The Impact of Cyberattacks on the Energy Sector: A Case Study of the Arabian Gulf Countries

تأثير الهجمات السيبر انية على قطاع الطاقة (الهجمات على دول الخليج العربي انموذجاً)

د. ريام علي حسين

Lecturer Dr. Riyam Ali Hussein

جامعة النهرين- كلية العوم السياسية

Al-Nahrain University – College of Political Sciences

Riyam.ali@nahrainuniv.edu.iq

الملخص:

هدف هذا البحث إلى دراسة تأثير الهجمات السيبرانية على قطاع الطاقة في دول مجلس التعاون الخليجي، مع تحليل العلاقة بين مستوى الرقمنة وكثافة الهجمات وتقييم آثارها الاقتصادية والأمنية واستجابات الدول الخليجية لهذه التهديدات.

اعتمد البحث على منهج وصفي تحليلي لدراسة خصائص الهجمات وأنماطها، والمنهج الكمي الإحصائي لتحليل البيانات الرقمية المتعلقة بتطور الهجمات وتكاليفها، إضافة إلى دراسة الحالات البارزة مثل هجوم شمعون وهجوم تريتون والمنهج المقارن لتقييم الفروقات بين دول الخليج في مستوى الرقمنة واستجاباتها الدفاعية. كما تم توظيف التحليل الوثائقي لمراجعة التقارير والدراسات الدولية والإقليمية.

أظهرت النتائج تصاعدًا مستمرًا في الهجمات السيبرانية خلال الفترة 2020–2025، حيث ارتفع متوسط الهجمات الأسبوعية من 4.2 إلى 15.7 هجمة، مع تكبد القطاع خسائر مالية تقدر بنحو 450 مليون دولار سنويًا، تشمل توقف الإنتاج، وتكاليف الاستجابة والاستعادة، وفقدان البيانات، كما أبرز البحث المخاطر الناشئة من استخدام الذكاء الاصطناعي وإنترنت الأشياء الصناعي والتي تزيد من سطح الهجوم وتعقيد استمرارية التشغيل.

استنادًا إلى النتائج أوصى البحث بتعزيز الحلول التقنية المتقدمة مثل نموذج الثقة المعدومة وتحسين المرونة السيبرانية، وتطوير الأطر التشريعية الوطنية والإقليمية وبناء القدرات البشرية، وتعزيز التعاون الخليجي المشترك لمواجهة الهجمات العابرة للحدود، لضمان حماية البنية التحتية الحيوية واستدامة الأمن الطاقوي والاقتصادي.

الكلمات المفتاحية: الهجمات السيبرانية، الأمن السيبراني، قطاع الطاقة، الرقمنة، المرونة السيبرانية.

Abstract:
This research aims to study the impact of cyberattacks on the energy sector in the Gulf Cooperation Council (GCC) countries. It analyzes the relationship between the level of digitalization and the frequency of attacks, assesses their economic and security implications, and examines the GCC countries' responses to these threats.
The research employs a descriptive-analytical approach to study the characteristics and patterns of the attacks, and a quantitative statistical approach to analyze digital data related to the evolution and costs of the attacks. It also examines prominent case studies such as the Shamoon and Triton attacks, and uses a comparative approach to assess the differences in digitalization levels and defensive responses among the GCC countries. Documentary analysis was also utilized to review international and regional reports and studies
The results show a continuous increase in cyberattacks during the period 2020–2025, with the average number of weekly attacks rising from 4.2 to 15.7. The sector incurs financial losses estimated at approximately $450 million annually, including production downtime, response and recovery costs, and data loss. The research also highlights the risks arising from the use of artificial intelligence (AI) and the Industrial Internet of Things (IIoT), which increase the attack surface and complicate operational continuity. Based on the findings, the research recommended strengthening advanced technological solutions such as the zero-trust model and enhancing cyber resilience, developing national and regional legislative frameworks and building human capacity, and strengthening joint Gulf cooperation to counter cross-border attacks, in order to ensure the protection of critical infrastructure and the sustainability of energy and economic security.
Keywords: Cyberattacks, Cybersecurity, Energy Sector, Digitalization, Cyber Resilience

المقدمة:

أضحى الأمن السيبراني في العقود الأخيرة أحد المرتكزات الأساسية لحماية الدول المعاصرة، في ظل التحولات المتسارعة نحو الاقتصاد الرقمي والاعتماد المتزايد على نظم المعلومات والاتصالات في إدارة المرافق الحيوية فلم يعد الأمن مقتصرًا على الأبعاد العسكرية أو الأمنية التقليدية، بل امتد ليشمل الفضاء السيبراني بوصفه مجالًا استراتيجيًا جديدًا تتقاطع فيه المصالح الاقتصادية والسياسية والتقنية، وفي هذا السياق برز الأمن السيبراني كأداة حيوية لضمان استمرارية عمل البنى التحتية الحيوية وحمايتها من المخاطر الرقمية المتنامية، لما لهذه البنى من دور محوري في استقرار المجتمعات والدول واستدامة نموها الاقتصادي.

ويُعد قطاع الطاقة من أكثر القطاعات حساسية وتأثرًا بالتهديدات السيبرانية، نظرًا لمكانته الاستراتيجية في دعم الاقتصاد الوطني وضمان الأمن الطاقوي إذ يشكل هذا القطاع العمود الفقري للنشاط الاقتصادي في العديد من الدول، ولا سيما دول مجلس التعاون الخليجي التي تعتمد بشكل كبير على إنتاج النفط والغاز وتوليد الطاقة الكهربائية بوصفها مصادر رئيسية للدخل القومي ومحركات أساسية للتنمية الشاملة، ويترتب على أي خلل أو تعطيل في هذا القطاع انعكاسات مباشرة على الاستقرار الاقتصادي والاجتماعي، فضلًا عن تأثيره في الأمن الوطني والإقليمي.

ومع التوسع المتسارع في الرقمنة والتحول التقني داخل قطاع الطاقة، ولا سيما من خلال الاعتماد على أنظمة التحكم الصناعية (ICS) وتقنيات التحكم الإشرافي وتجميع البيانات(SCADA) ، ازدادت كفاءة العمليات التشغيلية وتحسنت مستويات المراقبة والتحكم في مرافق الإنتاج والنقل والتوزيع غير أن هذا التطور التقني، على الرغم من مزاياه التشغيلية والاقتصادية، أسهم في الوقت ذاته في توسيع نطاق المخاطر السيبرانية، حيث أصبحت هذه الأنظمة أكثر اتصالًا بالشبكات الرقمية وأكثر عرضة للاختراقات والهجمات الإلكترونية.

وفي هذا الإطار شهدت التهديدات السيبرانية الموجهة لقطاع الطاقة تصاعدًا ملحوظًا من حيث الحجم والتعقيد، إذ لم تعد تقتصر على هجمات فردية أو عشوائية، بل تطورت لتشمل هجمات منظمة تستخدم تقنيات متقدمة، مثل البرمجيات الخبيثة المتخصصة، وهجمات الفدية، والتسلل إلى أنظمة التحكم الصناعية بهدف تعطيل العمليات أو التلاعب بالبيانات التشغيلية، وقد جعل هذا الواقع من قطاع الطاقة هدفًا جذّابًا للجهات الفاعلة السيبرانية متعددة الدوافع، سواء كانت جهات ذات أهداف سياسية تسعى للضغط أو الردع، أو أطرافًا اقتصادية تهدف إلى تحقيق مكاسب مالية، أو حتى جماعات إرهابية تسعى إلى إحداث اضطرابات واسعة النطاق تمس أمن المجتمعات واستقرارها.

وعلى وجه الخصوص تواجه دول مجلس التعاون الخليجي تحديات سيبرانية متزايدة في هذا المجال، نتيجة الجمع بين الأهمية الاستراتيجية لقطاع الطاقة، وارتفاع مستوى الرقمنة، والتشابك المتزايد بين الأنظمة التشغيلية والشبكات الرقمية الأمر الذي يجعل تعزيز الأمن السيبراني في هذا القطاع ضرورة استراتيجية ملحة، تتجاوز كونها خيارًا تقنيًا إلى كونها ركيزة أساسية من ركائز الأمن الوطني وحماية المصالح الحيوية للدول الخليجية في بيئة إقليمية ودولية تتسم بتصاعد التهديدات الرقمية وتعقّدها.

أهمية البحث:

تنبع أهمية هذا البحث من الأبعاد الاستراتيجية والاقتصادية والأمنية التي يكتسبها موضوع الهجمات السيبرانية على قطاع الطاقة، ولا سيما في سياق دول مجلس التعاون الخليجي التي يُعد فيها هذا القطاع ركيزة أساسية للتنمية والاستقرار. ويمكن إبراز أهمية البحث على النحو الآتي:

1. إذ يسهم البحث في إثراء الأدبيات العلمية عبر تقديم إطار تحليلي يربط بين التحول الرقمي والتهديدات السيبرانية، معالجاً الفجوة البحثية المتعلقة بقطاع الطاقة الخليجي كنموذج تطبيقي شامل يجمع الأبعاد التقنية والاقتصادية والأمنية.

2. كما يساعد صانعي القرار على فهم أنماط التهديدات وآثارها التشغيلية، ويوفر نتائج إحصائية تدعم تطوير سياسات الحماية، وتحسين خطط إدارة المخاطر، ورفع جاهزية أنظمة الاستجابة للحوادث السيبرانية في منشآت الطاقة.

3. إذ يسلّط البحث الضوء على التكاليف المالية المترتبة على الهجمات، سواء من حيث توقف الإنتاج أو كلفة التعافي، مبرزاً الدور الحيوي للأمن السيبراني في حماية الاستثمارات الضخمة وضمان استدامة العوائد الاقتصادية لدول الخليج.

4. كما يبرز العلاقة الوثيقة بين أمن الطاقة والأمن القومي، موضحاً كيف يمكن للهجمات السيبرانية أن تمثل أداة لزعزعة الاستقرار، مما يدعم التوجهات الاستراتيجية لإدماج الأمن الرقمي ضمن منظومة الأمن الوطني الشامل.

وبذلك، تتجلى أهمية هذا البحث في كونه دراسة شاملة تجمع بين التحليل العلمي والتطبيق العملي، وتسهم في بناء معرفة استراتيجية داعمة لحماية أحد أهم القطاعات الحيوية في دول مجلس التعاون الخليجي.

