الممارسات الدبلوماسية قديم نسبيا، ويعود بالتحديد إلى عام 1994 حينما أرسل وزير خارجية السويد آنذاك كارل بيلت Carl Bildt أول بريد إلكتروني دبلوماسي رسمي إلى الرئيس الأمريكي بيل كلينتون هنّأه فيه بمناسبة رفع الحظر الأمريكي المفروض على فيتنام.(4)

في منحى مماثل تقريبا، تحيلنا دبلوماسية تويتر *Twiplomacy* إلى استخدام تويتر كمنصة رائدة للتواصل الدبلوماسي، ليس فقط من خلال بث تغريدات القادة والدبلوماسيين وإتاحة فرص اجراء المقابلات المباشرة معهم، بل أيضا في تكسير النمط التقليدي للاتصالات وفتح نوافذ جديدة للعمل الدبلوماسي بين الدول، وكما ذكر أحد الباحثين، كان لإقدام وزارة الخارجية الامريكية على متابعة حساب تويتر للخارجية الكوبية في 25 ماي 2015 أثرا إيجابيا على العلاقات بين البلدين، حيث ردّت الخارجية الكوبية عبر حسابها بالمثل في نفس ذلك اليوم،(5) وقبل نهاية ذلك العام عادت العلاقات الدبلوماسية بين البلدين بعد عقود طويلة من القطيعة، وقد عُرف عن الرئيس الأمريكي السابق دونالد ترامب استخدامه الكثيف للمنصّة لأغراض دبلوماسية، فقبيل حضر حسابه على تويتر عشية نهاية عهدته الرئاسية حصدت تغريداته نحو مليار و700 مليون اعجاب، وقارب عدد متابعيه 89 مليون شخص،(6) وأشارت بيانات أخرى تعود إلى عام 2015، أن نحو 86% من قادة العالم كان لديهم حساب على منصة تويتر ذلك الحين.(7)

سواء تعلق الأمر بدبلوماسية تويتر أو بالدبلوماسية الرقمية أو بالدبلوماسيتين الإلكترونية والافتراضية، فهي تشير جميعا إلى التحول الحاصل في طريقة التواصل الدبلوماسي، وفي أساليب تأدية الوظائف الدبلوماسية اعتمادا على التقنيات الرقمية

ISSN: 2352-975X ——————————EISSN: 2588-2368

ومكونات الفضاء الإلكتروني، وتهدف في جوهرها إلى خدمة الأجندات الدبلوماسية باستخدام الأدوات الرقمية، وبذلك تختلف تلك المفاهيم بوضوح عن المعنى الذي تعبّر عنه الدبلوماسية السيبرانية، باعتبار هذه الأخيرة نهجا دبلوماسيا خاصا بالفضاء السيبراني، ويهدف في المقام الأول إلى حوكمة الفضاء السيبراني، والى إدارة مجمل القضايا السيبرانية ومعالجة المشاكل التي تنشأ في ذلك الفضاء بالوسائل والأساليب الدبلوماسية.(8)

ثانيا- في تبلور ممارسات الدبلوماسية السيبرانية

النحو الذي ذكرناه آنفا، تُجسِّد الدبلوماسية السيبرانية واحدة من أهم الاستجابات التي بلورتها الفواعل الرئيسية في النظام الدولي لوضع أسس للتعاون في المجال السيبراني، فقد أدى التقدم الحاصل في مجال المعلوماتية والاتصالات إلى فسح مجالات جديدة أمام الفواعل الدولية للتعاون، سواء لتأمين مصالحها في الفضاء الرقمي، أو لمجابهة الأشكال المختلفة من التحديات العابرة للحدود التي يطرحها الفضاء السيبراني وعلى رأسها قضايا القرصنة واتلاف الشبكات والبيانات والتعدي على الملكية الفكرية والحروب السيبرانية والسرقات البنكية وتعطيل الحسابات وغيرها، سيّما وأن جميع الدول ورغم كونها عرضة لتلك المخاطر، إلا أنها تبقى عاجزة عن مجابهتها بشكل منفرد لطبيعة التهديد المعقدة والديناميكية والعابرة للحدود، وكما جاء في تقرير للمعهد الدولي للدراسات الإستراتيجية بلندن، "سيشكل الفضاء الإلكتروني أحد أهم ميادين الصراعات والحروب المستقبلية، ولا توجد دولة مهما عظمت قدراتها العسكرية، ولا مؤسسة مهما عظمت قوتها الاقتصادية في مأمن من خطر الهجمات الإلكترونية".(9)

والدبلوماسية السيبرانية هي واحدة من المفاهيم القليلة التي تأخر ظهورها عن ظهور المصطلح ذاته، ناهيك عن وجود فجوة واسعة بين ازدهار ممارسات هذا النوع من النشاط الدبلوماسي في مقابل العدد المحدود من الادبيات التي اهتمت بهذا

المفهوم، فالدبلوماسية السيبرانية كمصطلح أُستخدِم في البداية لوصف أنشطة ما يسمى اليوم بـ "الدبلوماسية الإلكترونية"، وعلى سبيل المثال، في كتاب صدر عام 2002 بعنوان: "الدبلوماسية السيبرانية: إدارة السياسة الخارجية في القرن الحادي والعشرين"، لفت مؤلفه إيفان بوتر (Evan H. Potter) الانتباه إلى تأثيرات الإنترنت والتكنولوجيات الجديدة على أهداف الدبلوماسية وأدواتها وهياكلها، كما تم استخدام هذا المصطلح أيضًا لوصف تطور أنشطة الدبلوماسية العامة في العصر الرقمي، وقد ركّزت تلك الدراسات المبكرة في عمومها على التحول الرقمي الهائل، لكنها لم تتعرض إلى العمليات الدبلوماسية اللازمة للتعامل مع الجوانب الدولية الناشئة للقضايا السيبرانية.[10]

