Ashur Journal of Legal and political Sciences (AJLSP) is published by the Iraqi Association for Legal Sciences
ISSN: 3005-3269, Vol 3(No.2), pages: 610 -637 (2026)
https://ashurjournal.com/index.php/AJLPS/about

The Role of Modern Technology and Its Impact on National Sovereignty

Researcher. Hanaa Ali Majid[1], Prof. Dr. Mukhles Mahmoud Hussein[2]
[1] Imam Al-Kadhim College for Islamic Sciences University, mukhles.mahmoud@iku.ed.iq
[2] Imam Al-Kadhim College for Islamic Sciences University, ha9335497@gmail.com

ARTICLE INFORMATION

Received:10 Apr 2026
Accepted:25 Apr 2026
Published:1 Jun 2026

Keywords:

- National Sovereignty
-Modern Technology
-Digital Revolution
-Cybersecurity

ABSTRACT

Modern technology plays a pivotal role in reshaping the concept of national sovereignty .the state is no longer able to full control its borders and traditional domains as before. Tools such as the internet ,artificial intelligence ,cloud computing, and others have facilitated the of information across borders, weakening the states monopoly on information and control.

Conversely ,this technology has granted states new capabilities to enhance their sovereignty by developing cybersecurity systems, improving data management , and strengthening economic and technological power

Therefore, the impact of modern technology on national sovereignty is twofold,combining challenge and empowerment, and depends on the stats ability to adapt to these transformations and leverage them to its advantage.

مجلة آشور للعلوم القانونية والسياسية تصدر عن الجمعية العراقية للعلوم القانونية
المجلد الثالث (العدد الثاني)، الصفحات: 610- 637، (2026) ISSN: 3005-3269
https://ashurjournal.com/index.php/AJLPS/about

دَورُ التّكنولوجيا الحَدِيثَةِ وَأَثَرُهَا فِي السِّيَادَةِ الوَطَنِيَّةِ

الباحثة. هناء علي ماجد [1]، أ د. مخلص محمود حسين[2]

[1] كلية الامام الكاظم للعلوم الإسلامية الجامعة ، mukhles.mahmoud@iku.ed.iq

[2] كلية الامام الكاظم للعلوم الإسلامية الجامعة ، ha9335497@gmail.com

معلومات المقالة

تاريخ الاستلام : ١٠ نيسان ٢٠٢٦
تاريخ القبول :٢٥ نيسان ٢٠٢٦
تاريخ النشر : ١ حزيران ٢٠٢٦

الملخص

تلعب التكنولوجيا الحديثة دوراً محورياً في أعادة تشكيل مفهوم السيادة الوطنية، إذ لم تعدَ الدولة قادرة على التحكم الكامل بحدودها ومجالاتها التقليدية كما في السابق، فقد أسهمت الأدوات مثل الإنترنت، الذكاء الاصطناعي، والحوسبة السحابية...وغيرها، في تسهيل تدفق المعلومات عبرَ الحدود، مما أدى إلى إضعاف احتكار الدولة للمعلومة والرقابة.

وفي المقابل، منحت هذه التكنولوجيا الدول قدرات جديدة لتعزيز سيادتها، وذلكَ من خلال تطوير أنظمة الأمن السيبراني، وتحسين إدارة البيانات، وتعزيز القوة الاقتصادية والتقنية.

وعليه، فإنَ أثر التكنولوجيا الحديثة على السيادة الوطنية هو أثر مزدوج، يجمع بين التحدي والتمكين، ويعتمدَ على مدى قدرة الدولة على التكيف مع هذه التحولات واستثمارها لصالحها.

الكلمات المفتاحية:

-السيادة الوطنية
- التكنولوجيا الحديثة
- الثورة الرقمية
- الأمن السيبراني

المقدمة

تُعدُّ التحوّلاتُ التكنولوجيّةُ المعاصرةُ إحدى أبرزِ مظاهِرِ التحوّلاتِ الدوليّةِ التي شَهِدَهَا النِّظَامُ الدوليُّ المعاصرُ، إذ شَكَّلَتِ الثورةُ التكنولوجيّةُ ركيزةً أساساً في عمليّةِ تطويرِ قُدُرَاتِ الدُّوَل وتعزيزِ مكانَتِهَا وَقُوَّتِهَا على السَّاحةِ الدوليّةِ [1].

وقد أصبحَ المستوى التكنولوجيُّ لِلدَّولَةِ وما تُحقِّقُهُ من إنجازاتٍ تقنيّةٍ معياراً أساساً في تحديدِ موقِعِهَا الدوليّ ووزنِهَا في النِّظَامِ العالميّ؛ الأمرُ الذي انعكسَ بوضوحٍ في تجاربِ عدد من الدُّوَلِ، وفي مقدّمتها: الولاياتُ المُتّحِدَةُ الأمريكيّةُ والصين، حيثُ أسهمَ التفوّقُ التكنولوجيُّ لكلٍّ منهما في ترسيخِ نفوذهما الدوليّ في مسارِ المسرحِ الدوليّ والعلاقاتِ الدوليّةِ [2].

وقد أفرزتِ الثورةُ التكنولوجيّةُ -بوصفها إحدى أبعادِ التحوّلاتِ الدوليّةِ -إحداثَ تغييراتٍ جوهريّة في طبيعةِ التفاعلاتِ الدوليّةِ، إذ انتقلَ التنافُسُ بينَ الدُّوَلِ مِن صورتِهِ العسكريّةِ التقليديّةِ إلى أنماطٍ أكثرَ تعقيداً تقومُ على التفوّقِ التكنولوجيّ؛ وهوَ ما جعلَ التكنولوجيا عنصراً حاسماً في إعادةِ تشكيلِ موازينِ القُوّةِ وتوجيهِ مساراتِ العلاقاتِ الدوليّةِ؛ وبذلكَ لم تَعُدِ التكنولوجيا مجرّدَ أداةٍ مساندةٍ، بل أصبحت مِنَ المحدّداتِ الأساسِ لبُنيَةِ النِّظَامِ الدوليّ المعاصرِ [3]. وَمِن ناحيةٍ أخرى: أسهمتِ التغيّراتُ التكنولوجيّةُ في إحداثِ قدرٍ مِن عدمِ التوازنِ بَيْنَ المجالاتِ الإنتاجيّةِ والسياسيّةِ داخلَ الدَّولَةِ، وفيما بينها؛ وهو ما أدّى إلى تصاعُدِ مظاهرِ الصراعِ والاستقطابِ بَيْنَ القوى الكُبرى، ولا سيّما في ظلِّ سعي كلِّ دولةٍ إلى توظيفِ التفوّقِ التكنولوجيِّ لتحقيقِ مصالحها الاستراتيجيّة وتعزيزِ سيادتها في مواجهةِ التحوّلاتِ الدوليّةِ المتسارعةِ[4].

ويُقصَدُ بالثورةِ التكنولوجيّةِ: تلكَ المرحلةِ التحوّليَّةِ في مسارِ التطوّرِ البشريّ التي اتَّسَمَت بتسارعِ الابتكارِ العلميّ والتقنيّ، وما نَتَجَ عنها مِن تغييراتٍ جذريّةٍ في هياكلِ المجتمعاتِ والاقتصاديّاتِ وأنماطِ الحياةِ. وقد بَلَغَت هذهِ التحوّلاتُ ذُروَتَهَا مَعَ بُروزِ ما يُعرفُ بالثورةِ الصناعيّةِ الرابعةِ، التي قامت على تكنولوجيا المعلوماتِ والاتصالاتِ، والتي أفرزت مجالاتٍ تقنيّةٍ حديثةٍ، مِن أبرزها: الثورةُ الرقميّة وتنامي أهَميّةِ الأمنِ السيبرانيّ؛ الأمرُ الذي ألقى بتحدياتٍ جديدةٍ على مفهومِ السّيادةِ الوطنيّةِ وَحدودِ مُمَارستِهَا[5].

وعليه؛ نرى أنَّ التطوّرَ التكنولوجيَّ - ولا سيّما الرقمنة والذكاء الاصطناعيّ - أصبحَ عاملاً مؤثراً في السّيادةِ الوطنيّةِ، إذ لم تَعُدِ السّيادةُ تقتصرُ على السيطرة الإقليميّة، بل امتدّت لتشملَ حمايةَ المعلوماتِ والفضاءِ الرقميّ. وَرُغمَ ما توفِّرُهُ التكنولوجيا مِن فُرصٍ لتعزيزِ قدراتِ الدولةِ، فإنَّ سوءَ إدارتها قد يؤدّي إلى اختراقِ الأمنِ الوطنيّ والتأثيرِ في القرارِ السياديّ.

وانطلاقاً من ذلكَ؛ يأتي هذا لبحث ليتناول أثرَ التحوّلاتِ التكنولوجيّةِ -باعتبارها إحدى تَجَلّيَاتِ التحوّلاتِ الدوليّةِ على السّيادةِ الوطنيّةِ؛ وذلك من خلال تقسيمهِ إلى فرعينِ: سنتناول في الفرع الأول الثورة الرقميّة وأثرها على السّيادة الوطنيّة، ثم نتطرق في الفرع الثاني إلى الأمن السيبرانيّ وأثرهِ على السّيادة الوطنيّة.

اولاً / أهمية البحث:

تظهر أهمية هذا الموضوع في عدة جوانب، إذ أنه يسلط لضوء على التحول في مفهوم السيادة الوطنية في ظل الثورة التكنولوجيا، ويبرز التحديات التي تواجه الدول نتيجة الفضاء الرقمي وتدفق المعلومات العابرة للحدود، ويساعد على فهم دور التكنولوجيا في تعزيز أو صاف سلطة الدولة.

ثانياً / إشكالية البحث:

تثير التطورات المتسارعة في مجال التكنولوجيا الحديثة إشكالات عميقة بشأنَ مدى قدرة الدولة على الحفاظ على سيادتها في ظل الثورة الرقمية والتدفقات العابرة للحدود، إذ لم تعد السيادة مطلقة كما في السابق، بل أصبحت عرضة لتحديات تفرضها أدوات التكنولوجيا الحديثة وفاعلوها الجدد. وعلى ذلكَ تثار إشكالية جوهرية وهي إلى أي مدى تستطيع الدول إنَ تحقق التوازن بين متطلبات الانفتاح على التكنولوجيا الحديثة باعتبارها ضرورة للتنمية ومواكبة التطور العالمي، وبين الحفاظ على سيادتها الوطنية في ظل اعتمادها المتزايد على الخارج في المجال التكنولوجي؟ وتضمن هذه الإشكالية أسئلة فرعية تتمثل في:

. ما المقصود بالثورة الرقمية وما أبرز مظاهرها في العصر الحديث؟

. ما طبيعة التبعية التكنولوجية التي تعاني منها الدول النامية، وما أسبابها؟

. ما مفهوم الأمن السيبراني وكيف أثر على السيادة الوطنية؟

. كيف أثرت التهديدات السيبرانية في قدرة الدولة على بسط سيادتها؟

ثالثاً / منهج البحث:

يعتمد هذا البحث على المنهج الوصفي التحليلي، من خلال عرض وبيان الثورة الرقمية ونشأتها وتقنياتها الحديثة، ثم تحليل أثرها في السيادة الوطنية ولاسيما في ظل التحديات المرتبطة بالأمن السيبراني.

رابعاً /هيكلية البحث:

تشهد التكنولوجيا الحديثة، ولاسيما الثورة الرقمية، تطوراً متسارعاً أسهم في إعادة تشكيل بنية العلاقات الدولية ومفاهيم السلطة داخل الدولة، وقد انعكس هذا التحول بشكل واضح على السيادة الوطنية. وعلى ذلك سوف نبين الثورة الرقمية وأثرها في السيادة الوطنية والتي تكون لفي الفرع الاول، ثم نتطرق إلى الأمن السيبراني وأثره في السيادة الوطنية والتي تكون في الفرع الثاني.

الفرع الأول

الثورة الرقميّة وأثرها في السّيادة الوطنيّة

أفرزتِ الثورةُ الرقميّةُ تَحَوّلاتٍ جوهريّةً كبيرةً أثّرت بصورة مباشرةٍ على مفهوم السّيادة الوطنيّة، ولا سيّما في ظل المُتَغيّرات العالميّة المتسارعة التي طرأت في القرن الحادي والعشرين، إذ انتقل العالم بوتيرة سريعة نحو عصر رقميّ جديد يتّسم بخصائص وسمات مغايرة، ويفرض متطلّباتٍ مستحدثة على الدول؛ الأمرُ الذي انعكس بشكلٍ واضحٍ على بنية النِّظَام الدوليّ وطبيعةِ العلاقاتِ الدوليّةِ [6].

ولم يَعُدِ التطوّر الرقميّ مجرّد خيار، بل غدا ضرورةً استراتيجيّةً تفرضها طبيعة التحوّلات العالميّة، ولا سيّما في مجالاتِ نقلِ المعلوماتِ والتكنولوجيا الحديثة، حيث دخل العالم فعليّاً عتبة ثورة صناعيّة جديدة يُشار إليها اصطلاحاً بـ " الثورة الرقميّة الثانية" أو الثورة الصناعيّة الرابعة. وتقوم هذه الثورة على الاندماج بين التقنيّات المادية والرقميّة والحيويّة، ونشمل على وجه الخصوص: (تقنيّات الذكاء الاصطناعيّ، انترنت الأشياء، البيانات الضخمة)، وغيرها من الابتكارات التكنولوجيّة المتقدمة [7].

