وزارة التعليم العالي والبحث العلمي
المدرسة الوطنية العليا للعلوم السياسية
زدور محمد إبراهيم قاسم
قسم العلاقات الدولية

# أمن البنية التحتية الطاقوية في ظل التهديدات السيبرانية
# دراسة حالة إيران 2010_2025

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة الماستر في العلوم السياسية

تخصص : العلاقات الدولية

إعداد الطالبة :
فاطمة الزهراء جاب الله

تحت إشراف :
د. كلثوم بن دادة

لجنة المناقشة :

| | | |
|---|---|---|
| د. سامي كعبش | المدرسة الوطنية العليا للعلوم السياسية | رئيسا |
| د. كلثوم بن دادة | المدرسة الوطنية العليا للعلوم السياسية | مشرفة ومقررة |
| د. عامر ناصر | المدرسة الوطنية العليا للعلوم السياسية | مناقشا |

الموسم الجامعي : 2025 / 2026



﴿وَمَا تَوْفِيقِي إِلَّا بِاللَّهِ﴾

سورة هود، الآية 88.

# شكر وتقدير

**الحمد لله الذي وفقني وأعانني لإتمام هذا العمل .**

**أشكر عائلتي التي كانت الداعم الأول لي في مراحل إنجاز هذا العمل .**

**كما أتقدم بخالص الشكر والتقدير إلى أستاذتي المشرفة كلثوم بن دادة على ماقدمته لي من توجيه علمي ومتابعة مسؤولة كان لها أثر مباشر في إنجاح هذا العمل . كان أول بحث لي في رحاب هذه المدرسة في مقياس الفكر السياسي وكنت أنت من تدرسينني أنذاك مثلما قدمت لي أولى التوجيهات في مشواري الجامعي وشجعتني, شاءت الأقدار أن تكوني من يشرف على مذكرتي النهائية, سخرك الله لي وسط حيرتي وشتاتي, لك مني كل الحب والتقدير .**

**ولا أنسى الأستاذ عبد النور زيام الذي لاتكف الكلمات لوصف ما أكنه له من احترام, والأستاذ سامي كعبش والآنسة وردة الذين دعموني وساندوني في ظروفي الصعبة شكرا لكم من أعماق قلبي.**

**صديقاتي مروى, وصال, ميساء شكرا لكم على دعمكم الصادق, في لحظات الضغط خففتن عني الكثير بكلماتكن ووجودكن, ياخير من جمعتني بهم الأيام .**

**ابتسام وإيناس وكل من كان حضوره بسيطا لكنه ترك أثرا جميلا في تخفيف صعوبة الطريق ورسم لحظات من الطمأنينة وسط التعب**

**إليكم مني خالص الإمتنان والتقدير .**

# إهداء

**إلى من يشكلون جوهر حياتي ومعنى ثباتي في هذه الحياة**

**إلى أبي, مصدر فخري واعتزازي الدائم, الذي لم يكن مجرد والد, بل محارب صامت خاض العديد من صعوبات الحياة من أجل أن يمنحنا كرامة العيش وطمأنينة الغد.**

**إلى أمي, التي لا تكفي الكلمات لوصف ما قدمته من حب ورعاية وتضحيات لا تحصى, وكانت دائما القلب الذي يُبقي كل شيء متماسكا مهما اشتد التعب.**

**إلى أخي أحمد, السند الذي خفف عني الكثير وكان قريبا مني حين احتجتُ القوة لا الكلام.**

**إلى أختي مارية, بهجة البيت ونبضه البريء , التي لا تكتمل الأجواء دون حضورها.**

**أنتم السند الذي لا يميل مهما تغيرت الظروف, أنتم ملاذي الأول والأخير**

**هذا العمل هو اعتراف لي بفضلكم الذي لايرد .**

**ملخص الدراسة :**

شهد قطاع الطاقة في العقد الأخير تحولات كبيرة بفعل الرقمنة ماجعل بنيته التحتية تتبنى التقنيات المتقدمة في تسيير وإدارة عملياته لتتجاوز بهذا أنماط الحماية التقليدية, فبينما راكمت الدول خبرة واسعة في مواجهة التهديدات المادية كشفت الهجمات السيبرانية عن هشاشة جديدة, وذلك لقدرتها على اختراق الأنظمة الصناعية واحداث تعطيل وتخريب يفوق ماتخلفه العمليات الميدانية .

وتعد جمهورية إيران الإسلامية مثالا يُطرح كثيرا عند الحديث عن هذا التحول, إذ تعرضت لسلسلة هجمات إلكترونية متتابعة استهدفت منشآتها النووية والطاقوية, الأمر الذي طرح تحديات حول أمن المنظومة الطاقوية في البيئة الرقمية, وعليه تسعى هذه الدراسة إلى تحليل أثر التهديدات السيبرانية على أمن البنى التحتية الطاقوية مع إيران كدراسة حالة من 2010 إلى 2025 وتقييم جاهزية وفعالية استراتيجياتها السيبرانية في نظام دولي معقد. هذا واعتمدت الدراسة على المنهج الوصفي التحليلي ومنهج دراسة الحالة إلى جانب الاستعانة بالنظرية الواقعية(البنيوية) ونظرية الردع لفهم وتفسير أبعاد الظاهرة وتحليلها في سياقها الأمني والاستراتيجي .

**الكلمات المفتاحية :** أمن البنية التحتية الطاقوية, التهديدات السيبرانية, الأمن السيبراني, استراتيجية إيران .

**Abstract :**
The energy sector has undergone significant transformations over the past decade due to digitalization, which has led its infrastructure to adopt advanced technologies in the management and operation of its systems, moving beyond traditional security models. While states have accumulated extensive experience in dealing with physical threats, cyberattacks have revealed a new form of vulnerability due to their ability to penetrate industrial systems and cause disruption and sabotage that may exceed the impact of conventional physical operations.
The Islamic Republic of Iran is frequently cited as a relevant case in this transformation. It has been subjected to a series of successive cyberattacks targeting its nuclear and energy facilities, raising critical challenges regarding the security of energy infrustracture in the digital environment
Accordingly, this study aims to analyze the impact of cyber threats on the security of energy infrustructure, using Iran as a case study from 2010 to 2025, and to evaluate the readiness and effectiveness of its cybersecurity strategies within a complex international system. The study adopts the descriptive-analyse analytical method and the case study approach, in addition to relying on Structural Realism and Deterrence Theory to understand and interpret the dimensions of the phenomenon and analyzing it within its security and strategic context.
**Keywords :**
Energy Infrastructure Security, Cyber Threats, Cyber Security Iran Strategy

**خطة البحث:**

**مقدمة**

**الفصل الأول : الإطار النظري لأمن البنية التحتية الطاقوية في ظل التهديدات السيبرانية**

المبحث الأول : البنية التحتية الطاقوية المفهوم والأبعاد الاستراتيجية

المطلب الأول : تعريف البنية التحتية الطاقوية ومكوناتها

المطلب الثاني : الأهمية الاستراتيجية للبنية التحتية الطاقوية

المطلب الثالث : هشاشة البنية التحتية الطاقوية في عصر الرقمنة

المبحث الثاني : التهديدات السيبرانية وتأثيرها على البنية التحتية الطاقوية

المطلب الأول : الإطار المفاهيمي للأمن السيبراني

المطلب الثاني : طبيعة الهجمات السيبرانية التي تستهدف قطاع الطاقة

المطلب الثالث : التحول من التهديدات التقليدية إلى التهديدات السيبرانية

المبحث الثالث : ممارسات وسياسات حماية البنية الطاقوية

المطلب الأول : مبدأ حماية البنية التحتية الحيوية وتطبيقاته في الأجندة الحكومية

المطلب الثاني : أدوات وأساليب حماية البنية التحتية الطاقوية

**الفصل الثاني : التهديدات السيبرانية وأمن البنية التحتية الطاقوية الإيرانية**

المبحث الأول : ملامح البنية الطاقوية الإيرانية وأبعادها الاستراتيجية

المطلب الأول : قطاع النفط والغاز في إيران كأصل استراتيجي

المطلب الثاني : البنية النووية الطاقوية كأحد أبعاد الأمن القومي الإيراني

المطلب الثالث : التحول الرقمي في إدارة الطاقة الإيرانية

المبحث الثاني : تطور الهجمات السيبرانية التي استهدفت البنية الطاقوية الإيرانية

المطلب الأول : هجوم Stuxnet 2010 كنقطة تحول في المدركات الإيرانية

المطلب الثاني : هجمات سيبرانية لاحقة على قطاع الطاقة من 2010 إلى 2025

المطلب الثالث : الفاعلون و إشكالية اسناد الهجمات السيبرانية

المبحث الثالث : حماية البنية التحتية الإيرانية : المحددات وواقع الفعالية

المطلب الأول : الهيكل المؤسساتي لمجال الأمن السيبراني الإيراني

المطلب الثاني : الهيكل التشريعي لحماية البنية التحتية الحيوية الإيرانية

المطلب الثالث : تحليل واقع فعالية الحماية السيبرانية في القطاع الطاقوي الإيراني

**خاتمة**

# مقدمة

**مقدمة**

عايش النظام الدولي في العقود الأخيرة تحولات متزايدة نتيجة للثورة الرقمية التي طالت مختلف القطاعات الحيوية , أين تم اعتماد التقنيات المتقدمة في تسيير واستمرارية العمليات الأساسية, الأمر الذي جعل البنى التحتية لهذه القطاعات تنتقل إلى نمط جديد من الإدارة والتحكم بفضل الأتمتة الصناعية والبرامج المتطورة التي حلت محل الإنسان وزادت من الكفاءة الإنتاجية والتشغيلية . في المقابل أدى هذا التحول إلى بروز أنماط جديدة من التهديدات الأمنية التي لم تعد مقتصرة على الأساليب العسكرية التقليدية بل توسعت لتشمل التهديدات السيبرانية التي تستغل الترابط الشبكي بين البيئتين الفيزيائية والرقمية , واضعة بذلك تحديات أخرى أمام الدول حول كيفية حماية منظومتها الحيوية من مختلف التهديدات خصوصا وأنها ترتبط مباشرة بأمنها واستقرارها .

هذا ويعد قطاع الطاقة من أكثر القطاعات تأثرا بهذه التغيرات نظرا لمكانته الاستراتيجية ودوره في تزويد مختلف القطاعات الحيوية الأخرى بالطاقة اللازمة في أدائها لوظائفها واستمراريتها, ما زاد من تعرض بنيته التحتية للهجمات السيبرانية كنتيجة لاعتماده هو الآخر على الأنظمة المحدثة في إدارة منشآته وعملياته الصناعية .

وعلى إثر هذا بدأ الاهتمام الدولي بقضايا الأمن السيبراني يتزايد واعتبر أحد الأبعاد الأساسية المكملة للأمن القومي في العصر الحالي, بالنظر إلى حجم الخسائر التي تخلفها الهجمات الرقمية وصعوبة تحديد الجهات المسؤولة عنها وامتداد تأثيرها لباقي الميادين المرتبطة بالقطاع الطاقوي, إضافة إلى غموض الفواعل التي تقف وراء هذه التهديدات والذي سمح للدول بتطوير قدراتها التكنولوجية في هذا المجال واستخدامها كوسائل ضغط ونفوذ في تحقيق مصالحها الاستراتيجية دون خوض مواجهة مباشرة, وهو مانقل بيئة الصراع والتنافس الدولي إلى الفضاء الرقمي مازاد من تعقد المشهد الأمني .

ومنه تعد إيران من أبرز النماذج الدولية التي تعرضت بنيتها التحتية الحيوية للهجمات السيبرانية بالأخص تلك المنشآت الاستراتيجية المرتبطة بقطاع الطاقة منذ هجوم Stuxnet

عام 2010 واستمرار الهجمات بعده لتشمل باقي قطاعاتها الحيوية, ما دفعها لبناء وتطوير استراتيجيات وسياسات بهدف حماية بنيتها من التهديدات الرقمية المتزايدة .

# الإطار المنهجي

**المشكلة البحثية :**

أدى الاعتماد المتزايد على الأنظمة الرقمية والتقنيات المتقدمة في إدارة المنشآت الحيوية إلى تصاعد الهجمات السيبرانية على البنية التحتية الطاقوية, نظرا لأهميتها الإقتصادية والاستراتيجية والأمنية بالنسبة للكيانات السياسية .

وتمثل إيران أحد أكثر الدول تعرضا لهذا النوع من التهديدات منذ هجوم Stuxnet عام 2010 الذي استهدف منشآت حيوية ليوسع بعدها دائرة الهجمات وتشمل باقي القطاعات, ما كشف عن حجم التحديات التي يواجهها القطاع الطاقوي في ظل التحول الرقمي, الأمر الذي دفع بإيران إلى وضع استراتيجيات وتبني سياسات لتأمين منظومتها الطاقوية وتعزيز أمنها السيبراني في بيئة دولية غير مستقرة .

وانطلاقا من هذا تتمثل **إشكالية الدراسة** في ما يلي :

**كيف أثرت التهديدات السيبرانية على أمن البنية التحتية الطاقوية في إيران من 2010 إلى 2025 ؟**

**التساؤلات الفرعية :**

1) ما طبيعة التهديدات السيبرانية التي تستهدف البنى التحتية الطاقوية وماهي انعكاساتها على الأمن القومي ؟
2) كيف ساهم التطور التكنولوجي في تحويل الفضاء السيبراني إلى ساحة جديدة للصراع؟
3) ما هي الاستراتيجية التي اعتمدتها إيران لحماية بنيتها التحتية الطاقوية من التهديدات السيبرانية ؟

**الفرضيات :**

**1)** تشكل التهديدات السيبرانية الموجهة ضد البنى التحتية الطاقوية للدول خطرا على أمنها القومي وهذا كون قطاع الطاقة يرتبط بالقطاعات الحيوية الأخرى.

**2)** يؤدي التطور التكنولوجي والتحول إلى استخدام التقنيات الحديثة إلى جعل الفضاء الرقمي مجال جديد للصراع بين الدول مع تزايد استهداف البنى الاستراتيجية .

**3)** تدفع الهجمات المتكررة على منشآت إيران الحيوية إلى تطوير سياسات لتعزيز أمن بنيتها التحتية الطاقوية منذ بداية الهجمات في 2010 إلى يومنا هذا .

**مجالات الدراسة :**

يعد تحديد مجالات الدراسة أمرا ضروريا لأنها توضح الإطار الذي تتم من خلاله معالجة الموضوع, وتُقسم إلى :

**المجال الموضوعي :**

تتناول هذه الدراسة موضوع أمن البنية التحتية الطاقوية في ظل التهديدات السيبرانية, بالتركيز على طبيعة الهجمات الإلكترونية التي تستهدف المنشآت الطاقوية وانعكاساتها على الأمن الطاقوي خاصة والأمن القومي للدول عامة .

**المجال المكاني :**

ستركز الدراسة على الحالة الإيرانية باعتبارها نموذجا شهيرا لدولة تعرضت فيه بنيتها التحتية الطاقوية للعديد من الهجمات الرقمية خلال سنوات العقد الأخير, خاصة المنشآت الحيوية ذات الطابع الاستراتيجي كالمنشآت النووية ثم توسعت لتمس المنشآت المرتبطة بقطاعي النفط والغاز وغيرها .

**المجال الزماني :**

تم اختيار الفترة 2010_2025 نظرا لكونها فترة عرفت تصاعدا كبيرا في مستوى الهجمات السيبرانية وكذا التطور في الأساليب والتقنيات المستخدمة في الاستهداف خصوصا بعد هجوم Stuxnet الذي أثبت فرضية انتقال الصراع إلى الفضاء الرقمي , بالإضافة إلى أن إيران خلال هذه الفترة عملت على تطوير سياسات تتعلق بالأمن السيبراني خصوصا بعد تبني التقنيات الحديثة في القطاعات الحيوية .

