# Cyber Diplomacy: Governing Digital Conflicts and Shaping Norms in Cyberspace

## الدبلوماسية السيبرانية: حوكمة الصراعات الرقمية وتشكيل معايير الفضاء الإلكتروني

أ.م.د. رندا طلال حسن

Assist. Prof.PhD: Randa Talal Hassan

الاختصاص العام: العلوم السياسية

Political Science

الاختصاص الدقيق: العلاقات الاقتصادية الدولية

International Economic Relations

جامعة النهرين / كلية العلوم السياسية

AL-Nahrain University /College of Political Science

dr.randa.talal@nahrainuniv.edu.iq

07901782371

**الملخص**

تُعدّ الدبلوماسية السيبرانية أحد المفاهيم الحديثة في العلاقات الدولية، حيث ظهرت استجابة للتطور السريع في تكنولوجيا المعلومات وازدياد التهديدات في الفضاء الإلكتروني. وتركّز هذه الدبلوماسية على إدارة الصراعات الرقمية بين الدول، ووضع أطر وقواعد تنظّم السلوك في الفضاء السيبراني بما يحدّ من التصعيد ويعزز الاستقرار الدولي. هدفت الدبلوماسية السيبرانية إلى تحقيق التعاون بين الدول من خلال التفاوض وتبادل المعلومات وبناء الثقة، إضافة إلى وضع معايير دولية تضبط استخدام التكنولوجيا، خاصة فيما يتعلق بالأمن السيبراني، والهجمات الإلكترونية، وحماية البنية التحتية الحيوية. كما تسعى إلى تقليل مخاطر الحروب السيبرانية التي قد تؤثر على الأمن القومي والاقتصاد العالمي. وتواجه هذه الجهود تحديات كبيرة، من أبرزها غياب إطار قانوني دولي ملزم، وصعوبة تحديد مصدر الهجمات الإلكترونية، وتباين مصالح الدول الكبرى.

**الكلمات المفتاحية:** الدبلوماسية السيبرانية، الفضاء الالتكروني، الحوكمة، الصراعات الرقمية

## Abstract

Cyber diplomacy is a relatively new concept in international relations, emerging in response to the rapid development of information technology and the increasing threats in cyberspace. This form of diplomacy focuses on managing digital conflicts between states and establishing frameworks

and rules to govern behavior in cyberspace, thereby reducing escalation and promoting international stability.Cyber diplomacy aims to foster cooperation between states through negotiation, information sharing, and trust-building, as well as establishing international standards to regulate technology use, particularly concerning cybersecurity, cyberattacks, and the protection of critical infrastructure. It also seeks to mitigate the risks of cyber warfare, which can impact national security and the global economy. These efforts face significant challenges, most notably the absence of a binding international legal framework, the difficulty in identifying the source of cyberattacks, and the divergent interests of major powers.

**Keywords:** Cyber Diplomacy, Cyberspace, Governance, Digital Conflicts

**المقدمة**

شـهد النظام الدولي خلال العقود الأخيرة تحولات عميقة بفعل الثورة الرقمية والتطور المتسـارع في تكنولوجيا المعلومات والاتصـالات، الأمر الذي أدى إلى إعادة تشـكيل طبيعة التفاعلات بين الدول ووسـائل ممارسـتها للسياسة الخارجية. ولم يعد الفضاء الإلكتروني مجرد وسيط للتواصل، بل أضحى مجالا استراتيجيا تتقاطع فيه المصالح الأمنية والاقتصادية والسياسية، وتتنافس داخله الدول على النفوذ والتأثير.

في هذا السياق، برزت الدبلوماسية السيبرانية كأحد أبرز مخرجات هذا التحول، بوصفها إطارا حديثا لإدارة التفاعلات والصراعات في الفضاء الإلكتروني، وسعيا لوضع قواعد ومعايير تنظم سلوك الدول وتحدّ من مخاطر التصعيد. وقد تزايدت أهمية هذا المجال مع تصاعد الهجمات السيبرانية واستهداف البنى التحتية الحيوية، مما جعل الأمن السيبراني جزءا أساسيا من منظومة الأمن القومي.

ورغم الجهود الدولية المتزايدة لتطوير أطر حوكمة الفضاء الإلكتروني، إلا أنها ما تزال تواجه تحديات معقدة، من أبرزها غياب إطار قانوني دولي ملزم، وصعوبة تحديد مصادر الهجمات، وتباين الرؤى بين الدول. ومن هنا، تسعى هذه الدراسة إلى تحليل الدبلوماسية السيبرانية وأدوارها في إدارة الصراعات الرقمية، واستكشاف مدى قدرتها على تعزيز الاستقرار الدولي في ظل التحولات التكنولوجية المتسارعة.

**أولا: أهمية البحث**

تنبع أهمية هذا البحث من الدور المتصاعد للفضاء السيبراني في تشكيل العلاقات الدولية وتحوله إلى ساحة رئيسية للصراع والتعاون بين الدول، مما يجعل فهم الدبلوماسية السيبرانية ضرورة علمية وعملية. كما تسهم الدراسة في إثراء الأدبيات العربية في هذا المجال، وتقدم إطارا تحليليا يساعد في فهم التهديدات الرقمية وآليات إدارتها، بما يدعم تطوير سياسات أكثر فاعلية في ظل تزايد ارتباط الأمن القومي بالتكنولوجيا.

**ثانيا: أهداف البحث**

يهدف هذا البحث إلى تحليل مفهوم الدبلوماسية السيبرانية وتحديد أبعادها، وتتبع تطورها التاريخي والمؤسسي، وتشخيص التحديات التي تواجه حوكمة الصراعات الرقمية، فضلا عن تقييم الأطر القانونية والاستراتيجية الناظمة للفضاء الإلكتروني، واستشراف مستقبل هذا المجال في ظل التحولات التكنولوجية، وصولا إلى تقديم رؤى وتوصيات تسهم في تعزيز فعالية الحوكمة السيبرانية.

**ثالثا: إشكالية البحث**

ان الفضاء السيبراني بات يمثل ساحة مركزية للتفاعل والصراع في العلاقات الدولية، في ظل تصاعد التهديدات الرقمية وتزايد الاعتماد على البنى التحتية التكنولوجية. ورغم تنامي الاهتمام الدولي بالدبلوماسية السيبرانية بوصفها أداة لإدارة هذه التفاعلات، إلا أن الجهود المبذولة في هذا المجال ما تزال تواجه قيودا بنيوية وقانونية وسياسية تحدّ من فاعليتها. وعليه، تتمحور إشكالية البحث حول التساؤل الرئيس الآتي: إلى أي مدى تستطيع الدبلوماسية السيبرانية الإسهام في حوكمة الصراعات الرقمية وبناء نظام دولي مستقر في الفضاء الإلكتروني في ظل التنافس الجيوسياسي والتطور التكنولوجي المتسارع؟

ويتفرع عن هذا التساؤل عدد من التساؤلات الفرعية:

1. ما طبيعة الدبلوماسية السيبرانية وما أبعادها في العلاقات الدولية المعاصرة؟
2. كيف تطورت الأطر المؤسسية والقانونية الناظمة للفضاء السيبراني؟
3. ما أبرز التحديات التي تواجه حوكمة الصراعات الرقمية؟
4. ما حدود فاعلية المعايير الدولية الحالية في تنظيم سلوك الدول في الفضاء الإلكتروني؟
5. ما الآفاق المستقبلية للدبلوماسية السيبرانية في ظل التقنيات الناشئة؟

**رابعا: فرضية البحث**

ينطلق البحث من الفرضية الرئيسة الآتية:

أن الدبلوماسية السيبرانية تسهم في الحد من الصراعات الرقمية وتعزيز الاستقرار الدولي، إلا أن فاعليتها تظل محدودة بسبب غياب إطار قانوني ملزم، وتباين مصالح الدول، وتسارع التطور التكنولوجي، مما يحد من قدرتها على ضبط السلوك في الفضاء السيبراني بشكل كامل.

**خامسا: منهجية البحث**

تم الاعتماد على المنهج الوصفي التحليلي في عرض مفهوم الدبلوماسية السيبرانية وتطورها، إلى جانب المنهج التحليلي النقدي لتقييم الأطر القانونية والمؤسسية، كما توظف المنهج المقارن لتحليل تباين مواقف الدول تجاه حوكمة الفضاء السيبراني، وذلك بهدف تقديم فهم شامل ومتوازن للموضوع.

**سادسا: حدود البحث**

اقتصر البحث موضوعيا على تحليل الدبلوماسية السيبرانية وحوكمة الصراعات الرقمية دون التوسع في الجوانب التقنية البحتة، وتمتد زمنيا من بدايات الاهتمام الدولي بالأمن السيبراني في العقد الأول من الألفية الثالثة حتى الوقت الراهن، فيما تركز مكانيا على المستوى الدولي مع الإشارة إلى بعض النماذج الإقليمية عند الضرورة.