على صعيد الممارسة، يتّفق الباحثون على اعتبار نشر "الاستراتيجية الأمريكية الدولية للفضاء السيبراني" في عام 2011 بمثابة صافرة انطلاق الدبلوماسية السيبرانية، ذلك اعتبارا لكونها أول وثيقة حكومية على مستوى العالم تركز بشكل كامل على الجوانب الدولية للقضايا السيبرانية، تنصّ الوثيقة على التزام الولايات المتحدة، إلى جانب الدول الأخرى، بدعم السلوك المسؤول في الفضاء السيبراني، وعلى معارضة الجهات الساعية إلى تعطيل الشبكات والأنظمة وردعها،[11] كما حدّدت الإستراتيجية عددًا من الأولويات في مجالات الاقتصاد (ص17)، وحماية الشبكات (ص18)، وإنفاذ القانون (ص19)، والجيش والاستعداد لتحديات القرن الـ21 (ص20)، وحوكمة الإنترنت (ص21)، والتنمية الدولية (ص22)، وحرية الإنترنت (ص23)، مع التأكيد على اعتماد الاستراتيجية الامريكية على ثلاث ركائز لتحقيق تلك الأهداف وهي الدبلوماسية، والدفاع، والتنمية (3Ds: *Diplomacy+ Defense+ Development*) وللمرة الأولى، قدمت الوثيقة استراتيجية واضحة لاستخدام الأدوات والموارد الدبلوماسية في السعي لتحقيق الأهداف المتعلقة بالفضاء السيبراني، وتماشيًا مع تلك الاستراتيجية، تم إنشاء

ISSN: 2352-975X ——————————EISSN: 2588-2368

مكتب جديد لمنسق القضايا السيبرانية داخل وزارة الخارجية الأمريكية، ليصبح أول مكتب في العالم مخصص بالكامل للقضايا السيبرانية، في حين أصبح المنسق كريستوفر بينتر Christopher Painter- بحكم الأمر الواقع- أول دبلوماسي- سيبراني في العالم.[12]

اقتداء بتحرك الولايات المتحدة، بادر عدد محدود من الدول برسم استراتيجيات دولية قائمة بذاتها، ويمكن الإشارة على وجه الخصوص إلى استراتيجية اليابان بشأن التعاون الدولي في مجال الأمن السيبراني التي تم اعتمادها في شهر أكتوبر من عام 2013 وقامت على أربعة مبادئ هي: ضمان التدفق الحر للمعلومات؛ الاستجابة للمخاطر المتزايدة؛ تعزيز المقاربة المبنية على المخاطر؛ العمل في اطار شراكات مبنية على المسؤوليات الاجتماعية،[13] مع ذلك، لم يتم استخدام مصطلح "الدبلوماسية السيبرانية" في وثيقة حكومية رسمية إلى أن جاء تبني دول الاتحاد الأوروبي لـ "استنتاجات" مجلس الاتحاد بشأن الدبلوماسية السيبرانية عام 2015، وهي عبارة عن وثيقة ترسم مسار تطوير وتنفيذ نهج الاتحاد الأوروبي المشترك والشامل للدبلوماسية السيبرانية من خلال ضمان الحقوق في حرية التعبير وفي الوصول إلى المعلومات والخصوصية، وضمان عدم إساءة استخدام الانترنت لتأجيج الكراهية والعنف، وتعزيز الامن السيبراني وترقية التعاون في مجال مكافحة الجرائم السيبرانية وحماية القيم الأساسية للاتحاد الأوروبي، والمساهمة في بناء القدرات السيبرانية للدول النامية،[14] في حين التزمت استراتيجية الأمن السيبراني الأسترالية لعام 2016 بوضع استراتيجية مشاركة دولية، وقد سبق ذلك نشر فريق الخبراء الحكوميين التابع للأمم المتحدة (UNGGE) عام 2015 لتقرير عن التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي كما سيأتي الحديث عن ذلك لاحقا.

وعلى النقيض من الزخم الذي اكتسبته الدبلوماسية السيبرانية على صعيد الممارسة، ظلّت أدبيات هذا النوع من النشاط الدبلوماسي محدودة بشكل مثير للاستغراب، فمن خلال مراجعة شاملة لأدبيات الدبلوماسية السيبرانية أجراها فريق من الباحثين عام 2020، تم حصر واحد وعشرين (21) دراسة فقط لها صلة بموضوع الدبلوماسية السيبرانية، وكان جميع معدّيها باحثين من أوربا وأمريكا الشمالية،[15] كانت واحدة من الدراسات المبكرة التي تضمنت الإشارة إلى المفهوم الحالي في سياق اهتمامها بممارسات الدبلوماسية السيبرانية تلك التي نشرها معهد الشرق والغرب عام 2010 ومما جاء فيها:

"وبسبب المستويات العالية من الاتصالات عبر الحدود في العالم السيبراني، يجب أن تأخذ الأساليب الجديدة للأمن السيبراني في الاعتبار البعد الدولي. وبالتالي، فبدلاً من التركيز حصرياً على الدفاع السيبراني أو الحرب السيبرانية، من المهم أيضاً البدء في تطوير الدبلوماسية السيبرانية، لم تفكر سوى حكومات قليلة في البعد الدبلوماسي للأمن السيبراني، ومن المؤكد أنها لم تطور استراتيجيات دبلوماسية تتناسب مع التهديد".[16]

يمكن رد سبب التباين القائم بين ممارسات الدبلوماسية السيبرانية التي قطعت أشواطا كبيرة في سياق ترسيخ مكانتها كأداة هامة لتنفيذ السياسات الخارجية للدول، وحالة هذا المفهوم على صعيد الاهتمام الاكاديمي الذي يظل دون المستوى المطلوب من الناحية التنظيرية إلى عاملين رئيسيين: أولهما لعدم وجود حدود معروفة لدى الباحثين في البداية للتمييز بين استخدامات الوسائل السيبرانية من قبل الدبلوماسيين وبين وجود دبلوماسية خاصة بالمسائل السيبرانية، وقد زاد في حدة هذا الإرباك شيوع استخدام مصطلح الدبلوماسية السيبرانية في البداية للإشارة إلى ما يعرف حاليا بالدبلوماسية الإلكترونية أو الرقمية، وثانيهما يعود إلى أسبقية أطر التعاون الدولي في القضايا المتعلقة بالجرائم السيبرانية التي بلورتها أساسا اتفاقية

ISSN: 2352-975X ——————————EISSN: 2588-2368

بودابست لعام 2001، ودليل تالين لعام 2013، ومن ثم في إذكاء الحاجة إلى التحرك الدبلوماسي الفعلي لإقناع الدول الأخرى بجدوى الانخراط في جهود مأسسة التعاون الدولي في المجال السيبراني.