وتُعَدُّ الثورة الصناعيّة الرابعة امتداداً تاريخياً لسلسة الثورات الصناعيّة السابقة التي شَهِدَهَا العَالَمُ منذ النصف الثاني من القرن الثامن عشر، والذي شهد تطوّراً تدريجيّاً في وسائل الإنتاج، بدءاً من الاعتماد على القُوّة العضليّة، مروراً بالاعتماد على الآلة، وصولاً إلى النُّظُمِ الذكيّة المؤتمتة القائمة على المعرفة الرقميّة. غير أنَ خصوصية الثورة الصناعيّة الرابعة تكمن في سرعتها، وشموليتها، وتأثيره العابر للحدود، وهو ما يطرح تحديات قانونية وسياديّة الوطنيّة وآليات ممارستها في البيئة الرقميّة المعاصرة [8].

وعليه؛ نرى أنَ الثورة الرقميّة تمثل تحولاً نوعياً أحدثَت تغييراً عميقاً في طرق أنتاج المعرفة وإدارة المعلومات. وقد أدى ذلكَ إلى التأثير بشكل مباشر في السّيادة الوطنيّة كونهُ اضعفَ قدرة الدولة على التحكم في الفضاء الرقمي في ظل اتساع نطاق التدفقات المعلوماتية العابرة للحدود، إذ أصبح حماية المعلومات والفضاء الرقميّ جزءاً أساساً من سيادة الدولة، الأمر الذي يفرض عليها تعزيز قدراتها التكنولوجيّة وأمنها السيبرانيّ؛ وانطلاقاً من ذلكَ: سيتمّ بيان نشأة وتطوّر الثورة الرقميّة، ثم توضيح أهم تقنيّاتها الحديثة.

أوّلاً -الثورة الرقميّة نشأتها وتطوّرها: في البدء لا بُدَّ من التعريف بمفهوم "الثورات العلميّة" وطبيعتها، إذ كانت هذه الثورات سلسلة من التحوّلات النوعيّة غير التراكمية التي يتم من خلالها إحلال نموذج فكريّ جديد محلّ آخر سابق أقدم منه، سواء بصورة كلية أو جزئيّة، دون أن يكون هذا النموذج الجديد منسجماً بالضرورة مع سابقهِ، إذ يُعدُّ هذا التحوّل -وفقاً للتصورات الفلسفية للعلم -انتقالاً جذريّاً في أنماط التفكير وأساليب التفسير، لا مجرّد تطوّر تدريجيّ أو تعديل جزئيّ في إطار النموذج القائم[9].

غير أنَّ توصيف هذا التحوّل بوصفه "ثورة" يقتضي توافر إطار معياريّ محدّد، يميّز بين التغيرات التطوّرية العادية وبين التغيرات الثوريّة في بُنية النموذج الفكريّ. وفي هذا السياق، يمكن الاستعانة بمثال الثورات السياسيّة بوصفها النموذج الأكثر انتشاراً، إذ تبدأ هذه الثورات عادةً ب تنامي شعور عامٍّ، يكون في مراحلهِ الأولى محصوراً ضمن شريحةٍ من النخبة الاجتماعيّة، يوحي بأنَّ المؤسسات القائمة لم تَعُد قادرةً على تقديم حلول فعّالة للمشكلات المجتمعيّة التي أنشئت أساساً لمعالجتها [10].

وبطريقة مماثلة، تنشأ الثورات العلميّة بنشوء شعورٍ متزايدٍ -وهو غالباً ما يكون مقتصراً على فئة ضيّقة من العلماء والباحثين في المجتمع العلميّ -مفادهُ أنَّ النموذج الفكريّ السائد لم يعد قادراً على تفسير بعض الظواهر العلميّة أو الكشف عن جوانب معرفيّة جديدة، سبق لذلك النموذج الفكريّ السائد أن أدّى اليها. ومن هنا تبدأ الدعوة التي تبنّي منهجيّة علميّة بديلة، قادرة على تجاوز أوجه القصور التي يعاني منها النموذج القائم [11].

ومع ذلك، فإنَ هذه التحوّلات لا تبدو ثوريّة إلّا لأولئك الذين يتأثر إطارهم المعرفيّ مباشرةً بتغير النموذج الفكريّ، في حين قد تظهر، بالنسبة لمن هم خارج هذا الإطار، على أنّها مجرّد مراحل طبيعية من مسار التطوّر العلميّ. ومن ثم، فإنَّ وصف التغيير بكونه "ثورة" يرتبط بدرجة التأثير الذي يحدثهُ في البنية الفكريّة والمعرفيّة السائدة، وليس فقط بحجم التقدم التقنيّ أو المعرفيّ المتحقق، وانطلاقاً من هذا الفهم، يمكن النظر إلى الثورة الرقميّة بوصفها إحدى أبرز أنماط الثورات العلميّة التكنولوجيّة المعاصرة؛ لما أحدثتهُ من تحوّل جذريّ في نماذج المعرفة، وآليات الإنتاج، وأنماط التواصل، وإدارة السلطة والمعلومات؛ الأمر الذي يجعلها تمثّل مدخلاً نظرياً ضرورياً لتحليل انعكاساتها العميقة على مفاهيم الدَّولَة الحديثة، وفي مقدمتها مفهوم السّيادة الوطنيّة [12].

وقد أخذت ملامح حضارة جديدة تتشكّل في العصر الراهن وتختلف في طبيعتها ومرتكزاتها عن جميع الحضارات المعرفيّة التي عرفها التاريخ الإنساني، وهي حضارة تكنولوجيا المعلومات أو المعرفة الرقميّة، التي باتت تمارس تأثيراً كبيراً في مختلف أنماط الحياة الإنسانية، إلى حد تهديدها أو إعادة تشكيلها للحضارات التي سبقتها وقد قامت على أسس مغايرة [13].

فالثورة الرقميّة -إلى جانب مكاسبها الاقتصاديّة والمعرفيّة -تثير تساؤلات جوهريّة تمسُّ البُنَى الاجتماعيّة والاقتصاديّة والسياسيّة في القرن الحادي والعشرين، وتفتح المجال لإعادة النظر في عدد من المفاهيم التقليديّة التي قامت عليها الدَّولَة الحديثة [14].

وقد أفرزت الثورة الرقميّة الرابعة بوضوح البُعدَ المعلوماتيّ المتأصّل في هوية الإنسان، وهو أمرٌ يدعو إلى قَدرٍ من التواضع المعرفيّ، إذ لم يعد هذا البعد حكراً على الكائن البشريّ وحدة، بل بات يشترك فيه مع بعض من الأدوات الذكيّة التي قام بتصنيعها بيديه؛ فالكثير مما كان يُنظر إليه سابقاً بوصفه مظاهر تفرد إنساني، لم يعد يشكل معياراً حاسماً للتميّز في ظل تفوّق تقنيّات تكنولوجيا المعلومات والاتصالات في مجالات عديدة، كجلِّ المسائل المنطقية، ولعب الشطرنج، والتدقيق الاملائي للنصوص، والترجمة الآليّة بين اللغات، وغيرها [15].

وفي الوقت ذاته، تحمل هذه الثورة بُعداً تنويرياً، إذ أنَّ الإنسان تمكّن فيهها من فهم ذاتهُ على نحوٍ أعمقَ بوصفه كائناً حياً ذا طبيعة معلوماتيّة خاصّة، يتفاعل مع البيانات ويعيد إنتاجها ضمن سياقات اجتماعيّة وثقافيّة معقّدةٍ. غير أنَّ هذا الإدراك لا يعني بالضرورة اختزال الإنسان في تمثيلات رقميّة بديلة، كالحاسبات الالكترونيّة، أو المدونات، أو التغريدات، أو المعرفات التقنيّة المرتبطة بالفضاء الشبكي، وإنما يعكس تحولاً في أنماط الوجود والتفاعل الإنساني [16].

وقد باتَ مفهوم السّيادة الوطنيّة يواجه تحديات غير مسبوقة، إذ لم يعد مرتبطاً فقط بالسيطرة على الأرض والسكان، بل أصبح مرهوناً أيضاً بالقدرة على بسط النفوذ على الفضاء الرقميّ، وحماية البنية المعلوماتيّة، وضمان أمن البيانات، وتنظيم التدفقات العابرة للحدود للمعلومات والتكنولوجيا [17].

ومن أبرز التحديات التي أفرزتها الثورة الرقمية، لاسيما في الدول النامية هي التبعية الالكترونية، إذ نشأت هذه الظاهرة نتيجة الاختلال البنيوي في توزيع المعرفة والتطور التكنولوجي، ولاسيما تبني أنماط تكنولوجية محددة دون غيرها، تستند إلى مبررات نظرية وميدانية تناولها العديد من علماء اجتماع التنمية الاقتصادية والاجتماعية، غير إنَ هذه المبررات تظل مرتبطة بطبيعة الواقع الفعلي لهذه المجتمعات، من حيث إبعاده الاجتماعية-التاريخية-الثقافية-الاقتصادية، فضلاً عن خضوعها لما يُعرف بحتمية التكنولوجيا التي فرضتها التحولات المتسارعة في ظل الثورة الرقمية، ولا تقتصر هذه التبعية على البعد الاقتصادي ، بل تمتد لتؤثر بصورة مباشرة في سيادة الدول النامية لأنها تؤدي إلى تقييد قدراتها على التحكم في بياناتها الوطنية، حيث أدى الاعتماد المتزايد للدول النامية على التقنيات المستوردة إلى تكرس نوعاً من الاعتمادية الهيكلية على الدول المتقدمة والشركات التكنولوجيا العالمية، لاسيما في مجالات البرمجيات والبنية التحتية الرقمية وادارة البيانات، وهو ما تجلى بوضوح في هيمنة شركات كبرى مثل (Microsoft-Google)(مايكروسوف –جوجل)على الفضاء الرقمي العالمي[18].

وعلى ذلكَ، أن الثورة الرقمية لم تنشأ بصورة مفاجئة، وإنما جاءت نتيجة تطور تدريجي في تقنيات المعلومات والاتصالات، بدءاً من الحواسيب وشبكات الاتصال وصولاً إلى الانترنت والذكاء الاصطناعي والتي سوف نبينها مفصلاً فيما بعد، إذ اسهمَ هذا التطور في احداث تحول جذري في نمط الاتصال والمعرفة، وانتقال العالم إلى فضاء رقمي عابر للحدود.

ونرى أنَ هذا التطور لم يقتصر على الجانب التقني، بل امتد إلى الابعاد السياسية والعسكرية ...الخ، مما جعل الثورة الرقمية عاملاً مؤثراً في إعادة تشكيل بنية النظام الدولي ومفاهيم القوة والسيادة.

ثانياً -تقنيّات الثورة الرقميّة: التي يُطلق عليها بعض الباحثين تطبيقات الثورة الرقميّة، وهي مجموعة واسعة من التقنيّات الحديثة التي شملت مختلف جوانب الحياة الاقتصاديّة والصناعيّة والاجتماعيّة والتجارية وغيرها، وقد أسهم هذا الانتشار الواسع في إحداث تَحَوّلات جوهريّة في أنماط الإنتاج والتفاعل الاجتماعيّ وإدارة الأنشطة الاقتصاديّة [19].

أدى ظهور التقنيّات الرقميّة المتقدمة إلى خلق مؤشرات جديدة في ميدان العلاقات الدوليّة، وأسهمَ في إحداث تَحَوّلات جوهريّة في موازين القوى العالميّة، إذ باتت الدُّوَل تعتمد بدرجة كبيرة على التكنولوجيا، وتسعى إلى وضع استراتيجيّات وطنيّة للتعامل مع تطبيقاتها المختلفة في بيئة آمنة. وقد قادَ هذا التحوّل إلى نشوء أنماط جديدة من الصراع تختلف عن الصراعات التقليديّة القائمة على الصناعات العسكريّة النِّظَامية، حيث برزت صراعات رقميّة تقودها ما يُعرفَ بـ "الجيوش الالكترونيّة" التي تستهدف مهاجمة أجهزة الحواسيب أو شبكات المعلومات في دول أخرى؛ بما يتيح التأثير في بنيتها التحتيّة الحيويّة، وشلَ حركة منظومتها الدفاعية. كما أسفرَ هذا التطوّر عن بروز ما يسمى بـ "المجتمع الخامس" أو "مجتمع ما بعد المعلومات" وهو المجتمع الذي تندمج فيه الآلة مع العقل البشريّ لتحقيق الأهداف الاقتصاديّة والأمنيّة والاستراتيجيّة للدول [20]. ويمكن عرض أبرز هذه التقنيّات وعلى النحوِ التالي:

1-الذكاء الاصطناعيّ: ظهر مصطلح الذكاء الاصطناعيّ (Artiflciaal lntelligence) لأول مرة عام (1955)، ويُعرَّف على أنه أحد فروع علوم الحاسوب الذي يختص بتصميم وتطوير أنظمة وبرمجيّات قادرة على محاكاة التفكير البشريّ، من خلال تمكين الآلات من أداء مهام تتطلب عادةً قدراً من الذكاء الإنساني. وتتميز هذه الأنظمة بامتلاكها خصائص وسلوكيّات معينة تجعلها قادرة على محاكاة القدرات الذهنية البشريّة وأنماط عملها، ولا سيّما في مجال التعلّيم والاستنتاج، إذ تعد نماذج تحاكي الذكاء البشريّ لأداء وظائف محدّدة. ويُصنَّف الذكاء الاصطناعيّ إلى نوعيّن رئيسيين:

الأوّل -الذكاء الاصطناعيّ (Narrow Al): وهو الذي يركّز على أداء مهام أو مهارات محدّدة دون امتلاك وعي أو إدراك ذاتي، مثل: أنظمة القيادة الذاتية للمركبات أو برامج التعريف على الصوت والصورة.

الثاني -الذكاء الاصطناعيّ القوي: ويُعرف أيضاً ب الذكاء الاصطناعيّ العام (General Al)، والذي يمتلك قدرات عقلية شبيهة بالإنسان، تمكّنهُ من الفهم والتفكير وحلَ المشكلات عبرَ مجالات متعدّدة[21].

