E-ISSN : 2790-2404
P- ISSN 2070-9250
Qadaya siyasiyyat

Ministry of Higher Education
& Scientific Research
Al-Nahrain University
College of Political Science

وزارة التعليم العالي والبحث العلمي
جامعة النهرين
كلية العلوم السياسية

قضايا سياسية
Political Issues

مجلة فصلية محكمة

العدد ٨٥
Issue 85

نيسان - ايار - حزيران / ٢٠٢٦
Abr. - May. - June. / 2026

جامعة النهرين
كلية العلوم السياسية

E-ISSN 2790-2404
P- ISSN 2070-9250
DOI prefix: 10.58298

قضايا سياسية
Political Issues

مجلة فصلية محكمة تعنى بنشر الأبحاث والدراسات السياسية العراقية والعربية والدولية
http://pissue.iq

مجلة قضايا سياسية

pissue.iq

قواعد النشر

- لغة المجلة هي اللغة العربية والانكليزية على أن يراعى الوضوح وسلامة النص.
- ترحب المجلة بنشر البحوث والدراسات السياسية النظرية والتطبيقية ولا سيما التي تجعل من قضايا المنطقة والعالم محط اهتمامها، ماضياً وحاضراً ومستقبلاً، وعلى وفق الآتي:

1. أن لا يزيد عدد صفحات البحث أو الدراسة عن (15) صفحة مطبوعة بحجم خط (14) والتباعد (1,15) ونوع الخط Simplified Arabic تقدم عبر المنصة الاليكترونية للمجلة على الرابط : https://pissue.iq/index.php/pissue/about/submissions
2. أن تتصف البحوث والدراسات بالموضوعية والدقة العلمية.
3. أن تعتمد الترقيم العشري للعناوين الأساسية والفرعية او التنصيف المعياري العام.
4. يرفق مع كل بحث او دراسة ملخصين (احدهما باللغة العربية والآخر باللغة الانكليزية/ يتضمن اهداف البحث ، المنهج والمعالجة ، ابرز النتائج واهم الاستنتاجات والمقترحات) مع ضرورة مراعاة ان الملخص مختلف اختلافا جذريا عن المقدمة وليس تكرارا لها .
5. تخضع جميع البحوث المقبولة للنشر الى نظام الاستلال الالكتروني في كلية العلوم السياسية –جامعة النهرين.
6. يرفق مع كل بحث ودراسة سيرة ذاتية مختصرة للباحث وتعهد .

- تقوم المجلة بإخطار الباحثين بإجازة بحوثهم أو دراساتهم من عدمها بعد عرضها على محكمين تختارهم على نحو سري من بين أصحاب الاختصاص.

مجلة قضايا سياسية

pissue.iq

- يجوز للمجلة أن تطلب إجراء تعديلات شكلية أو شاملة على البحث أو الدراسة قبل إجازتها للنشر بما يتماشى مع أهدافها.
- البحوث المنشورة تعبر عن آراء أصحابها ، ولاتعبر عن راي المجلة .
- ترحب المجلة بالمناقشات الموضوعية لما ينشر فيها أو في غيرها من الدوريات وبأية ردود فكرية أو تصويب، وكذلك ترحب بنشر التقارير عن المؤتمرات والندوات ذات العلاقة ومراجعات الكتب وملخصات الرسائل الجامعية التي تتم إجازتها على أن تكون من إعداد أصحابها.

توجه جميع المراسلات إلى هيأة التحرير على العنوان الآتي
مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين-بغداد – الجادرية.
E.mail: pirj@nahrainuniv.edu.iq

الموقع الاليكتروني
https://pissue.iq/index.php/pissue

E-ISSN 2790-2404
P- ISSN 2070-9250
DOI prefix: 10.58298

جدول المحتويات

التهديدات السيبرانية للبنية التحتية الحيوية في الشرق الأوسط وانعكاساتها على الأمن الأوروبي[▽]

Cyber Threats to Critical Infrastructure in the Middle East and Their Implications for European Security

م.د. مصطفى حسن عواد* Dr. Mustafa Hassan Awad

الملخص

يتناول هذا البحث تحليل التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية في منطقة الشرق الأوسط، وبيان انعكاساتها على الأمن الأوروبي في ظل التحولات الرقمية المتسارعة في النظام الدولي. وينطلق البحث من فرضية مفادها أن تصاعد هذه التهديدات لا يقتصر تأثيره على النطاق الإقليمي، بل يمتد ليشكل تحديًا مباشرًا للأمن الاقتصادي والاستراتيجي للاتحاد الأوروبي، لاسيما في مجالات الطاقة والتجارة وسلاسل الإمداد. ولتحقيق أهداف الدراسة، تم اعتماد المنهج الوصفي التحليلي ومنهج تحليل السياسات العامة، من خلال دراسة طبيعة التهديدات السيبرانية في المنطقة وتحليل استجابات الاتحاد الأوروبي لها. وتوصل البحث إلى أن الهجمات السيبرانية أصبحت أداة رئيسية في الصراعات الجيوسياسية المعاصرة، وأن مواجهتها تتطلب تطوير استراتيجيات وطنية وإقليمية متكاملة، قائمة على تعزيز القدرات المؤسسية والتشريعية، فضلاً عن توسيع نطاق التعاون الدولي في مجال الأمن السيبراني.

الكلمات المفتاحية: الأمن السيبراني، البنية التحتية الحيوية، الشرق الأوسط، الاتحاد الأوروبي، الأمن الدولي.

Abstract

This study analyzes cyber threats targeting critical infrastructure in the Middle East and examines their implications for European security within the context of rapid digital transformation in the international system. The study is based on the assumption that the escalation of these threats extends beyond the regional level to pose significant challenges to the economic and strategic security of the European Union, particularly in areas such as energy, trade, and global supply chains. To achieve its objectives, the research adopts a descriptive-analytical approach combined with public policy analysis, focusing on the nature of cyber threats in the region and the European Union's response strategies. The findings indicate that cyberattacks have become a key instrument in contemporary geopolitical conflicts, and that addressing these threats requires the development of comprehensive national and regional cybersecurity strategies, strengthened institutional and legal frameworks, and enhanced international cooperation.