ورغم حداثة موضوعها، قطعت الدبلوماسية السيبرانية خطوات ملموسة نحو تعزيز الجهود الدولية في إدارة قضايا الفضاء السيبراني وحل الصراعات المحتمل حدوثها فيه، وتعترف جل الحكومات في العالم اليوم بأن تجاهل الدبلوماسية السيبرانية لم يعد خيارا ممكنا على الاطلاق، سيّما وأن موضوع هذا اللون من الدبلوماسية قد تخطى مسائل إدارة الانترنت والامن السيبراني ليشمل حزمة واسعة من المجالات تمتد من قضايا التنمية الاقتصادية وتصل حد الاستخدامات العسكرية للأنترنت.

المحور الثاني: مشكلات الفضاء السيبراني وأدوار دبلوماسية السيبرانية

كنتيجة للتقدم السريع في اعتماد التكنولوجيات السيبرانية مطلع القرن الحالي، اكتسبت جهات فردية ومنظمة عديدة درجة عالية من المهارات التي مكنتها من تهديد فواعل أكبر منها بكثير، وغالبا ما كانت تلك التهديدات تنتشر بسرعة ودون وجود رادع، وقد عرّض كل ذلك أمن الدول والمجتمعات للخطر وبسهولة، كما نجم عنه نشوء عدد من الاحتكاكات والصراعات في المجال السيبراني في وقت لم تكن فيه الدبلوماسية السيبرانية قد بلغت نضجا كافيا لبناء الثقة في هذا الفضاء، ناهيك عن ضعف استعدادها لمعالجة جل المشاكل السيبرانية وحلّها.

في هذا السياق، شكّلت الهجمات الإلكترونية التي تعرضت لها إستونيا عام 2007 أول اختبار لقدرة الأطراف الدولية على حل القضايا الناشئة في الفضاء السيبراني بطرق تعاونية، كما أماطت اللثام عن قدرة الجماعات السياسية على تدمير الأعمال الحكومية في الدول الأخرى أو تعطيلها، ففي 26 أبريل 2007 بدأت السلطات الاستونية في نقل نصب تذكاري يخلّد ضحايا التحرير السوفيتي للبلاد من النازيين من وسط العاصمة تالين إلى مكان آخر أقل بروزا، وبعد يوم من

EISSN: 2588-2368 ——————— ISSN: 2352-975X

المظاهرات والاحتجاجات العنيفة، شهدت استونيا موجة شديدة من الهجمات السيبرانية بدأت يوم 27 أفريل واستمرت لمدة اثنين وعشرين (22) يوما، وعلى الرغم من أن أنواع الهجمات كانت معروفة جيدا، إلا أنها كانت لا مثيل لها في الحجم والتنوع مقارنة بدولة بحجم إستونيا، شملت الكيانات المستهدفة الحكومة والرئيس والبرلمان والشرطة والبنوك ومقدمي خدمات الإنترنت ووسائل الإعلام عبر الإنترنت.(17)

كشفت الأدلة الجنائية السيبرانية عن الهجمات أن الجزء الأكبر من التدفقات الضارة جاء من خارج إستونيا، وكان هناك مؤشر واضح على الأصول اللغوية الروسية التي تم العثور عليها بشكل متكرر في الاتصالات الخبيثة، وفي أعقاب تلك الحادثة، ولكون استونيا أحد أعضاء حلف الناتو، تبنى الحلف اطارا استراتيجيا للدفاع السيبراني أسهم بشكل كبير في وقف الهجمات السيبرانية على استونيا، كما أقام الحلف في العاصمة تالين "مركز التميز للتعاون الدفاعي السيبراني"، وفي عام 2013، نشر المركز دليل تالين 1.0 الذي أصبح أحد المبادئ التوجيهية الرئيسية للدبلوماسية السيبرانية بالنسبة لدول الغرب.(18)

شكّل "دليل تالين للقانون الدولي المنطبق على الحرب السيبرانية *Tallinn Manual on the International Law Applicable to Cyber Warfare* الاستجابة الدولية الأبرز لمعالجة مسألة الهجمات الإلكترونية بعد دعوة "مركز التميز" المشار اليه سابقا لمجموعة من فقهاء القانون الدولي لإعداد صك قانوني منظم للحرب السيبرانية، نشرت الصيغة الأولى منه عام 2013، ويحتوى على 95 قاعدة قانونية إرشادية لعمل أو سلوك الدول في سياق الحرب الإلكترونية، وصدر الإصدار الثاني منه في العام 2017، ويحتوى على 154 قاعدة، ليشكل مستوى أكثر اتساعاً لمعالجة العمليات الإلكترونية، ومراجعة وحسم نقاط عدم الاتفاق في الإصدار الأول،(19)

ISSN: 2352-975X ——————————EISSN: 2588-2368

أما الإصدار الثالث منه فظهر عام 2021 (دليل تالين3.0) وتضمن مراجعة الفصول الحالية واستكشاف قضايا جديدة ذات صلة بالدولة.

بعد حوادث استونيا، وتحديدا في شهر جويلية من عام 2010، تم الإعلان عن ظهور ما عرف فيما بعد بـ"أول سلاح الكتروني" بعدما نشرت شركة مايكروسوفت وشركات أخرى تحذيرا أمنيا من برنامج ضار عرف باسم ستوكسنت *Stuxnet* أصاب نحو مئتي ألف جهاز حاسوب في جميع انحاء العالم، كانت ايران أكثر دول العالم تضررا بفعل اختراق برمجيات *Stuxnet* الخبيثة لأجهزة الحاسوب في المنشأة النووية الإيرانية الواقعة في مدينة نتنز بين عامي 2008 و2010، وبسبب البرمجيات الخبيثة، تضرر أكثر من ألف (1000) جهاز طرد مركزي في منشأة نتنز، لقد شكّل هذا الفيروس بأكورة البرامج الضارة المعروفة التي استهدفت أنظمة التحكم الصناعية، ووفقًا للتقديرات، أدى ذلك إلى انخفاض بنسبة 30٪ في كفاءة تخصيب اليورانيوم في إيران مما أدى في النهاية إلى زيادة الوقت الذي تستغرقه البلاد للحصول على اليورانيوم المستخدم في تصنيع الأسلحة، وبحسب المحللين فإن تلك البرامج الضارة والمعقدة لا يمكن تصميمها إلا برعاية دول أخرى،[20] وقد وجّهت ايران اتهاماتها بشكل مباشر لإسرائيل وتوعدت بالرد.