ظهر الذكاء الاصطناعيّ في خمسينات القرن الماضي [22]، وقد أجمع خبراء الدراسات الاستراتيجيّة على أنه سيسهم إسهاماً جوهريّاً في تغيير طبيعة الحروب في المستقبل، وذلكَ من نمطها الكلاسيكيّ القائم على توظيف القُوّة المادية والقدرات العسكريّة التقليديّة، إلى نمط أخر جديد تكون فيه القُوّة المعرفيّة والتكنولوجيّة هي المعيار الرئيس في تقييم قدرات الجيوش وفاعليتها. وتشير العديد من الدراسات إلى أنَّ دور الذكاء الاصطناعيّ يُعدُّ من أبرز محدّدات الجيل الرابع من الحروب [23]؛ لما يوفّره من أنظمةٍ وأجهزةٍ قادرة على محاكاة الذكاء البشريّ في أداء المهام المختلفة، فضلاً عن قدرتها على التعليم الذاتي وتحسين أدائها استناداً إلى المعلومات والبيانات التي تقوم بجمعها وتحليلها بصورة مستمرة[24].

ومن هذا المنطلق؛ يبرز التأثير العميق للذكاء الاصطناعيّ في مفهوم الأمن، ولا سيّما في علاقته المباشرة بسيادة الدُّوَل وقدرتها على ممارسة وظائفها السياديّة. إذ يدخل الذكاء الاصطناعيّ في نطاق المراقبة الأمنيّة الالكترونيّة لِلدَّولَةِ، حيث يمكن للخصوم تعلّم آليات التلاعب بأنظمة المراقبة من خلال تغذيتها بمعلومات مضللة بصورة مُمنهجه، بما يؤدي إلى

إضعاف كفاءتها التشغيلية، كما قد تلجأ بعض الجهات المعادية إلى نشر ما يُعرف ب "العميل المزدوج الآلي" بصورة سرية؛ بهدف اختراق الأنظمة الأمنيّة والتأثير في قراراتها، أمّا على صعيد تأثير الذكاء الاصطناعيّ في الأمن القوميّ، فإنَّ مخاطرة المعلوماتيّة أو الالكترونيّة تتجلّى في التلاعب الفعّال بالمعلومات والبيانات، وهو ما يندرج ضمن إطار حروب المعلومات والحروب السيبرانيّة، ولا سيّما عبرَ تطوّر التطبيقات الالكترونيّة الضارة، واستهداف "انترنت الأشياء". ويُعد انتشار الفايروسات والبرمجيّات الخبيثة مثالاً بارزاً على استخدام تقنيّات الذكاء الاصطناعيّ في تنفيذ عمليّات الاختراق التي تستهدف الأمني القومي للدول، وغالباً ما تُمَارَسُ هذه الأنشطة من قبل جهات خارجيّة بوصفها أساليب غير مباشرة للتدخل في الشؤون الداخلية للدول، وذلكَ عبرَ اختراق شبكاتها الحيويّة، وقد أفادت وكالة الاستخبارات المركزية الأمريكيّة بأنها تعتقد أن الانتخابات الرئاسية الأمريكيّة التي أُجريت في (2016) قد تعَرضت لتدخّلٍ أجنبيّ تجاوز حدود التأثير التقليديّ، وذلكَ من خلال هجمات الكترونيّة خارجيّة تمثّلت في نشرٍ انتقائيٍّ لبياناتٍ خاصّة مسرَّبة، في محاولة للتأثير في اتجاهات الرأي العام والناخبين. كما لجأت بعض التنظيمات الإرهابية إلى توظيف تقنيّات الذكاء الاصطناعيّ في تنفيذ عمليّاتها، ولا سيّما باستخدام الطائرات المسيَرة (الدرونز) في الهجوم على الأهداف العسكريّة، ومواقع تخزين النفط، والمطارات، فضلاً عن استهداف الدُّوَل المجاورة، وإضافة إلى ذلكَ، استخدمت الجماعات العنيفة السيارات ذاتية القيادة في تنفيذ هجمات عن بُعد كما حدث في بعض العمليّات الإرهابية التي شهدتها أوروبا عام (2016)، الأمر الذي مكّن هذه التنظيمات من تنفيذ هجمات دون الزج بعناصرها البشريّة في الميدان، ولا يقتصر خطر الذكاء الاصطناعيّ على المجال العسكريّ والأمني التقليديّ، بل امتدَّ ليشمل مجالات أكثر خطورة، كاستخدامه في تطوير وإنتاج الأسلحة البيولوجية، والتلاعب بالمضادات الحيويّة والأدوية، وإنتاج عقاقير سامة يمكن توظيفها من قبل الجماعات المتطرّفة في استهداف الدول، واختراق أمنها عن بعد وتهديد أمنها القومي بكلِّ أبعاده وأشكاله[25].

ويظهر تأثير الذكاء الاصطناعي على السيادة الوطنية، فإلى جانب البعد الاقتصادي، الذي يتمثل في هيمنة الشركات التكنولوجية العابرة للحدود والتحكم في تدفق البيانات، يبرز بعد سياسي لا يقل أهمية عن البعد الاقتصادي، لاتصاله الوثيق بالأمن الوطني والسيادة الوطنية، وعليه فإنَ البعد السياسي يتصل مباشرةً بإعادة تعريف السيادة الوطنية من منظور القوى الفاعلة ذات السيادة في النظام العالمي الجديد [26].

شهدت مجالات استخدام الذكاء الاصطناعي في الأغراض العسكرية توسعاً متسارعاً، لدرجة انها أصبحت غير محدودة وتتزايد يوماً بعد يوم كما انها غيرت من طبيعة الحروب التقليدية بين المتحاربين، ويساعد الذكاء الاصطناعي في تحسين جمع المعلومات الاستخبارية والعمليات المستقلة ودعم اتخاذ القرار العسكري، ويتجلى توظيف الذكاء الاصطناعي في الحروب العسكرية في مجالات متعددة من أبرزها: التوسع في استخدام الأسلحة ذاتية التشغيل، ولاسيما الانظمة الفتاكة المستقلة التي تمتلك القدرة على اختيار أهدافها وتنفيذ عمليات القتل دون تدخل بشري مباشر، وقد برزت هذه التطبيقات بوضوح في الحروب المعاصرة، كما في الحرب الروسية-الأوكرانية[27]. نزاع ناغورنو كاراباخ[28]. والعمليات الامريكية ضد التنظيمات الإرهابية [29].

كما يتم استخدام الذكاء الاصطناعي في تطوير وتحسين أنظمة الأسلحة الموجهة، مثل الطائرات من دون طيار والصواريخ الذكية؛ بما يعزز من دقتها وفعاليتها، ويسهم في تقليل الخسائر البشرية والمدنية، فضلاً عن ذلك، يُوظف الذكاء

الاصطناعي في عملية تحديد الأهداف وتصنيف المقاتلين، كما يسهم في تحسين عمليات التواصل والتنسيق بين الوحدات العسكرية المختلفة، بما يزيد من فعالية العمليات العسكرية ويقلل من الفوضى والارتباك [30].

وعليه، فإن إدماج الذكاء الاصطناعي في المجال العسكري يفرض تحديات كبيرة على مفهوم السيادة الوطنية والضوابط القانونية الحاكمة لاستخدام القوة في إطار النظام الدولي المعاصر.

وعلى ذلكَ، أنَ الذكاء الاصطناعي يمثل أحد أبرز مخرجات الثورة الرقمية وأكثرها تأثيراً في بنية الدولة الحديثة، إذ أسهمَ في إعادة تشكيل آليات اتخاذ القرار وإدارة البيانات على نحوَ غير مسبوق، وقد أدى هذا التطور إلى تأثير مباشر في السيادة الوطنية للدول، وذلك بسبب زيادة الاعتماد على الأنظمة الذكية مما يؤدي الى عدم السيطرة على الفضاء المعلوماتي.

إذ نرى إنَ هذا التأثير لا يعني تراجع السيادة بشكل كلي ومطلق، بل حول السيادة إلى نمطً أكثر تعقيداً يقوم على التشارك والتفاعل، مما يفرض على الدولة تطوير قدراتها في مجال الذكاء الاصطناعي وتعزيز أمنها السيبراني لضمان حماية مصالحها السيادية في العصر الرقمي المتطور.

2-البيانات الضخمة: يرتبط مصطلح "البيانات الضخمة" -بوصفه أحد أهم وأبرز تقنيّات الثورة الرقميّة -ارتباطاً وثيقاً بمفهوم الذكاء الاصطناعيّ، إذ يشير إلى الكمِّ الهائلِ من البيانات التي تتّسم بضخامة حجمها، وتعدد المصادر، وتنوّع أنماطها، فضلاً عن السرعة العالية في إنتاجها وتدفقها وتكاثرها بصورة متسارعة، كما تكتسب هذه البيانات أهَميّة خاصّة بالنظر إلى القيمة المعرفيّة والاقتصاديّة والاستراتيجيّة التي تمثلها. ويُعد الإنترنت المصدر الرئيس لتدفق البيانات الضخمة؛ لما يوفرهُ من بيئة رقميّة مفتوحة تسهم في توليدها وتبادلها وتحليلها على نطاق واسع. ويظهر تأثير البيانات الضخمة في مفهوم السّيادة الوطنيّة؛ لكونها تمسَ قدرة الدَّولَة على التحكم في بياناتها الوطنيّة، وحماية معلومات مواطنيها، وضمان استقلال قرارها السياسي والأمني في الفضاء الرقميّ[31].

بتالي، يمكن القول إنَ أثر البيانات الضخمة على السيادة الوطنية هو أثر مزدوج: فهي من جهة تضعف الشكل التقليدي للسيادة القائم على السيطرة المطلقة، ومن جهة أخرى تدفع نحوَ تطوير نموذج سيادي جديد يكون أكثر مرونة بحيث يتكيف مع البيئة الرقمية العالمية.

3-انترنت الأشياء: يُعرفُ انترنت الأشياء (lnternet of things) بأنهُ منظومة متكاملة من الأجهزة والوسائل التكنولوجيّا المتصلة التي تتيح التواصل بين الأجهزة نفسها من جهة، وبينها وبين الحوسبة السحابية من جهة أخرى، وذلكَ عبرَ شبكات الاتصال الرقميّة. وقد أسهم ظهور رقائق الحاسوب منخفضة التكلفة، إلى جانب تطوير تقنيّات الاتصال ذاتَ الناطق الترددي الاعتيادي، في الانتشار الواسع لهذه التقنيّة؛ الأمر الذي أدى إلى ربط مليارات الأجهزة بالإنترنت [32].

وتشمل هذه الأجهزة مختلف الأدوات المستخدمة في الحياة اليومية، مثل: فرش الاسنان، والمكانس الكهربائية، والسيارات، والآلات الصناعيّة، إذ أصبحت قادرة على جمع البيانات عبر أدوات الاستشعار، وتحليلها، والتفاعل الذكيّ مع المستخدمين. ويقوم انترنت الأشياء على دمج الأشياء المادية بالإنترنت من خلال تزويدها بمستشعرات ومعالجات رقميّة، بما يسمح بتبادل لبيانات واتخاذ قرارات آليّة دون تدخل بشريّ مباشر[33].

وقد بدأ الاهتمام بتطوير هذه التقنيّة منذ التسعينات القرن الماضي، إلّا إن التقدم كان بطيئاً في مراحلهِ الأولى؛ بسبب كِبر حجم الرقائق الالكترونيّة وارتفاع تكلفتها. وفي هذا السياق، استخدمت رقائق منخفضة الطاقة تُعرف بعلامات التعرَف بالترددات الراديوية (RFID) في بدايتها لتتبع المعدات ذات القيمة العالية. ومع التطوّر المستمر في تقنيّات الحوسبة

وتقليص حجم الأجهزة؛ أصبحت هذه الرقائق أصغر حجماً وأكثر سرعة وذكاء مما أسهمَ في تسريع انتشار تطبيقات إنترنت الأشياء وتوسيع مجالات استخدامها[34].

بتالي إنَ أثر أنترنت الأشياء على السيادة الوطنية يظهر من خلال تراجع السيطرة الكاملة للدولة على البيانات، كون أنترنت الأشياء تجمع كميات ضخمة من البيانات داخل الدولة، والتي غالباً ما تخزن أو تديرها شركات أجنبية وهذا يؤدي إلى أضعاف قدرة الدولة على الاحتكار السيادي للمعلومات.

4-الحوسبة السحابية: تُعد الحوسبة السحابية نتاجاً لتكامل مجموعة من تقنيّة الحاسوب والشبكات، ومن أبرزها الحوسبة الموزعة، والحوسبة الشبكية، والحوسبة المتوازية، والتقنيّات الافتراضيّة، والتخزين الشبكي، فضلاً عن تقنيّات موازنة الأحمال [35].

وتمثّل الحوسبة السحابية نهجاً حديثاً يقوم في أساسه على شبكة الإنترنت، إذ يربط عدداً من أجهزة الحاسوب ضمن بيئةٍ رقميّةٍ موحّدةٍ تُتِيح الاستفادة من الموارد الحاسوبية المشتركة بصورة مرنة وقابلة للتوسيع. ويهدف هذا النهج إلى معالجة المشكلات المتعلقة بتخزين البيانات الضخمة وإدارتها عن بعد[36].

ونرى أثر الحوسبة على السيادة الوطنية للدول يظهر من خلال فقدان الدولة السيطرة على البيانات الوطنية، لانَ في كثير من الأحيان تخزن بيانات الحكومات أو المؤسسات على خوادم خارج الدولة ويتم التحكم بها عبر شبكات اجنبية، وهذا يؤدي إلى أضعاف مبدأ السيادة المعلوماتية للدولة، إذ يعرضها إلى الاختراقات أو التجسس الالكتروني...وغيرها.