Keywords: Cybersecurity, Critical Infrastructure, Middle East, European Union, International Security.

▽ تاريخ التقديم : 2026/3/9 تاريخ القبول: 4 /5 /2026 تاريخ النشر: 30/6/ 2026

*كلية القانون / جامعة واسط mustafahd212@uowasit.edu.iq

المقدمة

يشهد النظام الدولي المعاصر تحولات عميقة بفعل الثورة الرقمية والتطور المتسارع في تكنولوجيا المعلومات والاتصالات، إذ أصبح الفضاء السيبراني أحد المجالات الاستراتيجية التي تؤثر بصورة مباشرة في الأمن الوطني والاستقرار الاقتصادي والسياسي للدول. وقد أدى الاعتماد المتزايد على الأنظمة الرقمية في إدارة القطاعات الحيوية، لاسيما الطاقة والاتصالات والنقل والأنظمة المالية، إلى جعل البنية التحتية الحيوية أكثر عرضة لمجموعة متزايدة من التهديدات السيبرانية التي قد تؤدي إلى تعطيل الخدمات الأساسية وإحداث اضطرابات واسعة النطاق. وتبرز منطقة الشرق الأوسط بوصفها إحدى أكثر المناطق حساسية في هذا السياق، نظرًا لما تتمتع به من أهمية جيوسياسية واقتصادية، فضلاً عن كونها مركزًا رئيسيًا لإنتاج ونقل الطاقة العالمية، الأمر الذي يجعل بنيتها التحتية هدفًا متكررًا للهجمات السيبرانية المرتبطة بالصراعات الإقليمية والدولية. وفي المقابل، يرتبط أمن هذه المنطقة ارتباطًا وثيقًا بالأمن الأوروبي، إذ يعتمد الاتحاد الأوروبي بدرجة كبيرة على استقرار الشرق الأوسط في مجالات الطاقة والتجارة وسلاسل الإمداد، مما يجعل أي تهديد يستهدف البنية التحتية الحيوية في المنطقة ذا انعكاسات مباشرة أو غير مباشرة على الأمن الأوروبي. وانطلاقًا من ذلك، يسعى هذا البحث إلى تحليل طبيعة التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية في الشرق الأوسط، وبيان تداعياتها، فضلاً عن دراسة السياسات التي يعتمدها الاتحاد الأوروبي في مواجهة هذه التهديدات ضمن إطار الأمن الدولي المعاصر.

أهمية البحث:

تكمن أهمية هذا البحث في معالجته لأحد أبرز التحديات الأمنية المعاصرة المتمثلة في التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية، إذ لم تعد هذه التهديدات تقتصر على البعد التقني، بل أصبحت تمثل أداة استراتيجية تؤثر في توازنات القوة والعلاقات الدولية. وتزداد أهمية الموضوع في سياق منطقة الشرق الأوسط التي تعد من أكثر المناطق حساسية من الناحية الجيوسياسية والاقتصادية، لاسيما في ظل تصاعد الهجمات السيبرانية التي تستهدف قطاعات حيوية مثل الطاقة والنقل والاتصالات. كما تنبع أهمية البحث من إبراز الترابط بين أمن الشرق الأوسط والأمن الأوروبي، إذ يعتمد الاتحاد الأوروبي بدرجة كبيرة على استقرار المنطقة في مجالات الطاقة والتجارة وسلاسل الإمداد، الأمر الذي يجعل أي خلل في البنية التحتية الحيوية ذا انعكاسات مباشرة على الأمن الأوروبي. ويسهم هذا البحث في سد فجوة علمية تتعلق بتحليل العلاقة بين التهديدات السيبرانية الإقليمية واستجابات الاتحاد الأوروبي لها، فضلاً عن تقديم إطار تحليلي يمكن أن يفيد صناع القرار في تطوير سياسات أكثر فاعلية في مجال الأمن السيبراني، وتعزيز آليات التعاون الدولي لمواجهة التهديدات الرقمية العابرة للحدود.

اشكالية البحث:

تتمثل مشكلة البحث في تصاعد التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية في منطقة الشرق الأوسط، وما يترتب على ذلك من تداعيات أمنية واقتصادية وسياسية لا تقتصر على النطاق الإقليمي، بل تمتد لتشمل الأمن الأوروبي، في ظل الترابط المتزايد بين النظم الاقتصادية والبنى التحتية العالمية.

ويأتي التساؤل الرئيس من: ما طبيعة التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية في الشرق الأوسط، وما انعكاساتها الاستراتيجية على الأمن الأوروبي؟

ويتفرع عن هذا التساؤل مجموعة من التساؤلات الفرعية، وهي:

أ- ما المقصود بالبنية التحتية الحيوية في الفضاء السيبراني؟

ب- ما طبيعة التهديدات السيبرانية التي تواجه البنية التحتية في الشرق الأوسط؟

ج- ما التحديات السياسية والمؤسسية التي تواجه دول المنطقة في حماية بنيتها التحتية الرقمية؟

د- كيف يتعامل الاتحاد الأوروبي مع التهديدات السيبرانية القادمة من مناطق عدم الاستقرار؟

هـ- ما انعكاسات هذه التهديدات على الأمن الأوروبي والاستقرار الدولي؟

و- ما مدى فاعلية سياسات الاتحاد الأوروبي في احتواء التهديدات السيبرانية ذات المصدر الإقليمي؟

فرضية البحث: ينطلق البحث من الفرضية الآتية:

1. كلما تصاعدت التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية في الشرق الأوسط، ازدادت أهمية تطوير استراتيجيات أوروبية متقدمة لحماية الأمن السيبراني وتعزيز التعاون الدولي في مجال حماية البنية التحتية الرقمية.
2. كما يفترض البحث أن ضعف القدرات المؤسسية والتشريعية في بعض دول المنطقة قد يزيد من هشاشة البنية التحتية الرقمية، الأمر الذي يرفع من مستوى المخاطر السيبرانية ذات التأثير العابر للحدود.