**الأهمية العلمية :**

تتمثل أهمية هذه الدراسة في كونها تتناول موضوع حديث في مجال العلاقات الدولية يدمج بين عدة مجالات كالدراسات الأمنية, الأمن السيبراني, البنية التحتية الحيوية والأمن الطاقوي, فأغلب الدراسات الأكادمية تركز على دراسة الأمن الطاقوي في صورته التقليدية من خلال الحديث عن الأسواق, أمن النقل, خطوط الأنابيب و الاعتماد المتبادل بين الدول حول ضمان أمن الامدادات الطاقوية, أما هذه الدراسة فتخصصت في عنصر أمن الأصول المادية والرقمية التي تضمن الانتاج والنقل والتوزيع الآمن للطاقة في عصر التقدم التكنولوجي أين أصبحت كل العمليات الصناعية مؤتمتة ما يجعلها معرضة للتهديدات السيبرانية أكثر مما كانت عليه سابقا .

كما تزداد أهمية الدراسة بتركيزها على دولة إيران باعتبارها من أبرز الدول التي عانت من الهجمات السيبرانية على بنيتها التحتية الطاقوية, وهو أمر يساهم في إضافة أكاديمية للدراسات المتعلقة بالحروب السيبرانية والأمن الطاقوي, بالإضافة إلى الدراسات المتعلقة بابراز العلاقة بين التحول الرقمي والتقدم التكنولوجي و أمن البنى التحتية الحيوية .

**الأهمية العملية :**

وتكمن أهمية موضوع هذه الدراسة عمليا في كونها تجيب عن سؤال كيفية الاستفادة من منها واقعيا من خلال توضيح طبيعة التهديدات السيبرانية التي تستهدف المنظومة الطاقوية والآثار المترتبة عن ما قد تسببه من انعكاسات أمنية واقتصادية كارثية على الدول من خلال دراسة طبيعتها ووسائلها وأهدافها, وتساعد أيضا على تحليل السياسات الدولية التي استحدثت في مجال الأمن السيبراني وتطويرها بما يتوافق مع متطلبات العصر الرقمي للتصدي لمختلف أنواع التهديدات الالكترونية .

**الهدف من الدراسة :**

- ✓ توضيح العلاقة بين الأمن السيبراني وأمن البنية التحتية الطاقوية .
- ✓ تحليل طبيعة التهديدات السيبرانية التي تستهدف المنشآت الطاقوية الحيوية .

- ✓ ابراز تأثير التطور التكنولوجي والتحول الرقمي على أمن البنية التحتية الطاقوية .
- ✓ تحليل انعكاسات الهجمات الرقمية على أبعاد الأمن القومي .
- ✓ دراسة الاستراتيجيات والسياسات الدولية التي تم اعتمادها لحماية البنى التحتية الحيوية بالتركيز على الاستراتيجية الإيرانية .

**أسباب الدراسة :** وتقسم بدورها إلى :

**أسباب موضوعية :**

تم اختيار هذا الموضوع نظرا لكون القطاع الطاقوي يتمتع بأهمية استراتيجية جد كبيرة بالنسبة للدول وكونه يمثل أحد أكثر المرتكزات التي تبنى على اثرها أغلب الاستراتيجيات الأمنية بحكم ارتباطه بغيره من القطاعات الحيوية الأخرى من خلال تزويدها بالطاقة اللازمة لضمان استمرارية تشغيلها .

هذا ويشكل أي استهداف سواء كان للبيئة الفيزيائية أو البيئة الرقمية للبنية التحتية الطاقوية إلى انعكاسات على استقرار الدولة وأمنها بمختلف أبعاده نتيجة الترابط البنيوي بين القطاع الطاقوي وبقية القطاعات الحيوية .

بالإضافة إلى قلة الأبحاث الأكاديمية في موضوع أمن البنية التحتية الطاقوية من زاوية الأمن السيبراني, فجل الدراسات تركز على تحليل الأمن الطاقوي من المنظور التقليدي دون إدراج الفضاء الرقمي كأرضية جديدة للصراع .

**أسباب ذاتية :**

تم اختيار هذا الموضوع نظرا للاهتمام الكبير بالدراسات الأمنية والاستراتيجية الحديثة خاصة مواضيع الأمن السيبراني وأمن البنى التحتية التي تشكل عصب الدول الحيوي , إلى جانب تطوير القدرة التحليلية وفهم كيف يؤثر الانتقال إلى استخدام الأنظمة الرقمية في طبيعة الصراعات الحديثة, ومن خلال هذا جاءت الرغبة في اختيار موضوع يدمج بين أمن البنية التحتية الطاقوية والأمن السيبراني باعتبارهما من أكثر المواضيع التي تشهد اهتماما في ميدان العلاقات الدولية .

أما فيما يخص اختيار إيران كدراسة حالة, فالسبب يرجع إلى معرفة قدرات إيران في هذا المجال وكيفية تعاملها مع هذا النوع من التهديدات خصوصا وأنها تحت قيود دولية تحد من امكانيتها في تطوير بيئتها التقنية نظرا لتكلفتها الباهضة, إلا أنها استطاعت إيجاد حلول بديلة وأصبحت تصنف ضمن الدول الرائدة في مجال الأمن السيبراني .

**مناهج الدراسة :**

لانجاز أي دراسة علمية يجب على الباحث الاعتماد على مجموعة من المناهج التي تنظم أفكاره وتساعده في تحليلها وعرضها للوصول إلى النتائج المرجوة, ومنه اعتمدت هذه الدراسة على المناهج التالية

**المنهج الوصفي التحليلي :**

يعد من أهم المناهج البحثية إذ يقوم بدراسة الظاهرة كما هي في الواقع من خلال وصفها وصفا دقيقا والتعبير عنها كميا أو كيفيا وتحليل أبعادها المختلفة للوصول إلى تفسير علمي لأسبابها وحتى نتائجها ,وقد تم توظيفه في هذا الموضوع لدراسة طبيعة التهدديدات السيبرانية التي تستهدف البنى التحتية الطاقوية للدول, إضافة إلى تحليل العلاقة بين أمن الفضاء الرقمي وأمن المنشآت الحيوية, وكذا تحليل تبني القطاع الطاقوي للتقنيات الحديثة ومواكبة التطور التكنولوجي . من جهة أخرى ساعد هذا المنهج في توصيف القطاع الطاقوي الإيراني وتحليل تعرضه لهذا النوع من الهجمات, إلى جانب دراسة السياسات و الإجراءات التي اعتمدتها لتعزيز أمن بنيتها الطاقوية والحيوية ضد التهديدات السيبرانية. ويتجلى هذا المنهج البحثي في كل فصول الدراسة .

**منهج دراسة الحالة :**

والذي يقوم على جمع البيانات العلمية المتعلقة بأية وحدة كانت فردا أو مؤسسة أو دولة, من خلال التركيز على حالة محددة من تلك الوحدة أو جميع حالاتها وتحليل أبعادها المختلفة بهدف الوصول إلى العوامل المؤثرة والمتأثرة بالموضوع والكشف عن الارتباطات والعلاقات السببية بين أجزائها. وقد تم توظيف هذا المنهج في هذه الدراسة من خلال عرض الدولة

الإيرانية على أنها أحد أكثر الدول تعرضا للهجمات السيبرانية منذ عام 2010 وبعده وتحليل طبيعة التهديدات الرقمية وتطور أساليبها في استهداف منشآتها الحيوية, هذا وساعد في فهم استراتيجيات وسياسات إيران المعتمدة لتأمين منظومتها الطاقوية وتحليل نجاعتها في هذا الميدان.

**الدراسات السابقة :**

**الدراسة الأولى :**

عالجت مذكرة الماستر تخصص تكنولوجيا الاتصالات المعنونة ب **Cyber Security Incident Management in the Electrical Energy Sector : Involvment of Suppliers** ل Sara Waaler Eriksen و Sarmilan Gunabala شهر جوان من عام 2020 موضوع إدارة حوادث الأمن السيبراني في قطاع الكهرباء وركزت على دور الموردين في هذا المسار, حيث عالجت فكرة تطور القطاع تكنولوجيا واعتماده على أحدث الأنظمة التقنية ما ساعد من زيادة كفاءته إلا أنه سمح لنوع جديد من الهجمات في الظهور المتمثل في الاختراقات السيبرانية التي تستغل ترابط الأنظمة شبكيا . دعمت هذه الدراسة تحليلها من خلال مقابلاتها مع عدة شركات توزيع كهرباء في دولة النرويج وموردين وجهة تنظيمية في مجال الطاقة, كما حللت نتائجها وفق معيار ISC/IEC27035 لإدارة الحوادث لتصل في النهاية إلى استنتاج أن قطاع الكهرباء لا يُشرك الموردين في عملية بناء المخططات والاستراتيجيات رغم الاعتماد عليهم كثيرا في استمرارية العمليات الصناعية, وحتى الهجمات السيبرانية تجد مدخلا من خلالهم لاستهداف البنية التحتية لهذا القطاع ما يزيد من هشاشته التقنية. وقد ساعدت هذه الدراسة بحثنا في فهم الترابط البنيوي بين قطاع الطاقة والقطاعات الأخرى بالإضافة إلى بناء الإطار المفاهيمي المتعلق بالهجمات السيبرانية وإبراز العلاقة بين التحول الرقمي وزيادة سلسلة الهجمات السيبرانية على البنى التحتية الطاقوية .

**الدراسة الثانية :**

كما اعتمدنا أيضا على دراسة **تقييم مستوى جاهزية البنية التحتية الرقمية في مواجهة الهجمات السيبرانية** للدكتور عبد الرزاق فرح بن حليم والمنشورة ضمن المجلة الشاملة للدراسات الإنسانية والتربوية في 31 ديسمبر 2025, والتي عالجت موضوع مدى جاهزية المنظومة الرقمية في التصدي لهذا النوع المتطور من التهديدات بالتركيز على تغير بنية الهجمات الحديثة وأساليب الحماية التي تم اعتمادها لمواجهة المخاطر الالكترونية, هذا وتوصلت الدراسة إلى أن تزايد الهجمات السيبرانية وتطور أساليبها فرضا على الدول والمؤسسات تطوير استراتيجيات فعالة في الأمن السيبراني, وهذا ما استعانت به دراسنتا في الجانب المتعلق بالتهديدات السيبرانية التي تستهدف البنية التحتية الحيوية .

**الدراسة الثالثة :**

تقرير **Guide to Industrial Control Systems (ICS) Security** الصادر عن المعهد الوطني الأمريكي للمعايير والتكنولوجيا NIST عام 2023 ل Keith Stouffer وآخرون, والذي تناول موضوع أمن أنظمة التحكم الصناعية بمختلف أنواعها والمستخدمة في تشغيل وإدارة البنى التحتية الحيوية, حيث ركز التقرير على التهديدات التي تستهدف الأنظمة الرقمية وتستغل الثغرات الأمنية بالإضافة إلى آليات الحماية التقنية, وقد ساعدتنا معلومات هذه المادة العلمية في التعرف على المكونات التقنية للبنى التحتية وخاصية الترابط الشبكي الذي أضافها التطور التكنولوجي والتي سمحت باستهدافها رقميا إلى جانب سبل تعزيز الأمن السيبراني.

ساهمت هذه المواد العلمية دراستنا باثراءها بالمعلومات الأساسية, إلا أنها لم تتطرق له بشكل مباشر مثلها مثل باقي الدراسات الأخرى, كونها تتناول الأمن الطاقوي بصفته الشاملة ومن المنظور الكلاسيكي بالحديث عن الموارد المتجددة وغير المتجددة أهميتها وأهمية المعابر والنزاعات حولها وغيرها, وحتى الاسهامات في مجال الأمن السيبراني نجدها تقنية أكثر مما تربط الموضوع بالجانب الجيواستراتيجي, هذا بالإضافة لغياب نماذج للدول لتوضيح أثر الهجمات السيبرانية والسبل لمحاربتها, ما يجعل الطلبة لايعيرون اهتمامهم كثيرا بمثل هذه

المواضيع, لذلك سعت دراستنا إلى الدمج بين المجالين وتقديم تحليل وتفسير خارج المنظور الكلاسيكي.

**المقاربات النظرية :**

لتحليل وتفسير مختلف الظواهر السياسية يعتمد الباحث على جملة من المقاربات والنظريات وذلك لمساعدته في دراسة وفهم جميع أبعاد الظاهرة, ومنه اعتمدت هذه الدراسة على :

**النظرية الواقعية (الواقعية البنيوية) :**

في مثل هذه الظواهر تعد الواقعية البنيوية من أنسب النظريات التي طورها Kenneth Waltz لقدرتها على تفسير طبيعة الصراعات والتنافس والسعي الدائم لامتلاك الدول للقوة من أجل حماية مصالحها الحيوية, فهي ترى أن الدول هي الفاعل الرئيسي في العلاقات الدولية وأن الأمن من أولويات الأجندة الحكومية في بيئة دولية **فوضوية (Anarchy)** تغيب فيها سلطة عليا لتضبط الاستقرار بشكل كامل, الأمر الذي يدفع بالدول إلى تعظيم قوتها وتطوير قدراتها في مختلف الميادين العسكري, الاقتصادي, التكنولوجي والسيبراني للحفاظ على بقائها بالاعتماد على قدراتها الذاتية Self-Help .

وانطلاقا من فرضيات هذه النظرية يمكن فهم سبب اعتماد هذه الدراسة عليها, لأنها تساعد على تفسير الاهتمام المتزايد بحماية البنية التحتية الطاقوية لارتباطها بالأمن القومي ودورها في ضمان الاستقرار بكافة مستوياته, هذا وتفسر سعي الدول إلى تطوير قدراتها السيبرانية وذلك لتعزيز أمن منشآتها الحيوية في مواجهة التهديدات الإلكترونية المتزايدة, ومنه تمكن من فهم جهود إيران الرامية إلى تدعيم وحماية منظومتها الحيوية وخاصة الطاقوية كونها مرتبطة ارتباطا مباشرا بأمنها القومي وسيادتها الوطنية في ظل الصراع الجيوسياسي.

**نظرية الردع وتطبيقاتها في المجال السيبراني :**

في حقل العلاقات الدولية يعتمد الباحثون على نظرية الردع في الدراسات الاستراتيجية والأمنية, والتي تقوم على فرضية أساسية مفادها أن منع وتثبيط الخصوم من القيام بسلوكات عدائية يتحقق من خلال اقناعهم بأن تكلفة سلوكاتهم العدائية ستكون أعلى بكثير من المكاسب المتوقع تحقيقها منها, في بداياتها ارتبطت بالمجال العسكري التقليدي مع أحداث الحرب الباردة بين المعسكرين الغربي والشرقي. ويقوم الردع على قاعدتين **الردع بالعقاب** من خلال ردع الطرف المهاجم بتهديده في حال تنفيذه للهجوم ستكون التكلفة جد مرتفعة عليه لأنه لديه القدرة على رد الهجمة وبقوة ضعف التي لدى الجانب المبادر, **والردع بالمنع أوالحرمان** من خلال تقليل فرص نجاح الهجوم وذلك من خلال تعزيز وسائل الحماية والقدرات الدفاعية المتطورة أي القدرة على امتصاص الضربة. هذا الأمر دفع بالدول إلى التفكير مرارا قبل الإقدام على أية خطوة نظرا لتكافئ الفرص والإمكانيات لكل الأطراف وجعلهم يطورون من أساليبهم ليتفوقوا على بعضهم البعض, ومع تطور التكنولوجيا وبروز الفضاء الرقمي كأحد المجالات الجديدة للصراع, تم توسيع تطبيقات هذه النظرية لتشمل التهديدات السيبرانية, وأصبح الحديث يشمل الردع السيبراني الذي يرتبط مباشرة بحماية البنى التحتية الحيوية كونه يعتمد على تعزيز القدرات الدفاعية وتحسين أنظمة الكشف والاستجابة وتقليص نقاط الضعف التقنية التي يمكن أن تستغل أثناء الهجمات, إلا أن الخلل في هذا النوع يكمن في كونه يواجه صعوبة في تحديد الجهة المسؤولة عن الاستهدافات وعدد الفواعل المشاركين فيها وهو مايزيد من تعقيد عملية الردع السيبراني مقارنة بالردع التقليدي.