5-الطابعات ثلاثية الابعاد: تُعدُّ هذه الطابعات من التقنيّات الحديثة التي تقوم على تصنيع مجسمات ثلاثية الأبعاد، وذلكَ من خلال ترسيب طبقات متتآليّة من المواد فوق بعضها البعض إلى أن يتم تكوين المنتج النهائي، وذلكَ اعتماداً على المعلومات الرقميّة الخاصّة بالنموذج ثلاثي الابعاد [37].

وتعتمد هذه التقنيّة على إنتاج الأجسام على شكل طبقات متراكمة، بخلاف الطباعة التقليديّة ذات البعد الواحد، حيث يتمَ التصنيع استناداً على نماذج رقميّة معدة مسبقاً. وقد مكنَ التطوّر المتسارع في تقنيّات الطابعات ثلاثية الابعاد من إنتاج مكوّنات بالغة التعقيد والدقة؛ الأمر الذي يُنذر باتساع نطاق استخدامها وانتشار منتجاتها في مختلف المجتمعات والقطاعات خلال المستقبل القريب [38].

وبتالي، نرى أنَ الطابعات ثلاثة الابعاد ما هي الا سلاحاً ذا حدين؛ فهي من جهة تعزز الاستقلال الاقتصادي والتكنولوجي للدولة، ومن جهة أخرى تضعف قدرتها على الرقابة والسيطرة، مما يستدعي تحديث الأطر القانونية والسياسات العامة للحفاظ على السيادة الوطنية في ظل العصر الرقمي الراهن.

الفرع الثاني

الأمن السيبرانيّ وأثرهُ على السّيادة الوطنيّة

يوصف القرن الحادي والعشرون بأنّه عصُر المعلومات والمعرفة، إذ أصبحت البيانات تُشكّلَ مورداً استراتيجيّاً بالغ الأهَميّة تعتمد علية الدُّوَل في تحقيق النهضة والتنمية الشاملة، وأضحت تؤدّي دوراً محورياً في دفع عجلة التقدم الاقتصاديّ والاجتماعيّ مقارنةً مع الدور المتعاظم الذي أداه النفط خلال القرنين الثامن عشر والتاسع عشر، حيث شكَّل كلٌّ منهما مُحَرّكاً رئيساً لإحداث التحوّلات الاقتصاديّة والاجتماعيّة وتعزيز مراكز القُوّة على المستويين الوطنيّ والدوليّ[39]. وأسهمَ

هذا التحوّل في إعادة توزيع القُوّى الدوليّة، بحيث لم تعد المعايير التقليديّة، كالثورة الاقتصاديّة، والقدرات العسكريّة، والموقع الجغرافي هي المحدّدات الحصرية لمكانة الدَّولَة في النِّظَام الدوليّ، بل باتت القدرات السيبرانيّة ومستوى الحماية الرقميّة والأمن المعلوماتيّ من أبرز مؤشرات القُوّة والنفوذ في العصر الرقميّ [40].

ويأتي ذلكَ في ظلِّ التزايد المستمر في أعداد الأفراد والجهات التي تحاول الوصول إلى المعلومات عبر شبكة الانترنت يومياً، وما يرافقه من تصاعد ملحوظ في حجم ونوعيّة التهديدات السيبرانيّة التي تستهدف البيانات والأنظمة المعلوماتيّة[41].

وتشير التقديرات الدوليّة إلى أنَ الخسائر الناتجة عن الجرائم الالكترونيّة تُقدّر بمليارات الدولارات سنوياً؛ الأمر الذي يعكس خطورة هذه الجرائم وتأثيرها المباشر في الأمن الاقتصاديّ والسياسي للدول. وبناءً على ذلكَ؛ فإنَّ الأمن السيبرانيّ يُمثّل إطاراً وقائيّاً أساساً يهدف إلى المحافظة على المعلومات والبيانات الخاصّة بالأفراد والمؤسسات، وحمايتها من محاولات الاختراق غير المشروع؛ بما يسهم في تعزيز الثقة بالفضاء الرقميّ وضمان استمراريّة عمل المؤسسات في ظل البيئة الرقميّة المعاصرة [42].

ويرتبط الأمن السيبرانيّ ارتباطاً وثيقاً، بأمن المعلومات، إذ يُعَدُّ الوصول غير المشروع إلى المعلومات، أو بثها، أو حتى مجرّد الاطلاع عليها دون إذن قانوني، إحدى أبرز الدوافع الكامنة وراء عمليّات اختراق الشبكات والأنظمة المعلوماتيّة. ويستدعي الحديث عن الأمن -من منظور قانوني وأكاديمي–بأنه مرتبط بمفاهيم القانون الدولي ولاسيما، مبدأ السيادة، ومبدأ عدم التدخل، وللوقوف عند مفهوم الخطر بوصفه التهديد الذي يتعرض له النِّظَام المعلوماتيّ، فضلاً عن تحديد نقاط الضعف أو الثغرات التقنيّة والتنظيمية التي تعتريه، ثم بيان الإجراءات الأمنيّة الواجب اتخاذها للحدِّ من هذه المخاطر ومنعها[43].

وتكمن خطورة هذه التهديدات في أنّها قد تؤدّي إلى اختراق معلومات أمنيّة أو شخصيّة؛ بما ينعكس سلباً على أمن المجتمع واستقرار الدولة، ولا سيّما في ظل التوسع المتسارع لاستخدام الفضاء السيبرانيّ بوصفه مجالاً حيويّاً للتفاعل الاقتصاديّ والسياسي والاجتماعيّ. ومن ثم فقد برزت الحاجة الملحة إلى إطار مفاهيمي وتنظيمي شامل يُعني بحماية هذا الفضاء، وهو ما يعرف بالأمن السيبرانيّ [44].

وقد تعددت التعاريف التي تناولت مفهوم الأمن السيبرانيّ، وذلكَ باختلاف الزاوية التي يُنظر من خلالها إلى هذا المصطلح، إلّا أنها اشتركت جميعها في مضمون واحد متقارب في المعنى، إذ يُقصد بالأمن السيبرانيّ مجموعة من الممارسات والإجراءات التي تهدف إلى حماية الأنظمة والشبكات والبرامج والمواقع الالكترونيّة من الهجمات الرقميّة، أيّاً كان مصدرها أو نوعها، والتي تُنفّذ عبر وسائل الكترونيّة مختلفة، ويشمل الأمن السيبرانيّ جملة من التدابير المتنوّعة التي تتوزع بين تدابير احترازية واستباقية قبل وقوع الخلل أو الاختراق، وتدابير علاجية تُطبّق بَعد وقوعه؛ وذلك بهدف الحدِّ من آثارهِ ومعالجةِ نتائجهِ وضمان استمراريّة عمل الأنظمة وحماية البيانات والمعلومات من أي تهديدات محتملة [45].

ويُعدُّ مفهوم الأمن السيبرانيّ من المفاهيم التي حظيت باهتمامٍ متزايد في الآونة الأخيرة؛ وذلك نتيجةً للتطوّر المتسارع في التقنيّات التكنولوجيّة الحديثة واتّساع نطاق استخدامها بصورة فعليّة في مختلف المنشآت والمؤسسات [46].

وتتجلى أهَميّة الأمن السيبرانيّ في ارتباطه الوثيق بالجريمة الالكترونيّة، التي تعدُّ من أبرز التهديدات المعاصرة التي تواجه الأمن المعلوماتيّ الذي يعمل على مكافحتها والحد من أثارها السلبية، إذ تُعرّف الجريمة الالكترونيّة بأنها: أنشطة إجرامية ذكيّة تنشأ في البيئة الالكترونيّة أو الافتراضيّة، حيث يقوم بها الأفراد أو الجماعات أو منظمات لديهم درجة عالية من المعرفة التقنيّة والقدرات التكنولوجيّة، بما يترتب عليها أضرار بالغة بالمصالح الحيويّة للدول والمجتمعات. وتظهر أهَميّة

في الوقت الحاضر بسبب ازدياد الترابط في الشبكة العنكبوتية، إذ أصبح يمثّل عنصراً مهمّاً في كافة المستويات، الاقتصاديّة منها والسياسيّة والاجتماعيّة، كما يُعدُّ الأمن السيبرانيّ عنصراً مكمّلاً للأمن القومي وجزءاً لا يمكن تجزئتهُ من الأمن الجماعي، وفي ظل الترابط الوثيق بين الأمن والتكنولوجيا، وما يترتب على ذلكَ من تصاعد احتمالات تعرض المصالح الاستراتيجيّة إلى مخاطر الالكترونيّة عابرة للحدود، إذ يؤدي هذا إلى تحوّل الأنظمة الالكترونيّة من مجرّد أدوات تقنيّة إلى وسائل مؤثرة في الصراعات الدوليّة، بل وحتى بوصفها أدوات لتغذية التورات والنزاعات بين الدول(47).

وعليه، أنَ الأمن السيبراني يمثل عنصراً جوهرياً في حماية السيادة الوطنية في العصر الرقمي، إذ امتدت السيادة لتشمل الفضاء الرقمي إلى جانب الإقليم التقليدي، فالهجمات السيبرانية قد تهدد أمن الدولة وتؤثر في استقلال قرارها، ولاسيما في ظل الاعتماد المتزايد على الأنظمة الرقمية، لذلكَ فأنَ تعزيز قدرات الأمن السيبراني يعدُ ضرورةً لضمان حماية المعلومات، وصون استقلال الدولة في مواجهة التهديدات الحديثة.

وعليه، لابد انَ نوضح أهم وأبرز تطبيقات الحروب السيبرانية على مستوى التهديدات العالمية والإقليمية. زمن ثم نتناول الإطار القانوني للأمن السيبراني.

أوّلاً -تطبيقات الحروب السيبرانيّة على مستوى التهديدات والهجمات العالميّة والاقليمية: تحتلّ الحروب السيبرانيّة أهَميّة متزايدة على المستويين العسكريّ والأمنيّ، وذلك نتيجةً للتحول الجوهريّ الذي طرأ على العقائد العسكريّة، ولا سيّما في الجانب الاستراتيجيّ. إذ اشارَ عددً من المسؤولين العسكريّين إلى أنَ عمليّات الاختراق السيبرانيّ تمثّل وسيلة فعّالة لتحقيق تفوّق عسكريّ بأقلَ تكلفة مقارنة بالوسائل التقليدية؛ كونها وفَرت ملايين النفقات العسكرية بشكل كبير، فضلاً عن توفير جهد ووقت بما يقارب (25) عاماً من البحث والتطوير، وهو ما يُعدُّ معضلةً استراتيجيّةً كبرى. إذ تتمثل هذه المعضلة في ثلاث قضايا رئيسة، أوّلها: الاختراقات المتعدّدة التي قامت بها الصين لشبكات الشركات الأمريكيّة، والتي ترتَّبَ عليها سرقة للملكيّة الفكريّة والمعلومات ذاتِ الطابع التجاري. أمّا القضيّة الثانية فتتمثل في استخدام الفضاء السيبرانيّ لأغراض تجسّسيّة تقليديّة مرتبطة ارتباطاً مباشراً بالأمن القومي. في حينَ يتمثل المصدر الثالث للقلق في احتمال شنِّ هجماتٍ سيبرانيّة تهدف إلى تدمير البنية التحتيّة للدول، بما قد يشكل تهديداً مباشراً لسيادتها وأمنها الوطنيّ (48).

تستخدم الولايات المُتّحِدَة وعددٌ من القوى الكبرى وسائلَ متعدّدةٍ لتحقيق أهدافها الاستراتيجيّة، تقوم في جوهرها على انتهاك سيادة بعض الدَّولَة التي تتعارض في سياساتها مع توجهاتها، وذلكَ تحت ذرائع مرتبطة بنشر قيم الديمقراطيّة ، وحقوق الإنسان، وقد تزامنَ ذلك مع التحوّل الجوهريّ الذي شهدهُ مفهوم القُوّة في العلاقات الدوليّة، إذ أنهُ لم يَعُد يُعتمدُ على الأدوات العسكريّة التقليديّة، بل أصبحَ اعتمادهُ بصورة متزايدة على مفهوم التقنيّة الالكترونيّة، ولا سيّما وسائل التواصل الاجتماعيّ؛ كونها تُمثّل أدواتٍ فعّالة للتأثير في الرأي العام المجتمعيّ، من أجل دفعه لتقبّل شعاراتٍ وقيمٍ وأفكارَ محدّدةٍ (49).

وعلى سبيل المثال، تصاعدت حدّة الهجمات السيبرانيّة بين الولايات المُتّحِدَة وروسيّا خلال العام (2020)، إذ تعرّضت العديد من الهيئات الرسمية والمؤسسات الأمريكيّة لهجمات واسعة النطاق، من بينها وزارات الخزانة والتجارة والامن الداخلي والدفاع، وكانت روسيّا المتّهم الرئيس في هذه الهجمات وفقاً لتصريحات أمريكيّة، وفي عام (2020) تعرّضت مجموعة من المستشفيات الأمريكيّة ومختبرات البحث، إضافةً إلى مزودي الخدمات الطبية وشركات الأدوية لهجمات

الكترونيّة ومحاولات اختراق نفّذها قراصنة الكترونيّون، ما يعكس اتساع نطاق استهداف البنى التحتية الحيوية في الفضاء السيبراني[50].

وعلى الصعيد الأوربيّ: حظيت مسالة أمن الفضاء الالكترونيّ بمكانة متقدّمةٍ ضمنَ استراتيجيّات الأمن القومي للحكومة البريطانية بعد عام (2010)؛ وذلك في ظلِّ اتّساع حجم التهديدات التي تواجهها المملكة المُتّحِدَة. وقد تراوحت هذه التهديدات بين أنشطة إجرامية منخفضة المستوى وعمليّات الكترونيّة متقدمة ومعقّدة؛ الأمر الذي دفعَ الحكومة البريطانية إلى تخصيص نحَو (650) مليون جنيه إسترليني خلال المدّة ما بين (2011- 2015)؛ بهدف تعزيز أمن الفضاء الالكترونيّ وحماية البنية التحتيّة والرقميّة للدول[51].