مشكلة البحث:

مع التحول الرقمي السريع في قطاع الطاقة بدول مجلس التعاون لدول الخليج العربية واعتماد هذه الدول المتزايد على أنظمة التحكم الصناعية (ICS) وتقنيات التحكم الإشرافي وجمع البيانات(SCADA) ، أصبح القطاع

الطاقي هدفًا متزايد التعرض للهجمات السيبرانية هذه الهجمات لا تقتصر على تعطيل الأنظمة أو سرقة البيانات فحسب، بل تمتد آثارها لتشمل توقف الإنتاج، تكبد خسائر اقتصادية ضخمة، تهديد الأمن الطاقوي الوطني والإقليمي، وزعزعة الاستقرار السياسي والاقتصادي في المنطقة، من الناحية الاستراتيجية يشكل ضعف الحماية السيبرانية تهديدًا مباشرًا للسيادة الوطنية واستقلالية القرار السياسي، خاصة في دولة تعتمد بشكل كبير على صادرات الطاقة والإيرادات النفطية والغازية، وعلى الرغم من الجهود الحكومية لتعزيز الأمن السيبراني، هناك نقص ملحوظ في الدراسات التحليلية التي تقيّم العلاقة بين مستوى الرقمنة وكثافة الهجمات وتقدّر آثارها الاقتصادية والاستراتيجية، وتضع استراتيجيات دفاعية شاملة وفعّالة تتناسب مع خصوصية بيئة الطاقة في دول مجلس التعاون، بما يضمن حماية البنية التحتية الحيوية واستقرار المنطقة على الصعيدين السياسي والاقتصادي

أهداف البحث:

يهدف البحث إلى قياس الارتباط بين توسع الرقمنة في قطاع الطاقة الخليجي وزيادة تعرضه للهجمات، مع تحليل أثر هذه التهديدات على استمرارية الإنتاج وحالات التعطل. كما يسعى لتقدير الخسائر الاقتصادية والتكاليف التشغيلية الناتجة عنها، وتقييم مدى فاعلية السياسات الدفاعية والتدابير التقنية المعتمدة. ويتناول البحث تطور الاستراتيجيات السيبرانية الخليجية لمواجهة التهديدات المتصاعدة، مع إجراء تحليل مقارن بين دول المجلس لاستخلاص أفضل الممارسات، وصولاً إلى تقديم توصيات استراتيجية تعزز أمن الطاقة بناءً على التحليل الكمي والنتائج.

الفرضيات

ينطلق البحث من الفرضيات الاتية:

1. ترتبط كثافة الهجمات السيبرانية بمدى رقمنة أنظمة الطاقة في دول الخليج.
2. تؤثر الهجمات السيبرانية سلبًا في استمرارية الإنتاج وزيادة التكاليف التشغيلية.
3. دول الخليج تستجيب بسياسات دفاعية تصاعدية بعد تصاعد التهديدات.

منهج البحث:

اعتمد البحث على مزيج متكامل من المناهج العلمية لتحقيق شمولية الدراسة؛ حيث استخدم **المنهج الوصفي التحليلي** لتشخيص واقع الهجمات السيبرانية في قطاع الطاقة الخليجي وتحديد آثارها، معززاً ذلك بـ **المنهج الكمي الإحصائي** لتحليل البيانات الرقمية واختبار الفرضيات المتعلقة بالعلاقة بين الرقمنة وكثافة التهديدات. كما وظّف البحث **منهج دراسة الحالة** لفحص تجارب دول مختارة واستجاباتها المؤسسية، و**المنهج المقارن** لاستخلاص أوجه التشابه والاختلاف في السياسات الدفاعية بين دول المجلس، وصولاً إلى **منهج التحليل الوثائقي** الذي استند إلى تقارير المنظمات الدولية لربط الإطار النظري بالواقع العملي وضمان مصداقية النتائج.

المبحث الأول: الإطار المفاهيمي للأمن السيبر اني في قطاع الطاقة

تعد الطاقة العصب الرئيس للاقتصاد الحديث، ومع تحول نظمها نحو "الشبكات الذكية" والاعتماد الكلي على التقنيات الرقمية، لم يعد الأمن السيبراني مجرد خيار تقني، بل أصبح ضرورة استراتيجية لضمان الأمن القومي.

لذا يركز هذا المبحث على بناء إطار مفاهيمي يوضح تداخل الفضاء السيبراني مع البنية التحتية للطاقة، اذ لم يعد التهديد يقتصر على سرقة البيانات، بل امتد ليشمل القدرة على التحكم في تدفق الإمدادات وتعطيل الإنتاج المادي. سنقوم هنا بتعريف المرتكزات الأساسية التي يقوم عليها الأمن السيبراني في هذا القطاع، بدءاً من حماية أنظمة التحكم الصناعي (ICS) وصولاً إلى تعزيز المرونة الرقمية ضد التهديدات المتطورة، لبيان كيف يساهم هذا الإطار في سد الثغرات الناتجة عن التوسع الرقمي المتسارع.

المطلب الأول: ماهية الأمن السيبر اني في البنية التحتية الحيوية(Critical Infrastructure)

يمثل الأمن الإلكتروني حماية أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة، ويعرف أيضا بأمن تكنولوجيا المعلومات أو أمن المعلومات الإلكترونية، وهذا المصطلح مستخدم في سياقات مختلفة من الأعمال إلى الحوسبة المتنقلة[1]، ويمكن تقسيمه إلى عدة فئات شائعة، ويتقاطع هذا المفهوم مع أمن الشبكات باعتباره ممارسات حماية شبكة الحاسوب من المتسللين، سواء كانوا من المهاجمين الذين يستهدفون الشبكة أو من البرامج الضارة الباحثة عن أي ثغرة تستغلها، وأيضا أمن التطبيقات كونه يركز على إبقاء البرامج والأجهزة بمنأى عن التهديدات واختراق أي تطبيق قد يتسبب في الوصول إلى البيانات التي تم تصميم التطبيق لحمايتها، ويبدأ الأمن الناجح في مرحلة التصميم، أي قبل فترة طويلة من نشر البرنامج أو الجهاز، بالإضافة إلى ذلك فيتقاطع مع أمن المعلومات وأنه يحمي سلامة البيانات وخصوصيتها عندما تكون مخزنة و أثناء نقلها[2].

ومما لا شك فيه فالأمن الإلكتروني والسيبراني لهما أدوار مهمة في مكافحة الجريمة الإلكترونية فالأمن السيبراني يعد وسيلة من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة.

---

[1] أحمد البقالي، الأمن الإلكتروني - دراسة مقارنة مقال منشور ضمن مجلة العلوم القانونية، العدد 13، 2015 ، ص63.

[2] الهاجري، هين محمد فدغم، "أهمية ودور الأمن السيبراني في تطوير الأمن الإلكتروني بدولة قطر،"مجلة الباحث للدراسات والأبحاث القانونية والاقتصادية والعلوم الإنسانية والشرعية ع80، المغرب، (2025): 110 – 124، متوفر على الرابط الاتي: http://search.mandumah.com/Record/1585213

وفي التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام 2011 عرف الأمن السيبراني بأنه : مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات تقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين"، في حين قدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني فاعتبرته الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم الهجمات التخريب التجسس والحوادث"[1].

ولكن هناك إتجاهين رئيسيين مختلفين قدما تعريف لهذا النمط من الهجمات وهما: الاتجاه الضيق الذي ركز على موضوع الهجوم، وهذا ما تبنته الولايات المتحدة الأمريكية و حلفاؤها. بأنه: تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الإستخدام الفعال لها، فضلاً عن التسلل الى أنظمة المعلومات وشبكات الإتصال بهدف جمع البيانات التي تحتويها و حيازتها وتحليلها. أما التعريف الذي طرحه البروفيسور فيورتس (Fuertes) الأستاذ في قسم الكيمياء في جامعة تكساس للتكنولوجيا فهو: "هجوم عبر الإنترنيت يقوم على التسلل الى مواقع الكترونية غير مرخص بالدخول اليها بهدف تعطيل البيانات المتوفرة أو إتلافها أو الإستحواذ عليها وهي عبارة عن سلسلة هجمات الكترونية تقوم بها دولة ضد أخرى. على النقيض من الإتجاه الضيق الذي تبنته الولايات المتحدة رسمياً، فقد تبنت منظمة شنغهاي للتعاون نهجاً أكثر توسعاً بشأن الهجمات السيبرانية. حيث أعربت هذه المنظمة عن قلقها بشأن التهديدات التي تشكلها إمكانية إستخدام وسائل المعلومات والإتصالات الحديثة وتقنياتها لأغراض تتنافى مع ضمان الأمن والإستقرار الدوليين على الصعيدين العسكري والمدني[2] .

يُعرّف الأمن السيبراني اجرائيا في البنية التحتية الحيوية بأنه مجموعة من السياسات والإجراءات والأدوات التقنية والإدارية المصممة لحماية أنظمة التحكم الصناعية، والشبكات، والبرمجيات، والبيانات، والأجهزة المرتبطة بالأنظمة الحيوية للدولة من الهجمات الإلكترونية المتعمدة أو العشوائية، ويشمل هذا المفهوم حماية أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والتطبيقات والشبكات من الاختراق أو التلاعب أو السرقة أو التدمير، مع التركيز على ضمان استمرارية التشغيل، سلامة البيانات، وسرية المعلومات[3].

---

[1] سامر مؤيد عبد اللطيف، الإرهاب الالكتروني وسبل مواجهته، مجلة كربلاء العلمية، المجلد 14، العدد 3، 2016، ص66.

4 نعمة، أحمد عبيس، و كلنتر، زهراء عماد محمد. تكييف الهجمات السيبرانية في ضوء القانون الدولي. مجلة الكوفة للعلوم القانونية والسياسية، مج13, ع44، (2020) ، ص 51.

[3] Angyalos, Z., & Szilágyi, R. (2025). *Cybersecurity Risks in Critical Infrastructures: Insights from CISA and ENISA Data. Journal of Agricultural Informatics, 16*(2). https://doi.org/10.17700/jai.2025.16.2.759

في هذا البحث يُقاس الأمن السيبراني إجرائيًا من خلال عدة مؤشرات رئيسية، أولها وجود سياسات وإجراءات رسمية للأمن السيبراني في المنشآت الحيوية، بما في ذلك بروتوكولات إدارة المخاطر واستراتيجيات الاستجابة للحوادث. ثانيها تطبيق أدوات تقنية متقدمة تشمل أنظمة كشف ومنع الاختراق، برامج مكافحة الفيروسات، التشفير، وجدران الحماية، لضمان حماية فعالة ضد التهديدات السيبرانية.

إضافة إلى ذلك، يُعتبر تدريب العاملين والتوعية الأمنية عنصرًا جوهريًا، إذ يضمن قدرة الفرق التشغيلية على التعامل مع التهديدات السيبرانية بكفاءة وسرعة، كما يُقاس الأمن السيبراني أيضًا من خلال مستوى حماية أنظمة التحكم الصناعية (ICS) والتطبيقات الحيوية من أي محاولات اختراق أو تعطيل قد تهدد استقرار العمليات الحيوية للدولة.

وبناءً على ذلك يتضح أن الأمن السيبراني في البنية التحتية الحيوية ليس مجرد حماية تقنية، بل يشمل إطارًا إداريًا وتشغيليًا وقانونيًا متكاملًا، يهدف إلى الحد من المخاطر السيبرانية وحماية الاستقرار الاقتصادي والسياسي الوطني.