تم الاستعانة بهذه النظرية لفهم وتفسير السياسات الإيرانية في مجال الأمن السيبراني لحماية بنيتها التحتية الحيوية من خلال استحداث هياكل مؤسساتية وقانونية تهدف إلى تقليل احتمالات نجاح الهجمات الرقمية ورفع تكلفتها.

**الاقتراب المؤسسي :**

يركز الاقتراب المؤسسي على دراسة دور المؤسسات الرسمية في صياغة وتنفيذ السياسات العامة, وفي هذه الدراسة سمح بتحليل أدوار المؤسسات الإيرانية المعنية بالأمن السيبراني وحماية البنى التحتية الحيوية, كالمجلس الأعلى للفضاء السيبراني, الحرس الثوري, وكيفية عملها مع بعضها البعض في مواجهة التهديدات السيبرانية.

**صعوبات الدراسة :**

- ✓ أغلب الدراسات العربية التي تجمع بين الأمن السيبراني وأمن البنية التحتية الطاقوية لايمكن الوصول إليها بسبب خصوصية النشر.
- ✓ تشعب موضوع الدراسة وتداخله بين عدة مجالات : أمن الطاقة, الأمن السيبراني والعلاقات الدولية, بالإضافة إلى تداخل المفاهيم المرتبطة بموضوع الدراسة مثل الأمن الطاقوي وأمن البنية التحتية الحيوية و أمن البنية التحتية الطاقوية الأمر الذي أدى بالرجوع إلى مراجع متخصصة لفهمها وفهم العلاقة بينها وتحليلها .
- ✓ صعوبة الوصول إلى معلومات دقيقة وحديثة تتعلق بالبنية التحتية الطاقوية والأمن السيبراني بسبب الطابع الأمني الحساس بالإضافة إلى صعوبة تفسير بعض الأمور التقنية المتعلقة بالأنظمة الرقمية خصوصا وأنه مجال بعيد كل البعد عن اختصاصي.
- ✓ صعوبة الوصول إلى بعض الإحصائيات والمعطيات المتعلقة بالهجمات السيبرانية التي تعرضت لها المنشآت الإيرانية, وكذا سياساتها المعتمدة في مجال الأمن السيبراني مقارنة بالعديد من الدول, فإيران لاتنشر تقارير دورية بخصوص هذا المجال الذي تعتبره حساس .

**هيكلة الدراسة :**

من أجل معالجة إشكالية الدراسة والوصول إلى الأهداف المرجوة تم تقسيم العمل إلى مقدمة وفصلين وخاتمة.

في الفصل الفصل الأول والذي جاء بعنوان الإطار النظري لأمن البنية التحتية الطاقوية في ظل التهديدات السيبرانية, سيتم تناول مفهوم البنية التحتية الطاقوية : تعريفها وذكر مكوناتها وأهميتها الاستراتيجية بالإضافة إلى إبراز هشاشتها في عصر الرقمنة في المبحث الأول, أما في المبحث الثاني سننتقل للحديث عن تأثير التهديدات السيبرانية وتأثيرها على البنية التحتية الطاقوية من خلال مدخل إلى الأمن السيبراني وذكر طبيعة الهجمات السيبرانية التي تستهدف قطاع الطاقة مع مقارنة التهديدات التقليدية بالتهديدات الرقمية .

لننتقل بعدها إلى المبحث الثالث والذي يعرض ممارسات وسياسات حماية هذه البنية , بالتطرق في المطلب الأول إلى مبدأ حماية البنية التحتية الحيوية وتطبيقاته باستعراض استرايجيات أربع دول مختلفة وهي الولايات المتحدة الأمريكية, الاتحاد الأوروبي, بريطانيا وسنغافورة, ثم توضيح أدوات حماية البنية التحتية الطاقوية الفيزيائية والسيبرانية باعتبارها محور الدراسة .

أما في الفصل الثاني والمعنون بالتهديدات السيبرانية التي وأمن البنية الطاقوية الإيرانية, سيتم عرض إيران كدراسة حالة لأحد أكثر الدول تعرضا للمثل هذه التهديدات الجديدة من خلال ثلاث مباحث, حيث يتحدث المبحث الأول عن ملامح بنية قطاع الطاقة في إيران : قطاع النفط والغاز كأصل استراتيجي, البنية النووية كأحد أبعاد الأمن القومي الإيراني والتحول الرقمي في إدارة الطاقة الإيرانية. أما في المبحث الثاني سنستعرض أول هجوم على المنشآت الحيوية الإيرانية كنقطة تحول في المدركات الإيرانية والهجمات اللاحقة على مختلف القطاعات الأخرى من 2010 إلى 2025, ثم تحليل الفواعل وإشكالية اسناد الهجمات السيبرانية. ليتطرق بعدها المبحث الثالث إلى محددات حماية البنية التحتية الإيرانية وواقع فعاليتها من خلال عرض كل من الهيكل المؤسساتي والتشريعي في المجال الأمن السيبراني الإيراني وليحلل بعد هذا المطلب الثالث والأخير واقع فعالية الحماية السيبرانية في القطاع الطاقوي لإيران .

لتنتهي دراستنا بخاتمة عامة تلخص أهم النتائج المتوصل إليها.

# الفصل الأول

## الإطار النظري لأمن البنية التحتية الطاقوية

## في ظل التهديدات السيبرانية

**تمهيد الفصل :**

شهد القطاع الطاقوي في العقد الأخير تحولا متسارعا نحو أتمتة العمليات الصناعية بفضل تقدم الأنظمة التقنية, الأمر الذي زاد من تعقيد وتشابك البنية التحتية الطاقوية أكثر من ذي قبل, بحيث لم تعد ترتكز على المنظومة المادية, بل أصبحت تعتمد على برامج و أنظمة رقمية تتحكم في جميع مراحل الإنتاج والنقل والتوزيع, وهو الشيء الذي جعل من أهميتها الاستراتيجية تتزايد بالنسبة للدول .

ونتيجة لهذا التحول برزت التهديدات السيبرانية كتحدي يواجه سياسات الدول الحمائية أين تستغل ترابط الأنظمة التقنية لاستهداف البنى الحيوية وشل حركتها, ما يجعل من وضع برامج وخطط لتأمينها والعمل على تطوير مجال تقني هو الآخر لدراسة طبيعة هذه التهديدات وايجاد حلول لها أمرا ضروريا .

ومن خلال ما سبق, سنتطرق في هذا الفصل إلى الإطار النظري لأمن البنية التحتية الطاقوية في المبحث الأول بعرض تعريفها ومكوناتها المادية والتقنية, وكذلك أهميتها الاستراتيجية وهشاشتها في عصر الرقمنة, ثم ننتقل للمبحث الثاني الذي يدرس التهديدات السيبرانية والأمن السيبراني, لنصل في المبحث الثالث لعرض أبرز السياسات والبرامج الدولية المعتمدة في حماية هذه الأخيرة.

## المبحث الأول : البنية التحتية الطاقوية : المفهوم والأبعاد الاستراتيجية

تعتبر البنية التحتية الطاقوية من أهم مرتكزات عمل الدولة اليوم نظرا لدورها في تأمين وإنتاج ونقل وتوزيع الطاقة, ومع التطور التكنولوجي الذي يشهده هذا القطاع أصبح الحديث عن الأنظمة الرقمية لايقل أهمية عن المنشآت المادية كونها تدير وتتحكم في العمليات الصناعية, و عليه سيتناول هذا المبحث تعريف البنية التحتية الطاقوية و مكوناتها وعلاقتها بالأمن الطاقوي, ثم إبراز أهميتها الاستراتيجية وصولا إلى مظاهر هشاشتها التقنية في عصر الرقمنة

### المطلب الأول : تعريف البنية التحتية الطاقوية ومكوناتها

تُعتبر البنية التحتية الطاقوية من المداخيل الرئيسية لتحليل طبيعة القطاع الطاقوي و فهمه, خاصة في ظل تعقد مكوناته وتعدد عناصره بين ما هو مادي وتقني. لذلك وجب التطرق إلى تعريف هذه البنية وتحديد أهم مكوناتها باعتبارها الإطار الذي تقوم عليه مختلف الأنشطة الطاقوية.

#### أولا : تعريف البنية التحتية الطاقوية

يعرَّف الأمن الطاقوي على أنه إمكانية الوصول الموثوقة وبأسعار معقولة إلى جميع أنواع الوقود ومصادر الطاقة حسب الوكالة الدولية للطاقة, الأمر الذي يستدعي على الدول أن تَضمن استمرارية الإمدادات من خلال حمايتها وحماية المنظومة التي تُنتج وتَنقل وتُوزع الطاقة. وعليه تُعد البنية التحتية الحيوية هي مايربط هذه المنظومة المعقدة التي تُعد أساس البقاء اليوم, والتي تُشكِّل البنية التحتية الطاقوية أحد ركائزها في تشغيل باقي القطاعات الحيوية.

ترى **المملكة البريطانية** البنية التحتية الحيوية على أنها تلك العناصر الحيوية للبنية التحتية (أي الأصول والمرافق والأنظمة والشبكات والعمليات والعمال الأساسيين الذين يُشغِلونها

ويُسهِلونها, والتي قد يؤدي فقدانها أو تعرضها للخطر إلى التأثير بشكل كبير على تقديم الخدمات الأساسية و الأمن القومي أو الدفاع الوطني أو سير عمل الدولة).[1]

وتقسم إلى 13 قطاع : الطاقة النووية المدنية, المواد الكيميائية, الإتصالات, الدفاع , خدمات الطوارئ, التمويل, الغذاء, الفضاء, الحكومة, الصحة, الماء, النقل, **الطاقة** .[2]

وينص **قانون حماية البنى التحتية الحيوية** لعام 2001 **بالولايات المتحدة الأمريكية**, **(القانون العام رقم 107-56, المادة 1016)** على أن البنى التحتية الحيوية هي الأنظمة والأصول سواء كانت مادية أو افتراضية, والتي تُعتبر حيوية جدا للبلاد لدرجة أن عجزها أو تدميرها سيكون له تأثير مدمر على الأمن الإقتصادي الوطني أو الصحة العامة أو السلامة الوطنية أو أي مزيج من هذه الأمور.[3]

وتشمل 16 قطاع وهي : المواد الكيميائية, المرافق التجارية, الاتصالات, التصنيع الحرج , السدود, قاعدة الصناعات الدفاعية, خدمات الطوارئ, **الطاقة (الكهرباء النفط والغاز الطبيعي)**, الخدمات المالية, الغذاء والزراعة, المرافق الحكومية, الرعاية الصحية والصحة العامة, تكنولوجيا المعلومات, **المفاعلات النووية** والمواد والنفايات, أنظمة النقل, أنظمة المياه والصرف الصحي [4]

ومنه نقصد بالبنية التحتية الحيوية مجموعة الأصول المادية والرقمية والتي تُعد حيوية للدول بحيث أي تعطيل يطالها له تأثير مباشر على الأمن القومي للبلاد, هذا وتختلف قطاعاتها من دولة إلى أخرى, فالتصنيف يتعلق بطبيعة القطاع و مدى أهميته الاستراتيجية ومساهمته في تنمية البلاد .

---

[1] National Protective Security Authority (NPSA), Critical National Infrastructure, available at **www.npsa.gov.uk/about-npsa/critical-national-infrastructure** accessed March 19,2026

[2] Ibid

[3] Congressional Research Service, Critical Infrastructure: Emerging Trends and Policy Considerations for Congress, Report R48878 (Washington, DC: Congressional Research Service), available at **https://www.congress.gov/crs-product/R48878** accessed March 19 ,2026

[4] Ibid

في حين تجتمع كبرى مراكز البحث الدولية ووكالة الطاقة الدولية على أن البنية التحتية الطاقوية هي مجموع الأنظمة الرقمية والشبكات والأصول المادية كالمنشآت في قطاع النفط والغاز, محطات توليد الكهرباء, شبكات النقل والتوزيع والتي يؤدي أي تهديد فيها إلى التأثير على الإقصاد الوطني والإستقرار العام للبلاد .

**ثانيا : مكونات البنية التحتية الطاقوية**

تَرتكز البنية التحتية الطاقوية على ثلاث قطاعات رئيسية مختلفة التكوين وهي قطاع النفط والغاز, قطاع الكهرباء, قطاع الطاقة النووية . وتشمل مكونات مادية و أخرى تقنية

- **المكونات المادية** : وهي كالتالي :
  - **قطاع النفط والغاز** : ويتكون من

**أدوات (معدات) الحفر والاستكشاف:** أبراج الحفر, رؤوس الحفر, أجهزة المسح الجيوفزيائي والجيولوجي[1]

**آبار النفط:** فتحة البئر ( الرأسية/ المائلة), بطانة البئر ( أنابيب فولاذية تثبت بالإسمنت), الإسمنت(بين البطانة وجدران البئر لتثبيتها ومنع التسربات), الأنابيب الإنتاجية (تُركب داخل البطانة لتمرير النفط أو الغاز ), رأس البئر(يتكون من مجموعة من الصمامات والمعدات تتحكم في التدفق), صمام الشجرة (صمامات مثبتة فوق رأس البئر تتحكم في ضغط وتدفق السوائل ), مضخات الرفع الإصطناعي (بمختلف أنواعها), أجهزة المراقبة والإستشعار (تُزرع داخل البئر لقياس الضغط ودرجة الحرارة والتدفق )[2]

[1] خالد أبو الخير،" أبراج حفر آبار النفط: 5 مكونات أساسية لنجاح عمليات الحفر", في **https://petro-news.com/43138/** تاريخ الإطلاع (2026/03/21)

[2] محمد أبو الخير، "مكونات آبار النفط .. 8 عناصر أساسية من الحفر إلى الإنتاج", في **https://petro-news.com/112811/** تاريخ الإطلاع (2026/03/21)

**معدات النقل والتخزين:** أنابيب نقل النفط والغاز (خطوط الأنابيب برا), ناقلات النفط البحرية (للكميات الضخمة عالميا), السكك الحديدية, شاحنات النقل, وصهاريج التخزين الضخمة ذات السقف العائم و السقف الثابت .[1]

**مصافي النفط والمصانع (البتروكيماويات)** : معدات التكسير(الحراري/البخاري والتكسير التحفيزي), معدات تقنية لمعالجة المادة من الشوائب كالكبريت , أبراج التقطير العملاقة لفصل المكونات وأبراج التقطير لإنتاج الوقود (بنزين, ديزل, كيروسين....)[2]

- **قطاع الكهرباء** : ويشمل

**التوليد ومكوناته** : هو عملية انتاج الكهرباء من مصادر الطاقة المختلفة وتشمل (الوقود الأحفوري, الطاقة النووية, الطاقة المتجددة) ويشمل محطات توليد الكهرباء وهي عدة أنواع : محطات الطاقة التي تعمل بالفحم, بالغاز, بالطاقة النووية, بالرياح ...., والمولدات الضخمة التي تُوَّلِد طاقة ميكانيكية ويتم تحويلها إلى طاقة كهربائية .[3]

**مكونات النقل والشبكة** : يتم توصيل الكهرباء المولدة في محطات الطاقة بالشبكة الكهربائية. والشبكة عبارة عن شبكة واسعة من خطوط النقل والتوزيع التي تنقل الكهرباء إلى المكان المناسب, عبر خطوط النقل الهوائية (الأكثر شيوعا) والخطوط تحت الأرض (عادة في المناطق الحضرية) والكابلات البحرية (للنقل تحت البحر) إضافة إلى محولات رفع/خفض الجهد (القدرة) بمحطاتها الفرعية والتي تعمل كنقاط رئيسية لتنظم الجهد وتتحكم في الشبكة الكهربائية, وتُستخدم لتحويل الجهد إلى المستوى المناسب للنقل الفعال لمسافات طويلة[4].