**سابعا: هيكلية البحث**

ينطلق هذا البحث من مقدمة تمهيدية تؤسس للإطار العام للدراسة وتعرض إشكاليتها وأهدافها، ثم يتدرج في معالجة الموضوع عبر تسلسل منطقي يبدأ بتأصيل المفهوم النظري للدبلوماسية السيبرانية من حيث تعريفها وأبعادها وخصائصها في سياق العلاقات الدولية المعاصرة، قبل أن ينتقل إلى تتبع تطورها التاريخي والمؤسسي على المستويين الدولي والإقليمي، مع إبراز أهم المبادرات والجهود التي أسهمت في تشكيل هذا الحقل. وبعد ذلك، يتناول البحث تحليل التحديات الرئيسية التي تواجه حوكمة الصراعات الرقمية، من خلال مناقشة الإشكاليات المرتبطة بتحديد المسؤولية، وتباين الرؤى بين الدول، وتعقيد البيئة التقنية، وضعف الثقة الدولية. وفي مرحلة لاحقة، يعرض البحث الأطر القانونية والاستراتيجية التي تسعى إلى تنظيم السلوك في الفضاء السيبراني، مع تقييم مدى فاعليتها وحدودها في ظل غياب التزامات قانونية ملزمة. ويختتم البحث بمحور يستشرف الآفاق المستقبلية للدبلوماسية السيبرانية في ضوء التطورات التكنولوجية المتسارعة، وصولا إلى خاتمة تتضمن أبرز النتائج التي توصلت إليها الدراسة، إلى جانب مجموعة من التوصيات التي يمكن أن تسهم في تعزيز فاعلية الحوكمة السيبرانية على المستوى الدولي.

**أولا: المفهوم – ماهية الدبلوماسية السيبرانية**

يشير مصطلح الدبلوماسية السيبرانية إلى ذلك الفرع الحديث من الدبلوماسية الذي يتعامل مع القضايا والنزاعات الناشئة في الفضاء الإلكتروني. وقد عرّف أحد الباحثين الدبلوماسية السيبرانية بأنها: "أسلوب محدد تنتهجه الفواعل الدولية في تعاملها مع المشكلات المختلفة التي تنشأ في الفضاء السيبراني، [1] .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 المسئول في الفضاء السيبراني" . يُستدل من هذا التعريف أن جوهر الدبلوماسية السيبرانية يتمثل في إدارة العلاقات بين الدول ضمن الفضاء السيبراني بهدف التصدي لمختلف القضايا والتهديدات الرقمية المترتبة على الاستخدام المتنامي لتقنيات المعلومات والاتصالات

[1] - محمد عبد الفتاح. (2025). "مفهوم الدبلوماسية السيبرانية". المركز المصري للفكر والدراسات الاستراتيجية (ECSS) – ورقة بحثية منشورة بتاريخ 11 مايو 2025.

على المستوى الدولي . وبعبارة أخرى، تسعى الدبلوماسية السيبرانية إلى حوكمة الفضاء الإلكتروني وكل ما يحدث فيه من تفاعلات عبر أدوات الدبلوماسية الحديثة، بما يضمن تحقيق أهداف السياسة الخارجية للدول وحماية أمنها القومي في العالم الرقمي .[1].

إن الدبلوماسية السيبرانية تشتمل على طيف واسع من الأنشطة والمجالات الفرعية. فمن جهة، هي امتداد للدبلوماسية التقليدية ولكن بأدوات عصرية، حيث تُستخدم المنصات الرقمية ووسائل الاتصال الحديثة للتفاوض وإدارة الأزمات والتواصل بين الحكومات بشكل آني وعابر للحدود الجغرافية . وقد نشأ هذا النمط الجديد مع بدايات انتشار الإنترنت والبريد الإلكتروني ووسائل التواصل الاجتماعي التي أخذت تُكمّل القنوات الدبلوماسية التقليدية، مما وسّع نطاق العمل الدبلوماسي بشكل غير مسبوق . ومن جهة أخرى، تتميز الدبلوماسية السيبرانية بتركيزها على قضايا أمن الفضاء الإلكتروني بكل جوانبها، بما في ذلك التعاون الدولي لمكافحة الجرائم الإلكترونية، وحماية البنية التحتية الحرجة من الهجمات السيبرانية، والتصدي لعمليات القرصنة والتجسس الإلكتروني، إضافة إلى وضع معايير لسلوك الدول المسؤول في الفضاء السيبراني لضمان استقرار هذا الفضاء ومنع انزلاق الصراعات الرقمية إلى حروب شاملة . وبذلك تختلف الدبلوماسية السيبرانية عن الدبلوماسية الرقمية (المعنية بتوظيف التكنولوجيا لتعزيز التواصل الدبلوماسي العام) في كون الأولى تركز بصورة أكبر على الجوانب الأمنية والاستراتيجية للفضاء الإلكتروني وكيفية ضبطها عبر التعاون الدولي.[2].

شكل 1: الأبعاد المتداخلة للدبلوماسية السيبرانية: يمكن تصور الدبلوماسية السيبرانية كنقطة تقاطع بين ثلاثة مجالات رئيسية هي الأمن القومي السيبراني، والتنمية الاقتصادية الرقمية، وحماية القيم وحقوق الإنسان في الفضاء الإلكتروني. يمثل الشكل ثلاثة دوائر متشابكة ترمز إلى هذه المجالات، بحيث تقع الدبلوماسية السيبرانية في منطقة التداخل الوسطي بينها. هذا يعبّر عن الطبيعة الشمولية للدبلوماسية السيبرانية التي تتطلب موازنة الاعتبارات الأمنية (كحماية البنى التحتية ومنع الصراعات الرقمية) مع الاعتبارات الاقتصادية (تعزيز التعاون الرقمي العابر للحدود من أجل ازدهار الاقتصاد الرقمي العالمي) ومع الاعتبارات الاجتماعية والأخلاقية (حماية خصوصية الأفراد وحقوقهم الرقمية). إن فهم هذه الأبعاد المتداخلة ضروري لرسم سياسات سيبرانية متوازنة تحقق الأمن الرقمي وفي الوقت ذاته تدعم الابتكار والتنمية وتحترم القيم الإنسانية في العالم الرقمي.[3].

---

[1] - محمد عبد الفتاح. مصدر سابق , ص11

[2]- سيمون هوتاجالونج. (2024). "الدبلوماسية السيبرانية.. فرص وتحديات". يوراسيا ريفيو (مقال مترجم إلى العربيةومنشور في بوابة الشروق ,ص23

[3]- سيمون هوتاجالونج.مصدرسابق ,ص26

**ثانيا: التطور التاريخي والمؤسسي**

ظهرت ملامح الدبلوماسية السيبرانية بشكل واضح خلال العقدين الأخيرين بالتوازي مع تصاعد أهمية الفضاء الإلكتروني كساحة للتنافس الدولي. فعلى الرغم من أن استخدام التقنيات الرقمية في العمل الدبلوماسي بدأ منذ انتشار الإنترنت في أواخر القرن العشرين، إلا أن ترسيخ الدبلوماسية السيبرانية كمجال مستقل ارتبط بتطور الوعي بالتهديدات السيبرانية وبروز الحاجة لإطار تعاون دولي لمواجهتها. ويمكن تتبع التطور التاريخي والمؤسسي لهذا المجال عبر مراحل ومحطات رئيسية نوجزها فيما يلي:

- البدايات (منتصف العقد 2000): شهدت أواخر العقد الأول من الألفية الجديدة نقطة تحول مهمة، حيث طرحت الولايات المتحدة عام 2008 مبادرة أول إستراتيجية دولية للفضاء الإلكتروني ركزت على قضايا الفضاء السيبراني بما فيها المصالح والتهديدات المرتبطة به . وقد مثلت هذه الوثيقة أول اعتراف رسمي على مستوى دولة كبرى بأهمية وجود إستراتيجية شاملة للتعامل مع فضاء الإنترنت عالميا.[1]. كما دفعت حوادث مثل الهجوم السيبراني واسع النطاق على إستونيا (2007) إلى تنبيه حلف الناتو لضرورة تطوير سياسة جماعية للأمن السيبراني، بعد أن كشفت تلك الهجمات مدى عدم جاهزية الحلف آنذاك للتعامل مع هذا الواقع الجديد .
- بناء أطر التعاون الدولي (2010–2015): بادرت الأمم المتحدة عبر الجمعية العامة بتناول قضية أمن المعلومات على المستوى الدولي. ففي عام 2010 تبنت الجمعية قرارا (رقم 24/66) بإنشاء فريق خبراء حكومي دولي (UN GGE) لدراسة التطورات في ميدان أمن المعلومات ، وذلك إثر مقترح روسي بهدف مواجهة الأخطار المتزايدة في الفضاء السيبراني العالمي . عملت مجموعات الخبراء هذه خلال السنوات التالية على بناء توافق دولي حول مبادئ السلوك المسؤول في الفضاء الإلكتروني. وقد تكللت جهودها عام 2013 بالاعتراف الدولي بأن القانون الدولي (بما فيه ميثاق الأمم المتحدة) ينطبق على الفضاء السيبراني، ثم في تقريرها لعام 2015 قدمت المجموعة أول مجموعة من المعايير السلوكية الطوعية للدول في الفضاء الإلكتروني (غير ملزمة قانونا لكنها تمثل توافقا سياسيا مهما) . شكّل ذلك تطورا محوريا حيث بات لدى المجتمع الدولي إطار مفاهيمي أولي لحوكمة السلوك السيبراني للدول، يتضمن مبادئ مثل عدم استهداف البنية التحتية المدنية الحيوية بهجمات سيبرانية في وقت السلم، والتعاون لوقف الأنشطة الضارة المنطلقة من أراضي الدول، واحترام مسؤولية كل دولة عن سلوك جهات الفضاء الإلكتروني الموجودة ضمن ولايتها .[2].