كما شَهِدَ عام (2015) تصاعداً في الهجمات السيبرانيّة الروسيّة من خلال اختراق شبكة الكهرباء الأوكرانيّة، وتكررَ ذلكَ في عام (2016)، فضلاً عن شَنِّ هجمات الكترونيّة استهدفت المواقع الحكومية الأوكرانيّة في العام نفسه، وقد استمرت هذه الهجمات في عام (2017)، وتكثّفت بصورة أكبر في (2022) في ظلِّ تصاعد حدّةِ التوتر في العلاقات الروسيّة – الأوكرانيّة؛ الأمر الذي يعكس توظيف الفضاء السيبرانيّ بوصفه أداة ضغط وصراع في إطار النزاعات الدوليّة المعاصرة[52].

أصبحَت تطبيقات الحروب السيبرانيّة أحد أبرز مصادر التهديدات الإقليميّة والدولية، إذ باتَ الفضاء الالكترونيّ ساحةً جديدة ومختلفة للصراع يتمّ فيها استخدام الحواسيب وشبكات الاتصال والمعلومات في تجاوز حدود السيادة الوطنيّة للدول في بعض الأحيان، ومن أبرز الأمثلة على ذلكَ، الهجمات السيبرانيّة التي شنتها إسرائيل بالتعاون مع الولايات المُتّحِدَة الأمريكيّة، من خلال إطلاق فيروس ستاكسنت(Stuxnet) ضد المنشآت النووية الإيرانية عام (2010)، والذي شكّلَ سابقة خطيرة في توظيف البرمجيّات الخبيثة من أجل تحقيق الأهداف التي تسعى إليها وهي ذات طابع استراتيجيّ عسكريّ. كما شهدت الفترة الممتدة بين (2008- 2012) مواجهات الكترونيّة متبادلة بين حركة حماس وإسرائيل، بالإضافة إلى الهجمات الالكترونيّة لفايروس شمعون (Shamoon) التي تعرضت لهُ المملكة العربية السعودية والتي كانت على نطاقً واسع، إذ تم فيها استهدفت أنظمة الحواسيب التابعة "لشركة أرامكو السعودية" وبعض الجهات الحكومية والمنشآت الحيويّة، وذلكَ خلال الفترة من (2012- 2017)، مخلفاً أضرار كبيرة على مستوى البنية التحتيّة الرقميّة، بالإضافة إلى هجوم فيروس دوكو (Duqu) الذي استهدفَ شبكة الفنادق التي استضافت المفاوضات المتعلقة بالملف النووي الإيراني خلال الفترة من (2014- 2015) [53].

وتُعدَ المواجهات السيبرانيّة الدائرة بين الولايات المُتّحِدَة الأمريكيّة وإيران، إحدى أبرز صور الصراع المعاصر؛ إذ اعتمدَ الطرفان على الأدوات السيبرانيّة المتقدمة بوصفها وسائل فعّالة ومؤثرة تهدف إلى إلحاق أكبر قدر ممكن من الضرر بالمواقع الحيويّة والبنى التحتيّة الاستراتيجيّة للطرفين [54].

وقد عَمِلَ الرئيس الأمريكيّ السابق "باراك أوباما" على توسيع نطاق الهجمات السيبرانيّة؛ لتشمل توظيف الأسلحة السيبرانيّة في استهداف منشآت تخصيب الوقود النووية الإيراني. وفي عام (2010) اعترف المسؤولون إيرانيون بتعرَض أجهزة الحاسوب في محطة "بوشهر النووية" لهجوم سيبرانيّ؛ أدى إلى تأثير كبير تمثلَ في تعطيل تخصيب اليورانيوم في محطة "نطنز" النووية بالكامل؛ وذلك نتيجة إصابتها بفيروس موجة ضدها والمعروف بـ "ستوكسنت" وقد اتهمت إيران الولايات المُتّحِدَة بالوقوف وراء هذا الهجوم. إذ أكدَ نائب المدير العام السابق للوكالة الدوليّة للطاقة الذرية، "أولي هينونن"

أن الفيروس تسبب في مشكلات تقنيّة جسيمة، وأدى إلى تعطيل آلاف من أجهزة الطرد المركزي المستعملة بتخصيب اليورانيوم [55].

وبناء على ذلكَ؛ نرى أنَ الحروب السيبرانيّة تشكل تهديداً متزايداً للأمن الإقليميّ والدولي؛ لما تنطوي عليه من هجمات عابرة للحدود تَمَسُّ البُنَى التحتيّة للدول وتثير إشكاليّات قانونية كبيرة مرتبطة بالسيادة الوطنيّة، ومبدأ عدم التدخل، والمسؤولية الدوليّة في إطار القانون الدولي العام، إذ تشير التطورات الحديثة في السنوات الأخيرة إلى استخدام الذكاء الاصطناعي والهجمات السيبرانية الموجهة في النزاعات المعاصرة، بما يعكس تعقيد الفضاء السيبراني وتحوله إلى ساحة رئيسية للصراع الدولي.

ثانياً: الإطار القانوني للأمن السيبراني: يشهد العالم تطوراً رقمياً متسارعاً جعل الفضاء السيبراني جزءاً من عمل الدول والمؤسسات، لكن في الوقت نفسه أدى إلى ظهور تهديدات الكترونية متزايدة تمس أمن البيانات والبنى التحتية، إذ لم يعد الأمن السيبراني مسالة تقنية فقط، بل أصبح موضوعاً قانونياً مهماً يرتبط بحماية الدولة لسيادتها الرقمية وتنظيم المسؤولية عن الهجمات الالكترونية، ومن هنا تبرز أهمية دراسة الإطار القانوني للأمن السيبراني وكما يلي:

1. **الإطار القانوني للأمن السيبراني على المستوى الوطني:** مع التطور المتسارع في مجال تكنولوجيا المعلومات والاتصالات، أضحى الامن السيبراني عنصراً اساسياً في حماية البنى التحتية للدول، لا سيما مع تزايد التهديدات والهجمات العابرة للحدود، وقد برزت أهمية هذا المجال بوصفه أحد المرتكزات الأمن الوطني، وفي العراق، ولاسيما بعد عام 2003، واجه تحديات أمنية رقمية متباينة نتيجة ضعف البنية التحتية التقنية، وانكشاف منظوماته الحكومية والمؤسساتية أمام موجات من القرصنة والتجسس السيبراني، وعلى الرغم من أهمية الأمن السيبراني المتنامية الا أن التشريعات العراقية ما زالت تعاني من قصور واضح في مواكبة هذا الواقع الرقمي المتسارع ،سواء من حيث التنظيم القانوني أو من حيث الأدوات والمؤسسات المعنية بالمواجهة[56].

ويتميز النظام القانوني العراقي بوجود إطار تشريعي عام ، يشمل مختلف المجالات القانونية ومن بينها حماية البيانات الشخصية والأمن السيبراني، وذلك من اجل ضمان استخدامها والحفاظ عليها من أي انتهاك او استغلال غير مشروع، وتعد هذه الحماية ضرورية في ظل التطور التكنولوجي السريع الذي يشهده العالم، حيث أصبحت البيانات الشخصية من الموارد الحساسة التي تتطلب تنظيماً قانونياً دقيقاً للحفاظ على خصوصية الافراد وضمان عدم التعدي عليها، ورغم تضمين بعض النصوص القانونية التي تعالج بصورة غير مباشرة الجرائم المعلوماتية[57].الا أن غياب تشريع متكامل خاص بالأمن السيبراني ومكافحة الجرائم الإلكترونية يخلق فراغاً قانونياً يُستغل من قبل مرتكبي هذه الجرائم ، مما يؤدي إلى ضعف فعالية الردع القانوني وصعوبة ملاحقة الجناة وتحقيق العدالة.

برزت محاولات تشريعية لسد هذا النقص، من أبرزها مشروع قانون جرائم المعلوماتية الذي طرح في البرلمان العراقي منذ عام2011، وأعيد طرحه عام 2023بعد إدخال تعديلات عليه [58].

إذ نص على" يعاقب كل من حاول استخدام شبكة المعلومات لتديمر الأمن والنظام العام بالسجن المؤبد أو بغرامة تتراوح بين(25-50) مليون دينار عراقي[59]. وايضاً تم النص على الحبس لمدة سنتين ودفع غرامة لا تقل عن مليوني دينار ولا تزيد على خمسة ملايين، لمن نسب إلى الغير عبارات أو أصوات أو صوراً تنطوي على القذف والسب من خلال شبكة المعلومات [60]. وقد تم سحب ذلك المشروع من قبل الحكومة، لغرض إضافة بعض التعديلات عليه[61].

وعلى الرغم، من أهمية هذا المشروع في تنظيم الفضاء الالكتروني، الا أنه واجه انتقادات واسعة، مما ادى إلى سحبه لإجراء تعديلات عليه، وهو ما يعكس استمرار التحديات التي تواجه المشرع العراقي في تحقيق التوازن بين حماية الأمن وضمان الحقوق والحريات، وعليه، نرى إنَ تعزيز الأمن السيبراني في العراق يتطلب تبني إطار قانوني متكامل وحديث، يشمل وضع تشريعات واضحة لمكافحة الجرائم السيبرانية، وتحديد آليات الوقاية والاستجابة، فضلاً عن بناء مؤسسات متخصصة قادرة على تنفيذ هذه القوانين بكفاءة.

2.الإطار القانوني للأمن السيبراني على المستوى الدولي: تُعد الجريمة الالكترونية من الظواهر التي تتجاوز الحدود الوطنية، الأمر الذي يفرض ضرورة تعزيز التعاون القانوني الدولي بين السلطات المعنية كافة، كونَ لا تقتصر أثار هذه الجرائم على الدولة التي تنشأ فيها الجريمة فحسب، بل تمتد لتشمل البلدان التي تم التنفيذ فيها، مما يستدعي وجود إطار تعاون دولي منظم وفعال. إذ تبرز أهمية إنشاء شبكات تعاون دولي مدعومة باليات إجرائية جنائية تسهل التواصل المباشر بين الأجهزة في مختلف الدول، بما يضمن سرعة الاستجابة لمكافحة الجرائم السيبرانية والحد من آثارها [62].

إذ إنَ المجتمع الدولي واجهة هذه الظاهرة بمجموعة من التشريعات وذلك عن طريق المعاهدات والاتفاقيات وعلى كافة المستويين الإقليمي والدولي، ومنها:

أ-على المستوى الأممي: وضعت الأمم المتحدة مجموعة من القواعد الموضوعية والاجرائية لمواجهة الجرائم السيبرانية،

. القواعد الموضوعية: تضمنت النص على قائمة الحد الأدنى للأفعال المتعين تجريمها أو اعتبارها من قبيل الجرائم السيبرانية، مع ضرورة تحديثها بصورة دورية لمواكبة التطور التكنولوجي، ومن أبرز هذه الجرائم: الاحتيال-الغش المرتبطة بالحاسوب-جريمة التزوير التي تطال برامج الحاسوب أو ما يعرف بالتزوير المعلوماتي، فضلاً عن جريمة تخريب واتلاف أنظمة الحاسوب-جريمة الدخول غير المصرح به، وكذلك جريمة الاعتراض غير المصرح به للبيانات أو الاتصالات.

. القواعد الإجرائية: فتتضمن مجموعة من الأسس التي ينبغي مراعاتها من أهمها: تحديد السلطة المختصة بإجراءات التفتيش والضبط في بيئة تكنولوجيا المعلومات، وضرورة تعزيز التعاون الفعال بما يتيح التنسيق بين الجهات المختصة للأغراض القضائية في مكافحة الجرائم السيبرانية، فضلاً عن تمكين السلطات العامة من اعتراض الاتصالات ضمن البيئة المعلوماتية، مع إجازة استخدام الأدلة المستمدة منها وفقاً للضوابط القانونية المقررة [63].

كذلك قرارات الجمعية العامة للأمم المتحدة إذ تم التصويت على القرار رقم 95/45 الذي تضمن المبادئ التوجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الالكترونية، ومثل هذه المبادئ غير ملزمة للدول الأعضاء لضمان التدابير التشريعية للتصدي للجريمة الالكترونية بالإضافة إلى قرارات أخرى[64]. وكما يلي:

-قرار رقم57/239 الصادر في 2003، بشأن انشاء ثقافة عالمية للأمن السيبراني، والذي يدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني.

-قرار لجنة مكافحة المخدرات رقم48/5 حول تعزيز التعاون من اجل منع استخدام شبكة الانترنت لارتكاب الجرائم المتصلة بالمخدرات.

قرار 55/63 الصادر عام 2000 وقرار 56/121 الصادر 2001، بشأنَ مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات.

ب-على المستوى الاتفاقيات الدولية: شكلت اتفاقية بودابست لمكافحة الجرائم الالكترونية أول معاهدة دولية متخصصة في هذا المجال [65].

جسدت هذه الاتفاقية مظهراً واضحاً للتعاون والتضامن الدولي في مواجهة الجرائم السيبرانية، وشكلت خطوة أساسية نحو بناء إطار قانوني دولي مشترك لمكافحة الجرائم المرتكبة عبر شبكة الانترنت وسوء استخدامها.

وقد أسهمت الاتفاقية في وضع قواعد قانونية موحدة لتجريم الأفعال المرتبطة بالفضاء السيبراني، إلى جانب إرساء آليات للتعاون الدولي، شملت تبادل المعلومات، المساعدة القانونية المتبادلة، تسليم المجرمين، الأمر الذي عزز من فعالية الجهود الدولية في مكافحة الجرائم الإلكترونية، كما أكدت على إشراك الفاعلين غير الحكوميين، ولاسيما القطاع الخاص ومزودي خدمات الانترنت، في بناء منظومة متكاملة للأمن السيبراني، وهو ما يعكس إدراكاً لطبيعة الفضاء الرقمي بوصفه مجالاً عابراً للحدود لا يمكن للدولة منفردة السيطرة عليه.