---

[1]"مراحل تشغيل مصفاة النفط: من استقبال النفط الخام إلى إنتاج الوقود"،في **https://arasenergy.co/ar/blog/the-stages-of-an-oil-refinerys-operation/** تاريخ الإطلاع (2026/03/21)

[2]نفس المرجع

[3]"المكونات الرئيسية لنظام نقل الكهرباء",في **https://www.cn-delixi.com/ar/news/key-components-of-the-electrical-transmission-system** تاريخ الإطلاع (2026/03/21)

[4] نفس المرجع

**مكونات التوزيع** : محطات التحويل الفرعية (حلقة وسيطة في نقل وتوزيع الكهرباء ) من خلال إدارة مستويات الجهد, وضمان التشغيل الفعال والموثوق لنظام الطاقة الكهربائية. إضافة إلى لوحات التوزيع الرئيسية والفرعية والكابلات[1]

**معدات الحماية والتحكم:** يتم تجهيز محطات التوزيع بأجهزة حماية ومرحلات للكشف عن الأعطال الكهربائية والإستجابة لها, مثل الدوائر القصيرة أو الأحمال الزائدة, إضافة إلى أنظمة تحكم ومعدات مراقبة, للإشراف على أداء النظام الكهربائي. إلى جانب أنظمة التأريض لضمان السلامة وحماية المعدات من الصواعق والإضطرابات الكهربائية الأخرى.[2]

- **قطاع الطاقة النووية:** وتنقسم مكوناته إلى :
  - **مكونات الحلقة الأولية:**

**وعاء وقلب المفاعل** : يقع قلب المفاعل داخل وعاء المفاعل, وهو وعاء سميك من الصلب يحتوي على حزم أعمدة الوقود النووي وأعمدة التحكم والتبريد .

**مضخات تبريد المفاعل** : تعمل على ضمان استمرارية سريان المياه عبر الحلقة الأولية . وتقوم هذه المياه بإزالة الحرارة المتولدة ونقلها إلى قلب المفاعل.

**مولد البخار**: يقوم بتحويل المياه إلى بخار من خلال الحرارة.

**الضاغط** : يحافظ الضاغط على توازن المياه والبخار في الحلقة الأولية[3].

  - **مكونات الحلقة الثانوية :**

**التوربينات** : تحول طاقة البخار إلى طاقة ميكانيكية .

---

[1] نفس المرجع

[2] المكونات الرئيسية لنظام نقل الكهرباء, مرجع سابق

[3] "مكونات الحلقة الأولية في توليد الكهرباء بمحطة الطاقة النووية"،في https://www.enec.ae/ar/discover/how-nuclear-energy-works/how-does-a-nuclear-energy-plant-generate-electricity-/primary-loop-components/ تاريخ الإطلاع(2026/03/22)

**المولد:** يتصل عمود التوربين بالمُولِد وعندما يدور عمود التوربين يُولِد التيار الكهربائي الذي يُزوِد المنازل وكافة القطاعات الحيوية بالطاقة.

**المكثِف :** بعد خروج البخار من التوربين فإنه يدخل إلى المكثف حيث يتم تبريده وتحويله مرة أخرى إلى ماء, ويدور ذلك الماء عائدا إلى مولد البخار لتبدأ العملية مرة أخرى.

**التبريد النهائي :** محطات الطاقة النووية تتطلب وجود حوض تبريد متكامل والذي يعمل على امتصاص الحرارة الزائدة لضمان تبريد النظام بالكامل[1].

- **المواد والوقود (المكونات التشغيلية ) :**

**الوقود النووي :** اليورانيوم عالي التخصيب (نظير اليورانيوم U–235) والبلوتونيوم (نظير البلوتونيوم Pu–239 ) .

**المُبردات والمُهدئات :** وهي مفاعلات الماء الخفيف (الماء العادي) ومفاعلات الماء الثقيل لتهدئة سرعة النيوترونات ونقل الحرارة .[2]

هذه المكونات المختلفة لكل القطاعات التي تم ذكرها, سابقا كانت تدار بواسطة التحكم البشري المباشر, كل مايخص عملية المراقبة والاشراف والصيانة يقوم بها عمال مختصون وعند حدوث أعطال تكون فيزيائية لا غير مثل انقطاع الكهرباء , ارتفاع في درجة حرارة المفاعلات, يتم التحكم فيها واستعادة السيطرة عليها سريعا لأنها تكون واضحة وملاحظة بالعين المجردة .

هذا ولا تعتبر مجرد مكونات تساهم في العملية الانتاجية أو التوزيعية للطاقة, بل تجاوزته لتشكل أحد أكثر العناصر الحيوية التي تعتمد عليها الدول لتضمن استقرارها الداخلي وتفرض وجودها في المسرح الدولي, بحيث لايكفي امتلاك الموارد الهيدروكربونية أو الموارد البديلة كالطاقة النووية عاملا كافيا لتوضفه حسب ماتقتضيه مصالحها, فامتلاك بنية تحتية قوية

[1] نفس المرجع

[2] نفس المرجع

يساعدها على تحقيق ذلك, ونتيجة لهذا تتعرض لعدة هجمات بهدف تعطيلها والتأثير في أنظمة الدول .

ومنه برزت الحاجة إلى تطوير هذه الأخيرة لضمان استمرارية العمليات الصناعية وكذا حمايتها من التهديدات التي تستهدفها, لذلك عملت على إدراج تقنيات جديدة ترفع من كفائتها في هذا الميدان

- **المكونات التقنية للبنية التحتية الطاقوية :**

إلى جانب مكوناتها المادية ترتكز البنية التحتية للقطاعات الثلاث إلى منظومة تقنية تتمثل في :

- **أنظمة التحكم الصناعي Industrial Control System :** وهي مجموعة من الأنظمة التقنية المتكاملة والتي تستخدم عادة لمراقبة والتحكم وإدارة العمليات الصناعية, من خلال مزيج بين المكونات المادية والبرمجية للتحكم في الجوانب الفيزيائية للعملية كالضغط في خط الأنابيب, درجة حرارة في المفاعل الكيميائي, سرعة المحرك في خط الإنتاج .[1]

وتشمل :

- **نظم التحكم الإشرافي وجمع البيانات (SCADA) :** وهو نظام تحكم صناعي آلي يستخدم لجمع البيانات في نفس الوقت ومراقبتها عن بعد والتحكم فيها, ويتكون من المستشعرات والمشغلات التي تلتقط الإشارات الفيزيائية كالضغط , وأجهزة التحكم المنطقي القابلة للبرمجة (PLC) التي تحقق اكتساب متعدد للمعلومات والحكم المنطقي في البيئات البعيدة, وشبكة اتصالات لبناء طريق معلومات سريع بين الأجهزة, وواجهة

[1]“ Industrial Control Systems (ICS)”, available at https://www.fortinet.com/resources/cyberglossary/scada-and-scada-systems/ ,accessed March 23, 2026

المستخدم البشرية (HMI) الحديثة التي تظهر البيانات للمشغلين وتتيح لهم التحكم في الوضع الإنتاجي أينما كانو[1].

ففي قطاعي النفط والغاز يتم الإعتماد على أنظمة SCADA لمراقبة وإدارة الضغط والتدفق داخل خطوط الأنابيب عبر مسافات واسعة, ضمان النقل الآمن, أما في قطاع الكهرباء فتستخدم لإدارة شبكات النقل والتوزيع ومراقبة المحطات الفرعية لضمان استقرار الشبكة ومنع الإنقطاعات المتكررة . وفي قطاع الطاقة النووية يُعتمد عليها لمراقبة الغلايات والتوربينات والمولدات لضمان العمل السليم للمنشأة[2], وبهذا تكون أنظمة التحكم الصناعي (ICS) منسقا بين العمليات الفيزيائية وقرارات التحكم الآلي ما يجعلها عنصرا أساسيا في إدارة العمليات الطاقوية الحديثة .

- **أنظمة التحكم الموزعة Distributed Control System (DCS)** : نظام تحكم صناعي يدير عدة وحدات تحكم في العمليات الصناعية داخل منشأة واحدة, مصمم لتوزيع مهام المراقبة والتحكم في وحدات ميدانية مستقلة لكنها مترابطة شبكيا, ويتم الإشراف عليها بواسطة نظام تحكم واحد لزيادة الكفاءة واستمرارية تشغيلية عالية, يتكون من وحدات التحكم المسؤولة عن إدارة النظام بشكل عام, وحدات الإدخال والإخراج التي تجمع البيانات وتحولها إلى إشارات رقمية لنقلها للأجهزة, واجهة الإنسان والآلة (HMI) لمراقبة النظام والتحكم فيه, شبكات الاتصال التي تربط جميع المكونات وتسمح بتنسيق وتبادل المعلومات في الوقت نفسه[3].

[1]“ SCADA and SCADA Systems” , available at **https://www.fortinet.com/resources/cyberglossary/scada-and-scada-systems/** ,accessed March 23 , 2026

[2] "Industrial Control Systems (ICS) Security" , available at **https://searchinform.com/articles/cybersecurity/type/industrial-control-systems/** accessed April 1, 2026

[3]" DCS Security," available at **https://www.darktrace.com/cyber-ai-glossary/dcs-security** ,accessed April 1, 2026

في قطاع النفط والغاز, تستخدم لمراقبة والتحكم عن بعد في عمليات الحفر وعمليات تركيب الأنابيب وآلات التكرير, أما في قطاع الكهرباء فتستخدم في التحكم في التوربينات, وإدارة الوقود, والتحكم في الانبعاثات ونواتج الاحتراق.[1] أما في مجال الطاقة النووية فتستخدم للتحكم في درجة حرارة المفاعل, تسيير أنظمة التبريد, وأنظمة السلامة لتوليد الطاقة [2].

- **وحدات التحكم القابلة للبرمجة Programmable Logic Controller (PLC) :**

حواسيب رقمية صناعية تستخدم في كل من أنظمة DSC وخاصة أنظمة SCADA بوصفها مكونات التحكم ضمن نظام هرمي شامل . تستخدم ذاكرة قابلة للبرمجة لتخزين التعليمات داخليا ومصممة للتحكم في الآلات والعمليات, وذلك من خلال تنفيذ وظائف محددة كالتحكم في المدخلات والمخرجات, التوقيت, العد, المنطق, تتكون من وحدة المعالجة المركزية (CPU) التي تقوم بمعالجة البيانات وتنفيذ البرامج ووحدات الإدخال والإخراج (I/O) والتي تستقبل الإشارات من المستشعرات وترسلها إلى المحركات مثلا, ومصدر الطاقة الذي يوفر الطاقة اللازمة للعمل, وبرنامج البرمجة الذي ينشىء ويعدل منطق التحكم.[3]

وفي مجال الأتمتة الصناعية تكون مهمة نظام SCADA الإشراف والتحكم المركزي في الأجهزة المحلية مثل وحدات التحكم المنطقية القابلة للبرمجة(PLCs) التي تتحكم مباشرة في الآلات والعمليات[4] .

---

[1] " ماهو نظام التحكم الموزع (DCS) ", في https://decowellauto.com/ar/ما-هو-نظام-التحكم-الموزع/dcs- تاريخ الإطلاع (2026/04/02)

[2] Industrial Control Systems (ICS) Security, available at https://searchinform.com/articles/cybersecurity/type/industrial-control-systems/, acessed April 2, 2026

[3] What is a PLC? Programmable Logic Controller, available at https://inductiveautomation.com/resources/article/what-is-a-PLC accessed April 2, 2026

[4] "كيفية تواصل نظام SCADA مع وحدات التحكم المنطقية القابلة للبرمجة : تحويل البروتوكول وتوافق الواجهة", في https://www.come-star.com/ar/blog/how-scada-communicates-with-plcs/ تاريخ الإطلاع (2026/04/03)

- **الوحدات الطرفية البعيدة Remote Terminal Unit (RTU) :** هي جهاز إلكتروني قائم على معالج دقيق يُستخدم ضمن نظام التحكم الصناعي (ICS) لربط المكونات المادية بنظام التحكم الموزع (DCS) أو نظام الإشراف والتحكم وجمع البيانات (SCADA), تُثبت عادة في المواقع النائية لالتقاط بيانات القياس عن بعد وارسالها للأنظمة والأجهزة الأخرى لأداء مهامها ومراقبة الأجهزة الميدانية والتحكم فيها عن بعد كالصمامات والمشغلات, خصوصا في البيئات التي تتسم بظروف قاسية كالاهتزازات القوية, درجات الحرارة المرتفعة, الضغط العالي. تتكون من واجهة اتصال / معالج دقيق/ ذاكرة غير متطايرة / حساسات بيئية / حساسات تجاوز (Override Sensors) بروتوكولات الاتصال / منطق التحكم المدمج الذي يسمح بالتحكم الذاتي / ناقل (Bus)يُستخدم للتواصل مع الأجهزة أو بطاقات الواجهة[1].

إن كل من وحدات التحكم القابلة للبرمجة (PLCs) و الوحدات الطرفية البعيدة (RTUs) أحد الأجزاء الأساسية في العمليات الصناعية إلا أنهما يختلفان في مهامهما وبرمجتهما

فوحدات PLCs مصممة **للاستخدام المحلي وأتمتة العمليات داخل نطاق محدود** لذلك تتطلب اتصالات **سلكية** عالية السرعة, أما وحدات RTUs فمصممة **للمراقبة والتحكم عن بعد عبر مساحات واسعة** مايعني اعتمادها على اتصالات **لاسلكية** للتشغيل و التواصل مع الأجهزة التي تراقبها[2].

- **أنظمة التشغيل Operational Technology (OT) :** وهي الأجهزة والبرامج المسؤولة عن المراقبة والتحكم وإدارة العمليات الفيزيائية في المنشآت الطاقوية كالتحكم في شبكات النقل والتوزيع وإدارة أجهزة التحكم القابلة للبرمجة(PLC) , وتعد هي المعيار

[1]Rahul Awati, Remote Terminal Unit (RTU), available at https://www.techtarget.com/whatis/definition/remote-terminal-unit accessed 3 April, 2026

[2] Rahul Awati, "Remote Terminal Unit (RTU)," available at, https://www.techtarget.com/whatis/definition/remote-terminal-unit accessed April 3, 2026

في أنظمة التحكم الصناعي (ICS) بحيث تسعى لكي تعمل أنظمة التحكم الصناعي بشكل صحيح ولتحقيق متطلبات التوافر العالي للأجهزة ووقت تشغيلها .[1]

- **أنظمة المعلومات Information Technology (IT) :** وهي استخدام الأنظمة الإلكترونية وتقنيات الاتصال التفاعلية التي تُمكِن المؤسسات من تبادل البيانات وإدارتها بما في ذلك تخزين البيانات, معالجة المعاملات مما يسهل عمليات الأعمال ويعزز التعاون بين مختلف الكيانات الوظيفية دون التحكم المباشر في العمليات الفيزيائية. إذ تعالج بيانات العمليات التي تتحكم فيها أنظمة التحكم الصناعي و تقدم معلومات للمستخدمين[2].

وفي مجال الأتمتة تعمل أنظمة التحكم الصناعي (ICS) **كحلقة وصل** بين أنظمة التشغيل (OT) و أنظمة المعلومات (IT) , إذ تستخدم لإدارة ومراقبة العمليات الفيزيائية في الوقت الفعلي بينما تتصل بالأنظمة المعلوماتية لتحلل البيانات وتتنبأ بالأعطال و تحسن كفاءة التشغيل, هذا الترابط والتشابك بين الأنظمة الرقمية جعل من السهل اختراقها إلكترونيا وتعطيلها .

يتضح من خلال عرض المكونات التقنية للقطاعات الثلاث أن هيكلة البنى الطاقوية لم تعد تشمل فقط مكونات مادية كما كانت في السابق, بل أصبحت تعتمد على أنظمة تقنية جد متطورة تدير مختلف العمليات الصناعية, رفعت من مستوى الكفاءة والفعالية الإنتاجية والتشغيلية وزادت من أهميتها الاستراتيجية في استمرارية بقية القطاعات الحيوية الأخرى, إلا أن هذا جعلها عرضة لمختلف أنواع التهديدات .