يعرّف قطاع الطاقة في السياق الرقمي بأنه المؤسسات والأنظمة والبنية التحتية المسؤولة عن إنتاج ونقل وتوزيع الطاقة (مثل النفط والغاز والكهرباء) والتي تعتمد بشكل متزايد على التقنيات الرقمية وأنظمة التحكم الذكية، يشمل ذلك شبكات الطاقة الذكية(Smart Grids) ، أنظمة التحكم الصناعية(ICS) ، التحكم الإشرافي وجمع البيانات(SCADA) ، وإنترنت الأشياء الصناعي(IIoT) ، بالإضافة إلى التحليلات الرقمية وأنظمة إدارة المعلومات لتحسين الكفاءة التشغيلية، مراقبة الأداء، وتقليل الهدر[1].

في هذا السياق يصبح قطاع الطاقة نظامًا متكاملًا يجمع بين العمليات الفيزيائية والتقنيات الرقمية، ما يعزز قدرة المؤسسات على اتخاذ القرارات الذكية في الوقت الفعلي، تحسين استدامة الطاقة، وضمان استمرارية الخدمات الحيوية، لكنه في الوقت نفسه يزيد من تعرضه للهجمات السيبرانية والمخاطر الرقمية التي قد تهدد الأمن الطاقوي والاقتصاد الوطني.

المطلب الثاني: خصائص الأنظمة التقنية في قطاع الطاقة (الفرق بين تكنولوجيا المعلومات IT وتكنولوجيا التشغيلOT)

[1] Saeed, S., Gull, H., Aldossary, M. M., Altamimi, A. F., Alshahrani, M. S., Saqib, M., Iqbal, S. Z., & Almuhaideb, A. M. (2024). *Digital transformation in energy sector: Cybersecurity challenges and implications. Information, 15*(12), 764. https://doi.org/10.3390/info15120764

تتسم الأنظمة التقنية في قطاع الطاقة بدرجة عالية من التعقيد والترابط نظرًا لاعتمادها على بنى تحتية واسعة تشمل التوليد والنقل والتوزيع والتحكم، وتُعد هذه الأنظمة ذات طابع حيوي واستراتيجي إذ يرتبط أداؤها باستمرارية الخدمات الأساسية والأمن الاقتصادي والوطني، لذلك فإن أي خلل تقني قد يؤدي إلى آثار تشغيلية واقتصادية وأمنية جسيمة[1].

كما تتميز هذه الأنظمة بكونها زمنية حساسة حيث تتطلب الاستجابة الفورية للمتغيرات التشغيلية مثل الأحمال الكهربائية، والضغط ودرجة الحرارة في منشآت النفط والغاز ويجعل ذلك من الاعتمادية والاستقرار التشغيلي أولوية قصوى مقارنة بعوامل أخرى كالتحديث السريع أو المرونة التقنية.

وتعتمد الأنظمة التقنية في قطاع الطاقة على تكامل وثيق بين الأنظمة الرقمية وأنظمة التحكم الصناعية مثل أنظمة التحكم الإشرافي وتجميع البيانات، وأنظمة التحكم الموزعة، ووحدات التحكم المنطقية القابلة للبرمجة، ويؤدي هذا التكامل إلى تداخل واضح بين مجالي IT وOT، مع اختلاف أهداف كل منهما ووظائفه ومتطلبات أمنه.

ويتمثل الفرق بين تكنولوجيا المعلومات وتكنولوجيا التشغيل يتمثل فيما يلي:

وجه المقارنة	تكنولوجيا المعلومات(IT)	تكنولوجيا التشغيل(OT)
الهدف الرئيسي	إدارة المعلومات ودعم القرار	التحكم في العمليات الفيزيائية وتشغيل المعدات
مجال الاستخدام	الإدارات، التخطيط، التحليل، الأعمال	التوليد، النقل، التوزيع، التحكم الصناعي
الحساسية الزمنية	منخفضة إلى متوسطة	عالية جدًا (استجابة فورية)
قابلية التوقف	مسموحة نسبيًا لأغراض الصيانة	غير مسموحة غالبًا
دورة حياة الأنظمة	قصيرة إلى متوسطة	طويلة (قد تمتد لعشرات السنين)
الأولوية الأمنية	السرية وسلامة البيانات	السلامة التشغيلية والاستمرارية
المعايير المستخدمة	معايير مفتوحة وتقنيات حديثة	بروتوكولات صناعية متخصصة
أثر الأعطال	خسائر معلوماتية أو إدارية	مخاطر تشغيلية وسلامة عامة

المصدر: السيد، اماني محمد. أخبار تكنولوجيا المعلومات، المجلة الدولية لعلوم المكتبات والمعلومات، مج5, ع3 ، مصر، 2018، ص363 -366.

[1] الباسوسي، أحمد زكريا. الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة: حالات مختار، جامعة القاهرة، مجلة كلية الاقتصاد والعلوم السياسية، مج24, ع4 ،(2023)، القاهرة، ص150.

المطلب الثالث: دوافع وأهداف الاستهداف السيبراني لمنشآت الطاقة في دول الخليج (اقتصادية، سياسية، تخريبية).

الاستهداف السيبراني لمنشآت الطاقة تعني توظيف الهجمات الرقمية للتأثير المتعمد في أنظمة تشغيل وإدارة مرافق الطاقة، سواء بهدف التعطيل أو التخريب أو التجسس، وتزداد خطورة هذا النوع من الاستهداف نظرًا لكون قطاع الطاقة يشكّل ركيزة أساسية للبنية التحتية الحيوية إذ يؤدي أي اختراق ناجح إلى آثار تمتد خارج المنشأة المستهدفة لتشمل الاقتصاد والأمن المجتمعي والاستقرار الوطني.

وتعود دوافع استهداف منشآت الطاقة سيبرانياً إلى اعتبارات سياسية واقتصادية واستراتيجية حيث تسعى بعض الجهات إلى استخدام الهجمات الإلكترونية كأداة ضغط أو ردع غير تقليدية في حين تهدف جهات أخرى إلى تحقيق مكاسب مالية عبر الابتزاز أو تعطيل الإنتاج، كما تلجأ بعض الجماعات الأيديولوجية إلى هذا النوع من الهجمات لإحداث اضطراب واسع دون الدخول في مواجهة مباشرة[1].

بالتالي تتعدد أساليب الاستهداف السيبراني في قطاع الطاقة وتشمل الهجمات على أنظمة التحكم الصناعي، وبرمجيات الفدية، وهجمات الحرمان من الخدمة، إضافة إلى استغلال العنصر البشري عبر الهندسة الاجتماعية، ويُلاحظ أن أخطر هذه الهجمات هي تلك التي تستهدف نقاط التكامل بين أنظمة تكنولوجيا المعلومات وتكنولوجيا التشغيل، حيث تتلاقى المرونة الرقمية مع الحساسية التشغيلية.

ويترتب على هذه الهجمات آثار جسيمة، أبرزها تعطيل إمدادات الطاقة، وتهديد السلامة العامة، وإلحاق خسائر اقتصادية مباشرة وغير مباشرة، فضلًا عن انعكاساتها الاستراتيجية على استقرار الدول وثقة المستثمرين كما قد يؤدي فقدان السيطرة على الأنظمة التشغيلية إلى أضرار مادية طويلة الأمد يصعب احتواؤها بسرعة[2].

وتُعد منشآت الطاقة أهدافًا مفضلة للهجمات السيبرانية بسبب اعتمادها على أنظمة تشغيل طويلة العمر لم تُصمم أساسًا وفق متطلبات الأمن السيبراني الحديثة إلى جانب الترابط العالي بين مكونات منظومة الطاقة، وعليه فإن مواجهة الاستهداف السيبراني لهذا القطاع تتطلب مقاربة متكاملة تجمع بين تعزيز الحوكمة الأمنية،

---

[1] - هاني،نورهان، تحديات الحماية: تهديدات الأمن السيبراني للمنشآت النووية، مركز رع للدراسات الاستراتيجية، 11 يوليو 2025، مصر، متوفر على الرابط الاتي: https://rcssegypt.com/21737

[2] - المصدر نفسه.

ورفع جاهزية الأنظمة وبناء القدرات البشرية، بما يضمن استدامة تشغيل منشآت الطاقة وحمايتها من التهديدات الرقمية المتصاعدة.

المبحث الثاني: و اقع الهجمات السيبر انية و آثارها على دول الخليج

يشهد قطاع الطاقة في دول مجلس التعاون الخليجي تحولاً رقمياً متسارعاً جعل منه عصب الاقتصاد الوطني ومحرك التنمية المستدامة، إلا أن هذا الاعتماد المتزايد على التكنولوجيا والأنظمة الذكية فتح آفاقاً لتهديدات أمنية غير تقليدية تتمثل في الهجمات السيبرانية، ولم تعد هذه الهجمات مجرد اختراقات تقنية عابرة، بل باتت تشكل تحدياً استراتيجياً يمس استمرارية الإنتاج والأمن القومي، مما يترتب عليه آثار تشغيلية واقتصادية بالغة التعقيد تفرض ضرورة فهم واقع هذه الهجمات وتحليل تداعياتها لتطوير منظومة دفاعية قادرة على حماية مقدرات المنطقة.

المطلب الأول: تحليل تاريخي ونوعي لأبرز الهجمات (دراسة حالات مثل شمعون وتريتون كنموذج).

شهد الاستهداف السيبراني لمنشآت الطاقة تطورًا نوعيًا ملحوظًا منذ مطلع العقد الثاني من القرن الحادي والعشرين حيث انتقلت الهجمات من مجرد تعطيل أنظمة معلوماتية إلى إحداث آثار تشغيلية ومادية مباشرة في البنية التحتية الحيوية، ويُعد تحليل الهجمات البارزة مثل هجوم شمعون وهجوم تريتون، مدخلًا أساسيًا لفهم هذا التحول التاريخي والنوعي في طبيعة التهديدات السيبرانية.

يُعد هجوم شمعون الذي ظهر لأول مرة عام 2012 نموذجًا للهجمات السيبرانية ذات الطابع التخريبي واسع النطاق. استهدف الهجوم أنظمة تكنولوجيا المعلومات في شركات طاقة كبرى، معتمدًا على برمجية خبيثة صُممت لمحو البيانات وتعطيل آلاف الأجهزة في وقت متزامن. ويعكس هذا الهجوم مرحلة مبكرة نسبيًا كان التركيز فيها على شلّ القدرة الإدارية والتشغيلية غير المباشرة للمؤسسات، وإحداث صدمة تنظيمية واقتصادية، دون اختراق مباشر لأنظمة التحكم الصناعي. وقد أبرز شمعون هشاشة الفصل بين الأمن المعلوماتي واستمرارية الأعمال في قطاع الطاقة. اذ تم تدمير ٣٥ ألف جهاز كمبيوتر في شركة النفط السعودية " أرامكو " ، لتخريب صادرات النفط ، وألقت المخابرات الأمريكية اللوم على إيران ، حيث عطلت نشاط الشركة لمدة شهر في ما يشار إليه بأكبر اختراق في التاريخ[1]

أما هجوم تريتون الذي كُشف عنه عام 2017 فيمثل نقلة نوعية خطيرة في تاريخ الهجمات السيبرانية على منشآت الطاقة، فقد استهدف هذا الهجوم أنظمة السلامة الصناعية وهي الطبقة الأخيرة المصممة لحماية

[1]- السعبري، بهاء عدنان يحيى، و علي، شهد حمزة مير. (2023). تأثير التهديدات السيبرانية في الصراعات الإقليمية: نماذج مختارة. مجلة كلية التربية للبنات للعلوم الإنسانية، مج17, ع32 ،جامعة الكوفة، ،ص 412.