بعد اعتماد دليل تالين عام 2013، حقّقت الدبلوماسية السيبرانية تطورا رئيسيا آخر على الصعيد العالمي مع توقيع اتفاقية الأمن السيبراني بين الولايات المتحدة والصين في عام 2015 بعد سنوات طويلة من تبادل الاتهامات، منذ مطلع القرن الحادي والعشرين انخرطت الصين في عدد كبير من أنشطة التجسس السيبراني على شبكات الحكومة الامريكية والشركات الكبرى وعلى المعارضة الصينية في الولايات المتحدة، وكانت واشنطن منزعجة بشكل خاص من انخراط الصين في التجسس لصالح شركاتها المحلية والمؤسسات المملوكة للدولة، وبعد وقوع تسريبات إدوارد سنودن، العميل السابق بوكالة الأمن القومي الأمريكية، التي تضمنت

EISSN: 2588-2368 ——————— ISSN: 2352-975X

تأكيدات عن تورط الولايات المتحدة في نشاطات واسعة للتجسس على الصين ودول أخرى من بينها حلفاء للولايات المتحدة، ناهيك عن التجسس على عدد من المؤسسات الدولية منها صندوق النقد الدولي، ردّت الصين باتهام الولايات المتحدة بـ "التِفاق وعسكرة الفضاء السيبراني"،[21] لكنها اضطرت في الأخير إلى التوقيع على اتفاقية الأمن السيبراني تحت وقع التهديدات الامريكية بفرض عقوبات عليها بسبب الاختراقات السيبرانية الصينية المتكرِّرة.

مثّلت تلك الاتفاقية حدثا هاما على الصعيد العالمي، فقد اعترفت الصين، التي طالما كانت في مرمى الانتقادات، بانطلاق عدد من الأنشطة السيبرانية الخبيثة من أراضيها رغم نفي ضلوعها فيها[22]، وقد رأى الكثير من الملاحظين في تلك الاتفاقية بداية واعدة لمأسسة قضايا الأمن السيبراني على المستوى الدولي من خلال العمل الدبلوماسي، وعلى الرغم من كون نجاحها يظل موضع خلاف كبير، وُصفت اتفاقية الامن السيبراني بين الولايات المتحدة والصين على أنها أبرز معالم الدبلوماسية السيبرانية العالمية.

لاحقا، أظهرت حزمة من الوقائع المتفرقة استمرار أعمال التجسس السيبراني بين البلدين ولو على نطاق أضيق، فقد كشفت تقارير عديدة عن اختراق شبكات وزارة الدفاع الأمريكية وسرقة كم هائل من البيانات العسكرية، ناهيك عن عدد غير محدد من أعمال التجسس على شركات التكنولوجيا والمؤسسات الاقتصادية والمالية، وقد وجهت أصابع الاتهام في كل الحالات تقريبا إلى القراصنة الصينيين، من جهتها، اتهمت بكين الولايات المتحدة مرارا وتكرارا بالوقوف خلف الهجمات الإلكترونية التي استهدفت الشركات الرائدة في الصين، ومعاهد الأبحاث، والبنى التحتية الحيوية.[23]

في نفس العام أيضا (2015)، تعزّز مسار الدبلوماسية السيبرانية العالمية بمحطة أخرى هامة تمثلت في ابرام اتفاقية الأمن السيبراني الصينية الروسية، تضمنت

ISSN: 2352-975X ——————————EISSN: 2588-2368

الاتفاقية، التي تم توقيعها في الكرملين في 8 ماي 2015، إنشاء قنوات اتصال للاستجابة المشتركة للتهديدات في مجال الامن السيبراني الدولي، والتدريب المشترك للمتخصصين، والتعاون بين الأجهزة المختصة في مجال سلامة البنى التحتية الحيوية للمعلومات، وكذا التنسيق بين روسيا والصين في قضايا الأمن السيبراني العالمي، سيّما في إطار المنظمات والمنتديات الدولية.[24]

جاءت الاتفاقية لتعكس التطابق الكبير في وجهات النظر بين روسيا والصين فيما يتعلق بالقضايا السيبرانية، كما عكس نصّها في كثير من الجوانب مقترح مدوّنة قواعد السلوك لمنظمة شنغهاي للتعاون التي تم تقديم نسختها الثانية إلى الجمعية العامة للأمم المتحدة في جانفي 2015، وتظهر هذه الاتفاقية تمسّك الدولتين بمفهوم "السيادة السيبرانية" في مقابل دعوة الولايات المتحدة إلى "الحرية السيبرانية" والى "أصحاب المصلحة المتعدّدين"، ويعطي ذلك إشارات واضحة على التوجهات الصينية والروسية نحو تحدي هيمنة الولايات المتحدة والغرب على أمن المعلومات الدولي.[25]

رغم الأشواط التي قطعتها حتى الآن، لا تزال الدبلوماسية السيبرانية تواجه عقبات كثيرة في سياق سعيها لحوكمة الفضاء السيبراني، ويتعيّن عليها قطع مسار طويل لبناء الثقة بين مختلف الفاعلين في ذلك الفضاء، ناهيك عن تقريب تصورات الدول الفاعلة بشأن جدوى بناء عالم سيبراني سلمي وآمن، لقد أظهر تدخل العملاء الروس في للتأثير على تصويت البريطانيين على البريكسيت من خلال استخدام وسائل التواصل الاجتماعي، ثم في التأثير على انتخابات الرئاسة الامريكية لعام 2016- من خلال اختراق أنظمة الكومبيوتر في مقر اللجنة الوطنية الديمقراطية وتسريب رسائل المترشحة هيلاري كلينتون، والاختراق الذي قادته الإمارات العربية المتحدة لأنظمة الحكومة القطرية في عام 2017 بنشر تصريحات كاذبة لتبرير الحصار على قطر، وهجمات التعطيل السيبرانية التي قام بها الإيرانيون ضد شركة النفط

EISSN: 2588-2368 ——————— ISSN: 2352-975X

السعودية "أرامكو"، الحاجة الماسة إلى إقامة تعاون دولي وثيق لدرء مخاطر التدمير السيبراني المتبادل، والى تحرك دبلوماسي فعال لحوكمة هذا الفضاء.