[1]" What is OT Security? An Operational Technology Security Primer", available at **https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security** accessed April 3, 2026

[2] "Information Technology", availabale at **https://www.sciencedirect.com/topics/computer-science/information-technology** accessed April 4, 2026

## المطلب الثاني : الأهمية الاستراتيجية للبنية التحتية الطاقوية

تكتسي البنية التحتية الطاقوية أهمية كبيرة في الوقت الحالي نظرا لدورها المحوري في ضمان استمرارية تزويد مختلف القطاعات بالطاقة, ومع تزايد الاعتماد عليها أصبحت تمثل عنصرا استراتيجيا يرتبط بالأمن والاستقرار عبر مختلف المستويات .

تعتبر البنية التحتية الطاقوية الركيزة الأساسية التي تقوم عليها الدول, بحيث لم تعد مجرد منظومة مادية لإنتاج ونقل وتوزيع الطاقة, بل تحولت إلى فضاء استراتيجي متعدد الأبعاد تتقاطع فيه اعتبارات الأمن القومي والاقتصادي وحتى السيبراني. إذ أن تدفق الكهرباء والوقود بشكل مستمر يمثل شرطا ضروريا لعمل مؤسسات وهياكل الدولة, من القطاع العسكري إلى القطاع القطاع الصحي والخدماتي, مايجعل أي اضطراب فيها يهدد الاستقرار بكافة مستوياته[1] .

حيث أظهرت العديد من الحالات ذلك على سبيل المثال : انقطاع الكهرباء في الولايات المتحدة الأمريكية عام 2003 المعروف ب Nourtheast Blackout of 2003 إذ أوضح أن مجرد عطل في نظام الإنذار بمحطة الكهرباء في أوهايو خلق أزمة اقتصادية وأمنية تمددت على نطاق واسع شرق البلاد وأجزاء من كندا (أونتاريو) فخلال 3 دقائق فقط توقفت 21 محطة كهرباء وعدة مطارات عن العمل, كما تعطلت أنظمة المياه وتأثر 50 مليون شخص لأكثر من يوم وقدرت الخسائر بنحو 6 مليارات دولار .كل هذا بسبب ما يعرف بالترابط البنيوي بين قطاع الطاقة وبقية القطاعات الحيوية الأخرى مايجعل الإهتمام به شرطا أساسيا.[2]

إضافة إلى هذا التحول الرقمي لأنظمة الطاقة وأتمتتها, خاصة اعتمادها على أنظمة التحكم الصناعية (ICS/SCADA /DCS..) الذي أضاف بُعدا جديدا في معادلة أمننتها وهو

[1] International Energy Agency, World Energy Outlook 2023 (Paris: International Energy Agency, 2023)

[2]" Northeastern Blackout of 2003",available at https://www.ebsco.com/research-starters/power-and-energy/northeastern-blackout-2003 accessed April 5, 2026

هشاشتها السيبرانية .[1] فالهجمات لم تعد تقتصر على التخريب المادي كتفجير المنشآت بل تجاوزته لتستهدف البنية الرقمية التي تدير الشبكات الكهربائية وخطوط الأنابيب ومحطات التوليد وغيرها عبر شن هجمات إلكترونية تتميز بسرعة الأداء وتحقيق الأهداف دون مجهود وانخفاض التكلفة, وشكلت العديد من الهجمات كالهجوم على شبكة الكهرباء الأوكرانية (Ukraine Pwer grid hack) هذا التجاوز , حيث أدى اختراق أنظمة التحكم عبر برامج خبيثة لثلاث شركات توزيع الطاقة إلى انقطاع التيار في ديسمبر 2015 عن مئات الآلاف من المواطنين في مناطق غربي البلاد في إطار توتر الأوضاع بين روسيا وأوكرانيا, وأوضحت هذه الحالة أن تعطيل الطاقة يمكن أن يستخدم كأداة ضغط سياسي ضمن أنماط الصراع الهجين والذي تفرض من خلاله الدول وجودها وقوتها وقدرتها على التأثير دون اللجوء إلى مواجهة عسكرية مباشرة .[2] هذا ما طرح تساؤلات عن كيفية ليس فقط حماية البنى التحتية الطاقوية من الهجمات السيبرانية وإنما القدرة على التصدي والإستجابة لها .

أما على الصعيد الاقتصادي فيؤدي أي تعطيل مهما كان نوعه إلى توقف الإنتاج الصناعي, حدوث اختلالات واضطرابات في سلاسل الإمداد والتوزيع وارتفاع تكاليف النقل وتزايد معدلات التضخم.[3] بحيث برزت هشاشة الترابط بين قطاعي الطاقة والإقتصاد خلال أزمة الطاقة العالمية 2021– 2022 global energy crisis أين انعكس اضطراب

[1] "Industrial Control Systems (ICS) Security" , available at https://searchinform.com/articles/cybersecurity/type/industrial-control-systems/ acessed April 5, 2026

[2] Cybersecurity and Infrastructure Security Agency (CISA). “Cyber Attack against Ukrainian Critical Infrastructure”, available at https://share.google/euDWSgi8oUHWvDMxZ accessed April 6, 2026

[3] Chloe Williment, “How Will The Energy Crisis Affect Global Supply Chains? ” , available at https://supplychaindigital.com/news/how-will-the-energy-crisis-affect-global-supply-chains accessed April 6, 2026

الإمدادات(إمدادات النفط والغاز) على الأسعار والنمو والاستقرار الإجتماعي في العديد من الدول خاصة الأوروبية أثناء جائحة كوفيد 19 وبعد الإجتياح الروسي لأوكرانيا .[1]

وجيوسياسيا يتجاوز الحديث عن أهمية ومكانة البنية التحتية الطاقوية مسألة تأمين الإمدادات لتصبح أداة تأثير في السياسة الدولية من خلال إعادة تشكيل ميزان القوة ويتجلى هذا من خلال التنافس بين الفواعل الدولية حول مسارات نقل الطاقة, خصوصا خطوط الأنابيب التي لا تعتبر وسيلة لنقل الموارد وإنما ورقة ضغط يتم التحكم عبرها في تدفقات الطاقة أو حتى توجيهها بما يتوافق مع أهداف الدول الاستراتيجية.[2]

وعليه فالأهمية الاستراتيجية للبنية التحتية الطاقوية تكمن في كونها حلقة تربط بين القوة الاقتصادية والسيادة السياسية والقدرة الردعية للدول في المجال السيبراني, فكلما كانت هذه البنية مؤمنة ماديا ورقميا وقائمة على تنويع ووفرة المصادر , ازدادت قدرة الدولة على امتصاص الصدمات وتقليل تعرضها للضغط أو الابتزاز الخارجي في بيئة دولية تتسم بالصراع والتعقيد.

## المطلب الثالث: هشاشة البنية التحتية الطاقوية في عصر الرقمنة

بعد أن كانت البنية التحتية الطاقوية تعتمد على الأنظمة الميكانيكية المغلقة ذات التدخل البشري المباشر والعزل الفيزيائي, أصبحت تتبنى تقنيات الرقمنة التي أصبحت مسؤولة عن كل جوانب العمليات الصناعية من خلال دمج الأنظمة الرقمية المعلوماتية والتشغيلية. إلا أن هذا التطور التكنولوجي خلق تحديات جعلت من المنظومة الطاقوية منكشفة على التهديدات والمخاطر الإلكترونية, وعليه سيتم التطرق في هذا المطلب إلى تعريف الرقمنة وتطبيقاتها في قطاع الطاقة, دمج أنظمة التشغيل مع أنظمة المعلومات وكيف أدى هذا إلى توسع سطح الهجوم.

---

[1] International Energy Agency (IEA), "2022 Energy Crisis The crises and global responses,"available **at** https://www.iea.org/topics/2022-energy-crisis accessed April 7, 2026

[2] Sahnoune Nor El Imen, "The Strategic Importance of Pipelines between Geopolitics and Cooperation Opportunities", ***Journal of Comprehensive Security and Strategic Affairs*** (1), no (3) (July 2024) ,pp 61–62.

تُعرف الرقمنة على أنها الاستعمال والاعتماد المتزايد لتكنولوجيا المعلومات والاتصالات عبر كافة القطاعات أين يزيد التفاعل بين العالم الرقمي والعالم المادي, و يتكون العالم الرقمي من البيانات والتحليلات ( استخدام البيانات لإنتاج معلومات ) والاتصال ( تبادل البيانات بين الإنسان والأجهزة والأجهزة فيما بينها ) والحديث عن تطور الرقمنة يكون بالاستثمار في هذه العناصر الثلاث .[1]

وقد كان قطاع الطاقة من أوائل القطاعات التي تبنت هذا النهج ففي سبعينات القرن الماضي استخدمتها شركات الكهرباء لتسهيل مراقبة أسواق الكهرباء والتحكم فيها في الوقت الفعلي عبر مناطق جغرافية واسعة, إلى جانب تحسين كفاءة التشغيل والصيانة, كما اعتمدت شركات النفط والغاز منذ فترة طويلة على التقنيات الرقمية لنمذجة أصول الإستكشاف والإنتاج بما في ذلك المكامن والأنابيب.[2]

فصناعة النفط والغاز اليوم أصبحت تعتمد على أحدث التكنولوجيات, إذ يمكن تشغيل معدات الحفر في أعماق البحار تصل إلى 3000 متر تحت البحر و الوصول إلى مكامن بعيدة قبل أعوام كانت شبه مستحيلة, كذلك في قطاع المنبع الذي يعد العنصر الأكثر ربحية في منظومة النفط والغاز, حيث يعالج بيانات ضخمة كالمسوحات الزلزالية والتي تتطلب أحدث الحواسيب لاتمام عملية المعالجة. إضافة إلى استخدام أجهزة الاستشعار المصغرة وأجهزة استشعار الألياف البصرية في نظام الإنتاج من أجل مثلا : زيادة الإنتاج وقياس الأداء البيئي كالكفاءة أو كثافة الانبعاثات, كذلك استخدام الطائرات المسيرة لتفقد خطوط الأنابيب البعيدة. هذا ويساعد أيضا اعتماد التقنيات الرقمية المتقدمة حسب وكالة الطاقة الدولية في خفض تكاليف الإنتاج حوالي 10−20% ومن جهة أخرى كشف وقياس انبعاثات الميثان[3].

ونظرا للتطور المستمر وتشابك الأنظمة الرقمية داخل القطاع الطاقوي تم دمج أنظمة التشغيل (OT) بما في ذلك أنظمة التحكم الصناعي المخصصة للتحكم في العمليات الفيزيائية

[1]International Energy Agency, "Digitalization and Energy," Paris2017 , p 22
[2] Ibid p 16-25
[3] Ibid p 67-73

كتشغيل المضخات ومراقبة الضغط داخل خطوط الأنابيب مع أنظمة المعلومات (IT) والمسؤولة عن جمع البيانات وتحليلها وإدارتها, لتقديم نسخ أفضل من المخرجات من حيث التكاليف والكفاءة وتمكين التحليل اللحظي للبيانات وإدارة الأصول بشكل أفضل, إلا أن هذا الدمج كشف عن خلل تقني وتحدي أمني في نفس الوقت وهو هشاشة البنية التحتية الطاقوية من خلال **تقليص العزل الشبكي** الذي كانت تعرف به الأنظمة التشغيلية عند تعرضها للأخطار, أين تستمر العمليات الصناعية دون أضرار بالغة, وبعد ربطها بأنظمة المعلومات أصبحت متصلة بشبكات أوسع ما زاد من نطاق التعرض للهجمات الإلكترونية أكثر من ذي قبل, وجعل أي هجوم يستهدف البيئة المعلوماتية يؤثر مباشرة في البيئة التشغيلية ويخلف خسائر مكلفة تمتد آثارها لبقية القطاعات .[1]

ويعد هجوم Colonial Pipeline ransomware attack عام 2021 أحد أبرز الأمثلة على هذه الهشاشة حيث تعد شركة Colonial Pipeline حجر الزاوية في نظام توزيع الطاقة شمال الولايات المتحدة الأمريكية عبر 13 ولاية, إذ تم اختراق شبكة أنظمة المعلومات (IT) الخاصة بهذه الشركة من قبل مجموعة قرصنة عبر حساب VPN غير محمي بمصادقة متعددة العوامل(MFA) , الهجوم في البداية استهدف **البنية المعلوماتية** لكن لاحقا قررت الشركة إيقاف **العمليات التشغيلية** (OT) نظرا لتداخلهما مع بعض ما أدى إلى تعطيل 45% من سلسلة إمداد الوقود على الساحل الشرقي, ونتيجة لهذا تأثر ما يقارب 50 مليون مستهلك في 13 ولاية. وانخفضت مستويات الوقود إلى حد كبير في عدة ولايات مع وصول نسبة نفاد المحطات في: جورجيا 71% كارولاينا الجنوبية 68% كارولاينا الشمالية 72%, وفيرجينيا 53%. وكانت التداعيات الإقتصادية كبيرة إذ بلغت الخسائر التشغيلية المباشرة 8.46 مليون دولار يوميا, بينما أدت اضطرابات سلسلة الإمداد إلى تكاليف إضافية بقيمة 27.2 مليون

[1] Keith Stouffer et al,.*Guide to Industrial Control Systems (ICS)*, NIST Publication 800-82 Rev 2 (Gaithersburg ,MD : National Institute of Standards and Technology , 2023 ) ,p 2-14

دولار يوميا, وبلغت تكاليف التدابير الطارئة 15.7 مليون دولار شملت نشر وسائل نقل بديلة وحلول تخزين طارئة ما يؤكد هشاشة المنظومة الطاقوية في ظل الرقمنة [1]

وختاما بالرغم من إيجابيات التطور الرقمي وما وفره من فعالية في تسيير قطاع الطاقة, كشف بالمقابل عن ثغرات قلصت العزل الذي كان بين أنظمة التشغيل وأنظمة المعلومات, ما زاد من تعرض البنية التحتية الطاقوية للتهديدات السيبرانية التي تستغل نقاط الضعف تلك سيبرانيا, الأمر الذي جعل من الضرورة البحث عن آليات لضمان استقرار وسلامة منظومتها المادية والتقنية بتطوير مجال البحث والتعليم في الأمن السيبراني .

[1]Srikanth Bellamkonda, "Ransomware Attacks on Critical Infrastructure: A Study of the Colonial Pipeline Incident," **International Journal of Research in Computer Applications and Information Technology** (7), no.( 2) (December 2024) pp 1423-1433.

## المبحث الثاني : التهديدات السيبرانية وتأثيرها على النبية التحتية الطاقوية

مع التطور التكنولوجي واعتماد البنية التحتية الطاقوية على الأنظمة التقنية لم تعد التهديدات التي تتعرض لها تتلخص في شكلها المادي, إذ ظهر نوع جديد من التهديدات يرتبط بالفضاء الرقمي ويستهدف المنظومة التقنية التي تدير العمليات الفيزيائية, فكان من الضروري استحداث تقنيات لحماية هذه البنى وهو ما يعرف بالأمن السيبراني الذي يُعنى بفهم طبيعة الهجمات الإلكترونية وكيفية عملها ومواجهتها. لذلك سيتطرق هذا المبحث إلى الإطار المفاهيمي للأمن السيبراني وطبيعة الهجمات الرقمية التي تستهدف القطاع الطاقوي لينتهي بمقارنة بين التهديدات التقليدية والتهديدات السيبرانية .

### المطلب الأول : الإطار المفاهيمي للأمن السيبراني

في عصر التقدم التكنولوجي أصبحت حماية الفضاء الرقمي شرطا أساسيا لاستمرار تشغيل أنظمة الدولة الحيوية ومؤسساتها وعلى إثر هذا تم إدراجه كأحد أبعاد الأمن القومي الذي يختص بتأمين البيئة الوطنية من كافة التهديدات السيبرانية .