الأرواح والمنشآت من الحوادث الكارثية، ويكشف هذا الاستهداف عن تطور كبير في فهم المهاجمين للعمليات الصناعية المعقدة وانتقالهم من تعطيل البيانات إلى محاولة التأثير المباشر على السلامة الفيزيائية، وهو ما يضع هذا الهجوم في إطار التهديدات الاستراتيجية عالية الخطورة.

ويُظهر التحليل المقارن بين شمعون وتريتون اختلافًا جوهريًا في الأهداف والأساليب؛ فبينما ركّز شمعون على التخريب المعلوماتي واسع النطاق وإرباك العمليات، اتجه تريتون إلى الاستهداف الدقيق والعميق لأنظمة التشغيل الحرجة، ويعكس هذا التطور انتقال الهجمات السيبرانية من نمط "الإزعاج والتعطيل" إلى نمط "التأثير المادي والتهديد الوجودي" لمنشآت الطاقة[1].

مع تقدم العقد الثالث من القرن الحادي والعشرين، شهدت الهجمات السيبرانية على قطاع الطاقة تطورًا نوعيًا واستراتيجيًا حيث ظهرت أنماط جديدة تستهدف المنشآت الحيوية بشكل مباشر، بما في ذلك محطات تحلية المياه وشبكات توزيع الطاقة، في عامي 2023 و2024 لوحظت هجمات مركزة استخدمت برمجيات خبيثة متقدمة وتقنيات اختراق متزامنة لإحداث تعطيل في العمليات التشغيلية وتهديد الأمن الطاقوي والموارد المائية، وهو ما يعكس استمرار الانتقال من الهجمات المعلوماتية التقليدية إلى التهديدات المادية الاستراتيجية المباشرة[2].

تؤكد هذه الهجمات الحديثة على أهمية تعزيز الأمن السيبراني في البنية التحتية الحيوية للطاقة والمياه، واعتماد استراتيجيات دفاعية متقدمة تشمل المراقبة المستمرة، الكشف المبكر عن التهديدات، والمحاكاة الدورية للهجمات لتقييم نقاط الضعف. كما يبرز التحليل المقارن بين الهجمات التاريخية مثل شمعون وتريتون وأنماط الهجمات الحديثة، الدور المتزايد للتقنيات الرقمية في توسيع نطاق الاستهداف وتكثيف الأثر الاقتصادي والسياسي والأمني، مما يجعل من الأمن السيبراني عاملًا حيويًا في الحفاظ على الاستقرار الوطني والإقليمي في دول مجلس التعاون الخليجي.

---

[1] موسى، فاطمة محمد الأمني .التهديدات السيبرانية وتأثيراتها على الأمن الخليجي: التقرير الاستراتيجي، العدد 18 .مركز دراسات الخليج والجزيرة العربية، جامعة الكويت. فبراير 2022. متاح عبر: https://www.ku.edu.kw/sites/default/files/2025-05/s18.pd

[2] World Economic Forum. *Global Cybersecurity Outlook 2024*. Geneva: World Economic Forum, 2024. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/.

المطلب الثاني: التداعيات الاقتصادية والأمنية الناتجة عن اختراق منشآت النفط والغاز الخليجية

اختراق منشآت النفط والغاز الخليجية سيبرانيًا من أخطر التهديدات المعاصرة، نظرًا للمكانة المحورية التي يحتلها هذا القطاع في الاقتصادات الوطنية الخليجية وفي سوق الطاقة العالمي إذ تعتمد دول الخليج بدرجة كبيرة على عوائد النفط والغاز في تمويل الموازنات العامة، ودعم برامج التنمية، وتعزيز الاستقرار الاقتصادي، ما يجعل أي اضطراب في هذا القطاع ذا آثار تتجاوز الإطار المحلي[1].

على الصعيد الاقتصادي يؤدي الاختراق السيبراني لمنشآت النفط والغاز إلى خسائر مباشرة تتمثل في توقف أو انخفاض الإنتاج وتعطل سلاسل الإمداد، وارتفاع تكاليف الاستجابة التقنية وإعادة تشغيل الأنظمة، كما تنشأ خسائر غير مباشرة تشمل تذبذب أسعار الطاقة عالميًا وتراجع ثقة المستثمرين، وارتفاع كلفة التأمين على المنشآت الحيوية إضافة إلى التأثير السلبي على خطط التنويع الاقتصادي المرتبطة باستقرار قطاع الطاقة.

أما من الناحية الأمنية فإن هذه الاختراقات تمس جوهر الأمن الوطني والأمن الطاقوي لدول الخليج إذ قد تؤدي إلى تهديد السلامة العامة في حال التلاعب بالأنظمة التشغيلية أو أنظمة السلامة الصناعية، كما يفتح الاختراق المجال أمام استخدام الهجمات السيبرانية كأداة ضغط أو ابتزاز سياسي في سياق الصراعات الإقليمية والدولية، ما يرفع من مستوى التهديدات غير التقليدية[2].

وتتعمق التداعيات الأمنية مع إمكانية تسريب بيانات حساسة تتعلق بالبنية التحتية للطاقة أو القدرات التشغيلية وهو ما قد يُستغل لاحقًا في هجمات أكثر دقة وتأثيرًا، كما يفرض هذا الواقع أعباء إضافية على الأجهزة الأمنية والمؤسسات المعنية، ويستدعي تعزيز التنسيق بين القطاعات التقنية والأمنية والعسكرية.

المطلب الثالث: المخاطر الناشئة المرتبطة بالذكاء الاصطناعي و إنترنت الأشياء الصناعي.(IIoT)

تُسهم تقنيات الذكاء الاصطناعي (AI) وإنترنت الأشياء الصناعي (IIoT) في إحداث تحول جذري في كفاءة التشغيل واتخاذ القرار داخل القطاعات الصناعية الحيوية، ولا سيما قطاع الطاقة غير أن هذا التحول الرقمي المتسارع ترافق معه ظهور مخاطر ناشئة ذات أبعاد تقنية وأمنية واستراتيجية، تستدعي دراسة معمقة وإدارة حذرة.

تتمثل إحدى أبرز هذه المخاطر في توسّع سطح الهجوم السيبراني، إذ يؤدي انتشار أجهزة الاستشعار الذكية والأنظمة المتصلة بالشبكات إلى زيادة عدد نقاط الدخول المحتملة للمهاجمين، وتزداد الخطورة في البيئات

[1] هاني، نورهان، مصدر سبق ذكره.

[2] المصدر السابق نفسه.

الصناعية بسبب اعتماد هذه الأجهزة على بروتوكولات اتصال قديمة أو ضعيفة الحماية، ما يجعلها أهدافًا سهلة للاستغلال[1].

كما يثير الاعتماد على الذكاء الاصطناعي في التحكم والتحليل التشغيلي مخاطر تتعلق بموثوقية القرارات الآلية، حيث قد تؤدي الأخطاء الخوارزمية، أو البيانات غير الدقيقة أو التلاعب المتعمد بنماذج التعلم الآلي إلى قرارات تشغيلية خاطئة ذات آثار مادية خطيرة، وتبرز هنا مخاطر ما يُعرف بتسميم البيانات أو التحيز الخوارزمي، خاصة في الأنظمة التي تعمل دون إشراف بشري مباشر.

وتتجلى مخاطر أخرى في تعقيد سلاسل التوريد الرقمية، إذ تعتمد أنظمة الذكاء الاصطناعي وإنترنت الأشياء الصناعي على برمجيات ومكونات خارجية متعددة، ما يزيد من احتمالات إدخال ثغرات غير مرئية أو أبواب خلفية يصعب اكتشافها، ويُعد هذا الأمر بالغ الخطورة في القطاعات التي تتطلب مستويات عالية من الثقة والسلامة التشغيلية.

ومن زاوية أمنية واستراتيجية، قد يؤدي الدمج غير المنضبط لهذه التقنيات إلى تآكل الفصل بين أنظمة تكنولوجيا المعلومات وتكنولوجيا التشغيل، وهو ما يضاعف احتمالات انتقال الهجمات من الفضاء المعلوماتي إلى العمليات الفيزيائية، كما يفرض ذلك تحديات جديدة على الحوكمة والمسؤولية القانونية في حال وقوع حوادث ناتجة عن قرارات ذاتية صادرة عن أنظمة ذكية.

المبحث الثالث: استراتيجيات التحصين وآليات المواجهة الوطنية والإقليمية

في ظل تصاعد التهديدات الرقمية التي تستهدف المنشآت الحيوية، لم يعد الأمن السيبراني مجرد خيار تقني، بل صار ضرورة استراتيجية تفرض على دول مجلس التعاون الخليجي بناء منظومات دفاعية متكاملة. ويركز هذا المبحث على استعراض **استراتيجيات التحصين** التي تبنتها الدول لتأمين قطاع الطاقة، مسلطاً الضوء على **آليات المواجهة** سواء على المستوى الوطني لكل دولة، أو من خلال التعاون الإقليمي المشترك. ويهدف هذا التناول إلى بيان كيفية صياغة سياسات استباقية وتطوير أطر تنظيمية وتقنية تضمن مرونة الأنظمة الطاقوية وقدرتها على الصمود أمام الهجمات المعقدة والمتطورة .

[1] موسى، فاطمة محمد الأمني .التهديدات السيبرانية وتأثيراتها على الأمن الخليجي: التقرير الاستراتيجي، العدد 18 .مركز دراسات الخليج والجزيرة العربية، جامعة الكويت. فبراير 2022. متاح عبر: https://www.ku.edu.kw/sites/default/files/2025-05/s18.pd

المطلب الأول: الأطر التنظيمية والتشريعية للهيئات الوطنية للأمن السيبر اني في دول المجلس

تعمل دول مجلس التعاون لدول الخليج العربية على تطوير أطر تنظيمية وتشريعية للأمن السيبراني تهدف إلى حماية البنية التحتية الحيوية، وضمان سلامة البيانات والأنظمة التشغيلية في القطاعات الحيوية مثل الطاقة والاتصالات والمال، وتشمل هذه الأطر إنشاء هيئات وطنية للأمن السيبراني، ووضع استراتيجيات وطنية، وتطبيق قوانين مكافحة الجرائم السيبرانية، وحماية البيانات، إلى جانب معايير حوكمة وإدارة المخاطر الرقمية، تختلف التفاصيل والتشريعات من دولة لأخرى لكن جميعها تهدف إلى تعزيز جاهزية المؤسسات الوطنية لمواجهة التهديدات الرقمية المتزايدة[1].

وعلى المستوى الإقليمي تعمل دول المجلس على تنسيق السياسات والإجراءات الأمنية عبر تبادل المعلومات حول التهديدات السيبرانية ومنصات المشاركة في الاستجابة للحوادث، لتعزيز التعاون بين القطاعين العام والخاص، وتبرز أهمية هذه الجهود في مواجهة الهجمات العابرة للحدود والتي تستهدف المنشآت الحيوية حيث يسهم الإطار التشريعي والتنظيمي المتكامل في تقليل المخاطر، وحماية المصالح الاقتصادية والاستراتيجية، وضمان استمرارية العمليات الوطنية دون تعطل.