الإطار المنهجي : يعتمد البحث على مجموعة من المناهج العلمية التي تساعد على تحليل موضوع الدراسة، ومن أبرزها:

1 .المنهج الوصفي التحليلي: يستخدم هذا المنهج في دراسة طبيعة التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية في الشرق الأوسط وتحليل أبعادها السياسية والأمنية.

2 .منهج تحليل السياسات العامة : يستخدم هذا المنهج في تحليل السياسات والاستراتيجيات التي يعتمدها الاتحاد الأوروبي في مجال الأمن السيبراني وحماية البنية التحتية الرقمية.

3 .المنهج المقارن: يساعد هذا المنهج في مقارنة السياسات السيبرانية الأوروبية مع التحديات الأمنية في منطقة الشرق الأوسط، وتحليل طبيعة التفاعل بينهما.

اولاً: التهديدات السيبرانية للبنية التحتية الحيوية في الشرق الأوسط

أدت التحولات الرقمية المتسارعة التي شهدها العالم خلال العقود الأخيرة إلى إعادة تشكيل طبيعة الأمن الوطني والدولي. فمع ازدياد اعتماد الدول على الأنظمة الرقمية في إدارة القطاعات الحيوية، أصبح الفضاء السيبراني أحد المجالات الاستراتيجية التي تؤثر بصورة مباشرة في استقرار الدول واقتصاداتها. (Nye, 2010) وقد أدى هذا الاعتماد المتزايد على الشبكات الرقمية وأنظمة التحكم الصناعية إلى جعل البنية التحتية الحيوية عرضة لمجموعة متزايدة من التهديدات السيبرانية التي يمكن أن تؤدي إلى تعطيل الخدمات الأساسية أو إحداث اضطرابات اقتصادية وسياسية واسعة النطاق. (.Singer & Friedman, 2014)

وتشير العديد من الدراسات في مجال الأمن السيبراني إلى أن الهجمات الرقمية لم تعد تقتصر على سرقة البيانات أو التجسس المعلوماتي، بل أصبحت تستهدف بشكل متزايد الأنظمة الحيوية التي يعتمد عليها الاقتصاد والمجتمع في إدارة الخدمات الأساسية. وقد أدى ذلك إلى بروز مفهوم أمن البنية التحتية الحيوية بوصفه أحد أهم مجالات الأمن القومي في العصر الرقمي. ((Cavelty, 2008

وفي هذا السياق، تُعد منطقة الشرق الأوسط من المناطق التي تواجه تحديات متزايدة في مجال الأمن السيبراني، نظراً لما تتمتع به من أهمية جيوسياسية واقتصادية كبيرة في النظام الدولي. فالمنطقة تضم عدداً من أهم منشآت الطاقة العالمية، إضافة إلى ممرات تجارية وبحرية استراتيجية، الأمر الذي يجعلها هدفاً رئيسياً للهجمات السيبرانية التي قد تستخدم كأداة في الصراعات السياسية أو التنافس الجيوسياسي بين الدول. وقد أدى ذلك إلى تصاعد الاهتمام بدراسة طبيعة التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية في المنطقة وتحليل التحديات السياسية والمؤسسية التي تواجه الدول في حماية هذه الأنظمة الحيوية. الدول Kello, (2017)

1. طبيعة التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية

تشير الأدبيات الحديثة في مجال الأمن السيبراني إلى أن البنية التحتية الحيوية أصبحت أحد الأهداف الرئيسية للهجمات الرقمية في النظام الدولي المعاصر. ويرجع ذلك إلى الدور الحيوي الذي تؤديه هذه البنية في تشغيل الاقتصاد الوطني وتوفير الخدمات الأساسية للمجتمع. وقد أدى الاعتماد المتزايد على الأنظمة الرقمية في إدارة هذه القطاعات إلى ظهور مجموعة واسعة من التهديدات السيبرانية التي تستهدف أنظمة التحكم الصناعية والشبكات الرقمية المرتبطة بها. (Lewis, 2018)

أ: مفهوم البنية التحتية الحيوية في الدراسات الأمنية

تشير البنية التحتية الحيوية إلى مجموعة الأنظمة والمنشآت التي يعتمد عليها المجتمع في تقديم الخدمات الأساسية والحفاظ على استقرار الاقتصاد الوطني. وتشمل هذه البنية عدداً من القطاعات الاستراتيجية، من أبرزها: (Singer & Friedman, 2014)

1) قطاع الطاقة مثل النفط والغاز والكهرباء.
2) شبكات الاتصالات والإنترنت.
3) أنظمة النقل والموانئ والمطارات.
4) الأنظمة المالية والمصرفية.
5) شبكات المياه والخدمات العامة.

وتشير الدراسات الأمنية إلى أن أي خلل في عمل هذه القطاعات قد يؤدي إلى اضطرابات واسعة النطاق في الاقتصاد والمجتمع. ولذلك أصبحت حماية البنية التحتية الحيوية أحد أهم التحديات التي تواجه الحكومات في العصر الرقمي. (Cavelty, 2008)

ب: تطور التهديدات السيبرانية في العلاقات الدولية

مع تطور القدرات الرقمية للدول، أصبحت الهجمات السيبرانية جزءاً من أدوات القوة في العلاقات الدولية. وتشير بعض الدراسات إلى أن الدول تستخدم الهجمات الرقمية كوسيلة لتحقيق أهداف سياسية أو استراتيجية دون اللجوء إلى القوة العسكرية التقليدية. وقد أدى ذلك إلى ظهور مفهوم القوة السيبرانية الذي يشير إلى قدرة الدول على استخدام الفضاء الرقمي لتحقيق أهدافها السياسية والاستراتيجية. (Nye, 2010)

وفي هذا الإطار، أصبحت الهجمات السيبرانية تستهدف بشكل متزايد البنية التحتية الحيوية للدول، نظراً لما يمكن أن تسببه من تأثيرات اقتصادية وسياسية كبيرة. (Buchanan, 2020)

ج: أنواع الهجمات السيبرانية التي تستهدف البنية التحتية

تتنوع الهجمات السيبرانية التي تستهدف البنية التحتية الحيوية، وتشمل عدداً من الأساليب التي تستخدمها الدول أو الجماعات المنظمة لتحقيق أهداف سياسية أو اقتصادية. ومن أبرز هذه التهديدات:

1) .التجسس السيبراني(Cyber Espionage) يشير التجسس السيبراني إلى استخدام الوسائل الرقمية لاختراق أنظمة المعلومات الحكومية أو الصناعية بهدف الحصول على معلومات حساسة. وغالباً ما تستهدف هذه الهجمات المؤسسات الحكومية أو الشركات التي تدير القطاعات الحيوية مثل الطاقة والاتصالات. (Valeriano & Maness, 2015)

2). التخريب السيبراني(Cyber Sabotage) يهدف التخريب السيبراني إلى تعطيل الأنظمة الرقمية أو إلحاق أضرار بالبنية التحتية الحيوية. وقد تشمل هذه الهجمات استهداف أنظمة التحكم الصناعية التي تدير منشآت الطاقة أو شبكات النقل. (Kello, 2017)

3) .هجمات الفدية(Ransomware)

تُعد هجمات الفدية من أكثر الهجمات السيبرانية انتشاراً في السنوات الأخيرة، حيث يقوم المهاجمون بتشفير الأنظمة الرقمية للمؤسسات وطلب مبالغ مالية مقابل إعادة تشغيلها. (World Economic Forum, 2024).

4) .الهجمات على أنظمة التحكم الصناعية

تعتمد العديد من المنشآت الحيوية مثل محطات الطاقة والمصانع الكبرى على أنظمة التحكم الصناعية، التي يمكن أن تكون عرضة للهجمات السيبرانية التي تستهدف تعطيل عمليات التشغيل. (Singer & Friedman, 2014)

ويرى الباحث أن تنوع أنماط الهجمات السيبرانية يعكس تحولًا نوعيًا في طبيعة التهديدات الأمنية، إذ لم تعد هذه الهجمات تقتصر على الأهداف التقليدية المرتبطة بجمع المعلومات، بل أصبحت تستهدف بشكل مباشر تعطيل البنية التحتية الحيوية وإحداث تأثيرات استراتيجية في استقرار الدول، الأمر الذي يجعلها أداة فعالة في إدارة الصراعات المعاصرة.

د: أمثلة للهجمات السيبرانية في الشرق الأوسط: شهدت منطقة الشرق الأوسط عدداً من الهجمات السيبرانية التي استهدفت البنية التحتية الحيوية، ومن أبرز هذه الحوادث:

1) الهجوم السيبراني على شركة Saudi Aramco عام 2012 الذي أدى إلى تعطيل آلاف الحواسيب في الشركة. .(Buchanan, 2020)
2) الهجمات السيبرانية المتبادلة بين إيران وإسرائيل التي استهدفت منشآت صناعية ومؤسسات حكومية. (Valeriano & Maness, 2015)
3) الهجمات التي استهدفت شركات النفط والموانئ في المنطقة.

وتشير هذه الحوادث إلى أن الهجمات السيبرانية أصبحت أداة تستخدم في الصراعات السياسية والجيوسياسية. (Kello, 2017)

2. التحديات السياسية والمؤسسية في حماية البنية التحتية الرقمية

على الرغم من تزايد إدراك الدول لأهمية الأمن السيبراني في حماية البنية التحتية الحيوية، فإن تطوير منظومات فعالة لحماية الأنظمة الرقمية ما زال يواجه مجموعة من التحديات السياسية والمؤسسية، لاسيما في

المناطق التي تعاني من عدم الاستقرار السياسي أو ضعف القدرات المؤسسية. وتشير العديد من الدراسات إلى أن الأمن السيبراني لا يقتصر على الجوانب التقنية فحسب، بل يرتبط أيضاً بالسياسات العامة والهياكل المؤسسية وقدرة الدول على تطوير استراتيجيات وطنية متكاملة لحماية الفضاء الرقمي.(Lewis, 2018)

ويمكن القول إن التحديات المؤسسية التي تواجه دول الشرق الأوسط لا ترتبط فقط بنقص الموارد، بل تعكس أيضاً إشكالية أعمق تتعلق بضعف الحوكمة الرقمية وغياب التنسيق بين الجهات المعنية، الأمر الذي يؤدي إلى وجود فجوات هيكلية في منظومات الأمن السيبراني.

وفي هذا السياق، تواجه العديد من دول الشرق الأوسط مجموعة من التحديات التي تعيق تطوير سياسات فعالة لحماية البنية التحتية الرقمية، ويمكن تحليل هذه التحديات من خلال مجموعة من الأبعاد السياسية والمؤسسية.

أ: ضعف الأطر التشريعية والتنظيمية

تُعد التشريعات القانونية أحد العناصر الأساسية في بناء منظومة فعالة للأمن السيبراني، إذ تتيح القوانين والتنظيمات المناسبة للدول القدرة على تنظيم الفضاء الرقمي ومكافحة الجرائم السيبرانية وحماية البنية التحتية الحيوية. غير أن العديد من دول الشرق الأوسط ما زالت تعاني من نقص في التشريعات المتخصصة في مجال الأمن السيبراني.

وتتمثل أبرز مظاهر هذا الضعف في: (European Commission, 2020)

1) غياب قوانين متخصصة لحماية البنية التحتية الرقمية.
2) ضعف التشريعات المتعلقة بالجرائم السيبرانية.
3) محدودية الأطر القانونية المنظمة للتعاون الدولي في مجال الأمن السيبراني.

وقد يؤدي هذا النقص في الأطر القانونية إلى صعوبة ملاحقة الجرائم الرقمية أو تطوير سياسات فعالة لحماية الأنظمة الحيوية من الهجمات السيبرانية.

ب: ضعف القدرات المؤسسية في إدارة الأمن السيبراني

يتطلب تطوير منظومة فعالة للأمن السيبراني وجود مؤسسات حكومية متخصصة قادرة على إدارة المخاطر الرقمية وتطوير السياسات المناسبة لحماية البنية التحتية الحيوية. غير أن العديد من دول الشرق الأوسط تواجه تحديات مؤسسية تتعلق بضعف التنسيق بين المؤسسات الحكومية أو محدودية الموارد المتاحة لتطوير القدرات التقنية. .(World Economic Forum, 2024)

وتشمل هذه التحديات: (James Andrew Lewis 2024)

1) نقص المؤسسات المتخصصة في الأمن السيبراني.