المحور الثالث: جيوسياسية الفضاء السيبراني وحدود الدبلوماسية السيبرانية

برهنت تفاعلات الفضاء السيبراني في العقدين الأخيرين عن تلاشي الاعتقاد الذي صاحب البدايات الأولى لانتشار الانترنت المتفائل بميلاد عالم جديد بدون حدود وبدون سيادة، وعلى النحو الذي تم مناقشته حتى الآن، تحولت القضايا السيبرانية بمختلف أشكالها إلى مسائل ذات أولوية عالية في أجندات السياسة الخارجية للدول سيّما الكبرى منها، وعادت الدول للبروز مرة أخرى كفواعل رئيسية في الفضاء السيبراني تعمل بلا هوادة على تطويعه لتأكيد سيادتها، وتستخدمه لمواصلة صراعها المستمر مع المنافسين.

إن المشكل الأساسي الذي يواجه الدبلوماسية السيبرانية في هذا العالم له علاقة مباشرة بتحول الفضاء السيبراني إلى ساحة رئيسية للصراع والتنافس الاستراتيجي، وفي الحقيقة، تسيطر على جيوسياسية الفضاء السيبراني حالة مفرطة من غياب الثقة بين أربعة لاعبين رئيسيين هم الولايات المتحدة وروسيا والصين والاتحاد الأوروبي، وفي ظل انتفاء قواعد ملزمة ومتفق بشأنها لضبط سلوك الفواعل الدولية ومساءلتها، تظل الفضاء السيبراني ساحة مفتوحة لـ"إطلاق النار على الخصوم"، ويحدث ذلك في خضم تضارب تصورات الدول الفاعلة حول طبيعة هذا الفضاء؛ وفي الاعتراف بالأطراف المتدخلة فيه، وفي مضمون سيادة الدولة وهي القضايا التي تكاد تحبط مساعي الدبلوماسية السيبرانية في خلق وحوكمة فضاء سيبراني سلمي.

أولا- تناقضات "الفضاء المفتوح" والسيادة السيبرانية":

مثّل تحول الفضاء السيبراني إلى ساحة للصراع القيمي بين القوى اللبرالية وغير اللبرالية أبرز العقبات الجيوسياسية في طريق الدبلوماسية السيبرانية، فالجهود التي

ISSN: 2352-975X ——————————EISSN: 2588-2368

بذلتها الأمم المتحدة برعايتها للمفاوضات الرامية إلى وضع قواعد منظِّمة للفضاء السيبراني آلت في نهاية العقد الثاني إلى طريق مسدود بسبب الانقسام الحاد بين معسكرين كبيرين، يتبنى أحدهما مبادئ "الانترنت المفتوح" و"حرية الانترنت" و"أصحاب المصلحة المتعددين"، ويتمسك الآخر بفكرة "السيادة السيبرانية"-أي بسيطرة الدولة على المجال السيبراني على غرار سيطرتها على المجالات البرية والبحرية والجوية، وتعكس تلك المواقف المتضاربة صورة مصغرة عن واقع التنافس الجيوسياسي في العالم حاليا.

فالولايات المتحدة، ومعها الاتحاد الأوروبي والدول الغربية بشكل عام، ترى نفسها "المشغل" المسؤول في الفضاء السيبراني، وترى أنّ هذا الأخير يجب أن يظل حاملا ومروِّجا للقيم اللبرالية التي ترعرع في بيئتها، ومن ثم يقع على عاتق الولايات المتحدة والقوى اللبرالية واجب التصدّي لكل ما من شأنه تهديد الحرية في الفضاء السيبراني وتقييد التدفق الحّر للبيانات فيه، ويدخل ضمن ذلك التزامها بمواجهة الأنظمة الاستبدادية والمدافعة عن السيادة على الإنترنت، كما تقترح الولايات المتحدة نموذجا لإدارة الانترنت من "أصحاب المصلحة المتعددين"، ويعتبر ذلك طبيعيا من وجهة نظر الولايات المتحدة أين نشأت الإنترنت في نطاق تعاون القطاعين العام والخاص.[26]

في المقابل تعارض الصين وروسيا فكرتي "الإنترنت المفتوح" و"الحماية من تدخل الدولة" وتتمسكان بفكرة "السيادة السيبرانية" والتي تعني تحكم الدولة الكامل في الفضاء السيبراني داخل حدودها، ولا تنظر الدولتان إلى الإنترنت باعتباره كائنا غريبا من صنع الولايات المتحدة فحسب، بل تخشيان الهيمنة الأميركية في الفضاء السيبراني وقدرتها على تقويض الاستقرار الداخلي فيهما، وقد عزّزت العمليات الاعلامية لتدخل الغرب في "الثورات الملونة" في أوكرانيا وجورجيا و"الربيع العربي" من تصميم بكين وموسكو ليس فقط على السيطرة على الإنترنت، بل أيضا

في خلق "انترنت محلي منفصل"، وينظر في هذا الشأن إلى مشروع بكين "طريق الحرير الرقمي" على أنه محاولة صينية لكسر هيمنة الولايات المتحدة على الانترنت،[27] ومن غير المستبعد ميلاد أنترنت آخر مواز للأنترنت الحالي، ما يجعل مساعي الدبلوماسية السيبرانية لحوكمة هذا الفضاء دون أفق للنجاح.