قبل التطرق إلى تعريف الأمن السيبراني وجب الحديث عن أصل كلمة سيبراني :

- كلمة سايبر ( Cyber) يونانية الأصل وترجع إلى مصطلح (kybernetes) , الذي ورد بداية في مؤلفات الخيال العلمي ويعني القيادة أو التحكم عن بعد[1].
- والسيبرانية في قاموس (المورد) هي علم الضبط ومصدرها (Cybernetics) , وهو مصدر يتطابق مع مفهوم الأمن السيبراني أي ضبط الأشياء عن بعد والسيطرة عليها.

[1] قانصو, مرجع سابق ص 42

ويعد عالم الرياضيات نوربرت وينر Norbert Winer أول من استخدم مصطلح السيبرانية عام 1948 أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان, فضلا عن حقل الهندسة الميكانيكية [1].

أما اصطلاحا فنجد العديد من الكلمات المشتقة منها : كالأمن السيبراني, الهجمات السيبرانية, التهديدات السيبرانية....إلخ[2]

**أولا : تعريف الأمن السيبراني :**

**حسب المعهد الوطني للمعايير والتكنولوجيا الأمريكي (NIST)** هو القدرة على حماية استخدام الفضاء الإلكتروني أو الدفاع عنه ضد الهجمات الإلكترونية[3].

**ويراه الإتحاد الاوروبي** على أنه الأنشطة اللازمة لحماية أنظمة الشبكات والمعلومات ومستخدمي هذه الأنظمة, والأشخاص الآخرين المتضررين من التهديدات السيبرانية.[4]

**أما المركز الوطني للأمن السيبراني بالمملكة البريطانية المتحدة** فيقصد به مساعدة الأفراد والمؤسسات على تقليل مخاطر وتأثير الهجمات السيبرانية. إذ تتمثل وظيفته الأساسية في حماية الخدمات والأجهزة الرقمية التي تعتمد عليها هذه المؤسسات من التهديدات الإلكترونية, بما في ذلك حماية كميات هائلة من البيانات والمعلومات الشخصية المخزنة محليا أو في السحابة. كما يضمن الأمن السيبراني إمكانية نشر التقنيات المبتكرة والناشئة (مثل الذكاء الاصطناعي) بطريقة آمنة, حتى يتسنى الإستفادة الكاملة من الفرص التي تتيحها.[5]

---

[1] نفس المرجع ص 43

[2] نفس المرجع ص 43

[3] Cybersecurity Research Center, “Cybersecurity Glossary,” available at ,**https://csrc.nist.gov/glossary/term/cybersecurity** accessed April 8, 2026

[4]European Parliament and Council of the European Union," Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union "(NIS2 Directive), Official Journal of the European Union L 333 (December 27, 2022), Art. 6(1), available at **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555** accessed March 29, 2026

[5]National Cyber Security Centre (NCSC), “What Is Cyber Security?,”available at,

وعليه يشير الأمن السيبراني إلى مجموعة السياسات والإجراءات والتدابير والتقنيات التي تهدف إلى حماية الأصول الرقمي , ومنع التهديدات الإلكترونية وضمان سرية البيانات وسلامتها وتوافرها بشكل مستمر.

إذ أصبح اليوم أحد الأبعاد الاستراتيجية للأمن القومي في ظل التحول الرقمي الذي طال موسسات الدولة وقطاعاتها, بحيث لم تعد الهجمات السيبرانية مجرد حوادث تقنية سرعان مايمكن تجاوزها بل تحولت إلى أدوات ووسائل ضغط جيوسياسية قادرة على تهديد سيادة الدول واستقرارها, ومنه أدرج الفضاء السيبراني في أجندة الدولة المعاصرة وبات جزءا لا يتجزأ من منظومتها الأمنية.

**ثانيا :** في مجال الأمن السيبراني لاطالما كان الحديث عن حماية وأمن التكنولوجيا التشغيلية(الأنظمة الصناعية), أمن البيانات, أمن الشبكات, أمن السحابة, أمن إنترنت الأشياء, أمن إدارة الهوية والأصول. وهم بيئات مختلفة مكملة لبعضها البعض, إذ أن هناك هجمات تستهدف كل عنصر من عناصر هذه الأجهزة ما يجعلنا ملزمين بتوضيحها :

- **أمن الأنظمة الصناعية Operational Technology (OT) security** يشير إلى التدابير والتقنيات المستخدمة لحماية أنظمة التكنولوجيا التشغيلية من الهجمات الإلكترونية. ويشمل هذا أنظمة التحكم الإشرافي وجمع البيانات SCADA وأجهزة التحكم المنطقي القابلة للبرمجة (PLCs) وأنظمة التحكم الموزعة (DCS) وغيرها من الأنظمة التي تدير العمليات الصناعية[1].
- **الأمن المعلوماتي Information security (InfoSec) :** يقصد به الإجراءات والممارسات التي تستخدم لحماية البيانات الرقمية من الوصول أو التعديلات غير

https://www.ncsc.gov.uk/section/information-for/individuals-families accessed March 29 ,2026

[1] Matthew Finio, Amanda Downie, and Nick Douglas, “What Is OT Security?”, available at https://www.ibm.com/think/topics/ot-security accessed April 9, 2026,

المصرح بها أو التعطيل أو التدمير أو السرقة. أي أن تطبيقات الأمن السيبراني تختلف باختلاف البيئة المستهدفة [1].

- **أمن الشبكات Network security:** نعني به إجراءات حماية شبكات الكمبيوتر وأنظمة الإتصالات الداخلية والخارجية التي تتبادل المعلومات و الموارد من أي تهديد[2]
- **أمن السحابة cloud security:** ويقصد به تقنيات حماية مايتم تخزينه وتشغيله عبر الإنترنت, والتي تحتاجها المؤسسات لحمايتها من التهديدات الداخلية والخارجية[3].
- **أمن إنترنت الأشياء Securing the Internet of Things (IoT) :** مخصص لحماية الأجهزة المادية المزودة بحساسات أو برمجيات يمكن من خلالها الإتصال بالإنترنت وإرسال واستقبال البيانات والمعلومات تلقائيا[4].
- **إدارة الهوية والوصول (IAM) :** ممارسات تستخدم لتوفير وحماية الهويات الرقمية وصلاحيات وصول المستخدمين ضمن نظام تكنولوجيا المعلومات. كما تساعد على ضمان الوصول الآمن للموارد المناسبة وفي الوقت المناسب.[5]

وعليه يعد الأمن السيبراني نتيجة حتمية لتطور وتوسع استخدام التقنيات الرقمية عبر كل القطاعات, ويشمل عدة أنواع متخصصة ومترابطة في حماية الأنظمة ما يجعله ضرورة استراتيجية تدخل في أبعاد الاستراتجيات الأمنية للكيانات السياسية من أجل التصدي للهجمات الرقمية .

---

[1] Jim Holdsworth and Matthew Kosinski, "What Is Information Security?", available at **https://www.ibm.com/think/topics/information-security** accessed April 10, 2026

[2] Mesh Flinders and Ian Smalley, "What is Network Security?," accessed April 10, 2026**, https://www.ibm.com/think/topics/network-security**

[3] "What Is Cloud Security?",availabale at **https://www.ibm.com/think/topics/cloud-security** accessed April 10, 2026

[4] Cybersecurity and Infrastructure Security Agency (CISA), "Securing the Internet of Things (IoT)", available **at https://www.cisa.gov/news-events/news/securing-internet-things-iot** accessed April 10, 2026

[5] What Is Identity & Access Management?,available at **https://www.ibm.com/think/topics/identity-access-management** accessed April 10, 2026

## المطلب الثاني: طبيعة الهجمات السيبرانية التي تستهدف قطاع الطاقة

بعد التطرق في المطلب الأول لتعريف الأمن السيبراني ومكوناته , وجب الحديث عن الهجمات السيبرانية التي استحدث من أجلها هذا المجال من خلال ابراز مفهومها و عناصرها ومميزاتها وأنواعها .

**أولا : تعريف الهجمات السيبرانية** : هي جرائم إلكترونية يقوم بها أشخاص محترفين يحاولون من خلالها الوصول غير المصرح به إلى شبكة حاسوبية أو نظام حاسوبي أو جهاز رقمي أو غيرها من الأصول الرقمية, بهدف سرقة البيانات أو كشفها أو التلاعب بها أو تعطيلها أو تدميرها[1] .

وكل هجوم سيبراني يتضمن ثلاث عناصر أساسية :

- **الجهات المُهدِّدة (threat actors):** دول أو جماعات أو أفراد (سواء كانوا مدعومين من دول أو لا) لديهم نية خبيثة ويستهدفون غالبا نقاط الضعف في المؤسسات[2].
- **النشاط الخبيث (Malicious activity)** : أفعال مصممة لإختراق أمان المؤسسات من خلال العبث بتدفق المعلومات أو سلامتها أو سريتها[3].
- **بيئة الاستهداف (Target environment)** : الفضاءات الرقمية التي يعمل فيها المهاجمون وينفذون أنشطتهم[4].

وفي السابق كان المجرمون الإلكترونيون أو مايسمون بالقراصنة يقومون بهذه الهجمات لدوافع شخصية أو مالية, لكن في العقدين الأخيرين دخلت الدول إلى هذا الميدان وأصبحت تنفق العديد من الأموال لتطوير دفاعاتها عن منشآتها وامتلاك القدرة التكنولوجية لاستخدامها لحماية فضائها الرقمي أو في الحروب كوسائل ضغط اتجاه أقرانها من الدول لتحقيق أهدافها

---

[1] What Is a Cyberattack?,available at **https://www.ibm.com/think/topics/cyber-attack** accessed April11,2026
**https://www.ibm.com/think/topics/cyber-attack**

[2] "Cyber Security Threats: What to Defend Against and How," available at **https://www.dataguard.com/cyber-security/threats/** accessed April 12, 2026

[3] Ibid

[4] Ibid

الاستراتيجية دون مساءلة أو عقوبات دولية, هذا ويمكن امتلاك تقنيات متطورة لا تمتلكها الدول الأخرى من خلق حالة من الردع تجعل الطرف الآخر يحسب حجم الخسارة إذا ماتم القيام بأي شيء ضد الطرف الذي يمتلك القدرة على إحداث ضعف مايمكن أن يقوم به الذي يخطط للهجوم أو أي مما يخطط له وهو اليوم مايطلق علية بالردع السيبراني نتيجة التحول التقني, الأمر الذي يوضح انتقال بيئة الصراع إلى مجال جديد أكثر تعقيدا .

**ثانيا** : تتميز الهجمات السيبرانية:

- بكونها تتجاوز الحدود الجغرافية : إذ يمكن لأي دولة من أي قارة أن تشن هجوما على دولة في قارة أخرى , مايجعلها تهديدا عالميا[1].
- تكلفتها المنخفضة ونتائجها عالية التأثير : إذ تعد أدوات الهجوم غير مكلفة مقارنة بالهجوم التقليدي إضافة إلى قدرتها التدميرية التي تكبد الدول وغيرها خسائر مادية وبشرية كبيرة .[2]
- قصر الوقت والسرعة: هجمات خاطفة ومخطط لها مسبقا وتتميز بغياب المؤشرات التحذيرية كما في السابق مايجعل التصدي لها شبه مستحيل[3].
- في تحديث وتطور مستمر : خصوصا مع إدراج الذكاء الإصطناعي اليوم والتقنيات الحديثة في المجال السيبراني لذلك هي متنوعة الأساليب[4].

**ثالثا:** تختلف الهجمات السيبرانية باختلاف أهدافها ووسائلها, فبعضها يسعى إلى سرقة البيانات و تعطيل الخدمات الأساسية والبعض الآخر يسعى إلى تدمير البنى التحتية الحيوية أو التجسس عليها بهدف استغلالها في أنشطة أخرى .

ومن أبرز وأشهر أنواع الهجمات السيبرانية ما يلي:

---

[1] قانصو, مرجع سابق, ص 47

[2] نفس المرجع ص 47

[3] نفس المرجع ص 47

[4] ScienceDirect Topics, Industrial Control System", available at , https://www.sciencedirect.com/topics/computer-science/industrial-control-system accessed April 14, 2026

- **التصيد الإحتيالي (phishing)** : أحد أكثر الهجمات انتشارا, يقوم على استخدام رسائل أو مواقع إلكترونية أو مكالمات هاتفية تبدو وكأنها صادرة عن الجهة الرسمية (شركات ...) لخداع الضحية واجباره على الكشف عن معلومات حساسة تتعلق بالمؤسسة, تتبنى نبرة رسمية مقنعة مايجعل الضحايا يتصرفون دون تفكير[1].
- **برامج الفدية (ransomware)** : من أخطر الهجمات التي تصيب قطاع الطاقة, تعتمد على أنواع خطيرة من البرامجيات الخبيثة التي تقوم بتشفير الملفات أو الأنظمة بشكل كامل مايجعل الوصول إلى البيانات دون مفتاح فك التشفير غير متوفر, وتظهر للضحايا اشعارات باستحالة الولوج إلى الملفات دون دفع مبالغ مالية من أجل استعادتها وعادة دفع مبلغ الفدية يكون بالعملات الرقمية لمنع تتبع المجرم. والمشكل هنا حتى وإن تم دفع الأموال لايوجد ضمانات على أن المهاجمين سيعيدون الملفات إلى أصحابها.[2]

تصيب عادة أنظمة المعلومات (IT) لكن الضرر يصيب الأنظمة التشغيلية (OT) هي الأخرى نظرا للدمج بينهما, ومن الأمثلة على هذه الهجمات نذكر: الهجوم الإلكتروني على شركة هاليبورتون الأمريكية Halliburton ransomware attack في 2024/08/23 والتي كشفت بأن طرفا ثالثا وصل لأنظمتها, وتسبب في خسائر بلغت 35 مليون دولار. استهدف الهجوم بيانات وعمليات حساسة وشل مؤقتا أنظمة بالغة الأهمية للإنتاج والخدمات اللوجستية, وتعد الشركة واحدة من أكبر شركات خدمات النفط في الولايات المتحدة الأمريكية و العالم[3]

- **هجمات الحرمان من الخدمة (DDoS)** : المعروف أيضا بالحرمان الموزع من الخدمة Distributed Denial of Services وهي هجمات إلكترونية تهدف إلى تعطيل

[1] Matthew Kosinski, "What Is Phishing?", available at https://www.ibm.com/think/topics/phishing accessed April 14, 2026

[2] فهد قطينة , "الهجمات السيبرانية : دليل أشهر أنواع الهجمات السيبرانية الشامل" ( Cyber Course) ص 3

[3] Monica Burgess", Halliburton Ransomware Attack : Impact , Victims ," Recovery available at https://www.huntress.com/threat-library/ransomware/halliburton-ransomware accessed 15 April,2026

الخدمات أو مواقع ويب وجعلهم غير متاحين للمستخدمين الشرعيين, عبر إغراق الخادم أو الشبكة المستهدفة بشريط كبير من حركة المرور والطلبات الوهمية في نفس الوقت.