2) ضعف التنسيق بين الجهات الحكومية المسؤولة عن إدارة الفضاء الرقمي.
3) محدودية الموارد المالية المخصصة لتطوير أنظمة الحماية الرقمية.

ويؤدي هذا الوضع إلى وجود فجوات في منظومات الأمن السيبراني، الأمر الذي يزيد من احتمالية تعرض البنية التحتية الحيوية للهجمات الرقمية.

ج: نقص الكفاءات البشرية المتخصصة

يُعد العنصر البشري أحد الركائز الأساسية في بناء منظومات فعالة للأمن السيبراني، إذ تعتمد الدول بشكل كبير على الخبرات التقنية المتخصصة في مجالات الأمن الرقمي وتحليل البيانات وإدارة الشبكات. غير أن العديد من دول الشرق الأوسط تواجه نقصاً في الكفاءات البشرية المتخصصة في هذه المجالات.

ويرجع ذلك إلى عدة عوامل، من أبرزها: .(Kello, 2017)

1) محدودية البرامج التعليمية المتخصصة في الأمن السيبراني.
2) هجرة الكفاءات التقنية إلى الدول المتقدمة.
3) ضعف الاستثمار في التدريب والتطوير التقني.

وقد يؤدي هذا النقص في الكفاءات إلى إضعاف قدرة الدول على تطوير سياسات فعالة لحماية البنية التحتية الرقمية.

د: تأثير الصراعات الجيوسياسية في المنطقة

تُعد منطقة الشرق الأوسط من أكثر المناطق التي تشهد مستويات مرتفعة من التوترات السياسية والصراعات الإقليمية، الأمر الذي يزيد من احتمالية استخدام الهجمات السيبرانية كأداة في الصراع السياسي أو التنافس الاستراتيجي بين الدول.

وقد أدى هذا الوضع إلى بروز ما يعرف بـ الصراع السيبراني، حيث تستخدم الدول أو الجماعات المدعومة من الدول الهجمات الرقمية لتحقيق أهداف سياسية أو استراتيجية. وتتميز هذه الهجمات بأنها غالباً ما تكون منخفضة التكلفة مقارنة بالحروب التقليدية، لكنها قد تؤدي إلى تأثيرات كبيرة في البنية التحتية الحيوية للدول المستهدفة. .(Valeriano & Maness, 2015)

كما تشير بعض الدراسات إلى أن الهجمات السيبرانية أصبحت جزءاً من الحرب الهجينة التي تستخدم مزيجاً من الأدوات العسكرية والاقتصادية والإعلامية لتحقيق أهداف سياسية دون الدخول في صراع عسكري مباشر.

ويرى الباحث أن تداخل البعد السيبراني مع الصراعات الجيوسياسية في الشرق الأوسط يعزز من تعقيد البيئة الأمنية في المنطقة، إذ تتحول الهجمات السيبرانية إلى أدوات منخفضة التكلفة وعالية التأثير، تُستخدم لتحقيق أهداف سياسية دون الانخراط في مواجهات عسكرية مباشرة.

هـ: تحديات السيادة الرقمية والاعتماد التكنولوجي

يُعد الاعتماد المتزايد على التكنولوجيا الأجنبية أحد التحديات الرئيسية التي تواجه العديد من دول الشرق الأوسط في مجال الأمن السيبراني. إذ تعتمد العديد من الدول على الشركات التكنولوجية العالمية في تطوير البنية التحتية الرقمية، الأمر الذي قد يثير تساؤلات حول الأمن السيبراني والسيادة الرقمية.

وتتمثل أبرز هذه التحديات في: .(Nye, 2010)

1) الاعتماد على البرمجيات الأجنبية في تشغيل الأنظمة الحيوية.
2) الاعتماد على الشركات الدولية في إدارة البنية التحتية الرقمية.
3) احتمالية وجود ثغرات أمنية في الأنظمة التكنولوجية المستوردة.

وقد دفع ذلك العديد من الدول إلى محاولة تطوير استراتيجيات وطنية لتعزيز السيادة الرقمية وتقليل الاعتماد على التكنولوجيا الأجنبية.

ويُستنتج من ذلك أن تحقيق السيادة الرقمية في دول الشرق الأوسط ما زال يواجه تحديات بنيوية، لاسيما في ظل الاعتماد الكبير على التكنولوجيا الأجنبية، الأمر الذي يحد من قدرة هذه الدول على التحكم الكامل في بنيتها التحتية الرقمية.

و: تحديات التعاون الإقليمي والدولي

يُعد الأمن السيبراني بطبيعته قضية عابرة للحدود، إذ يمكن أن تنطلق الهجمات الرقمية من دولة معينة وتستهدف بنية تحتية في دولة أخرى. ولذلك فإن مواجهة هذه التهديدات تتطلب مستوى عالياً من التعاون الدولي في مجالات تبادل المعلومات وتطوير آليات مشتركة للاستجابة للهجمات السيبرانية.

غير أن التعاون الإقليمي في مجال الأمن السيبراني في الشرق الأوسط ما زال محدوداً نسبياً، وذلك نتيجة التوترات السياسية بين بعض دول المنطقة واختلاف أولويات السياسات الأمنية بينها. وقد أدى هذا الوضع إلى صعوبة تطوير منظومات إقليمية فعالة للتعامل مع التهديدات الرقمية. (Lewis, 2018)

ومن خلال ما تقدم، يتضح أن حماية البنية التحتية الحيوية في الشرق الأوسط لا تقتصر على تطوير القدرات التقنية فحسب، بل تتطلب أيضاً إصلاحات سياسية ومؤسسية تهدف إلى تعزيز التشريعات الرقمية وتطوير المؤسسات المتخصصة وتعزيز التعاون الدولي في مجال الأمن السيبراني. كما أن مواجهة هذه التحديات أصبحت ضرورة ملحة في ظل تصاعد التهديدات الرقمية وتزايد اعتماد الدول على الأنظمة الرقمية في إدارة القطاعات الحيوية.