ثانيا- الهيمنة السيبرانية الأمريكية واشكالات بناء الثقة:

بسبب الطريقة التي تأسست بها الانترنت في سبعينيات القرن الماضي (كجزء من الأبحاث العسكرية الامريكية Arbanet)، ظل الجزء الأعظم من المكوّن المادي للأجهزة التي تقوم عليها الانترنت داخل الولايات المتحدة، ويأتي في مقدمة ذلك كابلات الألياف الضوئية ونقاط تبادل الإنترنت (IXPs) ومراكز البيانات الخاصة بمقدمي خدمات الإنترنت (ISPs)، ولذا السبب، يقدّر الخبراء أن نحو 80% من حركة الإنترنت اليوم تمر عبر كابلات الألياف الضوئية في أراضي الولايات المتحدة وذلك ما أعطاها ميزة فريدة،[28] ومثلما كشفت عن ذلك تسريبات إدوارد سنودن، استغلت وكالة الأمن القومي (NSA) تلك الميزة للقيام بعمليات غزيرة للرقابة على أنشطة الحلفاء والخصوم على حدّ سواء.

عزّزت تلك التسريبات المخاوف التي كانت قائمة بالفعل من دور الانترنت كأداة لحماية وتعزيز الهيمنة الامريكية، ومن التداعيات التي تحملها الهيمنة على الانترنت على مصالح وخصوصيات الدول الأخرى، وقد استغلت الصين وروسيا الجدل العالمي المحيط بالمراقبة التي قامت بها وكالة الأمن القومي لدفع نموذجهما لإدارة الإنترنت، والذي يشدّد على سيطرة الحكومات الوطنية على عمليات الإنترنت الرئيسية[29]، وكانتا أكثر وضوحا في دعوتها لإنشاء "تنظيم دولي" للفضاء السيبراني في شكل اتفاقية ملزمة (قد يكون الاتحاد الدولي للاتصالات)، وهي الفكرة التي رفضتها الولايات المتحدة ما قوّض الجهود الدبلوماسية للوصول إلى قرار توافقي، وعند مراجعة تصريحات المبعوثين الروسي والامريكي عام 2017 يظهر عمق حالة

ISSN: 2352-975X ——————————EISSN: 2588-2368

عدم الثقة المتبادلة وبحسب المبعوث الروسي الخاص، فإن التوصل إلى توافق تعرقله: "... بعض الدول التي تسعى إلى فرض قواعد اللعبة الخاصة بها في الفضاء المعلوماتي على العالم أجمع...استناداً إلى إنجازاتها التكنولوجية"[30]، بدوره صرح الممثل الخاص للولايات المتحدة: "لقد توصلت إلى نتيجة مؤسفة مفادها أن أولئك الذين لا يرغبون في تأكيد انطباق هذه القواعد والمبادئ القانونية الدولية يعتقدون أن دولهم حرة في التصرف في الفضاء السيبراني أو من خلاله".[31]

يحيلنا التصريح الأخير للممثل الأمريكي إلى مسألة أخرى في غاية الأهمية لتبرير حالة غياب الثقة المتبادل بين القوى اللبرالية وغير اللبرالية، ويتعلق الامر تحديدا بعدم وجود اتفاق عالمي بشأن فرص تطبيق القانون الدولي على الفضاء السيبراني، وحتى الاتفاقات الموجودة بالفعل (مثل اتفاقية بودابست) لم يتم التصديق عليها من قبل الجهات الفاعلة في الفضاء السيبراني كروسيا والصين والهند، ويعني ذلك ضمنيا تضاربا في المواقف بشأن تحديد معايير السلوك المقبول وغير المقبول في الفضاء السيبراني، وفي تحديد أسلوب التعامل مع الجهات المنتهكة للقواعد المتفق عليها في الفضاء السيبراني، وقد أسهم التوجس من خلفيات المواقف المعلنة في اذكاء حالة شبيهة بالمعضلة الأمنية في الفضاء السيبراني.

ثالثا- الفجوة الرقمية وعسكرة القضايا السيبرانية:

على النحو الذي تمت مناقشته أعلاه، تعطي البنية الحالية للفضاء السيبراني ميزة كبيرة لعدد محدود من الدول هي الولايات المتحدة والصين وروسيا بدرجة أقل، وليس للدول المشاركة "الصغيرة" أي فرص لموازنة الفاعلين الرئيسيين في ذلك الفضاء، بل أن قضايا الفضاء السيبراني لا تحظى لديها بأولوية كبيرة مثلما يعكس ذلك افتقارها لدبلوماسية سيبرانية، ويكمن جوهر المشكلة هنا في كون القوى الرئيسية التي بمقدورها صياغة جوانب المشهد السيبراني العالمي هي الأطراف المستفيدة من عدم الالتزام أو من الالتزام غير القسري باللوائح المنظمة، ذلك لأنها

EISSN: 2588-2368 ——————— ISSN: 2352-975X

تحتفظ بقدرات سيبرانية كبيرة لمنع الدول الأخرى من اختراق بنيتها التحتية الأساسية، وهي في نفس الوقت القوى الفاعلة وصاحبة الدبلوماسية السيبرانية الأكثر نشاطا، وعلى هذا النحو، قد تجد الدول الصغيرة بالمنظور السيبراني نفسها ملزمة بمعايير سلوك تتماشى والاستراتيجيات السيبرانية للقوى الفاعلة، وساحة مفتوحة لحروب سيبرانية متوقعة بين القوى الجيوسياسية الكبرى مستقبلا.

في الجانب الآخر، دفع تعاظم دور شركات الانترنت التي تتخذ من الولايات المتحدة مقرا لها كجوجل وتويتر وفايسبوك ويوتيوب بالإضافة إلى شركات التكنولوجيا كآبل وإنتل إلى منح الولايات المتحدة قاعدة تكنولوجية هائلة مكنتها من بناء قدرات سيبرانية دفاعية وهجومية، ويفسّر ذلك جزئيا مواقف روسيا والصين وحتى الهند المعارضة لنهج أصحاب المصلحة المتعددين الذي تتمسك به الولايات المتحدة في موقفها من حوكمة الفضاء السيبراني، ومن المثير للاهتمام مقارنة شركات الانترنت والتكنولوجيا الامريكية كقوى جيوسياسية في القرن الحادي والعشرين بحال "الاخوات السبع" في النصف الثاني من القرن الماضي.