يَستخدم المهاجمون عادة شبكة واسعة من الأجهزة المُخترَقة مسبقا والتي تسمى شبكة البوت نت (Botnet) لإرسال عدد ضخم جدا من الطلبات إلى خادم الضحية في وقت واحد. ونتيجة لهذا التدفق الهائل من البيانات تستنزف موارد الخادم (كقدرة المعالجة وعرض النطاق الترددي للأنترنت ), فيصبح غير قادر على الإستجابة لخدمات المستخدمين الشرعيين .[1]

- **هجمات سلاسل التوريد (supply chain attack) :** في السياق التقني تشمل سلاسل التوريد البرمجيات أو الأجهزة أو الخدمات التي تحصل عليها المؤسسة من موردين خارجيين, إذ لايتم استهداف المؤسسة مباشرة وإنما استهداف الشبكة البرمجية التي تورد لها هذه الخدمات أو الأنظمة من خلال استغلال واختراق الحلقة الأضعف في سلسلة التوريد والتلاعب بمدخلات الشركات من الموردين, ومن أمثلتها أن يقوم المهاجم بإضافة تعليمات برمجية ضارة للبرنامج المشاع استخدامه أثناء عملية تطويره أو تحديثه, وعندما يقوم المستخدمون بتنزيل التحديث الجديد للبرنامج تنتقل إليه مباشرة البرمجية الخبيثة . [2]

ويعد هجوم Solar winds cyber attack عام 2019 أشهر هذه الهجمات, إذ تعرضت شركة Solar Winds وهي فاعل مهم في مجال البرمجيات لهجوم بدأ في سبتمبر 2019 وامتد ل6 أشهر (26مارس 2020) ونتيجة لهذا قام أكثر من 18,000 من عملاءSolar Winds بتثبيت تحديثات تضمنت شيفرة خبيثة, استغل القراصنة هذه التحديثات لسرقة بيانات العملاء ثم التجسس على مؤسسات أخرى, ومن أبرز الخسائر التي تكبدتها الشركات 11% من إيراداتها السنوية وفق تقرير Iron Net حول تأثيرات الأمن السيبراني لعام 2021 خصوصا

[1] قطينة , مرجع سابق, ص 4

[2] نفس المرجع ص 11-12

في الولايات المتحدة الأمريكية (14%), المملكة البريطانية المتحدة (8,6%)، سنغافورة (9,1 %).[1]

- **هجمات يوم الصفر (Zero_Day attacks) :** هجوم إلكتروني يستغل ثغرة أمنية غير معروفة أو غير معالَجة (جديدة) في برامج الحاسوب أو أجهزته أو برامجه الثابتة, ويقصد بـ **اليوم الصفر** أن مُصنِع البرنامج أو الجهاز لا يملك أي فرصة لإصلاح هذه الثغرة, لأن الجهات الخبيثة تكون قد استطاعت استغلالها والوصول لها قبله, ويعد من أخطر الهجمات السيبرانية لعدم وجود أنظمة دفاعية مسبقة لها أحيانا[2].

ويعد هجوم Stuxnet على منشآت إيران النووية عام 2010 أشهرها بحيث استخدم Stuxnet(برنامج خبيث ) في سلسلة هجمات على منشآت نووية في إيران, بمجرد اختراق البرنامج لأنظمة الحاسوب في محطة نووية, أرسلت أوامر خبيثة إلى أجهزة الطرد المركزي المستخدمة لتخصيب اليورانيوم, تسببت هذه الأوامر لاحقا في دوران أجهزة الطرد المركزي بسرعة فائقة أدت إلى تعطلها واتلافها[3] .

والعديد من أنواع الهجمات السيبرانية كهجمات الهندسة الإجتماعية, هجمات سرقة الهوية, هجمات السحابة .

ومن خلال ما سبق يمكن القول أن الهجمات السيبرانية أصبحت تشكل تحديا كبيرا بالنسبة للقطاع الطاقوي في ظل التحول الالكتروني واعتماد الأنظمة الرقمية المترابطة خصوصا تطور وسائلها وتقنياتها جعل من الصعب التصدي لها, الأمر الذي دفع بالدول إلى تطوير استراتيجيات من شأنها حماية وتأمين بيئتها الطاقوية والتخفيف من آثار الهجمات المحتملة .

---

[1] "SolarWinds Cyber Attack: An Overview," available at https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack accessed April 17, 2026

[2] "Zero-Day (Explained)," available at https://www.ibm.com/think/topics/zero-day accessedApril 19, 2026

[3] Ibid

## المطلب الثالث: التحول من التهديدات التقليدية إلى التهديدات السيبرانية

تتخذ التهديدات التي تصيب البنية التحتية الطاقوية شكلين : تقليدي وآخر حديث(سيبراني), يختلفان من حيث الوسائل و طبيعة وفضاء التنفيذ, فإلى جانب التهديدات التقليدية ذات الوسائل المادية , برزت تهديدات تتعلق بالفضاء السيبراني وذات الاعتماد على الأنظمة الرقمية , ومنه وجب فهم العلاقة بين هذين الشكلين المختلفين .

سابقا كانت التهديدات ومجمل الهجمات مادية صلبة كالقصف, العمليات المسلحة...إلخ , و باستخدام أسلحة و معدات عسكرية بمختلف أنواعها وكان من الضروري الانتقال إلى بيئة الخصم لشن الهجمات التي تكون آثارها مباشرة وواضحة ويسهل تحديد الجهات المسؤولة عنها, هذا بالاضافة إلى أن نطاق تأثيرها لا يتجاوز المستوى المحلي أو الإقليمي.

ومن أمثلة ذلك : **هجوم عين أميناس بالجزائر** في جانفي 2013, أين شهدت منشأة الغاز بتيڤنتورين عين أميناس هجوما مسلحا تم فيه إختطاف رهائن من مختلف الجنسيات يعملون في المنشأة من قبل جماعة إرهابية [1], أيضا خلال حرب الخليج سنة 1991 أين تعرضت منشآت للنفط بالعراق لضربات جوية أتلفتها وشلت قدرتها الإنتاجية والعديد من الأمثلة على هذا .

ومع ازدياد تعقد البيئة الأمنية والتطور الرقمي كما تم تحليله في المطالب السابقة, برز مايسمى بالتهديدات السيبرانية التي تستهدف البنية الرقمية لقطاع الطاقة, باستخدام أدوات إلكترونية كبرامج خبيثة واختراقات رقمية دون اللجوء إلى القوة العسكرية ودون أي مجهودات أو تكاليف مالية كبيرة وفي ظرف وجيز , وبقدرة تدميرية تفوق ماتخلفه الهجمات التقليدية مهددة بذلك استقرار الدول في شتى مجالاته, نتيجة للترابط الشبكي بين مكونات البنية التحتية الطاقوية

[1] هجوم عين أميناس, في https://www.aljazeera.net/encyclopedia/2016/2/2/هجوم-عين-أميناس تاريخ الإطلاع(2026/04/20)

المادية والتقنية إضافة إلى صعوبة اسنادها ونسبها وضعف إمكانية المسؤولية الدولية أو حق الرد .

ومن أمثلة ذلك : هجمات على شركات الطاقة الأوروبية عامي 2022_2023, الهجوم على شركة Colonial Pipeline الأمريكية عام 2021, الهجوم على منشأة نطنز النووية في إيران عام 2010. الأمر الذي نقل التهديدات السيبرانية من كونها مجرد أعطاب تقنية إلى قضية أمن قومي تستدعي إيجاد حلول لها ليس فقط لإيقافها وإنما الإستجابة لها واستمرار العمليات دون تداعيات كارثية.

ومن خلال ما سبق نستطيع تلخيص الفروقات بين التهديدات التقليدية والتهديدات السيبرانية في هذا الجدول :

**الجدول رقم (1) : مقارنة بين التهديدات التقليدية والتهديدات السيبرانية**

| معيار المقارنة | التهديدات التقليدية | التهديدات السيبرانية |
|---|---|---|
| الهدف | تخريب أو تدمير المنشآت الحيوية بشكل مباشر | تعطيل الأنظمة التي تتحكم في تشغيل وإدارة المنشآت |
| الفاعل | فواعل دولاتية أو غير دولاتية واضحة نسبيا | مجهولين الهوية بسبب مشكلة اسناد الهجوم |
| نطاق التأثير | محلي وغالبا إقليمي | عابر للحدود بسبب الترابط الشبكي |
| طريقة التنفيذ | عمليات ميدانية , تفجيرات (هجوم مسلح) | عن بعد وباستخدام برمجيات خبيثة |

**المصدر** : من إعداد الباحثة

بعد ماتم عرض وتفسير وتحليل طبيعة التهديدات السيبرانية في المطالب السابقة وما تم التوصل إليه من خلال هذه المقارنة التي أوضحت أن التهديدات السيبرانية تعد الأخطر في العصر الحالي, يمكن طرح سؤال هل الهجمات أو الحرب السيبرانية (كما أطلق عليها العديد من الخبراء) بديل للحرب التقليدية أم مكملة لها؟, وهنا لايمكن الجزم بأن الهجمات السيبرانية حلت محل الحرب التقليدية بالرغم من قدرتها على إحداث تأثيرات كبيرة وبتكلفة أقل مقارنة بالوسائل العسكرية التقليدية. فصحيح أنها قادرة على تعطيل وشل حركة العديد من البنى الحيوية بتخريب أنظمتها الرقمية ومن ثم التأثير في أنظمة الدول وتحقيق غاياتها, إلا أنها تترجم إلى كونها تشكل جزءا من استراتيجية واسعة تجمع بين العديد من الوسائل والأدوات التي تستخدمها الدول خلال مسار صراعها وتنافسها فيما بينها, كل ماهو أن لكل فترة زمنية أدواتها وخصائصها وخططها الاستراتيجية التي تفرض الانتقال إلى شكل متطور من الأساليب. ولهذا أصبح الفضاء السيبراني اليوم ساحة جديدة ومناسبة للصراع بين الدول دون أن يلغي أهمية القوة العسكرية التقليدية, فقط أعاد تشكيل العلاقة بين مختلف أنواع القوة في البيئة الدولية الحديثة .

## المبحث الثالث : ممارسات وسياسات حماية البنية التحتية الطاقوية

نتيجة لتصاعد موجات الهجمات السيبرانية وتطور وسائلها وتقنياتها بالإضافة إلى اختلاف أهدافها, برزت الحاجة إلى استحداث برامج وتطوير سياسات وقوانين تهدف إلى تعزيز حماية البنية التحتية الحيوية فيزيائيا ورقميا عبر كافة دول العالم في إشارة واضحة لمدى أهميتها الاستراتيجية . وعليه سنستعرض في هذا المبحث أبرز التشريعات الدولية التي تزامنت و التطور الحاصل في الفضاء السيبراني وتطبيقاتها في القطاع الطاقوي في المطلب الأول ثم ننتقل في المطلب الثاني إلى تبيان أنواع و أدوات الحماية التي تعتمد عليها الدول لحماية منظومتها الحيوية .

### المطلب الأول : مبدأ حماية البنية التحتية الحيويةCIP وتطبيقاته في الأجندة الحكومية

لاطالما كانت حماية البنية التحتية الحيوية – Critical Infrastructure Protection) (CIP من المهام الأساسية للدولة, لكونها المسؤولة عن استمرارية الأصول والأنظمة التي تعتمد عليها في وظائفها الحيوية. وقد زاد اهتمام الدول بأمن البنية التحتية الحيوية خاصة بعد 11سبتمبر 2001 والأحداث التي أفرزها النظام الدولي وتغير طبيعة التهديدات, إذ تم على إثره تأسيس هياكل و برامج وطنية لحماية القطاعات الحيوية وخاصة قطاع الطاقة لكونه يُزود بقية القطاعات بالطاقة الضرورية لعملها, إضافة إلى تعقد أنظمتها واعتمادها على الرقمنة ودمج الحماية الفيزيائية بالحماية السيبرانية الأمر الذي جعلها عرضة للتهديدات أكثر من ذي قبل وتُستغل في الصراعات الجيواستراتيجية, ومنذ ذلك الحين تُطور الدول سياسات حمائية ( قطاع الطاقة مثله مثل باقي القطاعات الحيوية الأخرى السياسات المتبعة تشمل كل القطاعات دون استثناء) مايعرف في الأدبيات بمبدأ حماية البنية التحتية الحيوية[1] .

[1] Anandan Dhanaraj, The Evolution of Cyber Threats: From Traditional Attacks to AI-Powered Challenges, **European Journal of Computer Science and Information Technology** (13), no. (36) (7 June 2025)

في الولايات المتحدة الأمريكية تم إنشاء وكالة الأمن السيبراني وأمن البنية التحتية CISAعام 2018 والتي تعمل تحت إشراف وزارة الأمن الداخلي, تعد منبرا لتبادل معلومات الدفاع السيبراني والتعاون العملياتي الدفاعي بين الحكومة الفيدرالية وحكومات الولايات والحكومات المحلية والقبلية والإقليمية, والقطاع الخاص, والشركاء الدوليين

وللوكالة مهمتان رئيسيتان:

**أولا :** تتولى CISA القيادة التشغيلية للأمن السيبراني الفيدرالي حيث تكلف بحماية شبكات السلطة التنفيذية المدنية الفيدرالية والدفاع عنها بالتعاون مع مكتب الإدارة والميزانية ومكتب المدير الوطني للأمن السيبراني وكبار مسؤولي المعلومات ومسؤولي أمن المعلومات في الوكالات الفيدرالية. [1]

**ثانيا :** تعد CISA المنسق الوطني لأمن البنية التحتية الحيوية ومرونتها حيث تعمل مع شركاء من مختلف القطاعات الحكومية والصناعية لحماية البنية التحتية الحيوية للولايات المتحدة الأملريكية والدفاع عنها. وكل مرة تنشر عبر موقعها الرسمي آخر التطورات والمستجدات حول أفضل الممارسات في الأمن السيبراني ناهيك عن التدابير والخطط والبرامج التوعوية مثالا على ذلك **العاصفة السيبرانية** وهي سلسلة تمارين تقوم بتنظيمها الوكالة كل عامين وتجمع هذه السلسلة بين القطاعين العام والخاص لإقامة تجربة اكتشاف حادث سيبراني كبير يؤثر على البنية التحتية الحيوية للبلاد ودراسة كيفية الاستجابة له. وتعد تمارين **cyber Storm**جزءا من جهود CISA المستمرة لتقييم وتعزيز الجاهزية السيبرانية ودراسة عمليات الاستجابة للحوادث, وتستند إلى الدروس المستفادة من الحوادث الواقعية السابقة , أول دورة كانت في شهر فيفري عام 2006.[2]

[1], "Cybersecurity Best Practices," Cybersecurity and Infrastructure Security Agency (CISA), available at, **https://www.cisa.gov/topics/cybersecurity-best-practices** accessed April 20, 2026

[2] Ibid

أما في الإتحاد الأوروبي قام كذلك البرلمان الأوروبي بانشاء وكالة الأمن السيبراني للإتحاد عام 2004 تحت اسم الوكالة الأوروبية لأمن الشبكة و المعلومات ثم عام 2019 تم توسيع صلاحياتها ومهامها بموجب لائحة الإتحاد رقم 881/2019 . تتعاون الوكالة مع الجهات الرئيسية في مايخص وضع سياسات الطاقة (والعديد من المجالات الأخرى) وتنفيذها لتعزيز التعاون الفعال وتنسيق أفضل لممارسات الأمن السيبراني.[1]

وفي السنوات الأخيرة أقامت الوكالة شراكة وثيقة مع المفوضية الأوروبية حسب ما أفادته منشورات الموقع الرسمي للوكالة على المستوى التقني, حيث دعمت مسار عمل الطاقة التابع لمجموعة التعاون في مجال أمن الشبكات والمعلومات (NIS) من خلال توفير التدريب وتبادل التقارير القطاعية الخاصة بالوضع الراهن مع سلطات الأمن السيبراني في قطاع الطاقة. إضافة إلى ذلك تعمل الوكالة مع المفوضية الأوروبية لإجراء تقييمات للمخاطر ووضع سيناريوهات لها لمعالجة التهديدات أو الهجمات المحتملة ضد الدول الأعضاء أو الدول الشريكة.[2]

من الأمثلة على هذا : **لائحة قانون التضامن السيبراني** , وتنص اللائحة المعتمدة على إنشاء إطار عمل قائم على ثلاثة محاور أولها **نظام إنذار أوروبي للأمن السيبراني** وهو عبارة عن شبكة بنية تحتية أوروبية شاملة تتكون من مراكز عمليات أمنية وطنية وعابرة للحدود المترابطة أو ما يعرف بـ **المراكز السيبرانية**. وثانيتها **آلية طوارئ للأمن السيبراني** لتحسين مرونة الإتحاد الأوروبي في مواجهة التهديدات السيبرانية من خلال دعم إجراءات التأهب والاستجابة والمساعدة المتبادلة بين الدول الأعضاء بما في ذلك الدعم المالي, وإنشاء احتياطي أوروبي للأمن السيبراني من مزودي خدمات موثوقين . وثالثها **آلية لمراجعة حوادث الأمن السيبراني لتقييم ومراجعة الحوادث الهامة واسعة النطاق.** وتم نشر قانون التضامن السيبراني

[1] European Union Agency for Cybersecurity (ENISA), "What We Do," available at , https://www.enisa.europa.eu/about-enisa/what-we-do accessed April 20, 2026
[2] Ibid

في الجريدة الرسمية للإتحاد الأوروبي بتاريخ 15 جانفي 2025 وبدأ العمل به في 4 فبراير 2025 وأصبح ملزما بتطبيقه في جميع أراضي الدول الأعضاء [1].