وفي مواجهة هذه التحديات، اتجهت العديد من دول الشرق الأوسط إلى تبني مجموعة من الآليات لتعزيز الأمن السيبراني الوطني، تمثلت في إنشاء هيئات وطنية متخصصة بالأمن السيبراني، وتطوير

استراتيجيات وطنية شاملة تهدف إلى حماية البنية التحتية الحيوية من التهديدات الرقمية، فضلاً عن تحديث الأطر التشريعية المتعلقة بالجرائم السيبرانية وتنظيم الفضاء الرقمي (International Telecommunication Union,2021). كما عملت بعض الدول، لاسيما الإمارات العربية المتحدة والمملكة العربية السعودية، على الاستثمار في بناء القدرات التقنية والبشرية من خلال إطلاق برامج تدريبية متخصصة وتعزيز الشراكات مع القطاع الخاص والشركات التكنولوجية العالمية (World Economic Forum, 2024).

ويرى الباحث أن هذه الجهود، على الرغم من أهميتها، ما زالت تواجه تحديات تتعلق بضعف التنسيق الإقليمي وتباين مستويات التطور المؤسسي بين دول المنطقة، الأمر الذي يحد من فاعلية الاستجابة الجماعية للتهديدات السيبرانية العابرة للحدود

ومن خلال ما تقدم، يمكن القول إن التهديدات السيبرانية في الشرق الأوسط لا تمثل مجرد تحديات تقنية، بل تعكس إشكالية هيكلية ترتبط بضعف التكامل بين الأبعاد السياسية والمؤسسية والتكنولوجية (Kello, 2017; Lewis, 2018). ويُستنتج من ذلك أن معالجة هذه التهديدات تتطلب تبني مقاربات شاملة تتجاوز الحلول التقنية التقليدية، لتشمل إصلاحات مؤسسية وتعزيز الحوكمة الرقمية وتطوير أطر التعاون الإقليمي والدولي.

ثانياً: الاستراتيجية الأوروبية للأمن السيبراني واستجابتها للتهديدات السيبرانية القادمة من الشرق الأوسط

شهدت السياسات الأمنية الأوروبية خلال العقدين الأخيرين تحولاً ملحوظاً نتيجة التزايد المستمر في التهديدات السيبرانية التي تستهدف الدول والمؤسسات الاقتصادية والبنية التحتية الحيوية. ومع تزايد الاعتماد على الأنظمة الرقمية في مختلف القطاعات الاقتصادية والإدارية، أصبح الأمن السيبراني أحد الركائز الأساسية في السياسات الأمنية للاتحاد الأوروبي. وقد دفع ذلك الاتحاد الأوروبي إلى تطوير إطار مؤسسي وتشريعي متكامل يهدف إلى حماية الفضاء الرقمي الأوروبي وتعزيز قدرة الدول الأعضاء على مواجهة التهديدات الرقمية. (European Commission, 2020).

وفي هذا السياق، أدرك الاتحاد الأوروبي أن التهديدات السيبرانية لم تعد تقتصر على الحدود الوطنية، بل أصبحت ذات طبيعة عابرة للحدود، حيث يمكن للهجمات الرقمية التي تنطلق من مناطق عدم الاستقرار الجيوسياسي أن تؤثر في الأنظمة الحيوية في أوروبا. ومن بين هذه المناطق منطقة الشرق الأوسط، التي تُعد أحد أهم المناطق الجيوسياسية المرتبطة بالأمن الأوروبي بسبب دورها في إمدادات الطاقة والتجارة الدولية والاستقرار الإقليمي. (Valeriano & Maness, 2015)

وقد دفع ذلك الاتحاد الأوروبي إلى تطوير مجموعة من السياسات والاستراتيجيات التي تهدف إلى تعزيز الأمن السيبراني الأوروبي وتطوير آليات للتعاون الدولي في مواجهة التهديدات الرقمية العابرة للحدود. (European Parliament Research Service, 2022).

1. حوكمة الأمن السيبراني في الاتحاد الأوروبي ومفهوم السيادة الرقمية

شهدت منظومة الأمن السيبراني في الاتحاد الأوروبي تطوراً كبيراً خلال السنوات الأخيرة، حيث عمل الاتحاد على تطوير إطار متكامل لحوكمة الأمن الرقمي يعتمد على مجموعة من السياسات والتشريعات والمؤسسات المتخصصة. (European Commission, 2020).

أ: تطور الاستراتيجية الأوروبية للأمن السيبراني

أطلق الاتحاد الأوروبي عدة استراتيجيات لتعزيز الأمن السيبراني، من أبرزها استراتيجية الاتحاد الأوروبي للأمن السيبراني لعام 2020 التي هدفت إلى تعزيز قدرة الاتحاد الأوروبي على حماية الفضاء الرقمي وتعزيز مرونة البنية التحتية الحيوية في مواجهة التهديدات الرقمية. (European Commission, 2020).

وقد ركزت هذه الاستراتيجية على مجموعة من الأهداف الرئيسية، من أهمها: (European Parliament Research Service, 2022).

1) تعزيز قدرة الدول الأوروبية على مواجهة الهجمات السيبرانية.
2) حماية البنية التحتية الحيوية في القطاعات الاقتصادية الاستراتيجية.
3) تعزيز التعاون بين الدول الأعضاء في مجال الأمن السيبراني.
4) تطوير شراكات دولية لمواجهة التهديدات الرقمية العابرة للحدود.

وقد أدى ذلك إلى تطوير إطار أوروبي متكامل لحوكمة الأمن السيبراني يشمل مجموعة من التشريعات والسياسات التنظيمية.

ب: توجيه أمن الشبكات والمعلومات(NIS2)

يُعد توجيه أمن الشبكات والمعلومات (NIS2) أحد أهم الأدوات التشريعية التي اعتمدها الاتحاد الأوروبي لتعزيز الأمن السيبراني في الدول الأعضاء. ويهدف هذا التوجيه إلى تعزيز مستوى الأمن الرقمي في القطاعات الحيوية مثل الطاقة والنقل والاتصالات والأنظمة المالية. (European Commission, 2016).