---

[1] -NATO – North Atlantic Treaty Organization. CyberDefence“ .(2024),p45

[2] -Adina Ponta. (2021). “Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes”. ASIL Insights, p95

- تعزيز البنى المؤسسية الوطنية والإقليمية (2016–2022): مع تزايد الإدراك بخطورة التهديدات الإلكترونية، سارعت الدول والمنظمات إلى إنشاء هياكل دبلوماسية وأمنية متخصصة. فمثلا، اعترف حلف شمال الأطلسي (الناتو) في قمته عام 2016 بالفضاء السيبراني كميدان عمليات قتالية بجانب البر والبحر والجو ، مؤكدا أن أي هجوم سيبراني ذي أثر بالغ قد يفعّل مبدأ الدفاع المشترك (المادة 5). كما أطلق الناتو مبادرة "تعهد الدفاع السيبراني" (2016) لتعزيز قدرات الدول الأعضاء في التصدي للهجمات، وتم تحديثها بأهداف أكثر طموحا عام 2023 .[1] وعلى الصعيد الأوروبي، اعتمد الاتحاد الأوروبي أول إستراتيجية للأمن السيبراني عام 2013، ثم عيّن لاحقا منسقا خاصا (أشبه بسفير سيبراني) لتنسيق قضايا الفضاء الإلكتروني على المستوى الدولي . وبين عامي 2015 و2017 طوّر الاتحاد ما يعرف بـ**"صندوق أدوات الدبلوماسية السيبرانية" (CyberDiplomacyToolbox)** متضمنا سياسات وآليات للردع الدبلوماسي ضد الأنشطة السيبرانية الخبيثة . وفي عام 2019 أقرّ الاتحاد إطارا عاما لفرض عقوبات أوروبية على الجهات المسؤولة عن الهجمات السيبرانية ، وقد تم فعليا لاحقا إدراج كيانات وأفراد من دول مختلفة في قوائم العقوبات بعد اتهامهم بالتورط في هجمات خطيرة. أما على المستوى الوطني، فقد أنشأت العديد من الدول أقساما وهيئات متخصصة بالدبلوماسية السيبرانية ضمن وزارات الخارجية. وعلى سبيل المثال، قامت الولايات المتحدة في أبريل 2022 بإنشاء مكتب خاص للأمن السيبراني والسياسة الرقمية في وزارة الخارجية، يُعدُّ الأول من نوعه عالميا، بهدف تنسيق الاستراتيجيات الدبلوماسية لمواجهة التهديدات السيبرانية وتعزيز التعاون الدولي في هذا المجال .[2]
- توسيع المشاركة الدولية (من 2018 حتى الآن): في السنوات الأخيرة، انخرط عدد أكبر من الدول (بما فيها دول نامية) في مناقشات وضع معايير حوكمة الفضاء السيبراني. فإلى جانب مجموعات الخبراء محدودة العضوية، اتفقت الأمم المتحدة عام 2018 على إنشاء فريق عامل مفتوح العضوية (OEWG) يضم جميع الدول الراغبة في مناقشة أمن المعلومات الدولي . وقد أصدر هذا الفريق تقريرا توافقيا عام 2021 أكد فيه على تبنّي نفس مجموعة قواعد السلوك الـ11 التي خرج بها تقرير 2015، ودعا إلى تطوير إجراءات لبناء الثقة والقدرات بين الدول . وتم تمديد ولاية هذا الفريق العامل للعمل خلال 2021–2025 لضمان استمرار الحوار الشامل حول أمن الفضاء السيبراني . وبالتوازي، طرحت قوى كبرى رؤى متباينة: فبينما تدعو دول غربية إلى الحفاظ على انفتاح الإنترنت وحرية تدفق المعلومات مع تطبيق القواعد الدولية القائمة، تضغط دول أخرى كروسيا والصين نحو مفهوم "السيادة السيبرانية" واحترام حق كل دولة في التحكم بفضائها

[1] -Brad Smith. (2017). "The Need for a Digital Geneva Convention". Microsoft On the Issues Blog – p33

[2] -Laasme, M. (2012). "Estonia: Cyber Window into the Future of NATO". Joint Force Quarterly, 63(4), 58-63 – National Defense University Press p57

المعلوماتي الداخلي وبلورة معاهدة دولية جديدة لأمن المعلومات . هذه التجاذبات تعكس تعدد الأجندات في الدبلوماسية السيبرانية، مما يجعل تطورها المؤسسي عملية تفاوض مستمرة.[1] .جدول 1 يوضح بشكل مقارن أبرز الجهود الدولية والمؤسسية في ميدان الدبلوماسية السيبرانية وحوكمة الفضاء الإلكتروني:

جدول 1: أبرز المبادرات والمؤسسات الدولية في الدبلوماسية السيبرانية

| الجهة/الإطار | أهم المبادرات والإنجازات في حوكمة الفضاء السيبر اني |
|---|---|
| الأمم المتحدة | - إنشاء فرق خبراء حكومية (UNGGE) منذ 2010 لصياغة مبادئ السلوك المسؤول للدول في الفضاء السيبراني . - اعتماد تقارير توافقيّة (2013، 2015) تؤكد سريان القانون الدولي في الفضاء الإلكتروني وتوصي بمعايير طوعية للسلوك (مثل عدم مهاجمة البنى التحتية المدنية إلكترونيا) . - إطلاق فريق عمل مفتوح العضوية (OEWG) يضم جميع الدول (بدءا من 2019) لمتابعة الحوار وبناء القدرات والثقة سيبرانيا .[2] . |
| الاتحاد الأوروبي | - إصدار إستراتيجية الاتحاد للأمن السيبراني (2013) وتحديثها (2020) مع التركيز على السيادة التكنولوجية وبناء الشراكات . - تعيين سفير للأمن السيبراني لتمثيل قضايا الفضاء الإلكتروني دوليا . - تطوير صندوق أدوات للدبلوماسية السيبرانية (اعتمد في 2017) يتضمن إجراءات دبلوماسية منسقة للاتحاد للردع والرد على الهجمات السيبرانية . - اعتماد نظام عقوبات سيبراني أوروبي (2019) مكّن من معاقبة أطراف متورطة في هجمات رقمية تهدد دول الاتحاد . |
| حلف الناتو (NATO) | - الاعتراف بالفضاء الإلكتروني كمجال عمليات عسكرية (قمة وارسو 2016) والتأكيد أن الهجوم السيبراني الكبير قد يستدعي الدفاع الجماعي . - إقرار تعهد الدفاع السيبراني (2016) لتعزيز دفاعات الدول الأعضاء، وتحديثه بأهداف أعلى لعام 2023 . - إنشاء مركز الدفاع السيبراني للتميز (CCDCOE) في إستونيا (2008) لتبادل الخبرات والتدريب ووضع دراسات قانونية (مثل دليل تالين الذي أعده خبراء لتعريف كيفية انطباق القانون الدولي على النزاعات السيبرانية). - تكثيف التشاور وتبادل المعلومات بين الحلفاء حول التهديدات السيبرانية، ووضع آلية للتنسيق والرد المشترك على الهجمات عند الضرورة .[3] . |

---

[1]- Adina Ponta, p98

[2]- تقارير وأخبار الأمم المتحدة حول أعمال فريق الخبراء الحكومي والأعمال ذات الصلة (2010–2021) – مختلف الوثائق الرسمية الصادرة عن الأمم المتحدة بشأن أمن المعلومات الدولي.