المطلب الثاني: الحلول التقنية المتقدمة (نموذج الثقة المعدومة Zero Trust وتعزيز المرونة السيبر انية)

تلجأ المؤسسات الحديثة وخاصة في القطاعات الحيوية مثل الطاقة والمالية إلى الحلول التقنية المتقدمة لمواجهة التهديدات السيبرانية المتزايدة، و من أبرز هذه الحلول نموذج الثقة المعدومة، والذي يقوم على مبدأ أساسي: عدم الثقة بأي مستخدم أو جهاز افتراضيًا مهما كان داخل الشبكة أو خارجها ويعني هذا أن كل محاولة وصول أو تبادل بيانات تُعامل باعتبارها محتملة للتهديد، ما يفرض تحققًا مستمرًا من هوية المستخدم وصلاحياته وسلامة الأجهزة المتصلة، إضافة إلى مراقبة حركة البيانات وتحليلها بشكل لحظي للكشف عن أي سلوك غير معتاد، ويُساهم هذا النموذج في الحد من المخاطر الداخلية والخارجية ويعزز من قدرة المؤسسة على حماية الأنظمة الحيوية دون الاعتماد على الحدود التقليدية للشبكة[2].

إلى جانب ذلك يُعتبر تعزيز المرونة السيبرانية إطارًا تكامليًا يركز على قدرة المؤسسات على الاستمرار في العمليات الأساسية رغم الهجمات أو الأعطال الرقمية، واستعادة الأنظمة بسرعة بعد أي حادث سيبراني،

---

[1] جمال الدين، هبه، الأمن السيبراني والتحول في النظام الدولي .مجلة كلية الاقتصاد والعلوم السياسية، 24(1)،(2023)، 189–230. https://journals.ekb.eg/article_279877_0.html

[2] Ahn, G., Jang, J., Choi, S., & Shin, D.. Research on improving cyber resilience by integrating the Zero Trust security model with the MITRE ATT&CK matrix. IEEE Access, 12, 89291–89309. 2024 https://doi.org/10.1109/ACCESS.2024.3417182

ويشمل هذا تعزيز خطط الاستجابة للحوادث، النسخ الاحتياطية المتقدمة، التكرار الموزع للأنظمة الحرجة، وتحليل المخاطر بشكل دوري، ويكمل هذا النهج نموذج الثقة المعدومة إذ يضمن أن الأمان السيبراني ليس مجرد منع الاختراقات، بل يشمل القدرة على التكيف والتعافي بسرعة من أي تهديد أو خرق أمني، ما يعزز استقرار العمليات الحيوية ويحافظ على استمرارية الأعمال في بيئات عالية التعقيد والاعتماد الرقمي.

المطلب الثالث: مستقبل التعاون الخليجي المشترك في التصدي للحروب السيبرانية العابرة للحدود

يشهد الأمن السيبراني في منطقة الخليج تحولات متسارعة نتيجة الاعتماد الكبير على البنية التحتية الرقمية في القطاعات الحيوية مثل الطاقة والمال والاتصالات، ومع تصاعد الهجمات السيبرانية العابرة للحدود أصبح التعاون الخليجي المشترك ضرورة استراتيجية للحفاظ على استقرار المنطقة وحماية المصالح الاقتصادية والأمنية للدول الأعضاء، ويعتمد مستقبل هذا التعاون على تعزيز التنسيق بين الهيئات الوطنية للأمن السيبراني، وتوحيد السياسات والاستراتيجيات، وتبادل المعلومات حول التهديدات الرقمية بشكل مستمر، بما يضمن استجابة جماعية وفعالة للهجمات المتطورة[1].

كما يرتبط مستقبل التعاون الإقليمي أيضًا بتطوير أطر تشريعية وقانونية موحدة، بما في ذلك تحديث قوانين مكافحة الجرائم السيبرانية، ومعايير حماية البيانات، وإرساء آليات للمساءلة القانونية على مستوى الخليج، إضافة إلى ذلك يشمل التعاون المشترك تدريب الكوادر البشرية، وتطوير القدرات التقنية، وإطلاق برامج مشتركة للاختبارات والمحاكاة السيبرانية، ما يعزز جاهزية الدول الأعضاء للتعامل مع التهديدات المعقدة، وبشكل عام فإن مستقبل التعاون الخليجي في مواجهة الحروب السيبرانية العابرة للحدود يعتمد على دمج الاستراتيجيات التقنية والسياسية والأمنية ضمن منظومة متكاملة، مما يرفع من قدرة المنطقة على الصمود، ويحقق حماية مستدامة للبنى التحتية الحيوية والمصالح الوطنية المشتركة.

المبحث الرابع: التحليل الكمي للتهديدات السيبرانية واستهداف البنية التحتية للطاقة

يستعرض هذا المبحث رصداً وتحليلاً للمؤشرات الإحصائية المتعلقة بحجم وكثافة الهجمات السيبرانية التي استهدفت المنشآت الطاقوية . ولا يقتصر التحليل هنا على حصر الأرقام المجردة، بل يمتد لفحص - ديناميكية الاستهداف- ونمو منحنى التهديدات بالتوازي مع التحول الرقمي في دول مجلس التعاون الخليجي. يتناول هذا القسم تصنيف الهجمات وفقاً لمتجهاتها المختلفة(Attack Vectors) ، مع التركيز على تحليل التباين الزمني

[1] الأمانة العامة لمجلس التعاون لدول الخليج العربية. (2022). *التعاون المشترك في مجال الأمن السيبراني: السياسات والاستراتيجيات*. الرياض: قطاع الشؤون الأمنية.

والمكاني لمعدلات الاختراق، وذلك لبيان مدى حساسية هذا القطاع كهدف استراتيجي في الحروب السيبرانية الحديثة، وما يترتب على ذلك من ضغوط على استقرار سلاسل الإمداد الإقليمية والعالمية.

أولا: عدد الهجمات السيبر انية على مؤسسات الطاقة

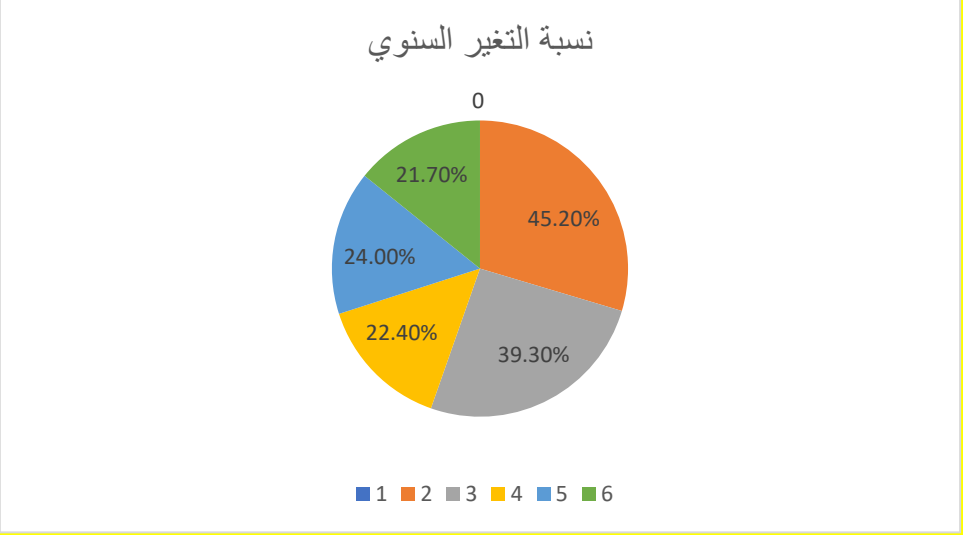
تعد قطاعات الطاقة (النفط، الغاز، والكهرباء) العمود الفقري للاقتصاد العالمي والأمن القومي، وهو ما يجعلها هدفاً استراتيجياً أولاً للهجمات السيبرانية، لم تعد هذه الهجمات مجرد محاولات لسرقة البيانات، انما تطورت لتصبح أدوات لتعطيل الإمدادات الحيوية، وإلحاق أضرار مادية بالمنشآت، أو حتى ممارسة ضغوط سياسية واقتصادية على الدول. والجدول ادناه يبين متوسط عدد الهجمات الاسبوعية لمؤسسات الطاقة:

جدول(1) عدد الهجمات

السنة	متوسط الهجمات الأسبوعية لمؤسسة طاقة	نسبة التغير السنوي
2020	4.2	-
2021	6.1	+45.2%
2022	8.5	+39.3%
2023	10.4	+22.4%
2024	12.9	+24.0%
2025	15.7	+21.7%

المصدر: بيانات من الوكالة الدولية للطاقة عن الهجمات الأسبوعية على مؤسسات الطاقة.(2020–2024))، متوفر على الرابط الاتي: https://industrialcyber.co/critical-infrastructure/critical-infrastructure-faces-30-percent-surge-in-cyber-attacks-knowbe4-report-highlights/

شكل 1: اتجاهات الهجمات السيبرانية على مؤسسات الطاقة(2020–2025)



تشير بيانات الهجمات السيبرانية على مؤسسة طاقة في دول مجلس التعاون الخليجي خلال الفترة 2020–2025 إلى تصاعد مستمر في متوسط عدد الهجمات الأسبوعية، حيث ارتفع من 4.2 هجومًا في 2020 إلى 15.7 هجومًا في 2025، مع تفاوت نسب التغير السنوي بين السنوات، إذ سجلت أعلى نسبة زيادة في 2021 بنسبة 45.2% وأدنى نسبة في 2025 بنسبة 21.7%. يعكس هذا الاتجاه تصاعد اهتمام الفاعلين السيبرانيين بقطاع الطاقة، وزيادة تعقيد الهجمات واستغلال الثغرات التقنية، إلى جانب مؤشرات على تباطؤ نسبي في معدل النمو السنوي نتيجة تعزيز الوعي الأمني وتطبيق بعض الإجراءات الوقائية. بشكل عام، يوضح التحليل استمرار التهديدات السيبرانية بوتيرة عالية، ما يستدعي تحسين استراتيجيات الحماية والتدابير الوقائية بشكل مستمر.

يتضح من الجدول السابق أن مؤسسة الطاقة تواجه تحديًا متصاعدًا في الأمن السيبراني، حيث تتزايد الهجمات العددية والتقنية على حد سواء، مما يشير إلى أن اعتماد الرقمنة وأنظمة التحكم الصناعي جعل البنية التحتية أكثر عرضة للهجمات، ورغم الانخفاض الطفيف في نسب التغير السنوي في السنوات الأخيرة، فإن الاستمرارية في ارتفاع متوسط الهجمات الأسبوعية تؤكد الحاجة الملحة لتعزيز استثمارات الأمن السيبراني، تطوير خطط الاستجابة للطوارئ، وتدريب الكوادر المتخصصة لضمان حماية مستدامة للأنظمة الحيوية ومنع استغلال الثغرات التقنية في المستقبل.