كما يفرض هذا التوجيه على المؤسسات الحيوية اتخاذ مجموعة من التدابير الأمنية لحماية أنظمتها الرقمية، إضافة إلى إلزامها بالإبلاغ عن الحوادث السيبرانية التي قد تؤثر في عمل هذه الأنظمة. (European Commission, 2016)

ج: دور المؤسسات الأوروبية في إدارة الأمن السيبراني: أنشأ الاتحاد الأوروبي عدداً من المؤسسات المتخصصة التي تعمل على دعم الدول الأعضاء في تطوير سياسات الأمن السيبراني، ومن أبرز هذه المؤسسات:

1) وكالة الاتحاد الأوروبي للأمن السيبراني(ENISA)

تُعد هذه الوكالة أحد أهم المؤسسات الأوروبية في مجال الأمن السيبراني، حيث تعمل على دعم الدول الأعضاء في تطوير استراتيجيات الأمن الرقمي وتعزيز تبادل المعلومات حول التهديدات السيبرانية. (ENISA, 2023)

2) المركز الأوروبي لمكافحة الجرائم السيبرانية

يعمل هذا المركز على تنسيق الجهود بين أجهزة إنفاذ القانون في الدول الأوروبية لمكافحة الجرائم السيبرانية وتعزيز التعاون الدولي في هذا المجال. .(European Parliament Research Service, 2022)

د: مفهوم السيادة الرقمية الأوروبية

برز في السنوات الأخيرة مفهوم السيادة الرقمية الأوروبية (Digital Sovereignty) الذي يشير إلى قدرة الاتحاد الأوروبي على التحكم في بنيته التحتية الرقمية وتقليل الاعتماد على التكنولوجيا الأجنبية. .(Kello, 2017) وقد ظهر هذا المفهوم نتيجة المخاوف الأوروبية من الاعتماد المتزايد على الشركات التكنولوجية الكبرى، خاصة الشركات الأمريكية والصينية، في إدارة البنية التحتية الرقمية الأوروبية. ولذلك يسعى الاتحاد الأوروبي إلى تطوير سياسات تهدف إلى تعزيز استقلاله الرقمي وتطوير قدراته التكنولوجية المحلية. (European Commission, 2020.

2. الانعكاسات الاستراتيجية للتهديدات السيبرانية في الشرق الأوسط على الأمن الأوروبي

أصبحت التهديدات السيبرانية القادمة من مناطق عدم الاستقرار الجيوسياسي أحد التحديات الرئيسية التي تواجه الأمن الأوروبي في العصر الرقمي. وتشير العديد من الدراسات إلى أن الهجمات السيبرانية التي تستهدف البنية التحتية الحيوية في الشرق الأوسط قد تكون لها انعكاسات مباشرة أو غير مباشرة على الأمن الاقتصادي والاستراتيجي للدول الأوروبية. (Buchanan, 2020)

أ: تأثير التهديدات السيبرانية على أمن الطاقة الأوروبي

يعتمد الاتحاد الأوروبي بدرجة كبيرة على استيراد الطاقة من منطقة الشرق الأوسط، الأمر الذي يجعل أي اضطراب في البنية التحتية الطاقوية في المنطقة مصدر قلق للأمن الأوروبي. وقد يؤدي استهداف منشآت الطاقة أو شبكات النقل المرتبطة بها إلى تعطيل إمدادات الطاقة أو إحداث اضطرابات في الأسواق العالمية. (International Institute for Strategic Studies, 2021).

ب: تأثير الهجمات السيبرانية على سلاسل الإمداد العالمية: تشكل منطقة الشرق الأوسط أحد الممرات الحيوية للتجارة العالمية، خاصة من خلال الممرات البحرية الاستراتيجية مثل مضيق هرمز وقناة السويس. وقد يؤدي استهداف البنية التحتية المرتبطة بهذه الممرات إلى تعطيل حركة التجارة الدولية وسلاسل الإمداد العالمية، الأمر الذي قد ينعكس بشكل مباشر على الاقتصاد الأوروبي. (World Economic Forum, 2024)

ج: التهديدات السيبرانية العابرة للحدود

تتميز الهجمات السيبرانية بطبيعتها العابرة للحدود، إذ يمكن أن تنطلق من دولة معينة وتستهدف بنية تحتية في دولة أخرى. وقد أدى ذلك إلى زيادة المخاوف الأوروبية من احتمال انتقال التهديدات السيبرانية من مناطق الصراع في الشرق الأوسط إلى الفضاء الرقمي الأوروبي. .(Valeriano & Maness, 2015)

د: السياسات الأوروبية في مواجهة التهديدات السيبرانية الخارجية

في ضوء تصاعد التهديدات السيبرانية ذات الطابع العابر للحدود، عمل الاتحاد الأوروبي على تطوير مقاربة شاملة تهدف إلى مواجهة المخاطر الرقمية القادمة من خارج حدوده، وذلك من خلال توظيف مزيج من الأدوات الدبلوماسية والقانونية والتعاونية (European Commission, 2020). وفي هذا السياق، تبنى الاتحاد الأوروبي ما يُعرف بـ "دبلوماسية الأمن السيبراني" التي تقوم على استخدام الوسائل السياسية والقانونية في الرد على الهجمات السيبرانية، لاسيما من خلال فرض عقوبات على الجهات المسؤولة عن هذه الهجمات وتعزيز قواعد السلوك الدولي في الفضاء الرقمي (.European External Action Service, 2022)

كما عزز الاتحاد الأوروبي من آليات التعاون الدولي عبر تطوير شراكات استراتيجية مع عدد من الدول والمنظمات الدولية، لاسيما حلف شمال الأطلسي (NATO)، بهدف تبادل المعلومات الاستخباراتية المتعلقة بالتهديدات السيبرانية وتنسيق الاستجابة للهجمات الرقمية (European Parliament Research Service, 2022). وفي الإطار ذاته، يسعى الاتحاد الأوروبي إلى دعم الدول الشريكة، خاصة في مناطق عدم الاستقرار مثل الشرق الأوسط، من خلال برامج بناء القدرات وتطوير البنية التحتية الرقمية، بما يسهم في تقليل مصادر التهديدات السيبرانية قبل انتقالها إلى الفضاء الأوروبي European Parliament Research Service, 2022).