[3]- اتفاقية بودابست لمكافحة الجرائم المعلوماتية (2001) – النص الرسمي للمعاهدة الصادر عن مجلس أوروبا (ساري النفاذ 2004)

| | |
|---|---|
| مبادرات متعددة الأطراف | - مدونة قواعد السلوك لأمن المعلومات (قدمتها منظمة شنغهاي للتعاون بقيادة الصين وروسيا، 2015): طرح لمبادئ سيادة الدولة على الفضاء المعلوماتي والتعاون ضد الاستخدام العدائي للتقنية (لم تعتمد دوليا من قبل الغرب). - نداء باريس من أجل الثقة والأمن في الفضاء السيبراني (2018): مبادرة غير ملزمة بقيادة فرنسا، وقّعتها عشرات الدول ومئات المنظمات والشركات، تدعو لحماية المدنيين والبنية التحتية ومنع نشر أدوات الاختراق . - مبادرة مايكروسوفت ("اتفاقية جنيف الرقمية"): دعوة أطلقتها شركة مايكروسوفت عام 2017 لصياغة اتفاقية دولية تلزم الدول بحماية المدنيين من الهجمات السيبرانية في زمن السلم، على غرار اتفاقيات جنيف للحروب . رغم الدعم من شركات وخبراء، لا تزال هذه الفكرة في طور الحشد المعنوي دون مسار تفاوض رسمي. |

**ثالثا: التحديات الكبرى في حوكمة الصراعات الرقمية**

رغم التقدم الملحوظ في الاهتمام الدولي بقضايا الفضاء الإلكتروني، تواجه الدبلوماسية السيبرانية جملة تحديات معقدة تجعل مهمة حوكمة الصراعات الرقمية ووضع معايير عالمية للسلوك مهمة شاقة. وفيما يلي أبرز هذه التحديات:

- صعوبة تحديد الجهات الفاعلة ومبدأ المحاسبة: تتميز الهجمات السيبرانية بأنها غالبا مخفية المصدر أو تحمل طابعا مراوغا (انتحال هويات إلكترونية أو استخدام شبكات بروكسي)، ما يجعل نسبة الهجمات إلى الجهة المنفذة (Attribution) أمرا صعبا تقنيا وسياسيا. هذا الغموض يقوّض إمكانية محاسبة الدول أو الجهات التي تقف خلف الهجمات، ويشجع على الإنكار المعقول. إن غياب آليات تحقيق دولية فعالة في الجرائم السيبرانية يُسهم في خلق جو من عدم اليقين، حيث لا توجد عواقب واضحة على من يرتكب سوء السلوك السيبراني .[1] وبالتالي تتراجع قدرة مبادئ الردع التقليدية على منع الهجمات في الفضاء الإلكتروني

[1]- د.رندا طلال حسن. تحولات الاقتصاد العالمي في ظل عصر الذكاء الاصطناعي )الفرص والمخاطر ,مجلة كلية الامام الجامعة / العلوم الانسانية ,المجلد 2– العدد 8 ، 2025، ص19

إذا لم يُضمن كشف ومعاقبة الفاعلين. يتصل بذلك التحدي مسألة المساءلة القانونية؛ فحتى مع توافق الدول على معايير طوعية للسلوك، يبقى تطبيقها محدودا بغياب التزامات قانونية صريحة وآليات رصد دولية.

- تباين الرؤى والمعايير بين الدول: يظهر انقسام عالمي حول كيفية إدارة الإنترنت والفضاء السيبراني. فالدول الديمقراطية الصناعية تميل إلى دعم رؤية الإنترنت الحر والمفتوح وتؤكد عالمية المعايير مع احترام حرية تدفق المعلومات، بينما تدفع دول أخرى باتجاه مفهوم "السيادة الرقمية" حيث يكون لكل دولة حق تنظيم فضائها الإلكتروني الداخلي وفق قوانينها وثقافتها (بما في ذلك الرقابة على المحتوى أو تقييد حركة البيانات) . هذا التباين ينعكس في المفاوضات الدولية؛ فمثلا تطالب روسيا والصين منذ سنوات بمعاهدة دولية ملزِمة حول أمن المعلومات تُنظم المحتوى وتمنع ما تعتبرانه "استخداما عدائيا للمعلومات لزعزعة الاستقرار"، فيما ترفض دول غربية ذلك خشية المساس بحرية التعبير وتدعو بدلا من ذلك للالتزام بالمعايير الطوعية المتفق عليها ضمن إطار الأمم المتحدة. وينبغي أن تبدأ هذه التشريعات بوضعمعاييرواضحةللشفافيةوالمساءلةفي تصميم الخوارزميات، ال سيما في القطاعات الحساسة كالرعاية الصحية والعدالة والتعليم والماليه[1] .هكذا يعرقل الاستقطاب الجيوسياسي بناء توافق شامل حول قواعد ملزمة للسلوك، ويؤدي أحيانا إلى وجود أطر متوازية أو منافسة (كما حدث عبر إنشاء مجموعتي GGE وOEWG بشكل متزامن بفعل خلاف روسي-أمريكي حول آلية التفاوض).
- التوازن بين الأمن والانفتاح وحقوق الإنسان: يطرح الانتشار الرقمي تحديات ذات أبعاد اجتماعية وأخلاقية، إذ يتعين على الدبلوماسية السيبرانية إيجاد توازن دقيق بين متطلبات الأمن السيبراني (حماية الشبكات ومكافحة الإرهاب السيبراني والجريمة المنظمة إلكترونيا) وبين احترام الحقوق والحريات الفردية في الفضاء الإلكتروني. من أكبر الإشكاليات هنا قضية الخصوصية والمراقبة؛ فجهود الاستخبارات الإلكترونية ومراقبة البيانات لملاحقة المخاطر قد تنتهك خصوصيات الأفراد وحرية التعبير. وقد برزت مخاوف حقوقية من قوانين أمن سيبراني صارمة أقرتها بعض الدول لأنها تمنح السلطات صلاحيات موسعة للرقابة على الإنترنت. على الدبلوماسية السيبرانية معالجة هذه التخوفات الأخلاقية عبر تضمين معايير حقوق الإنسان في المفاوضات الرقمية، مثل التأكيد على مبادئ حرية المعلومات وحماية الخصوصية عند بناء أي إطار عالمي للأمن السيبراني. إضافة لذلك، يبرز تحدي انتشار المعلومات المضللة التي تتناقلها الجيوش الإلكترونية وحملات التأثير عبر وسائل التواصل. هذه الظاهرة تقوّض الثقة بين الدول وقد تساهم

[1]- رند طلال حسن. مصدر سابق , ص20

في تأجيج الأزمات الدبلوماسية، ما لم يتم تطوير معايير تعاون دولي لرصد حملات التضليل والتصدي لها دون المساس بحرية الإنترنت.[1].

- تصاعد وتيرة التهديدات وتعقيدها التقني: مع تحول الفضاء الإلكتروني إلى ساحة مواجهة نشطة، تزداد حجم الهجمات السيبرانية وكفاءتها التخريبية يوما بعد يوم. فقد أصبحت الهجمات المتقدمة المستمرة (APT) التي ترعاها دول أو مجموعات محترفة قادرة على اختراق شبكات حساسة والبقاء كامنة لفترات طويلة لجمع المعلومات أو التخريب. يضاف إلى ذلك التوسع في أساليب الهجوم (مثل هجمات الفدية ransomware، وهجمات سلسلة التوريد supplychainattacks، والبرمجيات الخبيثة المدمرة) مما يجعل مشهد التهديد السيبراني أكثر تنوعا وتغيرا سريعا. إن التطور التقني المتسارع يفوق في كثير من الأحيان قدرة الدول والمؤسسات الدولية على مواكبة أخطاره من ناحية وضع الأطر التنظيمية المناسبة . ونتيجة لذلك نلاحظ فجوة زمنية بين ظهور التقنيات الجديدة (كالذكاء الاصطناعي، وإنترنت الأشياء، والحوسبة الكمية في المستقبل القريب) وبين صياغة قوانين أو اتفاقيات تضبط استخدامها العسكري أو الإجرامي. وقد أشار خبراء إلى أن المنظومة القانونية الدولية تتأخر عقودا عن ركب التكنولوجيا الراهنة ، الأمر الذي يستوجب مبادرات استباقية ضمن الدبلوماسية السيبرانية لسد هذه الفجوة من خلال إطلاق حوارات حول التقنيات الناشئة وآثارها الأمنية قبل تفشي استخدامها الضار.[2].
- ضعف الثقة والتعاون بين الدول: يتطلّب التصدي للتهديدات السيبرانية العابرة للحدود مستوى عاليا من التنسيق وتبادل المعلومات بين الدول، إلا أن الواقع يشهد نقصا في الثقة المتبادلة يعيق التعاون المنشود. فالهجمات الإلكترونية كثيرا ما تتسم بحساسية سياسية تجعل الدول مترددة في مشاركة معلومات الاستخبارات السيبرانية أو الإقرار بوقوع حوادث (خشية الإضرار بالصورة العامة أو كشف مصادر استخبارية). كما أن انخراط بعض الدول نفسها في عمليات تجسس أو اختراق ضد دول أخرى يقوّض الثقة ويخلق ازدواجية معايير. لقد أكدت الأمم المتحدة ومنظمة الأمن والتعاون الأوروبي وغيرها على أهمية بناء إجراءات لبناء الثقة (CBMs) في الفضاء السيبراني – مثل الإخطار المسبق بالتمارين السيبرانية الكبيرة، وإنشاء خطوط اتصال ساخنة بين مراكز الاستجابة للطوارئ الإلكترونية (CERTs) في الدول المختلفة – وذلك لتفادي سوء الفهم والتصعيد غير المقصود . غير أن هذه الإجراءات لا تزال في مراحلها الأولية، وتحقيق تعاون فعّال يتطلب بناء الثقة السياسية الأعمق بين الدول. ومن دون هذه الثقة، تخشى الدول من

---

[1]- سلمان داود سلمان نجم,المسؤليه المدنيه عن الاضرار الناتجة عن استخدام التكنلوجيا الحديثة ,مجلة كلية الامام الجامعة / العلوم الانسانية المجلد 2– العدد: 8 2025, ص45

[2]- هديل تومان محمد البعاج ,الوعي الاجتماعي بالامن السيبراني لدى الطلبة ( دراسة ميدانية على طلبة الجامعات طلبة كلية الامام الكاظم انموذجا ,مجله لارك 2023 ,ص34

أن أي اتفاقيات أو تبادل معلومات قد يُستغل ضدها استخباراتيا. لذا يمثل انعدام الثقة أحد أكبر العقبات أمام إبرام تعهدات قوية للتضامن السيبراني الجماعي أو المساعدة المتبادلة في حال وقوع هجوم كبير.[1].