أخيرا وغير بعيد عن قضايا إدارة الانترنت، تعاني الدبلوماسية السيبرانية من التقليل الرسمي من مقدرتها على معالجة قضايا الأمن السيبراني، لا تنظر معظم الدول في الوقت الحالي إلى الفضاء السيبراني باعتباره مجالا للسياسة الخارجية، وتركت بذلك العديد من قضايا الأمن السيبراني للفنيين والعسكريين، وكنتيجة، أصبح موضوع الامن السيبراني أكثر بروزا في الاستراتيجيات الدفاعية والأمنية منه في وثائق السياسة الخارجية، واضطلعت الوكالات العسكرية وأجهزة الاستخبارات بالدور الأهم في إيجاد حلول لمشاكل الفضاء السيبراني، في حين كانت العديد من مشكلات هذا الفضاء ذات طابع سياسي وجيوسياسي، وقد أظهر الجدل بشأن دور شركة هواوي الصينية في وضع المعايير الصناعية وتطوير تقنيات اتصالات الجيل الخامس G5 العواقب الوخيمة لتجاهل اشراك الدبلوماسيين الأمريكيين في

ISSN: 2352-975X ——————————EISSN: 2588-2368

بداية الأمر، فعند ادراك الولايات المتحدة المتأخر لتلك الأهمية، كانت الصين قد نجحت بالفعل في تطوير غالبية معايير تكنولوجيا المرحلة الثانية من الجيل الخامس في الصين، ولم يكن بوسع الولايات المتحدة حينها سوى اطلاق حملة واسعة لتقويض شركة هواوي في العالم.[32]

في المجمل، دفع وضع الفضاء السيبراني ونقاط الخلاف السابقة بين الفاعلين الرئيسيين فيه إلى تعثّر الجهود الدبلوماسية التي قادها فريق الخبراء التابع للأمم المتحدة[33] لتنظيم سلوك الدول في هذا الفضاء، فبعد نجاح الفريق الرابع مبدئيا في التوصل إلى مبادئ أولية لقواعد السلوك في الفضاء السيبراني عام 2015، تعرضت تلك الجهود لاحقا لانتكاسات كبيرة بسبب تجذر عناصر الخلاف بين كبار الفاعلين، فقد رفضت الولايات المتحدة التصويت على تقرير الفريق الخامس بحجة عدم إشارة مسودته إلى انطباق القانون الدولي الإنساني على الهجمات السيبرانية، وهدّدت بالتصرف المنفرد مع حلفائها لوضع قواعد لمعاقبة المعتدين، ورغم التطور الذي حصل مع الفريق السادس الذي نجح في اصدار تقرير توافقي حول معايير السلوك السيبراني المقبول عام 2021، جاء انشاء فريق ثان-باقتراح من روسيا ومعارضة أمريكية- يضم جميع أعضاء الأمم المتحدة (مجموعة العمل المفتوحة العضوية OEWG) ليؤكد مرة أخرى خضوع جهود الدبلوماسية الجماعية التي ترعاها الأمم المتحدة لقواعد اللعبة الجيوسياسية الكبرى في هذا العالم، وتظل مع تلك التجاذبات فرص التوصل إلى قواعد سيبرانية عالمية هدفا بعيد المنال.

خاتمة:

لقد شكل الفضاء السيبراني مجالا جديدا لنشاط الدبلوماسية يتخطى استخدام التقنيات ووسائط التواصل الاجتماعي التي وفّرتها الثورة الصناعية الرابعة في تأدية وظائفها التقليدية، فعلى الرغم من تخلفها عن ادراك هذا المجال مقارنة بالأجهزة الأمنية والقضائية، انخرطت الدبلوماسية بشكل متزايد في النشاطات الهادفة إلى ضبط

EISSN: 2588-2368 ——————— ISSN: 2352-975X

تفاعلات هذا الفضاء في العقدين الأخيرين، سيّما في ظل عجز الحلول التقنية والأمنية على معالجة تعقيدات الامن السيبراني وقضايا التجسس وقرصنة الشبكات وتدمير أنظمة البنى التحتية من جهة، ولطبيعة تلك التحديات العالمية والمتخطية للحدود التي تستوجب ردودا جماعية ومنظمة من جهة ثانية، ومن هنا تحولت تلك الوظائف إلى مهام رئيسية يسترشد بها لون جديد من الدبلوماسية يسمى بالدبلوماسية السيبرانية.

على هذا النحو، تعتبر الدبلوماسية السيبرانية أداة لتنفيذ أجندات السياسة الخارجية للدول ومتابعة أهدافها فيما يتعلق بالفضاء السيبراني، وتشمل تلك الأهداف تعزيز التعاون الدولي لصيانة الأمن السيبراني وضبط التفاعلات السيبرانية ووضع قواعد لتنظيم هذا الفضاء والاحتكام اليها عند الضرورة، لذلك يظل التفاوض الأسلوب الرئيسي الذي ينتهجه الدبلوماسيون في التعامل مع مجمل القضايا المرتبطة بهذا الفضاء، كما أنه يعد عاملا مهما في تمييز مفهوم الدبلوماسية السيبرانية عن مفاهيم الدبلوماسية الإلكترونية والدبلوماسية الرقمية والدبلوماسية الافتراضية التي يكثر الخلط بين معانيها، وكما تمت مناقشته أعلاه، تشير الدبلوماسية السيبرانية إلى الفضاء السيبراني كمجال لنشاط الدبلوماسية، بينما تنظر المفاهيم الثلاثة السابقة إلى ذلك الفضاء كمصدر لأدوات تأدية الوظائف الدبلوماسية.