ويرى الباحث أن هذه السياسات تعكس تحولًا في الاستراتيجية الأوروبية من التركيز على الحماية الداخلية إلى اعتماد مقاربة استباقية تقوم على إدارة مصادر التهديد خارج الحدود، من خلال الجمع بين الردع السيبراني والتعاون الدولي. ومع ذلك، فإن فعالية هذه السياسات تبقى مرتبطة بمدى قدرة الاتحاد الأوروبي على تحقيق تنسيق فعّال مع الدول الشريكة، خاصة في البيئات الإقليمية التي تعاني من ضعف البنى المؤسسية والتشريعية.

الخاتمة

في ضوء التحولات الرقمية المتسارعة في النظام الدولي، باتت التهديدات السيبرانية تمثل أحد أبرز التحديات التي تواجه الأمن الوطني والدولي، لاسيما عندما تستهدف البنية التحتية الحيوية التي تشكل الركيزة الأساسية لاستقرار الدول واقتصاداتها. وقد أظهر هذا البحث أن منطقة الشرق الأوسط تمثل بيئة خصبة لتصاعد هذه التهديدات، نتيجة التداخل بين العوامل الجيوسياسية وضعف الأطر المؤسسية والتشريعية في بعض دول المنطقة.

كما بينت الدراسة أن انعكاسات هذه التهديدات لا تقتصر على النطاق الإقليمي، بل تمتد لتؤثر بشكل مباشر في الأمن الأوروبي، في ظل الاعتماد المتبادل في مجالات الطاقة والتجارة وسلاسل الإمداد. وفي المقابل، يسعى الاتحاد الأوروبي إلى تبني مقاربة شاملة للأمن السيبراني تجمع بين تطوير القدرات الداخلية وتعزيز التعاون الدولي، بهدف احتواء التهديدات الرقمية العابرة للحدود.

ويرى الباحث أن فعالية هذه المقاربة تظل مرهونة بمدى القدرة على معالجة مصادر التهديد في بيئاتها الأصلية، لاسيما في المناطق التي تعاني من هشاشة مؤسسية، الأمر الذي يستدعي تعزيز التكامل بين البعدين الإقليمي والدولي في إدارة الأمن السيبراني.

النتائج

توصلت الدراسة إلى مجموعة من النتائج، من أبرزها:

1. تصاعد التهديدات السيبرانية التي تستهدف البنية التحتية الحيوية في الشرق الأوسط، وتحولها إلى أداة رئيسية في الصراعات الجيوسياسية المعاصرة.
2. وجود ارتباط وثيق بين ضعف الأطر المؤسسية والتشريعية في بعض دول المنطقة وزيادة قابلية البنية التحتية الرقمية للاختراق.
3. تنامي أهمية الفضاء السيبراني بوصفه مجالاً استراتيجياً للصراع الدولي، يتجاوز الأبعاد التقنية ليشمل أبعاداً سياسية واقتصادية.
4. تأثر الأمن الأوروبي بشكل مباشر أو غير مباشر بالتهديدات السيبرانية في الشرق الأوسط، خاصة في مجالات الطاقة وسلاسل الإمداد.
5. اعتماد الاتحاد الأوروبي على مقاربة متعددة الأدوات في مواجهة التهديدات السيبرانية، تجمع بين الردع والتعاون الدولي وبناء القدرات.
6. استمرار التحديات المرتبطة بضعف التنسيق الدولي وتباين القدرات بين الدول، مما يحد من فاعلية الاستجابة الجماعية للتهديدات السيبرانية.

التوصيات

في ضوء النتائج التي توصلت إليها الدراسة، يمكن تقديم مجموعة من التوصيات، من أبرزها:

1. ضرورة تطوير استراتيجيات وطنية شاملة للأمن السيبراني في دول الشرق الأوسط، تقوم على تعزيز الأطر المؤسسية والتشريعية.
2. تعزيز الاستثمار في بناء القدرات البشرية والتقنية في مجال الأمن السيبراني، بما يسهم في تقليل الفجوة الرقمية.
3. دعم إنشاء آليات إقليمية للتعاون السيبراني بين دول الشرق الأوسط، بهدف تبادل المعلومات والتنسيق في مواجهة التهديدات المشتركة.
4. تعزيز التعاون بين الاتحاد الأوروبي ودول الشرق الأوسط في مجال الأمن السيبراني، لاسيما في مجالات التدريب ونقل التكنولوجيا.
5. تطوير أطر قانونية دولية أكثر فاعلية لتنظيم الفضاء السيبراني ومساءلة الجهات المسؤولة عن الهجمات الرقمية.
6. تبني مقاربات استباقية تقوم على إدارة مصادر التهديد قبل انتقالها إلى نطاقات أوسع، بدلاً من الاكتفاء بسياسات الاستجابة.

References:

1. Buchanan, B. (2020). The hacker and the state: Cyber-attacks and the new normal of geopolitics. Harvard University Press.
2. Cavelty, M. D. (2008). Cyber-security and threat politics: US efforts to secure the information age. Routledge.
3. European Commission. (2016). Directive on security of network and information systems (NIS Directive). European Union.
4. European Commission. (2020). EU cybersecurity strategy for the digital decade. European Commission.
5. European External Action Service. (2022). EU cyber diplomacy toolbox. Brussels.

6. European Parliament Research Service. (2022). Cybersecurity and cyber defence in the European Union. European Parliament.
7. European Union Agency for Cybersecurity (ENISA). (2023). ENISA threat landscape report 2023. ENISA.
8. International Institute for Strategic Studies. (2021). Cyber capabilities and national power: A net assessment. IISS.
9. International Telecommunication Union. (2021). Global cybersecurity index 2020. Geneva: ITU.
10. Kello, L. (2017). The virtual weapon and international order. Yale University Press.
11. Lewis, J. A. (2018). Cybersecurity and critical infrastructure protection. Center for Strategic and International Studies.
12. Nye, J. S. (2010). Cyber power. Belfer Center for Science and International Affairs, Harvard University.
13. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
14. Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.
15. World Economic Forum. (2024). Global cybersecurity outlook 2024. World Economic Forum.