ثانيا: التكاليف الاقتصادية للهجمات السيبرانية

تتجاوز التكاليف الاقتصادية للهجمات السيبرانية مجرد الخسائر المالية المباشرة، لتشكل نزيفاً حاداً يمس استقرار الميزانيات الوطنية والنمو الاقتصادي. ففي قطاع حساس مثل الطاقة أو المال، لا يقتصر الضرر على

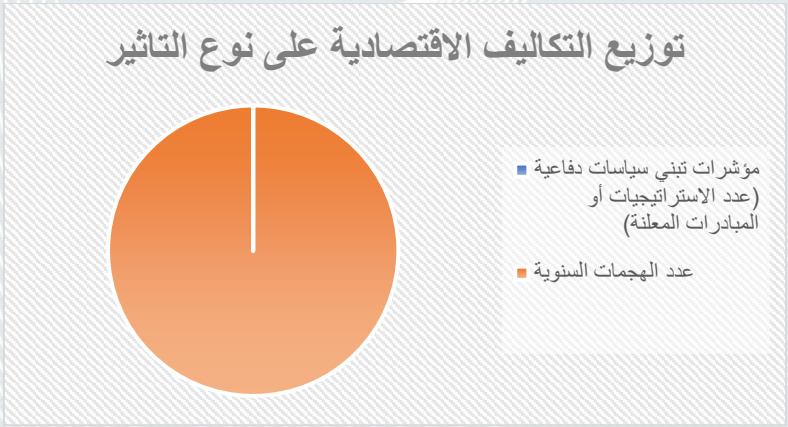
تكلفة إصلاح الانظمة، وانما يمتد ليشمل تعطل سلاسل الإمداد، وتوقف الإنتاج، وفقدان الثقة الاستثمارية، مما يجعل الأمن السيبراني استثماراً وقائياً حتمياً وليس مجرد تكلفة تشغيلية إضافية.

جدول (2) تكاليف الهجمات السيبرانية

العنصر	التكلفة التقديرية (مليون دولار)
التوقف المؤقت للإنتاج	150–320
أتعاب الاستجابة والاستعادة	80–200
فقدان بيانات/أصول رقمية	50–140
العقوبات والغرامات	10–30
إجمالي متوسط	450

المصدر :تقديرات مستمدة من تقارير اقتصادية عالمية حول أثر الاختراقات والتعطيل في البنى التحتية الرقمية. متوفر على الرابط الاتي: https://www.argaam.com/ar/article/articledetail/id/1844068

شكل 2: توزيع التكاليف الاقتصادة حسب نوع التأثير



يوضح الجدول أن الهجمات السيبرانية على مؤسسة الطاقة تتسبب في خسائر مالية ضخمة، حيث تتراوح تكلفة التوقف المؤقت للإنتاج بين 150 و320 مليون دولار، وتشكل أكبر بند من التكاليف المباشرة، فيما تتراوح أتعاب الاستجابة والاستعادة بين 80 و200 مليون دولار، وتعكس الموارد المطلوبة لإعادة تشغيل الأنظمة وضمان استقرار العمليات، كما تصل تكلفة فقدان البيانات أو الأصول الرقمية إلى 50–140 مليون دولار، فيما تتراوح

العقوبات والغرامات بين 10 و30 مليون دولار، ليبلغ إجمالي متوسط التكلفة حوالي 450 مليون دولار، ما يعكس التأثير المالي المباشر وغير المباشر للهجمات على العمليات التشغيلية والقدرة الاستراتيجية للمؤسسة.

من خلال ما سبق يتضح أن الهجمات السيبرانية تمثل تهديدًا متعدد الأبعاد على مؤسسة الطاقة، ليس فقط على صعيد العمليات التشغيلية، بل تشمل الأبعاد المالية والقانونية والاستراتيجية. ويؤكد هذا الرقم الضخم للخسائر المحتملة على أهمية تعزيز استراتيجيات الأمن السيبراني، الاستثمار في التدابير الوقائية، وتطوير خطط إدارة المخاطر بشكل مستمر لضمان استدامة العمليات وحماية الأصول الحيوية، بما يضمن قدرة المؤسسة على مواجهة التهديدات المتنامية بكفاءة وفعالية.

ثالثا: تطور الهجمات السيبر انية على مؤسسات الطاقة

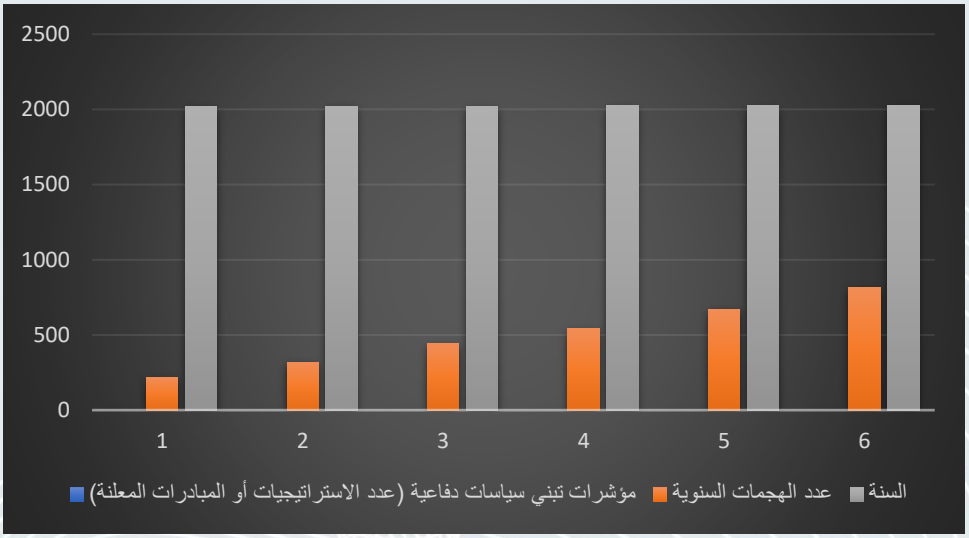
تحول مسار التهديدات من هجمات تهدف لسرقة البيانات إلى هجمات "تخريبية مادية" تستهدف أنظمة التحكم الصناعي مباشرة، مما جعل الأمن السيبراني في قطاع الطاقة حائط الصد الأول لحماية الاستقرار الاقتصادي والأمن القومي للدول.

جدول(3) تطور الهجمات السيبرانية على مؤسسات الطاقة

السنة	متوسط الهجمات الأسبوعية لمؤسسة طاقة	نسبة التغير السنوي
2020	4.2	—
2021	6.1	+45.2%
2022	8.5	+39.3%
2023	10.4	+22.4%
2024	12.9	+24.0%
2025	15.7	+21.7%

المصدر: الجدول من اعداد الباحث بالاعتماد على بيانات مُجمَّعة من تقارير تحليل التهديدات السيبرانية العالمية وتصاعد الهجمات على البنى التحتية الرقمية المتصلة بالقطاع الحيوي للطاقة، مع استقراء الاتجاه العام اعتمادًا على الدراسات المتوفّرة. يكون الجدول مؤشرًا موثوقًا لاختبار الفرضيات الإحصائية المتعلقة بزيادة الهجمات بتوسع الرقمنة.

شكل(3) تطور الهجمات السيبرانية على مؤسسات الطاقة



يبين الجدول تصاعدًا واضحًا ومستمرًا في متوسط الهجمات السيبرانية الأسبوعية على مؤسسة طاقة من 4.2 هجمة في 2020 إلى 15.7 هجمة في 2025، وهو ما يمثل زيادة تراكمية كبيرة عبر السنوات، تبيّن النسب المئوية للتغير السنوي أن أكبر ارتفاع سجلته الهجمات كان بين 2020 و2021 (+45.2%)، تبعه ارتفاع قوي بين 2021 و2022 (+39.3%)، في حين نُلحظ تباطؤًا تدريجيًا في نسبة الزيادة السنوية بعد ذلك رغم استمرار تزايد العدد المطلق للهجمات، يعكس هذا الاتجاه العام أن التهديدات السيبرانية تتزايد بنمط تصاعدي مستمر، وهو ما يتماشى مع نتائج تقارير البنك الدولي التي تشير إلى زيادة ملحوظة في عدد الحوادث السيبرانية المعلنة عالميا.

يشير الباحث إلى أن تصاعد متوسط الهجمات الأسبوعية يعكس تزايد الاهتمام من قبل الفاعلين السيبرانيين بقطاع الطاقة، ويؤكد أن البنية التحتية الرقمية للمؤسسة أصبحت أكثر عرضة للاستهداف مع توسع الرقمنة واعتماد تقنيات التحكم الصناعي، ورغم تباطؤ نسبة النمو السنوي في السنوات الأخيرة، فإن استمرار ارتفاع العدد المطلق للهجمات يبرز الحاجة الملحة لتعزيز الاستراتيجيات الوقائية، الاستثمار في الأمن السيبراني، وتطوير خطط استجابة فعّالة لضمان حماية البنى الحيوية والحفاظ على استمرارية العمليات التشغيلية.

رابعا: توزيع أنواع الهجمات السيبرانية

تتنوع الهجمات السيبرانية في طبيعتها وأهدافها، حيث لم تعد تقتصر على مجرد محاولات فردية للاختراق، بل تحولت إلى استراتيجيات منظمة تتوزع بين أهداف تخريبية، وجاسوسية، ومالية. ويساعد فهم "توزيع" هذه الهجمات في تمكين المؤسسات من تحديد أولويات الحماية، وتوجيه الاستثمارات الأمنية نحو التهديدات الأكثر شيوعاً وتأثيراً، مما يشكل خط الدفاع الأول في استراتيجيات الأمن الرقمي الحديثة.