نجحت الدبلوماسية السيبرانية في تحقيق بعض المكاسب على صعيد ترسيخ دورها كأداة لا غنى عنها في عصر تكنولوجيا الاتصالات والمعلوماتية، فمعظم الدول اليوم-سيّما الكبرى منها- لديها اليوم استراتيجياتها السيبرانية وقامت بتعيين مفوضيها وسفرائها السيبرانيين، كما تحقق حتى الآن الاتفاق على أرضيات مشتركة للتعامل مع القضايا السيبرانية على مستويات ثنائية (كالاتفاق الروسي الصيني لعام 2015، والاتفاق الأمريكي الصيني في نفس العام أيضا) أو على مستوى إقليمي (مثل دليل تالين بالنسبة لدول حلف الناتو)، أما على المستوى الدولي فقد نجح فريق الخبراء

ISSN: 2352-975X ——————————EISSN: 2588-2368

الأممي في تحقيق شكل من أشكال التوافق على معايير السلوك المسؤول في الفضاء السيبراني عام 2021.

مع ذلك، مازال أمام الدبلوماسية السيبرانية مسار طويل وشاق لبلوغ مبتغى حوكمة الفضاء السيبراني، لقد أظهر مسار التفاوض التي قاده فريق الخبراء الأمميين، واستمرار الوقائع الخطيرة للتجسس السيبراني والقرصنة وتخريب الشبكات وسرقة البيانات، تحول هذا الفضاء بوضوح إلى مجال للتنافس الجيوسياسي بين الفاعلين الرئيسيين في النظام الدولي، ان التعارض الحاصل في مواقف الولايات المتحدة وروسيا والصين بشأن حرية تدفق الانترنت، ومكانة أصحاب المصلحة المتعددين، ونمط إدارة الانترنت العالمي، تشكِّل القيود الرئيسية التي أخفقت جهود الدبلوماسية السيبرانية في تخطيها حتى الآن، ومن غير المرجّح تجاوزها في المستقبل القريب لارتباطها بمنظومتين متعارضتين من القيّم، وبالتنافس الجيوسياسي الأكبر في القرن الحادي والعشرين.

الهوامش والمراجع:

(1)- Amel Attatfa et al, "Cyber Diplomacy: A Systematic Literature Review", Procedia Computer Science, Vol. 176 (2020), p. 64.

(2)- Agnes Kasper, Anna-Maria Osula & Anna Molnár, "EU cybersecurity and cyber diplomacy", IDP-INTERNET LAW AND POLITICS 34: (December 2021) p. 03.

(3)- Amel Attatfa et al, Op.Cit, p. 64.

(4)- Agnes Kasper, Anna-Maria Osula & Anna Molnár, Op.Cit, p. 04.

(5)- العربي العربي، "الدبلوماسية الرقمية وتأثيراتها في العلاقات الدولية"، مجلة لباب (مركز الجزيرة للدراسات)، السنة الثالثة، العدد العاشر (ماي 2021)، ص.136.

(6)- Mohd Razman Achmadi Muhammad & Noor Nirwandy, "A Study on Donald Trump Twitter Remark: A Case Study on the Attack of Capitol Hill", Journal of Media and Information Warfare Vol. 14(2), December 2021, p.76 75-104,

(7)- العربي العربي، مرجع سابق، ص.135.

(8)- Agnes Kasper, Anna-Maria Osula & Anna Molnár, Op. Cit, p.04.

(9)- Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", The Yale Journal of International Law, Vol.36 (2011), p.423

(10)- André Barrinha & Thomas Renard, "Cyber-diplomacy: the making of an international society in the digital age", Global Affairs, Vol.3, No. 4-5(2017), p. 356.

EISSN: 2588-2368 ——————————— ISSN: 2352-975X

(11)- The White House, International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World, (Washington D.C, May 2011), p. 12.
(12)- André Barrinha & Thomas Renard, Op.Cit, p. 359.
(13)- Information Security Policy Council, "International Strategy on Cybersecurity Cooperation - j-initiative for Cybersecurity", Tokyo: October, 2. 2013, p. 02.
(14)- Council of the European Union, "Council Conclusions on Cyber Diplomacy", Brussels, 11 February 2015, p.04.
(15)- Amel Attatfa et al, Op. Cit, p. 64.
(16)- André Barrinha & Thomas Renard, Op. Cit, p. 356.
(17)- Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", Journal of Strategic Security, Vol. 4, No. 2 (Summer 2011), p.52.
(18)- Avinash Kumar, "Cyber Diplomacy- The Concept, Evolution and its Applicability", International Journal of Cyber Diplomacy, Volume 3(2022), p. 24-25.
(19)- شريف نسيم قلتة بخيت، دليل "تالين": الهجمات الإلكترونية وحظر استخدام القوة في القانون الدولي"، نشر بتاريخ 25 نوفمبر 2017، متاح على الرابط: https: //accronline.com/article-detail.aspx?id=28958
(20)- Avinash Kumar, Op, Cit, p.25.
(21)- Maj J. Johnson, "The Implication Of Cyber On US-China Relations", Canadian Forces College, JCSP 43 (2016-2017), p.04.
(22)- Ibid, p.22
(23)- Ruqiya Anwar, "Why the US and China need a detente in cyberspace", South China Morning Post (On Line), 13 Sep, 2022, retrieved from: https: //www.scmp.com/comment/opinion/article/3192188/why-us-and-china-need-detente-cyberspace
(24)- E. Dilipraj, "Russia-China Nexus In Cyber Space", Newdelhi: Centre for Air Power Studies [CAPS], 15 june 2015, p.03.
(25)- Avinash Kumar, Op. Cit, p.29
(26)- Ruqiya Anwar, "Why the US and China need a detente in cyberspace", Op. Cit.
(27)- Shaun Riordan, The Geopolitics of Cyberspace: a Diplomatic Perspective, Boston: BRILL, 2019, p. 18
(28)- Ibid, p.17.
(29)- Michael Kolton, Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence, The Cyber Defense Review, Vol. 2, No. 1 (WINTER 2017), pp. 123.
(30)- Vladimir Korovkin, International regulation in cyber space: is effective mutual understanding possible? / English transl. by Nikulichev M.Y. // Social Novelties and Social Sciences. – Moscow: INION RAN, 2022, p.19
(31)- Ibid, p.20
(32)- Shaun Riordan, Op.Cit, p.73-74.
(33)- اسمه الكامل "فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي" تم تشكيله لأول مرة عام 2004، وهو يعمل ضمن لجنة نزع السلاح التابعة للجمعية العامة للأمم المتحدة.

ISSN: 2352-975X ——————————EISSN: 2588-2368