- الفجوة الرقمية وعدم تكافؤ القدرات: هناك تفاوت كبير بين الدول في الجاهزية السيبرانية وبناء القدرات الدفاعية والهجومية في الفضاء الإلكتروني. فبينما تمتلك الدول المتقدمة إمكانات تقنية وبشرية عالية لحماية فضاءاتها الرقمية (مثل فرق الاستجابة لحوادث الأمن السيبراني، وبحوث متطورة في الأمن المعلوماتي، وتحالفات مع شركات التكنولوجيا)، تعاني العديد من الدول النامية من ضعف البنية التحتية المعلوماتية وندرة الخبرات المتخصصة مما يجعلها أكثر عرضة للهجمات، وكذلك أقل مشاركة في صنع القواعد الدولية. هذا الخلل يبرز تحدي شمولية الحوكمة السيبرانية؛ إذ ينبغي للدبلوماسية السيبرانية أن تراعي إشراك كافة الدول وضمان بناء قدراتها، وإلا فإن معايير الفضاء الإلكتروني قد تُصاغ بمعزل عن احتياجات الدول الأضعف لتصبح حبرا على ورق. وقد أكدت التقارير الدولية على ضرورة سد الفجوة الرقمية بين الدول عبر مبادرات التدريب والمساعدة التقنية وتبادل أفضل الممارسات . أيضا، يظهر هنا بُعد متعلق بدور الشركات التقنية الكبرى: فهي غالبا صاحبة الخبرة الأعمق في تأمين الشبكات ورصد التهديدات، وتتفاوت استفادة الحكومات من تعاونها مع هذه الشركات. إن غياب إطار عالمي يحدد دور القطاع الخاص في تعزيز أمن الفضاء الإلكتروني يمثل تحديا، نظرا لكون معظم البنية التحتية للإنترنت ومكونات العالم الرقمي مملوكة ومدارة من قبل شركات مدنية متعددة الجنسيات.باختصار، تمثل هذه التحديات مجتمعة عقبات أمام نجاح الدبلوماسية السيبرانية في تحقيق غايتها. فالتوازن بين الأمن والانفتاح، وتحقيق التوافق الدولي في ظل التنافس الجيوسياسي، وضمان العدالة الرقمية في بناء القدرات، كلها أهداف صعبة التحقق ولكنها ضرورية لضمان فضاء إلكتروني مستقر وآمن. إدراك صانعي القرار لهذه التعقيدات هو الخطوة الأولى لمعالجتها عبر مبادرات خلاقة وترتيبات دولية جديدة تطرحها الدبلوماسية السيبرانية في قادم السنوات..[2].

**رابعا: الأطر القانونية والاستراتيجية الناظمة للفضاء السيبراني**

رغم حداثة مجال الفضاء الإلكتروني، بدأت تتبلور تدريجيا مجموعة من الأطر القانونية والاستراتيجية على المستويات الوطنية والإقليمية والدولية تهدف إلى تنظيم سلوك الفواعل في هذا الفضاء ودرء مخاطر الصراع الرقمي المنفلت. فيما يلي عرض لأهم هذه الأطر:

- انطباق القانون الدولي على الفضاء السيبراني: يعد هذا المبدأ حجر الأساس في النقاش الدولي. فمنذ تقرير الأمم المتحدة عام 2013 بات هناك إجماع سياسي على أن القواعد العامة للقانون الدولي تنطبق

[1]- سلمان داود سلمان نجم,مصدر سابق ص46

[2]- ماجد صدام سالم ,الامن السيبراني العراقي واثره في قوة الدولة .مجله العلوم التربويهوالانسانيه ,2022 ,ص7

على أنشطة الدول في الفضاء الإلكتروني ، بما يشمل ميثاق الأمم المتحدة (مبادئ عدم الاعتداء واحترام السيادة وحل النزاعات سلميا) وكذلك القانون الدولي الإنساني في حالة النزاعات المسلحة السيبرانية. هذا يعني مثلا أن الهجوم السيبراني ذو الأثر التخريبي البالغ قد يرقى إلى مستوى "القوة المسلحة" المحظورة وفق المادة 2(4) من ميثاق الأمم المتحدة، مما يتيح للدولة المتضررة حق الدفاع عن النفس ضمن شروط المادة 51 إذا استوفى الهجوم معايير العدوان . كذلك ينطبق مبدأ سيادة الدول على فضائها السيبراني الداخلي، فلا يجوز اختراق شبكات دولة ما وانتهاك سيادتها دون سند قانوني (كما هو الحال تماما في المجالين الجوي والبري). ومع ذلك، تبقى تفاصيل تطبيق هذه المبادئ محل جدل: مثل ماهية "الهجوم المسلح" إلكترونيا وحدّه الأدنى، وكيفية تطبيق قواعد القانون الإنساني (كالتناسب والتمييز) على الهجمات السيبرانية . ولم يصل المجتمع الدولي بعد إلى معاهدات ملزِمة تغطي هذه الجزئيات، لكن دليل تالين 2.0 (الذي أعده خبراء قانونيون عام 2017 تحت إشراف مركز CCDCOE التابع للناتو) يُعد مرجعا مهما يقدّم تفسيرا غير رسمي لكيفية انطباق قواعد القانون الدولي على الفضاء السيبراني في السلم والحرب.

- المعايير الطوعية للسلوك المسؤول (القواعد غير الملزمة): تمثل مجموعة المعايير الـ11 التي أقرها إجماع تقرير الأمم المتحدة لعام 2015، والمكرسة أيضا في مخرجات الفريق المفتوح لعام 2021، إطارا مهما لضبط السلوك الدولي في غياب معاهدة ملزمة . من هذه المعايير مثلا: الامتناع عن إلحاق الضرر متعمدا بالبنى التحتية الحيوية التي يعتمد عليها المدنيون (كشبكات الطاقة والمستشفيات) عبر الفضاء الإلكتروني، وعدم استهداف فرق طوارئ الحاسوب (CERTs) التابعة لدولة أخرى واعتبارها مرافق محمية يجب التعاون معها ، وواجب كل دولة أن تمنع انطلاق أنشطة سيبرانية ضارة من أراضيها تستهدف دولا أخرى عند علمها بذلك. هذه القواعد طوعية بطبيعتها لكنها تحمل وزنا معنويا مهما، وقد دأبت الدول الغربية وحلفاؤها على الدعوة إلى تبنيها عالميا والامتثال لها كمعيار للسلوك المسؤول. وقد أدرج حلف الناتو دعم هذه المعايير في سياسته، حيث أعلن الحلفاؤهم التزامهم بتعزيز فضاء إلكتروني حر وآمن ودعم المبادئ الطوعية لسلوك الدول . التحدي بالطبع يكمن في تنفيذ هذه المعايير؛ لذا تُجرى نقاشات حاليا حول تطوير آليات إشراف أو تقارير دورية في الأمم المتحدة لتقييم مدى التزام الدول بها، علما بأن عدم طابعها الإلزامي وقصور الثقة الدولية يجعلانها عُرضة للانتهاك دون عواقب تُذكر..[1].

[1]- ماجد صدام سالم , مصدر سابق ص35

- الاتفاقيات الدولية لمكافحة الجرائم السيبرانية: على صعيد الجرائم الإلكترونية (وهي جانب مهم من الصراعات الرقمية غير العسكرية)، هناك اتفاقية بودابست لعام 2001 التابعة لمجلس أوروبا، والتي تُعد أول معاهدة دولية متعددة الأطراف حول الجرائم المعلوماتية. انضمت للاتفاقية أكثر من 65 دولة من مختلف القارات، ووضعت إطارا لتجريم أفعال مثل الاختراق غير المشروع والاحتيال الإلكتروني واستغلال الأطفال عبر الإنترنت، مع ترتيبات للتعاون القانوني وتبادل المعلومات بين الدول الموقّعة . ورغم أهميتها، امتنعت دول عديدة (بينها روسيا والصين) عن الانضمام بدعوى أنها وُضعت دون مشاركتها، وتسعى هذه الدول عبر الأمم المتحدة حاليا إلى صياغة معاهدة عالمية جديدة للجريمة السيبرانية تأخذ بالاعتبار شواغل أوسع (وقد بدأت بالفعل مفاوضات لصياغة نص جديد تحت مظلة مكتب الأمم المتحدة للمخدرات والجريمة – UNODC). إن مكافحة الجرائم الإلكترونية عبر التعاون الدبلوماسي تمثل مكونا رئيسيا في الدبلوماسية السيبرانية، نظرا للترابط الوثيق بين الجرائم العابرة للحدود (كالهجمات على المصارف أو استهداف البنى التحتية) ومسألة الأمن القومي والثقة بين الدول..[1].