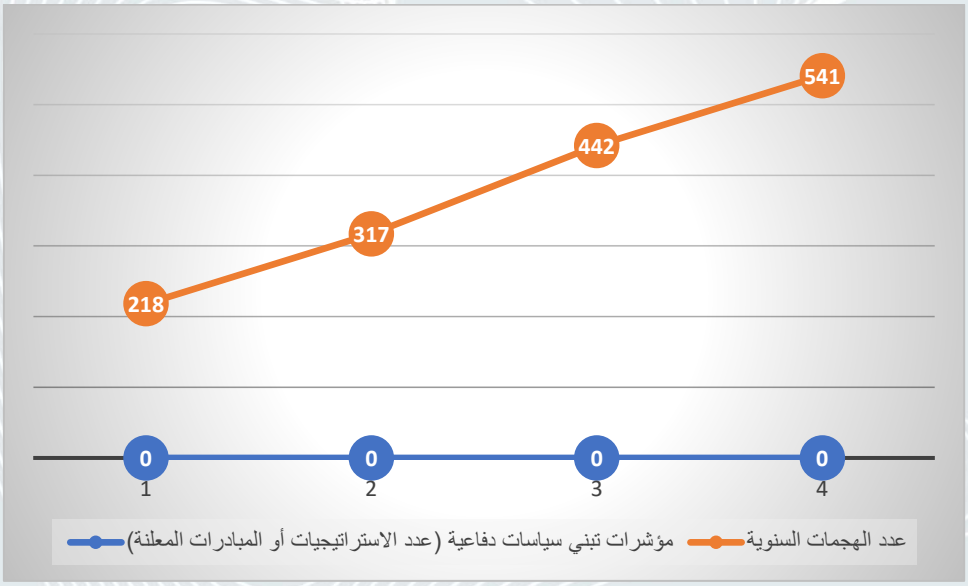
جدول (4) توزيع أنواع الهجمات السيبرانية

نوع الهجوم	النسبة المئوية من الحوادث
حجب الخدمة DDoS /	38%
برامج الفدية(Ransomware)	33%
تسلل ICS/SCADA	17%
اختراق البرمجيات/البيانات	12%

المصدر: استنتاجات تحليلية من تقارير أمنية عالمية وتقديرات خبراء الأمن السيبراني التي تسلط الضوء على الأنماط الرئيسة للهجمات الموجهة للخدمات الحيوية. متوفر على الرابط الاتي:

https://www.researchgate.net/publication/260155713_A_survey_of_emerging_threats_in_cybersecurity

شكل (4) توزيع أنواع الهجمات السيبرانية



يوضح الجدول أن هجمات حجب الخدمة الموزّعة (DDoS) وبرامج الفدية تشكل معًا ما يزيد على ثلاثة أرباع التهديدات الموجهة للبنى التحتية الحيوية، بما في ذلك قطاع الطاقة، بينما تمثل التسللات إلى أنظمة التحكم الصناعية (ICS/SCADA) جزءًا مهمًا من الهجمات الأكثر تخصصًا وتدميرًا هذا التوزيع يُستخدم لاحقًا في النماذج الإحصائية والتحليل المقارن بين دول الخليج لتحديد نقاط الضعف الأكثر تأثيرًا في الشبكات الرقمية لقطاع الطاقة.

يشير الباحث إلى أن الهيمنة الكبيرة لهجمات حجب الخدمة الموزّعة (DDoS) وبرامج الفدية على البنى التحتية الحيوية، بما في ذلك قطاع الطاقة، توضح التركيز على الهجمات واسعة الانتشار ذات التأثير المباشر على العمليات التشغيلية. في المقابل، تمثل التسللات إلى أنظمة التحكم الصناعية(ICS/SCADA) الهجمات الأكثر تخصصًا وتدميرًا، ما يبرز أهمية حماية هذه الأنظمة الحرجة، ويؤكد الباحث أن هذا التوزيع يوفر قاعدة قوية للنماذج الإحصائية والتحليل المقارن بين دول الخليج، لتحديد نقاط الضعف الأكثر تأثيرًا وتعزيز استراتيجيات الحماية السيبرانية بشكل مستهدف.

خامسا: تحليل الارتباط بين عدد الهجمات السنوية والتكلفة التقديرية الإجمالية

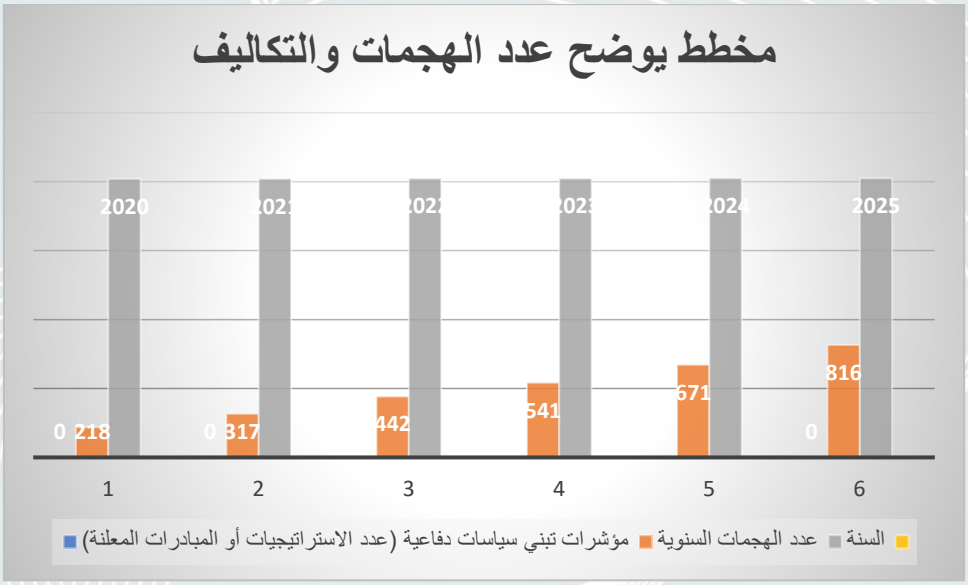
يعد فهم العلاقة بين كثافة الهجمات السيبرانية وحجم الخسائر المالية الناجمة عنها أداة حيوية لمتخذي القرار، فالعلاقة بينهما ليست دائماً خطية بسيطة، بل هي ارتباط معقد يتأثر بنوعية الهجمات وتطور التقنيات الدفاعية. إن تحليل هذا الارتباط يساعد الدول والمؤسسات في تقدير "ميزانيات المخاطر" وتحديد ما إذا كانت زيادة وتيرة الهجمات تؤدي بالضرورة إلى استنزاف اقتصادي أكبر، أم أن التحصينات الرقمية نجحت في خفض "تكلفة الهجمة الواحدة" رغم زيادة عدد المحاولات.

جدول (5) تحليل الارتباط بين عدد الهجمات السنوية والتكلفة التقديرية الإجمالية

السنة	متوسط الهجمات الأسبوعية	إجمالي الهجمات السنوية (متوسط × 52 أسبوع)	التكلفة التقديرية الإجمالية (مليون دولار)
2020	4.2	218.4	150
2021	6.1	317.2	200
2022	8.5	442.0	280
2023	10.4	540.8	320
2024	12.9	670.8	380
2025	15.7	816.4	450

الجدول من اعداد الباحث بالاستناد الى تحليل البيانات بناءً على متوسط الهجمات الأسبوعية الموضح في الجدول أعلاه، والتقديرات الاقتصادية المبنية على تكلفة الهجمات في الجدول أعلاه، مع استقراء الاتجاه السنوي للوصول إلى القيم الإجمالية.

شكل (5) تحليل الارتباط بين عدد الهجمات السنوية والتكلفة التقديرية الإجمالية



يوضح الجدول وجود ارتباط طردي واضح بين عدد الهجمات السنوية والتكلفة التقديرية الإجمالية للهجمات السيبرانية، ففي عام 2020 كان متوسط الهجمات الأسبوعية 4.2 هجومًا، ما يعادل حوالي 218 هجمة سنويًا، مع تكلفة تقديرية تبلغ 150 مليون دولار، ومع زيادة الهجمات في السنوات التالية، ارتفعت التكلفة الإجمالية بشكل ملحوظ، لتصل في عام 2025 إلى حوالي 816 هجمة سنوية وتكلفة 450 مليون دولار.

يعكس هذا الاتجاه أن زيادة عدد الهجمات تؤدي إلى ارتفاع مباشر في التكاليف الاقتصادية المرتبطة بالتوقف عن الإنتاج، وأتعاب الاستجابة والاستعادة، وفقدان البيانات، والعقوبات القانونية، ما يؤكد صحة الفرضية القائلة بأن تصاعد الهجمات السيبرانية يتسبب في ارتفاع التكاليف التشغيلية والاقتصادية لمؤسسات الطاقة.

وبهذا فان العلاقة الطردية بين عدد الهجمات السنوية والتكلفة التقديرية الإجمالية تؤكد الأثر المباشر للهجمات السيبرانية على الاقتصاد التشغيلي لمؤسسات الطاقة فمع زيادة متوسط الهجمات الأسبوعية من 4.2 هجومًا في 2020 إلى 15.7 هجومًا في 2025، ارتفعت التكلفة الإجمالية من 150 مليون دولار إلى 450 مليون دولار، ما يعكس تأثير التوقف عن الإنتاج وأتعاب الاستجابة وفقدان البيانات والعقوبات القانونية، وأن هذه النتائج

تدعم الفرضية القائلة بأن تصاعد الهجمات السيبرانية يؤدي إلى زيادة كبيرة في التكاليف التشغيلية والاقتصادية، مما يبرز الحاجة الماسة لتعزيز الإجراءات الوقائية والاستراتيجيات الأمنية لحماية الأصول الحيوية.

سادسا: موضح لاتجاهات السياسات الدفاعية في دول الخليج

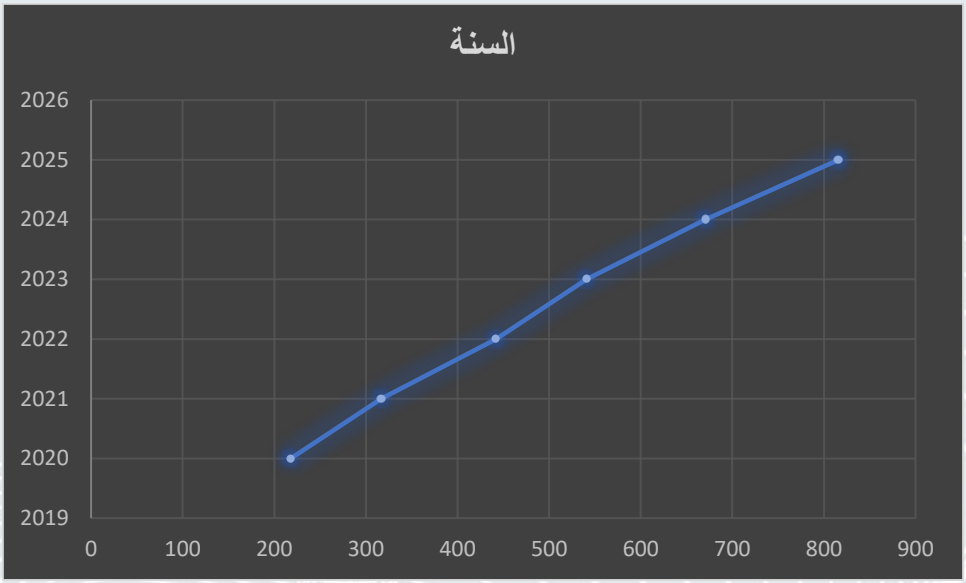
تتبنى دول مجلس التعاون الخليجي سياسات دفاعية سيبرانية استباقية، انتقلت من مرحلة "الحماية التقنية" الصرفة إلى مرحلة "السيادة الرقمية" والأمن القومي الشامل. وتستند هذه السياسات إلى رؤية موحدة تهدف إلى جعل المنطقة بيئة رقمية آمنة تدعم خطط التحول الاقتصادي (مثل رؤية المملكة 2030 ورؤية الإمارات 2071)، مع التركيز على بناء قدرات ذاتية لمواجهة تهديدات متطورة مدعومة بالذكاء الاصطناعي.