عالجت هذه الاتفاقية: طائفة من الجرائم السيبرانية الأكثر شيوعاً على المستوى الدولي، كالارهاب السيبراني-تزوير بطاقات الائتمان-استغلال الأطفال عبر الانترنت؛ وكما وضعت إطاراً إجرائياً واضحاً للتحقق في هذه الجرائم، مع التأكيد على التزام الدول الأطراف بالتعاون المشترك في مكافحتها، وبما يحقق التوازن بين متطلبات إنفاذ القانون من جهة، وضمان حماية حقوق الانسان والحريات الأساسية من جهة أخرى[66].

وعليه، نرى إن اتفاقية بودابست لمكافحة الجرائم الإلكترونية من أهم الاتفاقيات الدولية في مجال مكافحة الجرائم السيبرانية، كونها أسهمت في وضع إطار قانوني دولي موحد يهدف: إلى تجريم الأفعال المرتبطة بالفضاء السيبراني.

كما أرست مبادى التعاون الدولي وتوحيد التجريم في الفضاء الرقمي، وكرست مبدأ الطبيعة العابرة للحدود لهذه الجرائم، حيث تمثل هذه الاتفاقية أساساً مهماً في بناء القانون الدولي للأمن السيبراني، لكنها تعاني من محدودية في الشمولية وضرورة التحديث المستمر لمواكبة التطور التكنولوجي، مما يحد من فعاليتها العالمية.

وعليه، فإنَ هذه الاتفاقية لا تتعارض مع مبدأ السيادة الوطنية بقدر ما تَعيد صياغتها ضمن مفهوم أكثر مرونة يتناسب مع طبيعة الجرائم السيبرانية العابرة للحدود.

الخاتمة

في ضوء ما تقدم، يتضح أنَ التكنولوجيا الحديثة أسهمت في إعادة تشكيل مفهوم السيادة الوطنية، فبينما عززت قدرات الدول في مجالات متعددة، أوجدت في الوقت ذاتهُ تحديات جديدة تمسَ استقلالها.

اولاً /الاستنتاجات :

1. أسهمت التكنولوجيا الحديثة في تقليص مفهوم السيادة التقليدية وتوسيعه ليشمل الفضاء الرقمي.
2. زادت التحديات المرتبطة بالأمن السيبراني والتدخلات غير المباشرة بين الدول.
3. عززت التكنولوجيا من قوة الدول المتقدمة بينما أدت إلى اتساع الفجوة في الدول النامية.
4. أصبح التحكم بالمعلومات والبيانات عنصراً أساسياً في ممارسة السيادة.

ثانياً / المقترحات:

1. تطوير استراتيجيات وطنية شاملة للأمن السيبراني.
2. سنَ تشريعات قانونية تنظم استخدام التكنولوجيا وتحمي البيانات الوطنية.
3. تعزيز التعاون الدولي لمواجهة التهديدات الرقمية المشتركة.
4. الاستثمار في بناء القدرات التقنية والبشرية لمواكبة التطور التكنولوجي.

ـ الهوامش :

(1) جمال سند السويدي، وسائل التواصل الاجتماعي ودورها في التَحَوّلات المستقبلية من القبلية الى الفيس بوك، (د. ن) 2013، ص38.

(2) محمد سعيد الكعبي، التكنولوجيا والتحول في إطار العملية السياسية، أطروحة دكتوراه، جامعة الجزائر، كلية العلوم السياسية والعلاقات الدولية، 2024، ص4.

(3) خالدية بلحاج وفرعون محمد، السيادة الرقمية، مجلة البحوث في الحقوق والعلوم السياسية، مجلد11، العدد1، 2025، ص461.

(4) شريف درويش، الثورة الرقمية وتَحَوّلات القوة الناعمة، المجلة العربية لبحوث الاعلام والاتصال، العدد46، 2024، ص 6-7.

(5) حامد محمود مسار الثورة التكنولوجية وانعكاساتها في العلاقات الدولية أطروحة دكتوراة جامعة بيروت العربية كلية الحقوق والعلوم السياسية 2025ص409-410

(6) فايق حسن جاسم، أثر الانفتاح المعلوماتي في السيادة الوطنية، المجلة السياسية والدولية، العدد18، 2011، ص206.

(7) مصطفى سحاري، السيادة الوطنية للدول في ظل ثورة المعلومات، مجلة المعيار، مجلد 10، العدد4، 2019، ص53.

(8) عبد السلام احمد حسين وبشرى ناجي صالح تقنيات الثورة الرقمية الثانية ودورها في تحقيق التنمية المستدامة بالجامعات اليمنية مجلة جامعة المهرة للعلوم الإنسانية، العدد1، 2025 ص 744.

(9) عبد الوهاب بريكة وزينب ابن تركي، أثر تكنولوجيا الإعلام والاتصال في رفع عجلة التنمية، مجلة الباحث، عدد7، 2010، ص246.

(10) سمير عبد الرسول، الثورة الرقمية: نشأتها وأثرها على التعليم العالي والبحث العلمي، مجلة المستنصرية للعلوم الإنسانية، مجلد2، العدد1، 2024، ص363.

(11) حسن محمد جواد الجبوري، منهجية البحث العلمي مدخل لبناء المهارات البحثية، دار صفاء للنشر والتوزيع، عمان، الأردن، ص 23-24-25.

(12) سمير عبد الرسول، الثورة الرقمية: وأثارها على التعليم العالي والبحث العلمي، مصدر سابق، ص364.

(13) عبد الوهاب بريكة وزينب ابن تركي، أثر تكنولوجيا الإعلام والاتصال في رفع عجلة التنمية، مصدر سابق، ص247.

(14) جاسم محمد، الطريق الى مجتمع المعرفة وقطاع المكتبات والمعلومات في الوطن العربي، دار الفكر للطباعة والنشر، دمشق، 2014، ص5-6.

(15) سوزان موزي، الثورة المعلوماتية والتكنولوجية وسياسات التنمية، دار المنهل اللبناني، بيروت، لبنان، 2009، ص1.

(16) لوتشيانو فلوريد، الثورة الرابعة (كيف يعد الغلاف المعلومات يتشكيل الواقع الإنساني)، ترجمة لؤي عبد المجيد السيد، المجلس الوطني للثقافة والفنون والآداب، سلسلة عالم المعرفة، الكويت، 2017، ص 129-130-131.

(17) حسين علي، تطبيقات أنترنت الأشياء في المكتبات ومراكز المعلومات الآفاق والتحديات، مجلة جامعة صبراتة العلمية، مجلد9، العدد5، 2019، ص178.

(18) سهى حمزاوي، نقل التكنولوجيا إلى الدول النامية بين حتمية مدرسة التبعية ومنطق الخصوصية التاريخية، مجلة العلوم الاجتماعية، العدد21، 2016، ص75.

(19) عبد السلام حسين وبشرى ناجي صالح، تقنيات الثورة الرقمية الثانية ودورها في تحقيق التنمية المستدامة بالجامعات اليمنية، مصدر سابق، ص749.

(20) دليلة العوفي، الحرب السيبرانية في عصر الذكاء الاصطناعي ورهاناتها على الامن الدولي، مجلة الحكمة للدراسات الفلسفية، مجلد9، العدد 2، 2021، ص778-779.

(21) مناصري جوهر، تأثير الذكاء الاصطناعي على الاقتصاد العالمي، مجلة اقتصاد المال والاعمال، مجلد9، العدد1، 2024، ص83.

(22) أمينة شريف، خدمة الذكاء الاصطناعي: للمجتمع الخامس مجتمع ما بعد المعلومات، مجلة الدراسات القانونية والسياسية، مجلد9، العدد2، 2023، ص 113-114.

(23) علي عبيد اليساري، الذكاء الاصطناعي واثره في إدارة المعارك العسكرية الذكاء الاصطناعي واثره في إدارة المعارك العسكرية، رسالة ماجستير، جامعة الدفاع للدراسات العسكرية، كلية الحرب، العراق، 2023، ص 61.

(24) شريفة كلاع، الامن السيبراني واشكال التهديد تحديات عالمية، الفا للنشر والتوزيع، الجزائر، 2023، ص 91-92.

(25) دينا لملوم المخاطر والتحديات كيف تؤثر تكنولوجيا الذكاء الاصطناعي على الامن القومي للدول مقال منشور بتاريخ 2023/9/17 تم الاطلاع عليها بتاريخ 2026/1/12 متاح على الموقع المخاطر-والتحديات-كيف-تؤثر-تكنولوجيا https://shafcenter. org/

(26) عبير محمد عباس، الذكاء الاصطناعي ومبدأ السيادة في ظل القانون الدولي العام، مجلة اشور للعلوم القانونية والسياسية، مجلد2، العدد3، 2025، ص569.

(27) تعد الحرب الروسية-الأوكرانية، من أبرز النماذج التي شهدت توظيفاً متزايداً لتقنيات الذكاء الاصطناعي في العمليات العسكرية، ولاسيما في مجالات تحليل البيانات الاستخبارية، وتعزيز الوعي الميداني، ودعم أنظمة القيادة والسيطرة، فضلاً عن تطوير الأنظمة غير المأهولة مثل الطائرات المسيرة والأنظمة شبه المستقلة. متوفر على الرابط: Center for Strategic and International studies(CSIS),"Understanding the Military Al Ecosystem of Ukraine",2024. تاريخ الزيارة2026/4/22.

(28) يعد نزاع ناغورنو كاراباخ بين أذربيجان وأرمينيا، ولاسيما حرب عام2020، من أبرز النماذج التي شهدت توظيفاً للتقنيات المتقدمة المرتبطة بالذكاء الاصطناعي، حيث برز الاستخدام المكثف للطائرات المسيرة والذخائر الذكية في عمليات الاستطلاع والاستهداف، إلى جانب توظيف أنظمة تحليل الصور والبيانات في تحديد الأهداف وتعزيز دقة العمليات العسكرية، الأمر الذي أسهم في احداث تحول نوعي في طبيعة النزاعات المسلحة الحديثة. متوفر على الرابط: OECD.AI,"AI-enabled systems in the Nagorno-Karabakh Conflict"m2020,https://oecd.ai

(29) اعتمدت الولايات المتحدة الامريكية في عملياتها العسكرية ضد التنظيمات الإرهابية على توظيف تقنيات الذكاء الاصطناعي، ولاسيما ضمن مشروع (Mave) ، الذي يهدف إلى تحليل الصور والفيديوهات الملتقطة بواسطة الطائرات المسيرة والاقمار الاصطناعية، بما يسهم في تحديد الأهداف بدقة عالية وتسريع عمليات اتخاذ القرار العسكري، وقد مكنت هذه التقنيات من تحسين كفاءة العمليات الاستخبارية وتقليل الوقت اللازم لمعالجة البيانات، مع إبقاء الدور البشري حاضراً في الاشراف واتخاذ القرار النهائي، الامر الذي يعكس توجهاً متزايداً نحو ادماج الذكاء الاصطناعي في العمليات العسكرية الحدية. للمزيد أنظر: Project Maven متوفر على الرابط: https://www.defense.gov تاريخ الزيارة، 2026/4/22.

(30) احمد ماجد احمد، استخدام الذكاء الاصطناعي في الحرب العسكرية وأثره على الامن الدولي2021-2024، رسالة ماجستير، جامعة بغداد، كلية الآداب، 2025، ص867.

(31) عبد الله، خالد عتيق سعيد، والهنائي عبدالله بن سالم بن حمد، لبيانات الضخمة في مكتبات جامعة السلطان قابوس: واقعها وأثر دور المدراء كمُتَغيّر وسيط للاستفادة منها في تحسين الخدمات، المجلة العراقية لتكنولوجيا المعلومات، العدد1، 2018، ص23-24. متاح على الموقع الالكتروني: https://search. mandumah. com/Record/870210

(32) صادوق خضرة و نبيل خيرة، تطبيقات أنترنت الأشياء في المكتبات:دراسة نظرية، مجلة الرواق للدراسات الاجتماعية والإنسانية، 2022، ص 99-100

(33) ما المقصود بأنترنت الأشياء IOT، متوفر على الموقع الالكتروني: https://aws. amazon. com/ar/what-is/iot

(34) حسين علي، تطبيقات أنترنت الأشياء في المكتبات ومراكز المعلومات، مصدر سابق، ص183-184.

(35) عبد السلام احمد حسين وبشرى ناجي صالح، تقنيات الثورة الرقمية الثانية ودورها في تحقيق التنمية المستدامة بالجامعات اليمنية، مصدر سابق، ص 749.

(36) إبراهيم ادم، مشروع عن الحوسبة السحابية، 2015 متوفر على الموقع: https://www. kutub. info/library/book/19276

(37) معيد سلامة عبد المجيد و عمران محمد احمد و محمد اشرف و عبد العزيز الخطاط، دور تقنية الطابعة ثلاثية الابعاد في تصميم وتصنيع الأثاث، مجلة دراسات: العلوم الإنسانية والاجتماعية، الجامعة الأردنية، مجلد51، عدد5، 2024، ص402.

(38) احمد حسين الصغير، الجامعات المصرية وتحقيق متطلبات ووظائف المستقبل في ضوء الثورة الصناعية الرابعة، المجلة التربوية، العدد88، 2021، ص 15-16

(39) حسن عماد مكاوي، تكنولوجيا الاتصال الحديثة في عصر المعلومات، ط7، الدار المصرية اللبنانية، القاهرة، 2017، ص32.

(40) خالد وليد محمود، الفضاء السيبراني وتَحَوّلات القوة في العلاقات الدولية، المركز العربي للأبحاث ودراسة السياسات، بيروت، 2025، ص17.