الاستراتيجيات والسياسات الوطنية ذات البعد الدولي: أصدرت دول كثيرة إستراتيجيات وطنية للأمن السيبراني، وبعضها تضمّن بُعدا دوليا/دبلوماسيا واضحا. على سبيل المثال، تضمنت الإستراتيجية الأمريكية للأمن السيبراني (نسخة 2023) ركيزة خاصة بتعميق التعاون الدولي ووضع معايير عالمية للأمن السيبراني . كذلك ركّزت إستراتيجية الأمن السيبراني الفرنسية والبريطانية وغيرها على دور التحالفات الدولية في تعزيز أمن الفضاء الإلكتروني. وعلى مستوى كتل الدول، تبنى الاتحاد الأوروبي إستراتيجية "دبلوماسية سيبرانية" مكمِّلة لإستراتيجية الأمن السيبراني، بهدف توحيد مواقف دوله في المنتديات الدولية وتنسيق مساعدات بناء القدرات للدول الشريكة في مجال الأمن الرقمي، بالإضافة إلى إجراءات دبلوماسية جماعية (كاستدعاء السفير أو البيان المشترك) عند تعرض أي دولة عضو لهجوم سيبراني خطير. هذه التحركات تدل على تنامي الطابع المؤسسي للدبلوماسية السيبرانية ضمن سياسات الدول، بحيث لم يعد التعامل مع قضايا الفضاء الإلكتروني حكرا على الفنيين، بل أصبح عنصرا ثابتا في أجندات السياسة الخارجية..[2].

---

[1]- موقع بوابة الشروق الإخباري – عدة مقالات وتقارير مترجمة تتناول قضايا الدبلوماسية الرقمية والأمن السيبراني (2023–2024)

[2]- منى عبدالله السمحان ,متطلبات تحقيق الأمن السيبراني لأنظمة المعلوماتالإدارية بجامعة الملك سعود, مجله كليه التربيه جامعه المنصور ,العدد11 ,ص5

- مبادرات بناء الثقة والتدابير الوقائية: أدخلت عدة منظمات إقليمية ودولية بنودا خاصة لبناء الثقة وتجنب سوء الفهم في الفضاء السيبراني. مثلا، أقرت منظمة الأمن والتعاون في أوروبا (OSCE) حزمة إجراءات لبناء الثقة السيبرانية تشمل تبادل الدول الأعضاء المعلومات حول الهجمات الكبرى حال وقوعها، وتبادل جهات الاتصال للطوارئ المعلوماتية، وإجراء اجتماعات دورية بين خبراء الأمن المعلوماتي لتفادي التصعيد غير المقصود. كما ناقش منتدى الآسيان الإقليمي (ARF) إجراءات مماثلة في سياق آسيا. هذه الجهود الوقائية تعتبر مكملة للأطر القانونية، إذ تهدف لخلق عادات تعاون وشفافية بين الدول في الفضاء الإلكتروني تخفف فرص نشوب نزاع نتيجة سوء تقدير أو تفسير خاطئ لنوايا الطرف الآخر. ومع أن هذه الإجراءات ما زالت تطوعية أيضا، إلا أن الالتزام الواسع بها (مثلا تبادل الإخطارات بشكل منتظم) من شأنه أن يعزز الاستقرار الرقمي الدولي..[1].
- دور الجهات الفاعلة غير الحكومية والأطر المتعددة الأطراف: يتميز الفضاء السيبراني بأنه ميدان يضم إضافة إلى الدول، جهات فاعلة أخرى مؤثرة تشمل شركات التكنولوجيا العملاقة، ومنظمات تقنية (مثل هيئة الإنترنت للأسماء والأرقام ICANN المعنية بإدارة موارد الشبكة)، فضلا عن المجتمع المدني وخبراء الأمن السيبراني. لذا نشأت مبادرات متعددة الأطراف تجمع أصحاب المصلحة المتعددين لصياغة قواعد ومبادئ للسلوك. من الأمثلة البارزة "نداء باريس" المذكور آنفا الذي جمع دولا وشركات ومنظمات مجتمع مدني على طاولة واحدة لدعم مبادئ أمنية مشتركة . كذلك أسست بعض الشركات تحالفات فيما بينها (مثل مبادرة TechAccord 2018 حيث تعهدت أكثر من 150 شركة تقنية بالتعاون لصد الهجمات وحماية المستخدمين المدنيين وعدم مساعدة أي حكومة في شن هجمات ضد الأبرياء). هذه الجهود وإن كانت غير حكومية الطابع، لكنها أصبحت جزءا من مشهد الدبلوماسية السيبرانية الأشمل، حيث تستفيد الدول منها لدعم رؤاها (مثال ذلك: استشهاد دول غربية بموقف شركات التقنية الرافض للقرصنة لتعزيز طرحها بضرورة التزام الجميع بمعايير مسؤولة). ومن جهة أخرى، ضغطت الشركات نفسها عبر قنوات دبلوماسية غير رسمية لتحقيق أهداف مثل اتفاقية جنيف الرقمية التي اقترحتها مايكروسوفت . وعلى الرغم من عدم دخول هذه المبادرات طي التنفيذ الرسمي، فإنها تؤكد اتساع ساحة الدبلوماسية السيبرانية لتشمل جهات متباينة المصالح، مما يفرض تحديا في تنسيق الأصوات ضمن إطار قانوني موحد.وخلاصة القول، أن الأطر القانونية والاستراتيجية الحالية للفضاء السيبراني لا تزال في طور التشكل. إذ يهيمن عليها طابع المبادئ غير الملزمة والتفاهمات السياسية أكثر من كونها معاهدات صلبة. ومع ذلك، فهي توفر أساسا ضروريا يمكن البناء عليه.

[1]- إبراهيم خليل البلعزي , القانون السيبراني: قراءة تجربة في التحديات الدولية والجاباتالوطنية ,مجله المنتدى الاكاديمي ,مجلد 9 العدد 2 ,2025 ,ص34

فاعتراف المجتمع الدولي بقاعدة انطباق القانون الدولي، ووجود معايير سلوك متفق عليها (ولو طوعا)، واعتماد استراتيجيات وطنية تراعي البعد الدولي، كلها خطوات مهمة نحو بناء نظام حوكمة للفضاء الإلكتروني. وسيكون التحدي القادم هو الانتقال من هذه الأطر المرنة إلى قواعد أكثر إلزاما وتحديدا، وهو ما قد يتطلب جهودا دبلوماسية مستمرة وتنازلات متبادلة بين مختلف الأطراف..[1].

**خامسا: آفاق مستقبلية للدبلوماسية السيبرانية**

مع استمرار الاعتماد العالمي على التقنيات الرقمية وتزايد المخاطر المرتبطة بها، يُتوقع أن تكتسب الدبلوماسية السيبرانية زخما أكبر في السنوات القادمة. وستتشكل ملامح مستقبلها عند تقاطع تطورات تقنية سريعة من جهة، والتحولات في النظام الدولي من جهة أخرى. وفيما يلي أبرز الآفاق والتوجهات المستقبلية المتوقعة في هذا المجال:

- تصاعد أهمية التعاون متعدد الأطراف: ستزداد الحاجة إلى منصات شاملة تجمع أكبر عدد من الدول لمناقشة قضايا الفضاء الإلكتروني وصياغة الحلول المشتركة. من المنتظر أن يلعب الفريق العامل المفتوح العضوية الأممي (OEWG) (وبعد انتهاء ولايته في 2025 ربما يتم تجديدها أو إنشاء هيئة دائمة) دورا محوريا كمنتدى عالمي جامع لمفاوضات الأمن السيبراني. كذلك قد نشهد مبادرات تقودها تكتلات دولية جديدة؛ فمثلا قد تتعاون دول من الجنوب العالمي لصياغة موقف موحد يوازن بين حقها في التنمية الرقمية وبين مطالب الأمن العالمي، ما يعزز صوتها في المفاوضات التي كانت تاريخيا تهيمن عليها الدول الكبرى. .[2] . وسيبقى تأسيس ثقة رقمية بين المعسكرات المختلفة شرطا أساسيا لتفعيل أي تعاون متعدد الأطراف. لذلك يُرجح أن تستمر الجهود لتعزيز بناء إجراءات الثقة وتوسيع قنوات الاتصال المباشر بين خبراء الدول (على غرار خطوط الاتصال الطارئة بين مراكز الأمن السيبراني) لتفادي سوء الفهم وحل الحوادث بسرعة قبل تصعيدها . على الصعيد المؤسسي، قد نشهد تحديثا لأدوار منظمات دولية قائمة أو حتى استحداث منصب مبعوث أممي معني بالفضاء السيبراني يتولى تنسيق جهود المنظومة الدولية كما هو الحال في قضايا التغير المناخي ومكافحة الإرهاب.
- نحو إطار قانوني عالمي أكثر شمولا: بالرغم من التحفظات الحالية، يلاحظ تنامي التأييد لفكرة تطوير اتفاقيات دولية ملزمة في بعض جوانب الفضاء السيبراني. فعلى المدى المتوسط، قد تتبلور معاهدة متفق عليها لمكافحة الجرائم السيبرانية عبر الأمم المتحدة (المفاوضات جارية فعلا) مما سيشكل إنجازا مهما. أما في شق النزاعات السيبرانية بين الدول، فإن الوصول إلى اتفاقية شاملة قد يكون بعيد المدى نظرا للتعقيدات السياسية، إلا أن بعض الخبراء يدعون إلى البدء باتفاقيات جزئية تغطي مواضيع