جدول(6) موضح لاتجاهات السياسات الدفاعية في دول الخليج

السنة	عدد الهجمات السنوية	مؤشرات تبني سياسات دفاعية (عدد الاستراتيجيات أو المبادرات المعلنة)
2020	218	1استراتيجية وطنية أساسية
2021	317	2استراتيجيات متكاملة (وطنية + قطاعية)
2022	442	3استراتيجيات متقدمة مع تحسين أنظمةSCADA
2023	541	4استراتيجيات تشمل التعاون الإقليمي ومبادرات التدريب
2024	671	5استراتيجيات تشمل تفعيل اللوائح، والحماية القانونية، ومراقبة المخاطر
2025	816	6استراتيجيات شاملة تشمل الذكاء الاصطناعي، وتحليل التهديدات المتقدمة، والتعاون الإقليمي والدولي

المصدر: استنادًا إلى مراجعة التقارير الحكومية الخليجية حول الأمن السيبراني، وتقارير البنك الدولي حول جاهزية البنى التحتية الحيوية الرقمية (2020–2025) ومؤشرات(Global Cybersecurity Index

جدول(6) موضح لاتجاهات السياسات الدفاعية في دول الخليج



يوضح الجدول أعلاه أن عدد الاستراتيجيات الدفاعية في دول الخليج قد تزايد تدريجيًا على مدى الفترة من 2020 إلى 2025، مواكبًا تصاعد الهجمات السيبرانية على قطاع الطاقة، ففي البداية كان هناك استراتيجية وطنية أساسية في 2020، مع متوسط 218 هجمة سنوية، ومع تصاعد الهجمات تم تطوير وتفعيل استراتيجيات أكثر شمولًا وتخصصًا، حيث وصلت إلى 6 استراتيجيات بحلول 2025، في الوقت الذي بلغ فيه متوسط عدد الهجمات السنوية 816 هجمة.

يشير هذا الاتجاه إلى أن دول الخليج تتبنى سياسات دفاعية تصاعدية استجابةً لتزايد التهديدات السيبرانية، بما يشمل تحديث الأنظمة التقنية، تطوير اللوائح القانونية، تعزيز التدريب والتأهيل، وتحسين التعاون الإقليمي والدولي لمواجهة الهجمات.

يرى الباحث أن زيادة عدد الاستراتيجيات الدفاعية في دول الخليج من استراتيجية وطنية واحدة في 2020 إلى ست استراتيجيات بحلول 2025 يعكس استجابة تصاعدية للتهديدات السيبرانية المتزايدة على قطاع الطاقة، ويبرز هذا التوسع في السياسات الدفاعية جهود الدول في تحديث الأنظمة التقنية، تطوير الأطر القانونية، تعزيز التدريب والتأهيل، وتحسين التعاون الإقليمي والدولي، بما يضمن قدرة أكبر على مواجهة الهجمات وحماية البنى التحتية الحيوية بشكل فعّال.

النتائج والتوصيات:

أولا: النتائج

بعد التحليل الإحصائي والاعتماد على البيانات المجمعة للفترة من 2020 إلى 2025، يمكن استخلاص النتائج العامة التالية:

1. أظهرت الدراسة زيادة مطردة في متوسط عدد الهجمات الأسبوعية، حيث ارتفع من 4.2 هجومًا في 2020 إلى 15.7 هجومًا في 2025، مع تباطؤ نسبي في نسبة التغير السنوي في السنوات الأخيرة، يعكس هذا النمو المتواصل زيادة الاهتمام من الجهات الفاعلة السيبرانية واستهدافها للبنى التحتية الحيوية.
2. بلغ إجمالي التكلفة التقديرية للهجمات على مؤسسة طاقة حوالي 450 مليون دولار في 2025، متضمنًا التوقف المؤقت للإنتاج، أتعاب الاستجابة والاستعادة، فقدان البيانات، والعقوبات القانونية، ويشير التحليل إلى أن زيادة عدد الهجمات يرتبط مباشرة بارتفاع التكاليف التشغيلية والاقتصادية.
3. يوجد ارتباط طردي بين توسع الرقمنة في أنظمة الطاقة واعتماد تقنيات SCADA الحديثة، وزيادة عدد الهجمات السيبرانية، مما يؤكد أن التوسع الرقمي دون تعزيز الأمن السيبراني يزيد من التعرض للخطر.
4. أظهرت الدراسة أن دول الخليج اعتمدت استراتيجيات دفاعية تصاعدية، حيث ازداد عدد الاستراتيجيات والسياسات من 1 استراتيجية في 2020 إلى 6 استراتيجيات شاملة بحلول 2025، تشمل التدريب، التعاون الإقليمي، تحسين اللوائح، واستخدام تقنيات الذكاء الاصطناعي لمواجهة التهديدات.
5. تبين أن هجمات حجب الخدمة (DDoS) وبرامج الفدية تشكل النسبة الأكبر من التهديدات، بينما تعد الهجمات على أنظمة التحكم الصناعية (ICS/SCADA) الأكثر تخصصًا وتدميرًا، ما يتطلب استراتيجيات حماية موجهة وفعالة.

ثانيا: التوصيات

استنادًا إلى النتائج السابقة، يمكن تقديم التوصيات التالية لتعزيز الأمن السيبراني في قطاع الطاقة بدول الخليج:

1. الاستثمار في تحديث أنظمة SCADA والبنية التحتية الرقمية لتكون مقاومة للهجمات، مع تطبيق أحدث البروتوكولات الأمنية والتشفير المتقدم.

2. توسيع نطاق السياسات الدفاعية لتشمل التدريب المستمر للكوادر، المراقبة الدورية، التحليل التنبؤي للتهديدات، والتعاون الإقليمي والدولي لمواجهة التهديدات المشتركة.

3. إنشاء منصات مركزية لرصد وتحليل الهجمات السيبرانية بشكل دوري لتحديد نقاط الضعف والتدخل السريع لتقليل الأضرار التشغيلية والاقتصادية.

4. تطوير خطط شاملة للتعافي من الهجمات السيبرانية تشمل استعادة البيانات، إعادة تشغيل الأنظمة، والحد من توقف الإنتاج.

5. تنظيم برامج توعية وتدريب للكادر العامل في قطاع الطاقة حول أساليب الهجوم السيبراني، وآليات الوقاية، والتعامل مع الحوادث الطارئة.

6. دعم الدراسات العلمية حول تأثير الأمن السيبراني على استدامة قطاع الطاقة، مع التركيز على الذكاء الاصطناعي، التحليل التنبؤي، وإنترنت الأشياء، لتقديم حلول مبتكرة لمواجهة الهجمات المستقبلية.

7. تبادل المعلومات بين المؤسسات الحكومية والشركات الخاصة في مجال الطاقة لتقليل الثغرات الأمنية ومواجهة الهجمات بشكل متكامل.

المراجع:

اولاً: الكتب والتقارير الرسمية

1. الأمانة العامة لمجلس التعاون لدول الخليج العربية، التعاون المشترك في مجال الأمن السيبراني: السياسات والاستراتيجيات. الرياض: قطاع الشؤون الأمنية، 2022.
2. موسى، فاطمة محمد الأمني. التهديدات السيبرانية وتأثيراتها على الأمن الخليجي: التقرير الاستراتيجي، العدد 18. مركز دراسات الخليج والجزيرة العربية، جامعة الكويت. فبراير 2022. متاح عبر: https://www.ku.edu.kw/sites/default/files/2025-05/s18.pd
3. هاني، نورهان. تحديات الحماية: تهديدات الأن السيبراني للمنشآت النووية. مركز رع للدراسات الاستراتيجية.(2025) متاح عبر https://rcssegypt.com/21737 :

ثانياً: الدوريات والمجلات العلمية المحكمة

1. أحمد البقالي، الأمن الإلكتروني - دراسة مقارنة مقال منشور ضمن مجلة العلوم القانونية، العدد 13، 2015.

2. الهاجري، هين محمد فدغم. "أهمية ودور الأمن السيبراني في تطوير الأمن الإلكتروني بدولة قطر." مجلة الباحث للدراسات والأبحاث القانونية والاقتصادية والعلوم الإنسانية والشرعية ع80 (2025).

3. سامر مؤيد عبد اللطيف الإرهاب الالكتروني وسبل مواجهته، مجلة كربلاء العلمية، المجلد 14، العدد 3، 2016.

4. الباسوسي، أحمد زكريا. الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة: حالات مختارة. مجلة كلية الاقتصاد والعلوم السياسية، مج24, ع4 ،(2023).

5. السيد، اماني محمد. أخبار تكنولوجيا المعلومات، المجلة الدولية لعلوم المكتبات والمعلومات، مج5, ع3 ، مصر، (2018).

6. السعبري، بهاء عدنان يحيى، و علي، شهد حمزة مير. تأثير التهديدات السيبرانية في الصراعات الإقليمية: نماذج مختارة. مجلة كلية التربية للبنات للعلوم الإنسانية، مج17, ع32 ، (2023).

7. جمال الدين، هبه، الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية، 24(1)،(2023).

8. نعمة، أحمد عبيس، و كلنتر، زهراء عماد محمد. تكييف الهجمات السيبرانية في ضوء القانون الدولي. مجلة الكوفة للعلوم القانونية والسياسية، مج13, ع44 ،(2020).

ثالثا: المراجع الأجنبية:

9. Ahn, G., Jang, J., Choi, S., & Shin, D.. Research on improving cyber resilience by integrating the Zero Trust security model with the MITRE ATT&CK matrix. IEEE,2024 12, 89291–89309. https://doi.org/10.1109/ACCESS.2024.3417182

10. Angyalos, Z., & Szilágyi, R. (2025). Cybersecurity Risks in Critical Infrastructures: Insights from CISA and ENISA Data. Journal of Agricultural Informatics, 16(2). https://doi.org/10.17700/jai.2025.16.2.759

11. International Energy Agency (IEA). (2024). Cyberattacks per week per energy organisation, 2020–2024. IEA. https://www.iea.org/data-and-statistics/charts/cyberattacks-per-week-per-energy-organisation-2020-2024?

12. International Telecommunication Union (ITU). (2025). Global Cybersecurity Index. ITU. https://data360.worldbank.org/en/dataset/ITU_GCI?

13. Taveras, Pedro (2019). Cyber Risk Management, Procedures and Considerations to Address the Threats of a Cyber Attack. In Proceedings of the ForenSecure: Cybersecurity and Forensics Conference, Chicago, Illinois April 12th.
14. World Bank. (2021). Global Cybersecurity Capacity Program: Lessons learned and recommendations towards strengthening the program. The World Bank. https://documents1.worldbank.org/curated/en/947551561459590661/pdf/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.pdf?
15. World Bank. (2021). Strengthening the cybersecurity of electricity grids. The World Bank. https://documents1.worldbank.org/curated/en/099615010242261655/pdf/P17037408f256f031091380ad6d77b64e8c.pdf?
16. World Bank. (2022). A review of the economic costs of cyber incidents. The World Bank. https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf
17. World Bank. (2023). The role of cybersecurity in economic performance. The World Bank. https://documents1.worldbank.org/curated/en/099092324164526526/pdf/P178769189c7360111ac1f1185e04824dec.pdf?
18. World Economic Forum. (2025). Global cybersecurity outlook 2025. World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf?
19. World Economic Forum. *Global Cybersecurity Outlook 2024*. Geneva: World Economic Forum, 2024. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/