(41) Everett C. Doiman , pure Strategy ; powerand principle in the space and information Age(London/Now York ;frank Cass,2005) p. 6

(42) خالد مخلف الجنفاوي، التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ظباط الشرطة الأكاديميين بالكويت، المجلة العربية للآداب والدراسات الإنسانية، مجلد5، العدد19، 2021، ص84.

(43) هشام محمد خليل، الجوانب الاجرامية للجوانب المعلوماتية، مجلس الامن والقانون، عدد2، 2012، ص.38

(44) نورة الصانع واخرون، العلاقة بين الوعي بالامن السيبراني والقيم الوطنية والأخلاقية والدينية لتلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف، مجلة البحث العلمي، مجلد11، العدد 4، 2020، ص 278-279-280.

(45) حسين ابن سلمان، الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية، مجلة جامعة الطائف للعلوم الإنسانية، مجلد6، العدد21، المملكة العربية السعودية، 2020، ص264.

(46) راشد محمد المري، الأمن السيبراني وحماية الأنظمة الإلكترونية: دراسة تحليلية تأصيلية، مجلة الدراسات القانونية والاقتصادية،

(47) علاء الدين فرحان، من الردعة النووي إلى الردع السيبراني، دراسة لمدى تحقيق مبدأ الردع في القضاء السيبراني، مجلة الفكر، مجلد16، العدد1، الجزائر، 2021، ص2246.

(48) سليم دحماني، أثر التهديدات "السيبرانية" على الأمن القومي: الولايات المُتّحِدَة الأمريكية-أنموذجاً، رسالة ماجستير، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، الجزائر، 2017، ص67.

(49) حيدر زايد وايسر علي الياسري، دور القوى الكبرى في توظيف مفاهيم حقوق الانسان ومنظمات المجتمع المدني في تهديد امن وسيادة الدول العربية، ص 190.

(50) سماح عبدالصبور، القوة السيبرانية في العلاقات الدولية: دراسة في الحروب السيبرانية بالتطبيق عام 2020، مركز الحضارة للدراسات والبحوث، مقال منشور على الرابط: https://share. google/BvhTcVAMa2s9bzGzj تاريخ الزيارة 2026/2/2.

(51) رشا سهيل محمد، التحولات المعاصرة للقوة وتأثيرها في مستقبل سيادة الدولة القومية بعد عام 2010: نماذج مختارة، مصدر سابق، ص 232.

(52) شيماء معروف فرحان، التحول في مفهوم القوة والصراع: دراسة في الحروب السيبرانية، مجلة قضايا سياسية، العدد57، جامعة النهرين، كلية العلوم السياسية، 2023، ص508-509. متوفر على الرابط: https://www. iasj. nPt/iasj/download/8237ed65b87729la تاريخ الزيارة 2026/2/8.

(53) علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، مجلة قضايا سياسية، العدد57، 2019، ص111.

(54) Andrew hanna,the lnvis lble U. S .

(55) كرار عباس متعب، الحرب السيبرانية : دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وايران، مصدر سابق، ص 206.

(56) محمد كاظم هادي، الواقع التشريعي للأمن السيبراني في العراق: التحديات والطموحات، مجلة العلوم الإنسانية والطبيعية، مجلد6، عدد8، 2025، ص568.

(57) 1. قانون العقوبات العراقي رقم(111) لسنة 1969، كجرائم (السب والقذف والتشهير)، (جرائم الاحتيال)، (جرائم افشاء الاسرار)، (جرائم التزوير واستعمال المحررات المزورة).

2. قانون أصول المحاكمات الجزائية رقم(23) لسنه 1971.

3. قانون التوقيع الالكتروني والمعاملات الالكترونية رقم(78) لسنة 2012.

4. نصوص دستورية، كحماية الخصوصية، حرية الاتصالات.

(58) تم طرح مشروع قانون جرائم المعلوماتية في العراق لأول مرة داخل مجلس النواب عام2011، بهدف تنظيم استخدام شبكة المعلومات ومكافحة الجرائم الالكترونية، مثل: الاختراق-الابتزاز الالكتروني. الا إنَ المشروع واجه اعتراضات واسعة بسبب اتساع بعض نصوصه القانونية وإمكانية استخدامها لتقييد حيرة التعبير، مما أدى إلى تعطيله وعدم إقراره بشكل نهائي.

ايضاً أعيد طرحه في البرلمان عامي 2019-2020، مع إدخال تعديلات عليه من قبل لجان مختصة، الا إنَ الجدل القانوني والحقوقي استمر حوله، خصوصاً فيما يتعلق بالعقوبات المشددة والعبارات الفضفاضة في النصوص القانونية.

وفي عام 2023، أعيدَ طرحه داخل البرلمان، حيث تم سحبه من قبل الحكومة لإجراء تعديلات إضافية تهدف إلى مواءمة مع التطور الرقمي ومعالجة الانتقادات المتعلقة بالحريات العامة.متوفر على الرابط: https://www.hrw.org/ar/report/2012/07/11/256341 تاريخ الزيارة 2026/4/22.

(59) أنظر: المادة(6) من مشروع قانون جرائم المعلوماتية العراقي.

(60) أنظر: المادة(22) من مشروع قانون جرائم المعلوماتية العراقي.

(61) رغد خضير صليبي، تعزيز الأمن السيبراني في العراق: التحديات والفرص، مجلة الدراسات الدولية، العدد99، 2024، ص519.

(62) سعود جاسم المرزوقي، التعاون الدولي في مكافحة الجريمة الالكترونية (اتفاقية بودابست ودور دولة قطر)، المجلة الدولية للعلوم الإنسانية والاجتماعية، مجلد69، العدد69، 2025، ص216.

(63) هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، مجلد24، العدد الأول، 2023

([64]) عادل حمامي ومحي الدين علي، الأمن السيبراني والتحديات المعاصرة، وحدة بحث المشكلات المعاصرة وقضايا التنمية، الجزائر، 2022، ص6.

([65]) تم اعتماد هذه الاتفاقية في 2001/11/23 في مدينة بودابست-المجر، وكانت تحت إشراف مجلس أوربا، ودخلت حيز النفاذ في 2004، وقد تضمنت 48مادة موزعة على فصول. متوفر على الرابط https://www.coe.int/en/web/portal/home تاريخ الزيارة2026/4/22.

([66]) مصطفى فضائلي وحسن سامي نور، الآليات القانونية الدولية لمكافحة الهجمات السيبرانية-دراسة تحليلية في إطار القانون الدولي العام والإنساني، مجلة الجامعة العراقية، مجلد74، العدد8، 2025،ص291.

المصادر

أولاً / الكتب العامة:

1. إيهاب خليفة، الحروب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، مركز المستقبل للأبحاث والدراسات المتقدمة، الإمارات العربية المتحدة، 2021.
2. جاسم محمد، الطريق إلى مجتمع المعرفة وقطاع المكتبات والمعلومات في الوطن العربي، دار الفكر للطباعة والنشر، دمشق، 2014.
3. جمال سند السويدي، وسائل التواصل الاجتماعي ودورها في التحولات المستقبلية من القبلية إلى الفيسبوك، (د. ن)، 2013.
4. حسن عماد مكاوي، تكنولوجيا الاتصال الحديثة في عصر المعلومات، ط7، الدار المصرية اللبنانية، القاهرة، 2017.
5. حسن محمد جواد الجبوري، منهجية البحث العلمي مدخل لبناء المهارات البحثية، دار صفاء للنشر والتوزيع، عمان، الأردن، (د. ت).
6. حيدر زايد وأيسر علي الياسري، دور القوى الكبرى في توظيف مفاهيم حقوق الإنسان ومنظمات المجتمع المدني في تهديد أمن وسيادة الدول العربية، (د. ن)، (د. ت).
7. خالد وليد محمود، الفضاء السيبراني وتحولات القوة في العلاقات الدولية، المركز العربي للأبحاث ودراسة السياسات، بيروت، 2025.
8. سوزان موزي، الثورة المعلوماتية والتكنولوجية وسياسات التنمية، دار المنهل اللبناني، بيروت، لبنان، 2009.
9. شريفة كلاع، الأمن السيبراني وأشكال التهديد تحديات عالمية، ألفا للنشر والتوزيع، الجزائر، 2023.
10. عادل عبد النور بن عبد النور، مدخل إلى عالم الذكاء الاصطناعي، مدينة الملك عبد العزيز للعلوم والتقنية، المملكة العربية السعودية، 2005.
11. علي زياد العلي وعلي حسين حميد، تكتيكات الحروب الحديثة: الأمن السيبراني والحروب المعززة والهجينة، دار العربي للنشر والتوزيع، القاهرة، 2023.
12. علي عبد الرحيم العبودي، (بدون عنوان ومكان تفاصيل النشر)، (د. ت).
13. قيس خلف رحيمة المحمداوي، الحروب الجديدة والتحول في مفاهيم القوة بعد الحرب الباردة، (د. ن)، (د. ت).

ثانياً / الكتب المترجمة:

1. لوتشيانو فلوريدي، الثورة الرابعة (كيف يعد الغلاف المعلوماتي بتشكيل الواقع الإنساني)، ترجمة: لؤي عبد المجيد السيد، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، 2017.

ثالثاً /الأطاريح والرسائل:

1. حامد محمود، مسار الثورة التكنولوجية وانعكاساتها في العلاقات الدولية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة بيروت العربية، 2025.
2. رشا سهيل محمد زيدان، التحولات المعاصرة للقوة وتأثيرها في مستقبل سيادة الدولة القومية بعد عام 2010: نماذج مختارة، أطروحة دكتوراه، كلية العلوم السياسية، جامعة النهرين، 2024.
3. محمد سعيد الكعبي، التكنولوجيا والتحول في إطار العملية السياسية، أطروحة دكتوراه، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر، 2024.
4. إيمان قديح، تحول مفهوم القوة في العلاقات الدولية بعد نهاية الحرب الباردة، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، الجزائر، 2018.
5. سليم دحماني، أثر التهديدات "السيبرانية" على الأمن القومي: الولايات المتحدة الأمريكية أنموذجاً، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، الجزائر، 2017.
6. علي عبيد اليساري، الذكاء الاصطناعي وأثره في إدارة المعارك العسكرية، رسالة ماجستير، كلية الحرب، جامعة الدفاع للدراسات العسكرية، العراق، 2023.

رابعاً / البحوث والمقالات:

1. أحمد حسين الصغير، الجامعات المصرية وتحقيق متطلبات ووظائف المستقبل في ضوء الثورة الصناعية الرابعة، المجلة التربوية، العدد (88)، 2021.
2. أمينة شريف، خدمة الذكاء الاصطناعي: للمجتمع الخامس مجتمع ما بعد المعلومات، مجلة الدراسات القانونية والسياسية، المجلد (9)، العدد (2)، 2023.
3. حسين ابن سلمان، الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية، مجلة جامعة الطائف للعلوم الإنسانية، المجلد (6)، العدد (21)، المملكة العربية السعودية، 2020.
4. حسين علي بوغزاله، تطبيقات إنترنت الأشياء IOT في المكتبات ومراكز المعلومات: الآفاق والتحديات، مجلة جامعة صبراتة العلمية، العدد (5)، 2019.
5. خالد مخلف الجنفاوي، التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت، المجلة العربية للآداب والدراسات الإنسانية، المجلد (5)، العدد (19)، 2021.
6. خالدية بلحاج وفرعون محمد، السيادة الرقمية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد (11)، العدد (1)، 2025.

7. دليلة العوفي، الحرب السيبرانية في عصر الذكاء الاصطناعي ورهاناتها على الأمن الدولي، مجلة الحكمة للدراسات الفلسفية، المجلد (9)، العدد (2)، 2021.
8. راشد محمد المري، الأمن السيبراني وحماية الأنظمة الإلكترونية: دراسة تحليلية تأصيلية، مجلة الدراسات القانونية والاقتصادية، (د. ت).
9. رحمن عبد الحسين ظاهر، الطائرات المسيرة ودورها في تطوير أجيال الحروب، المجلة السياسية الدولية، كلية العلوم السياسية في الجامعة المستنصرية، العدد (56)، 2023.
10. سمير عبد الرسول، الثورة الرقمية: نشأتها وأثرها على التعليم العالي والبحث العلمي، مجلة المستنصرية للعلوم الإنسانية، المجلد (2)، العدد (1)، 2024.
11. شريف درويش، الثورة الرقمية وتحولات القوة الناعمة، المجلة العربية لبحوث الإعلام والاتصال، العدد (46)، 2024.
12. شيماء معروف فرحان، التحول في مفهوم القوة والصراع: دراسة في الحروب السيبرانية، مجلة قضايا سياسية، كلية العلوم السياسية في جامعة النهرين، العدد (57)، 2023.
13. صادوق خضرة ونبيل خيرة، تطبيقات إنترنت الأشياء في المكتبات: دراسة نظرية، مجلة الرواق للدراسات الاجتماعية والإنسانية، 2022.
14. عبد السلام أحمد حسين وبشرى ناجي صالح، تقنيات الثورة الرقمية الثانية ودورها في تحقيق التنمية المستدامة بالجامعات اليمنية، مجلة جامعة المهرة للعلوم الإنسانية، العدد (1)، 2025.
15. عبد الله خالد عتيق سعيد، والهنائي عبد الله بن سالم بن حمد، البيانات الضخمة في مكتبات جامعة السلطان قابوس: واقعها وأثر دور المدراء كمتغير وسيط للاستفادة منها في تحسين الخدمات، المجلة العراقية لتكنولوجيا المعلومات، العدد (1)، 2018.
16. عبد الوهاب بريكة وزينب ابن تركي، أثر تكنولوجيا الإعلام والاتصال في رفع عجلة التنمية، مجلة الباحث، العدد (7)، 2010.
17. عزيز نوري وسميرة سلمان، التهديدات الهجينة بين إشكالية التعريف وأنماط المواجهة، المجلة الجزائرية للأمن والتنمية، المجلد (10)، العدد (1)، الجزائر، 2021.
18. علاء الدين فرحان، من الردع النووي إلى الردع السيبراني، دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني، مجلة الفكر، المجلد (16)، العدد (1)، الجزائر، 2021.
19. فايق حسن جاسم، أثر الانفتاح المعلوماتي في السيادة الوطنية، المجلة السياسية والدولية، العدد (18)، 2011.
20. كرار عباس متعب، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران، مجلة حمورابي للدراسات، العدد (40)، 2021.
21. مصطفى سحاري، السيادة الوطنية للدول في ظل ثورة المعلومات، مجلة المعيار، المجلد (10)، العدد (4)، 2019.