[1]- إبراهيم خليل البلعزي , مصدر سابق ,ص34

[2]- محمد عبد الفتاح. مصدر سابق

محددة، مثل: اتفاقية لعدم استهداف البنى التحتية الحيوية المدنية (كالمستشفيات وشبكات الكهرباء) حتى في زمن النزاع، أو اتفاقية لحماية الكابلات البحرية للإنترنت من التخريب. ومما قد يعزز هذا التوجه وقوع حوادث سيبرانية جسيمة ذات أثر عالمي (لا قدر الله) تضغط على المجتمع الدولي لاتخاذ تدابير أكثر صرامة. كما أن مبادرات مثل فكرة "اتفاقية جنيف الرقمية" التي طالبت بها شركات تقنية كبرى قد تكتسب دعما شعبيا وسياسيا أكبر، خاصة إذا تضافرت جهود القطاع الخاص والمجتمع المدني مع دول ذات تفكير مشابه للدفع نحو مثل هذه الالتزامات. وفي الأثناء، يُتوقع الاستمرار في تعميق المعايير الطوعية وتفصيلها، وربما الانتقال من مجرد سرد مبادئ عامة إلى وضع إرشادات تنفيذية لكيفية تحقيق تلك المبادئ (مثال: وضع دليل أمني لكيفية حماية الدول لبناها التحتية رقميا وتعاونها ضد الهجمات على شبكات الصحة والقطاع المالي). كل ذلك سيكون خطوات تمهيدية نحو نظام قانوني أكثر شمولا.[1].

- تعزيز بناء القدرات والفجوة الرقمية: ستحتل مسألة بناء القدرات السيبرانية للدول الضعيفة نصيبا متزايدا من الاهتمام في المستقبل. فمن دروس التجارب أن الأمن الجمعي في الفضاء الإلكتروني يتطلب ألا تبقى هناك حلقات أضعف يُستغل فضاؤها أو أراضيها لشن الهجمات. لذا ستستمر برامج تدريب الخبراء وتأسيس فرق الاستجابة السريعة وتطوير التشريعات الوطنية في الدول النامية عبر مبادرات كبرى مثل مبادرة بناء القدرات السيبرانية العالمية (GFCE) وغيرها . كما يُتوقع أن يزداد التمويل الدولي المخصص لمساعدة الدول على تطوير إستراتيجياتها الوطنية للأمن السيبراني وإنشاء مراكز لعمليات الأمن (SOCs) وتعزيز وعي المجتمعات بالمخاطر الرقمية. هذا التوجه تحفزه أيضا المنظمات الإقليمية؛ فالاتحاد الأفريقي مثلا تبنى اتفاقية للأمن السيبراني وحماية البيانات (مالابو 2014) ويعمل على دعم الأعضاء في التنفيذ. وسيحرص المجتمع الدولي مستقبلا على جعل سد الفجوة الرقمية جزءا لا يتجزأ من حوارات الدبلوماسية السيبرانية، إدراكا أن عالما رقميا غير متكافئ سيُنتج هشاشة أمنية للجميع. ومن هنا ستظهر أيضا مبادرات لدمج موضوع الشمول الرقمي ضمن توصيات التعاون الدولي، لضمان وصول مزايا التقنية لجميع الدول وتقليل الفوارق التي قد تستغلها المجموعات الإجرامية أو حتى بعض الدول لبسط نفوذها.[2].
- تصاعد دور التقنيات الناشئة في المفاوضات: ستكون التقنيات الجديدة نفسها موضوعا للتفاوض ضمن الدبلوماسية السيبرانية المستقبلية. فالاختراقات التقنية مثل الذكاء الاصطناعي (AI)، والحوسبة الكمية، وإنترنت الأشياء (IoT)، تفتح آفاقا ولكن تصاحبها مخاطر أمنية غير مسبوقة (مثال:

---

[1]- فهد قطينة ,كتاب القانون السيبراني - تعلم القانون السيبراني ,2025كلية نيو مكسيكو جونيور,ص46

[2]- فهد قطينة ,مصدر سابق ,ص46

إمكان استغلال الذكاء الاصطناعي في شن هجمات سيبرانية أكثر تطورا أو إنتاج معلومات مضللة عالية الجودة، أو قدرة الحوسبة الكمية مستقبلا على كسر التشفير الذي يحمي البيانات الحساسة). من المرجح أن تسعى الدول بشكل متزايد إلى تنظيم استخدام التقنيات الناشئة ووضع أطر أخلاقية لها عبر التعاون الدولي . بالفعل بدأت مناقشات أولية حول حوكمة الذكاء الاصطناعي في محافل كمجموعة السبع والأمم المتحدة، وقد يتمخض عنها مبادئ أو اتفاقيات خاصة تكمل منظومة الأمن السيبراني الشاملة. وقد نرى في الأفق تشكيل لجان خبراء دولية جديدة تركز على كل تقنية على حدة لاستكشاف آثارها الأمنية وصياغة التوصيات (مثل لجنة دولية لأمن الذكاء الاصطناعي). وستتعاظم أهمية التقييمات الأخلاقية للتقنيات قبل تبنها على نطاق واسع ، الأمر الذي قد تؤديه مجموعات عمل مشتركة بين الحكومات وشركات التقنية لضمان أن الابتكار الرقمي لا يأتي على حساب أمن المجتمعات واستقرارها.[1].

- موازين قوى سيبرانية جديدة وتحالفات رقمية: مع تحول القدرات السيبرانية إلى عنصر من عناصر قوة الدولة الشاملة، يمكن أن نشهد تشكّل تحالفات رقمية أو كتل سيبرانية إلى جانب التحالفات السياسية التقليدية. فمثلا، توسع التعاون بين الاتحاد الأوروبي وحلف الناتو في الفضاء الإلكتروني (عقد أول حوار منظم بينهما حول الأمن السيبراني عام 2022) يؤشر لإمكان بناء جبهة موحدة بين الحلفاء الغربيين في مواجهة التهديدات الرقمية المشتركة . في المقابل، قد تعمّق دول أخرى تعاونها خارج الإطار الغربي (مثل تعاون روسيا والصين في تبادل تقنيات المراقبة والسيطرة على الإنترنت، أو مبادرات آسيوية-إفريقية لبناء بدائل للبنية التحتية الغربية للإنترنت). هذه الاستقطابات إن تعمّقت ربما تقود إلى ازدواجية معايير ومعسكرات رقمية متنافسة، ما لم تنجح الدبلوماسية المتعددة الأطراف في المحافظة على أرضية مشتركة. وفي هذا الإطار، ستبرز أهمية إشراك القوى الصاعدة (كدول الهند والبرازيل وجنوب إفريقيا واندونيسيا وغيرها) في صياغة قواعد الفضاء السيبراني لضمان أنها تعكس مصالح الجميع وليست فقط مصالح القوى العظمى. بعض المحللين يشير إلى أن الدول المتوسطة القوة يمكن أن تلعب دورا تجسيريا في ردم الفجوة بين المعسكرين الغربي والشرقي في قضايا الإنترنت عبر ما يملكونه من علاقات جيدة مع الطرفين ورؤية وسطية .بالنتيجة، يبدو مستقبل الدبلوماسية السيبرانية مرهونا بقدرة المجتمع الدولي على التعلم من التجربة وابتكار صيغ خلاقة للتعاون تتناسب مع الطبيعة المترابطة والعابرة للحدود للفضاء الإلكتروني. ومع استمرار التقدم التقني المطّرد، ستغدو الدبلوماسية السيبرانية أكثر أهمية وحضورا في تشكيل نظام عالمي آمن ومستقر ومزدهر رقميا .

[1]- ظلال محمد رضا شويلية ,الأمن السيبراني في العراق,جامعة بابل,2023 ,ص35

وسيكون لزاما على كافة الأطراف مواصلة التنسيق واليقظة لمعالجة التحديات السيبرانية الناشئة واستثمار الفرص الكامنة في التكنولوجيا من أجل خدمة السلم والأمن الدوليين .[1].