22. معيد سلامة عبد المجيد، عمران محمد أحمد، محمد أشرف، وعبد العزيز الخطاط، دور تقنية الطابعة ثلاثية الأبعاد في تصميم وتصنيع الأثاث، مجلة دراسات: العلوم الإنسانية والاجتماعية، الجامعة الأردنية، المجلد (51)، العدد (5)، 2024.
23. مناصري جوهر، تأثير الذكاء الاصطناعي على الاقتصاد العالمي، مجلة اقتصاد المال والأعمال، المجلد (9)، العدد (1)، 2024.
24. نورة الصانع وآخرون، العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لتلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف، مجلة البحث العلمي، المجلد (11)، العدد (4)، 2020.
25. هشام محمد خليل، الجوانب الإجرامية للثورة المعلوماتية، مجلة مجلس الأمن والقانون، العدد (2)، 2012.

ب- المقالات والتقارير (والمصادر الإلكترونية):

1. إبراهيم آدم، مشروع عن الحوسبة السحابية، 2015، تاريخ الاطلاع: 16 أبريل 2026، منشور على الموقع الإلكتروني: https://www.kutub.info/library/book/19276
2. التقرير الأمريكي، بشأن التدخل الروسي بالانتخابات، (بدون تاريخ النشر)، تاريخ الاطلاع: 16 أبريل 2026، منشور على الموقع الإلكتروني: https://share.google/GINuk0ql0yN4jBTCw
3. دينا لملوم، المخاطر والتحديات كيف تؤثر تكنولوجيا الذكاء الاصطناعي على الأمن القومي للدول، مقال منشور بتاريخ 2023/9/17، تاريخ الاطلاع: 16 أبريل 2026، متاح على الموقع الإلكتروني: https://shafcenter.org/
4. سماح عبد الصبور، القوة السيبرانية في العلاقات الدولية: دراسة في الحروب السيبرانية بالتطبيق عام 2020، مركز الحضارة للدراسات والبحوث، 2020، تاريخ الاطلاع: 16 أبريل 2026، مقال منشور على الموقع الإلكتروني: https://share.google/BvhTcVAMa2s9bzGz j
5. شركة أمازون لخدمات الويب (AWS)، ما المقصود بإنترنت الأشياء IoT، (بدون تاريخ النشر)، تاريخ الاطلاع: 16 أبريل 2026، متوفر على الموقع الإلكتروني: https://aws.amazon.com/ar/what-is/iot
6. فرانك غاردنر، البرنامج النووي الإيراني: لماذا لا تزال منشآته معرضة للهجوم، مقال منشور بتاريخ 2021/1/19، قناة BBC العربية، تاريخ الاطلاع: 16 أبريل 2026، متوفر على الموقع الإلكتروني: https://www.bbc.com/arabic/middleeast-55717913

خامساً /المصادر الأجنبية:

1. Andrew Hanna, The Invisible U.S., (N.d).
2. Everett C. Dolman, Pure Strategy; Power and Principle in the Space and .

Sources

First / General Books:

1. Ehab Khalifa, Cyber Warfare: Preparing to Lead Military Battles in the Fifth Field, Future Center for Advanced Research and Studies, United Arab Emirates, 2021.

2. Jassim Mohammed, The Road to a Knowledge Society and the Library and Information Sector in the Arab World, Dar Al-Fikr for Printing and Publishing, Damascus, 2014.

3. Jamal Sand Al-Suwaidi, Social Media and Its Role in Future Transformations: From Tribalism to Facebook, (n.p.), 2013.

4. Hassan Emad Makawi, Modern Communication Technology in the Information Age, 7th ed., Egyptian-Lebanese House, Cairo, 2017.

5. Hassan Mohammed Jawad Al-Jubouri, Scientific Research Methodology: An Introduction to Building Research Skills, Safaa Publishing and Distribution House, Amman, Jordan, (n.d.).

6. Haider Zayed and Ayser Ali Al-Yassiri, The Role of Major Powers in Employing Human Rights Concepts and Civil Society Organizations to Threaten the Security and Sovereignty of Arab States, (n.p.), (n.d.).

7. Khaled Walid Mahmoud, Cyberspace and Power Shifts in International Relations, Arab Center for Research and Policy Studies, Beirut, 2025.

8. Suzanne Mouzi, The Information and Technological Revolution and Development Policies, Dar Al-Manhal Al-Lubnani, Beirut, Lebanon, 2009.

9. Sharifa Kelaa, Cybersecurity and Forms of Threat: Global Challenges, Alpha Publishing and Distribution, Algeria, 2023.

10. Adel Abdel Nour Ben Abdel Nour, An Introduction to the World of Artificial Intelligence, King Abdulaziz City for Science and Technology, Saudi Arabia, 2005.

11. Ali Ziad Al-Ali and Ali Hussein Hamid, Modern Warfare Tactics: Cybersecurity and Enhanced and Hybrid Warfare, Dar Al-Arabi Publishing and Distribution, Cairo, 2023.

12. Ali Abdel Rahim Al-Aboudi, (no title or place of publication details), (n.d.).

13. Qais Khalaf Rahima Al-Muhammadawi, The New Wars and the Transformation in Concepts of Power after the Cold War, (n.p.), (n.d.).

Second / Translated Books:

1. Luciano Floridi, The Fourth Revolution (How the Information Sphere Shapes Human Reality), translated by Louay Abdel-Majeed El-Sayed, World of Knowledge Series, National Council for Culture, Arts and Letters, Kuwait, 2017.

Third /Theses and Dissertations:

1. Hamed Mahmoud, The Course of the Technological Revolution and its Repercussions in International Relations, PhD dissertation, Faculty of Law and Political Science, Beirut Arab University, 2025.
2. Rasha Suhail Mohammed Zeidan, Contemporary Transformations of Power and their Impact on the Future of Nation-State Sovereignty after 2010: Selected Models, PhD dissertation, Faculty of Political Science, Al-Nahrain University, 2024.
3. Mohammed Saeed Al-Kaabi, Technology and Transformation within the Framework of the Political Process, PhD dissertation, Faculty of Political Science and International Relations, University of Algiers, 2024.
4. Iman Qaddih, The Transformation of the Concept of Power in International Relations after the End of the Cold War, Master's thesis, Faculty of Law and Political Science, Mohamed Boudiaf University, Algeria. 2018.
5. Salim Dahmani, The Impact of Cyber Threats on National Security: The United States of America as a Model, Master's Thesis, Faculty of Law and Political Science, Mohamed Boudiaf University, Algeria, 2017.
6. Ali Obeid Al-Yassari, Artificial Intelligence and its Impact on Military Battle Management, Master's Thesis, War College, National Defense University for Military Studies, Iraq, 2023.

Fourth / Research and Articles:

1. Ahmed Hussein Al-Saghir, Egyptian Universities and Meeting the Requirements and Functions of the Future in Light of the Fourth Industrial Revolution, Educational Journal, Issue (88), 2021.
2. Amina Sharif, The Service of Artificial Intelligence: For the Fifth Society, the Post-Information Society, Journal of Legal and Political Studies, Volume (9), Issue (2), 2023.

3. Hussein Ibn Salman, Cybersecurity from the Perspective of the Objectives of Islamic Law: A Foundational Study, Taif University Journal of Humanities, Volume (6), Issue (21), Kingdom of Saudi Arabia, 2020.

4. Hussein Ali Bughazala, Internet of Things (IoT) Applications in Libraries and Centers Information: Prospects and Challenges, Sabratha University Scientific Journal, Issue (5), 2019.

5. Khaled Mukhlif Al-Janfawi, Digital Transformation of National Institutions and Cybersecurity Challenges from the Perspective of Academic Police Officers in Kuwait, Arab Journal of Arts and Humanities, Volume (5), Issue (19), 2021.

6. Khalida Belhaj and Faroun Muhammad, Digital Sovereignty, Journal of Research in Law and Political Science, Volume (11), Issue (1), 2025.

7. Dalila Al-Awfi, Cyber Warfare in the Age of Artificial Intelligence and its Stakes for International Security, Al-Hikma Journal of Philosophical Studies, Volume (9), Issue (2), 2021.

8. Rashid Muhammad Al-Marri, Cybersecurity and the Protection of Electronic Systems: An Analytical and Fundamental Study, Journal of Legal and Economic Studies, (n.d.).

9. Rahman Abdul Hussein Thahir, Drones and Their Role in Developing Generations of Warfare, International Political Journal, College of Political Science, Al-Mustansiriya University, Issue (56), 2023.

10. Samir Abdul Rasoul, The Digital Revolution: Its Origins and Impact on Higher Education and Scientific Research, Al-Mustansiriya Journal of Humanities, Volume (2), Issue (1), 2024.

11. Sharif Darwish, The Digital Revolution and the Transformations of Soft Power, Arab Journal of Media and Communication Research, Issue (46), 2024.

12. Shaimaa Marouf Farhan, The Transformation in the Concept of Power and Conflict: A Study in Cyber Warfare, Political Issues Journal, College of Political Science, Al-Nahrain University, Issue (57), 2023.

13. Sadouk Khadra and Nabil Khayra, Internet of Things Applications in Libraries: A Theoretical Study, Al-Riwaq Journal for Social and Human Studies, 2022.

14. Abdul Salam Ahmed Hussein and Bushra Naji Saleh, Technologies of the Second Digital Revolution and Their Role in Achieving Sustainable Development in Yemeni Universities, Journal Al-Mahra University for Humanities, Issue (1), 2025.
15. Abdullah Khalid Atiq Saeed and Al-Hinai Abdullah bin Salem bin Hamad, Big Data in Sultan Qaboos University Libraries: Its Reality and the Impact of Managers' Role as an Intermediary Variable for Utilizing It to Improve Services, Iraqi Journal of Information Technology, Issue (1), 2018.
16. Abdul Wahab Brika and Zainab Ibn Turki, The Impact of Information and Communication Technology on Accelerating Development, Al-Bahith Journal, Issue (7), 2010.
17. Aziz Nouri and Samira Salman, Hybrid Threats: Between the Problem of Definition and Patterns of Confrontation, Algerian Journal of Security and Development, Volume (10), Issue (1), Algeria, 2021.
18. Alaa El-Din Farhan, From Nuclear Deterrence to Cyber Deterrence: A Study of the Extent of Achieving the Principle of Deterrence in Cyberspace, Al-Fikr Journal, Volume (16), Issue (1), Algeria, 2021.
19. Fayeq Hassan Jassim, The Impact of Information Openness on National Sovereignty, Political and International Journal Issue (18), 2011.
20. Karrar Abbas Mutab, Cyber Warfare: A Study in Strategy Cyberattacks between the United States and Iran, Hammurabi Journal of Studies, Issue (40), 2021.
21. Mustafa Sahari, National Sovereignty of States in the Age of the Information Revolution, Al-Mi'yar Journal, Volume (10), Issue (4), 2019.
22. Mu'eed Salama Abdul Majeed, Imran Muhammad Ahmad, Muhammad Ashraf, and Abdul Aziz Al-Khatat, The Role of 3D Printing Technology in Furniture Design and Manufacturing, Journal of Studies: Humanities and Social Sciences, University of Jordan, Volume (51), Issue (5), 2024.
23. Manasri Jawhar, The Impact of Artificial Intelligence on the Global Economy, Journal of Economics, Finance and Business, Volume (9), Issue (1), 2024.
24. Noura Al-Sanea et al., The Relationship between Cybersecurity Awareness and National, Ethical, and Religious Values of Primary and Intermediate School Students in Taif, Journal of Scientific Research, Volume (11), Issue (4), 2020.

25. Hisham Muhammad Khalil, The Criminal Aspects of the Information Revolution, Journal of the Security and Law Council Issue (2), 2012.

B- Articles and Reports (and Electronic Sources):

1. Ibrahim Adam, A Project on Cloud Computing, 2015, accessed April 16, 2026, published on the website: https://www.kutub.info/library/book/19276

2. The American Report on Russian Interference in Elections (no publication date), accessed April 16, 2026, published on the website: https://share.google/GINuk0ql0yN4jBTCw

3. Dina Lamloum, Risks and Challenges: How Artificial Intelligence Technology Affects National Security, article published on September 17, 2023, accessed April 16, 2026, available on the website: https://shafcenter.org/

4. Samah Abdel Sabour, Cyber Power in International Relations: A Study in Cyber Warfare with Applications in 2020, Center for Civilization Studies and Research 2020, accessed April 16, 2026, article published on the website: https://share.google/BvhTcVAMa2s9bzGz

5. Amazon Web Services (AWS), What is the Internet of Things (IoT), (no publication date), accessed April 16, 2026, available at: https://aws.amazon.com/ar/what-is/iot

6. Frank Gardner, Iran's nuclear program: Why its facilities remain vulnerable to attack, article published on January 19, 2021, BBC Arabic, accessed April 16, 2026, available at: https://www.bbc.com/arabic/middleeast-55717913

Fifth / Foreign Sources:

1 Andrew Hanna, The Invisible U.S., (N.d).

2 Everett C. Dolman, Pure Strategy; Power and Principle in the Space and .