**الخاتمة والتوصيات**

برزت الدبلوماسية السيبرانية خلال سنوات قليلة كأحد العناصر الحيوية في بنية العلاقات الدولية المعاصرة، بعدما أعادت تشكيل أساليب الدبلوماسية التقليدية وطبيعة التفاعلات العالمية في عصر الرقمنة . لقد استعرضت هذه الدراسة المفهوم والأسس النظرية والتاريخية لهذا الحقل، كما تناولت التحديات البنيوية والاختلافات بين رؤى الدول، وأبرزت الأطر القانونية والاستراتيجية الحالية لتنظيم الفضاء الإلكتروني. وعلى الرغم من جسامة التحديات التي تواجهها الدبلوماسية السيبرانية – من صعوبة attribution ومسألة الثقة، مرورا بالتباينات القيمية بين الشرق والغرب، ووصولا إلى السباق التقني المحموم – إلا أنها تحمل أيضا إمكانات هائلة لتعزيز التعاون الدولي والابتكار والتنمية إذا ما أحسن صناع القرار توجيهها . وفي الختام، لا مفر من الإقرار بأن الفضاء السيبراني بات جزءا لا يتجزأ من هيكل النظام الدولي المعاصر. فمع تزايد ترابط العالم رقميا، تصبح التهديدات السيبرانية تحديا جماعيا يتطلب استجابة جماعية منسقة. والدبلوماسية السيبرانية هي الأداة الأبرز لتحقيق هذه الاستجابة عبر مد جسور الحوار ووضع القواعد وبناء التحالفات لمواجهة الأخطار وتأمين الفرص. إن النجاح في حوكمة الصراعات الرقمية وصياغة معايير الفضاء الإلكتروني يعتمد على مدى قدرتنا على الابتكار الدبلوماسي والتضامن الدولي في آن واحد؛ وفي هذا تكمن مهمة السنوات القادمة لصناع السياسات والدبلوماسيين والجهات الفاعلة كافة في المشهد السيبراني. وفي ضوء ما تقدم، يمكن استخلاص التوصيات الرئيسية التالية لدفع حوكمة الصراعات الرقمية قدما وتشكيل معايير فاعلة للفضاء الإلكتروني:

1. ينبغي إعطاء أولوية لتعزيز المنتديات متعددة الأطراف (كالأمم المتحدة ومنتديات إقليمية) وتوسيع حوارات الأمن السيبراني لتشمل جميع الدول على قدم المساواة. يتطلب ذلك تطوير آليات فعالة لتبادل المعلومات بين الحكومات حول التهديدات وحوادث الاختراق، وإنشاء قنوات اتصال دبلوماسية وأمنية دائمة بين العواصم لتنسيق الاستجابات للأزمات الرقمية. كما توصى الدول بالانخراط في تدابير بناء الثقة المتفق عليها، مثل الإخطار المسبق بالأنشطة السيبرانية المهمة والتعاون في التحقيقات السيبرانية العابرة للحدود، باعتبارها أدوات لمنع سوء الفهم وخفض التوترات.
2. على المدى القريب، دعم المفاوضات الجارية لصياغة اتفاقية دولية لمكافحة الجريمة السيبرانية وجعلها تتضمن آليات فعالة للتعاون القضائي وتبادل الأدلة الإلكترونية. وعلى المدى الأبعد، السعي نحو بلورة

[1]- ظلال محمد رضا ,مصدر سابق ,ص36

معاهدات أو اتفاقيات قطاعية تخص سلوك الدول في النزاعات السيبرانية – كتحييد البنى التحتية المدنية – ووضع مدونات سلوك دولية تكون بمثابة "قانون عرفي" رقمي . وفي الأثناء، يجب العمل على تحويل المعايير الطوعية القائمة إلى ممارسات مُلزمة ضمنيا من خلال إدماجها في السياسات الوطنية وتحويلها إلى خطوط حمراء دبلوماسية يتم التحذير صراحة من عواقب تخطيها.

3. يتعين على الدول المتقدمة وأيضا المنظمات الدولية والإقليمية تقديم دعم مكثف لبناء البنية التحتية والموارد البشرية للدول الأقل قدرة في مجال الأمن السيبراني. ويشمل ذلك نقل المعرفة وأفضل الممارسات، والمساعدة في إنشاء فرق الاستجابة للحوادث، وتطوير تشريعات محلية متماشية مع الاتفاقيات الدولية. إن تقليص الفجوة في القدرات سيرفع من مستوى الأمن الجماعي. بالإضافة، ينبغي إيلاء اهتمام خاص لحماية القطاعات الحيوية عبر تبادل المعلومات حول التهديدات والثغرات ووضع خطط طوارئ مشتركة لحماية الشبكات الحيوية (كقطاع الطاقة والنقل والمال) من الهجمات الكبرى.
4. تبني نهج يوازن بين متطلبات الأمن ومبادئ الانفتاح. فعلى المستوى الدولي، ينبغي تضمين أهداف تقليص الفجوة الرقمية كجزء من جهود الأمن السيبراني لضمان توزيع أكثر عدالة لمنافع التقنية وحماية المجتمعات الأقل اتصالا من أن تصبح ملاذاتللجريمة السيبرانية أو ساحات لصراعات بالوكالة. وفي الوقت ذاته، يتعين إدماج معايير حقوق الإنسان الرقمية ضمن أطر الحوكمة، بحيث تراعي أي اتفاقيات أمنية سيبرانية حماية خصوصية المستخدمين وحرية التعبير وعدم إساءة استخدام تقنيات المراقبة. إن بناء فضاء إلكتروني ينعم بالأمن والثقة يستدعي أيضا فضاء يحترم الحقوق ويحقق التنمية للجميع.
5. إنشاء منصات تعاون دولية لمراقبة التطورات التقنية الجديدة ذات الصلة بالأمن (كالذكاء الاصطناعي والحوسبة الكمية وعلوم البيانات) وبحث سبل توجيهها لخدمة البشرية وتجنب إساءة استخدامها. قد يكون ذلك عبر تشكيل مجالس استشارية عالمية أو فرق خبراء مشتركة تقدم توصيات حول أفضل الممارسات وسياسات الأمان المتعلقة بهذه التقنيات. كذلك يُقترح إدراج موضوع أخلاقيات التقنية كمادة تفاوضية ضمن الدبلوماسية السيبرانية، بحيث تلتزم الدول بإجراء تقييمات مشتركة لتأثير أي تقنية جديدة على السلم والأمن قبل انتشارها الواسع، تماما كما يجري اليوم في تنظيم التكنولوجيا الحيوية أو الأسلحة ذاتية التشغيل.

## المراجع

### أولا: المصادر العربية


- إبراهيم خليل البلعزي .(2025) .القانون السيبراني: قراءة تجربة في التحديات الدولية والاستجابات الوطنية .مجلة المنتدى الأكاديمي، مجلد 9، العدد 2.
- اتفاقية بودابست لمكافحة الجرائم المعلوماتية .(2001) .النص الرسمي للمعاهدة .مجلس أوروبا (دخلت حيز التنفيذ 2004).
- تقارير وأخبار الأمم المتحدة .(2010–2021) .أعمال فريق الخبراء الحكومي والأعمال ذات الصلة بأمن المعلومات الدولي.
- رندا طلال حسن .(2025) .تحولات الاقتصاد العالمي في ظل عصر الذكاء الاصطناعي (الفرص والمخاطر) .مجلة كلية الإمام الجامعة / العلوم الإنسانية، المجلد 2، العدد 8.
- سلمان داود سلمان نجم .(2025) .المسؤولية المدنية عن الأضرار الناتجة عن استخدام التكنولوجيا الحديثة .مجلة كلية الإمام الجامعة / العلوم الإنسانية، المجلد 2، العدد 8، ص45.
- سيمون هوتاجالونج .(2024) .الدبلوماسية السيبرانية: فرص وتحديات .مقال مترجم، منشور في بوابة الشروق.
- ظلال محمد رضا شويليه .(2023) .الأمن السيبراني في العراق .جامعة بابل.
- فهد قطينة .(2025) .القانون السيبراني: تعلم القانون السيبراني.
- ماجد صدام سالم .(2022) .الأمن السيبراني العراقي وأثره في قوة الدولة .مجلة العلوم التربوية والإنسانية.
- محمد عبد الفتاح .(2025) .مفهوم الدبلوماسية السيبرانية .المركز المصري للفكر والدراسات الاستراتيجية.(ECSS)
- منى عبدالله السمحان .متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود .مجلة كلية التربية، جامعة المنصور، العدد 11.
- هديل تومان محمد البعاج .(2023) .الوعي الاجتماعي بالأمن السيبراني لدى الطلبة .مجلة لارك، ص34.
- موقع بوابة الشروق .(2023–2024) .مقالات وتقارير حول الدبلوماسية الرقمية والأمن السيبراني.

**ثانيا: المصادر الأجنبية**


- Adina Ponta. (2021). *Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes*. ASIL Insights, Vol. 25, Issue 14.
- Brad Smith. (2017). *The Need for a Digital Geneva Convention*. Microsoft On the Issues Blog.
- Laasme, M. (2012). *Estonia: Cyber Window into the Future of NATO*. Joint Force Quarterly, 63(4), 58–63.
- NATO – North Atlantic Treaty Organization. (2024). *Cyber Defence*. Official Report