أما في المملكة البريطانية المتحدة فيعد المركز الوطني للأمن السيبراني(NCSC) , جزء من جهاز الإستخبارات البريطانية GCHQ , يساعد الشركات والقطاع العام والأفراد على حماية الخدمات والأجهزة الإلكترونية التي تعتمد عليها المملكة.[2]

فمنذ عام 2016 يقوم المركز بحماية الأنظمة والخدمات الإلكترونية الحيوية مقدما إرشادات و أدوات و نماذج عمل رائدة عالميا للشركات والمواطنين. وعند حدوث هجمات سيبرانية أو تعطل للخدمات يقدم استجابة للحوادث لتقليل الضرر واستعادة العمليات ومساعدة المؤسسات على العودة إلى عملها الطبيعي, كما يقدم دورات للتوعية من المخاطر السيبرانية وكيفية تفاديها وأشهر أنواع الهجمات, تأسس من خلال دمج أجزاء منفصلة من الحكومة و GCHQ وMI5 لإنشاء السلطة التقنية الوطنية للأمن السيبراني.[3]

ومن أجل تعزيز الوعي السيبراني وبناء القدرة الوطنية على مواجهة التهديدات السيبرانية وحماية فضائها الالكتروني, قامت سنغافورة بتأسيس وكالة الأمن السيبراني (CSA) عام 2015 التابعة لمكتب رئيس الوزراء والتي تديرها وزارة التنمية الرقمية والمعلومات (MDDI) , إذ تقوم بتحليل المخاطر التي تشكلها التهديدات وتتخذ التدابير اللازمة للاستجابة لها من خلال استحداث هيئات ولجان متخصصة كتحالف التوعية بالأمن السيبراني الذي يوحد جهود القطاعين العام والخاص في هذا المجال لضمان أمن الأنشطة عبر الأنترنت في كافة أنحاء البلاد. ولجنة خبراء الأمن السيبراني لتكنولوجيا التشغيل التي تجمع بين المختصين والمهندسين لتعزيز ممارسات الأمن السيبراني والمرونة داخل جميع قطاعات البنية التحتية الحيوية . في حين يختص فريق الاستجابة للطوارئ السيبرانية (SingCERT) بمهام التصدي واستكشاف

[1] European Union Agency for Cybersecurity (ENISA) **op. cit**
[2] National Cyber Security Centre (NCSC), "What We Do at the NCSC," Available at , **https://www.ncsc.gov.uk/section/about-ncsc/what-we-do**accessed April 21, 2026
[3] Ibid

حوادث الأمن السيبراني التي تصيب البلاد. هذا وأصدرت سنغافورة قانون الأمن السيبراني لأول مرة عام 2018 حيث تقوم بادخال تعديلات عليه من فترة لأخرى ليواكب تطورات الفضاء الرقمي و الحفاظ على أمن و سلامة مجال الأنترنت الخاص بها في إطار دعم استراتيجية أمنها القومي .[1]

ومن خلال استعراض السياسات والبرامج التي تتبناها الولايات المتحدة الأمريكية و الإتحاد الأوروبي وبريطانيا وسنغافورة في مجال الأمن السيبراني, نستنتج أن هناك نهجا واهتماما مشتركا في كل أنحاء العالم حول حماية البنية التحتية الحيوية من ضمنها الطاقوية باعتبارها أولوية استراتيجية وأساس استقرار العديد من الدول خاصة بعد تصاعد موجات الهجمات السيبرانية ضدها, ورغم اختلاف الوسائل والمؤسسات المعتمدة في هذا الميدان إلا أنها تتفق كلها على دمج الحماية الفيزيائية بالحماية السيبرانية وضرورة تعاون القطاع العام والخاص إلى جانب إجراء خطط استباقية للاستجابة لمختلف أنواع الهجمات الالكترونية كتمارين العاصفة السيبرانية, الأمر الذي يظهر أن أسس حماية البنى الحيوية لا تتوقف عند وضع سياسات عامة بل تتطلب تطبيقها على أرض الواقع, ما ترجم في الكثير من المرات ابطال العديد من الهجمات الرقمية حسب ما تنشره مراكز الأمن السيبراني الدولية.

ومنه تقتضي الضرورة الحديث عن أساليب وأدوات حماية المنظومة الطاقوية .

[1] Cyber Security Agency of Singapore, “available at https://www.csa.gov.sg/legislation/cybersecurity-act/ accessed April 21 , 2026

## المطلب الثاني : أدوات وأساليب حماية البنية التحتية الطاقوية

في العصر الحالي زاد اعتماد القطاع الطاقوي على تقنيات الرقمنة الجديدة التي أصبحت تدير العمليات الصناعية وتتحكم فيها بعد أن كانت قائمة على أنظمة فيزيائية و أساليب حماية مادية, الأمر الذي جعل من تبني أدوات متنوعة تجمع بين الأسلوبين الفيزيائي والرقمي لضمان استمرارية الخدمات و التصدي للتهديدات المختلفة وتقليل أثرها .

وعليه سنتناول في هذا المطلب أساليب الحماية التي تعتمدها الدول في تأمين بنيتها الطاقوية .

### أولا : الحماية الفيزيائية :

من خلال الاطلاع على أبرز ما كتب في الحماية الفيزيائية يمكن تلخيصها في مايلي :

تقتصر الحماية الفيزيائية للبنى التحتية على مجموعة من الإجراءات والأساليب لتأمين المنشآت الطاقوية والعمال من التخريب المباشر, الوصول غير المصرح به, حوادث العمل الكوارث الطبيعية وغيرها من خلال استخدام أنظمة انذار الحريق والإبلاغ الجماعي, دواليب الإطفاء, قواطع الدوائر لقطع الإمداد تلقائيا عند حدوث خلل, كميرات مراقبة عالية الجودة, حراسة مشددة من قبل أشخاص مدربين, مانعات صواعق, أنابيب خرسانية محكمة التصنيع لمنع التسربات وغير قابلة للتآكل .[1]

وسابقا كانت تقوم عملية تأمين القطاع الطاقوي على هذا النوع من الحماية فقط, إلى أن برزت الحاجة إلى استخدام التقنيات الجديدة لما تحمله من ميزات أفضل من التي يتمتع بها البشر ما وسع من أساليب الحماية .

[1] Senstar, "Physical Infrastructure Security,"available at ,
, https://senstar.com/senstarpedia/physical-infrastructure-security accessed April 22, 2026

**ثانيا : الحماية السيبرانية :**

والتي تعد الأهم بحيث تُطبق فيها كل أنواع الإختراعات وما توصل إليه العلم في المجال السيبراني من برامج, تحديثات .... لضمان استمرارية الأصول والأنظمة الرقمية ومنع أي تهديدات قد تصيبها .

ومن بين الآليات والتقنيات المستخدمة :

- **جدران الحماية (Firewalls) :** تستخدم لحماية الشبكات والتي تعمل كحاجز بين شبكة داخلية موثوقة وشبكة خارجية غير موثوقة (مثل الإنترنت), تراقب حركة البيانات الواردة والصادرة وتسمح بمرورها أو تقوم بحظرها بناء على قواعد أمنية محددة مسبقا[1].
- **أنظمة كشف ومنع التسلل (IDS/IPS) :** من أدوات حماية الشبكات, بحيث تقوم أنظمة كشف التسلل (IDS) بالمراقبة بحثا عن الأنشطة المشبوهة والخبيثة أو الإنتهاكات المحتملة للسياسات الأمنية ثم تقوم بتنبيه المسؤولين. أما أنظمة منع التسلل(IPS) تتخذ إجراءات استباقية لمنع الهجوم مثل حظر حركة المرور من المصدر المشبوه[2].
- **التشفير (Encryption) :** يستخدم في أمن البيانات, حيث يقوم بتحويلها إلى صيغة مشفرة لا يمكن فكها إلا باستخدام مفتاح فك التشفير ويحمي التشفير البيانات أثناء التخزين وأثناء النقل وأثناء المعالجة[3].

[1] "*What Is a Firewall? Definition and Types of Firewall*,"available at, **https://www.fortinet.com/resources/cyberglossary/firewall** accessed April 22, 2026
[2] "Intrusion Detection and Prevention Systems (IDS/IPS),"available at **https://www.group-ib.com/resources/knowledge-hub/ids/**, accessedApril 24, 2026,
[3] "What Is Encryption?,"available at **https://www.ibm.com/think/topics/encryption**, accessed April 24, 2026

- **حلول منع فقدان البيانات (DLP)** :هي أدوات وسياسات تستخدم لفحص البيانات في كل أنحاء الشبكة لمنع تسربها, وتقوم بمراقبة وتصنيف وحماية البيانات بناء على محتواها وسياقها[1].
- **إخفاء البيانات (Data Masking)** : تقنيات تُستخدم لإنشاء نسخ مزيفة تشبه البيانات الأصلية, تستخدم لتدريب الموظفين من أجل الحفاظ على خصوصية البيانات ما يقلل من مخاطر التسريب[2].
- **ممارسات الترميز الآمن (Secure Coding)** تطبيق تقنيات وإرشادات لتقليل نقاط الضعف في إنتاج البرمجيات لمنع الإختراقات الأمنية[3] .
- **إدارة الوضع الأمني للسحابة (CSPM)** : أدوات تقوم بتحديد ومعالجة الثغرات الأمنية والتكوينات الخاطئة في البيئات السحابية[4].
- **المصادقة متعددة العوامل (MFA)** : وهي وسيلة للتحقق من هوية المستخدمين من خلال طلب دليلين أو أكثر مثل كلمة مرور الحساب الصحيحة و بصمة الإصبع وغيرها من البيانات الشخصية وتعد جزءا من استراتيجيات أمن الهوية والأصول (IAM) للمؤسسات.[5]
- **النسخ الاحتياطي والاستعادة (Bacup and Recovery)** : وهي تقنية تقوم على تخزين نسخ دورية من البيانات و التطبيقات على أجهزة ثانوية من أجل سهولة

[1] "*What Is DLP* (Data Loss Prevention)?,"available at **https://www.fortinet.com/resources/cyberglossary** , accessed April 21, 2026
[2]Paul Kirvan and Michael Cobb, "What Is Data Masking?," available at **https://www.techtarget.com/searchsecurity/definition/data-masking** accessed April 24 ,2026
[3] Rina Diane Caballar and Cole Stryker, "What Is Secure Coding?,"available at**,** **https://www.ibm.com/think/topics/secure-coding** accessed April 24 ,2026
[4] "What is Cloud Security Posture Management , available at **https://www.ibm.com/think/topics/cspm** accessed April 25,2026
[5] Matthew Kosinski,et al, "What Is MFA (Multifactor Authentication)?," available at, **https://www.ibm.com/think/topics/multi-factor-authentication** accessed April 25, 2026

استرجاعها وا ستمرارية الأنشطة عند حدوث هجوم إلكتروني أو خطأ بشري أو أي خلل آخر .[1]

- **تجزئة الشبكة (Network Segmentation)** : عبارة عن نموذج معياري يقسم شبكة الحاسوب إلى عدة شبكات و أجزاء فرعية تعمل بشكل مستقل من أجل تعزيز سياسات الأمان ومنع تمدد الاختراقات الالكترونية من أنظمة المعلومات إلى أنظمة التشغيل و تحسين الأداء .[2]
- **التوعية والتدريب المستمر للموظفين** : من خلال تقديم ورشات للتعرف على مختلف الهجمات الإلكترونية و كيفية الاستجابة لهم .[3]

يُظهر تنوع الوسائل وآليات الحماية المستخدمة أن تأمين المنظومة الطاقوية يدمج بين العنصرين المادي والتقني, بحيث أي خلل يصيب أحدهما يؤثر مباشرة على الآخر ويعرقل العمليات الصناعية في بيئة تترابط فيها الأنظمة الفيزيائية و التقنية .

ومنه نستخلص أن التطور التقني أفرز نوعا جديدا من التهديدات يتمثل في الهجمات السيبرانية, التي فرضت على الدول والمؤسسات تطوير وتنويع أساليب الحماية من تقليدية مادية إلى رقمية أكثر تعقيدا وحساسية لتأمين بنيتها التحتية الطاقوية, فمسألة تطوير منظومة وترك أخرى لم يعد كافيا لذلك أصبحت عملية الحماية تمزج بين تأمين المنشآت المادية و الأنظمة الرقمية ضد التهديدات الإلكترونية .

---

[1] "What Is Backup and Restore?,"available at **https://www.ibm.com/think/topics/backup-and-restore**, accessedApril 25, 2026

[2] "What Is Network Segmentation & How Does It Work?,"available at**https://www.dashlane.com/blog/what-is-network-segmentation** , accessedApril 25, 2026

[3] " أنواع التهديدات السيبرانية للشركات وكيفية الوقاية منها," في **https://keytime.sa/** **أنواع-التهديدات-السيبرانية-للشركات** /تاريخ الاطلاع 27 أفريل 2026

**خلاصة الفصل :**

أظهر محتوى الفصل الأول أن البنية التحتية الطاقوية لم تعد تعتمد على المنشآت المادية في انتاج ونقل وتوزيع الطاقة, إذ أصبحت اليوم تتبنى تقنيات التقدم التكنولوجي بجمعها بين كل من المكونات الفيزيائية والأنظمة الرقمية التي تسير وتدير العمليات الصناعية خصوصا مع خاصية دمج أنظمة المعلومات بأنظمة التشغيل التي رفعت من مستوى الكفاءة الانتاجية والتشغيلية, ونتيجة لهذا الترابط الشبكي بين الأنظمة ظهرت التهديدات السيبرانية التي تستغل الثغرات التقنية من أجل استهداف البنى التحتية باعتبارها ذات أهمية استراتيجية للعديد من الدول, وتعطيلها دون مجهودات مكلفة وفي وقت وجيز مأثرة بذلك في استمرارية الخدمات الحيوية والأمن الإقتصادي والاجتماعي وحتى استقرار الدول السياسي. الأمر الذي جعل من الضروري ادراج الفضاء الرقمي كأحد أبعاد الأمن القومي والذي يختص بتأمين البلاد من التهديدات السيبرانية داخليا وخارجيا .

هذا وخلُص الفصل إلى أن الهجمات السيبرانية تطورت من حيث وسائلها وطرق استخداماتها وأهدافها لتزيد من تعميق المشهد الأمني في بيئة دولية غير مستقرة, كل الدول أصبحت تحتكر فيها القدرة التكنولوجية لتحقيق غاياتها دون مساءلة قانونية دولية .

وعلى إثر هذا كان من الضروري تبني مقاربة شاملة تجمع بين الحماية المادية والسيبرانية مع تطوير سياسات وطنية وآليات استجابة مرنة لحماية القطاع الطاقوي خاصة .

# الفصل الثاني

## التهديدات السيبرانية وأمن البنية التحتية الطاقوية الإيرانية

**تمهيد الفصل :**

يتناول هذا الفصل البنية التحتية الطاقوية الإيرانية كدراسة حالة لما تم عرضه في الفصل الأول, أين سينتقل من توصيف القطاع الطاقوي باعتباره ركيزة البلاد الأساسية نظرا لتزويد بقية القطاعات الحيوية الأخرى بالطاقة اللازمة ومساهمته الكبيرة في انعاش الخزينة الوطنية, إضافة إلى الحديث عن البرنامج النووي الإيراني ودوره في توجيه مصالح البلاد وكونه أحد الأسباب التي جعلت إيران تواجه العديد من التحديات, إلى تحليل أغلب الهجمات السيبرانية التي تعرضت لها البنية التحتية الطاقوية الإيرانية من 2010 إلى 2025, ولماذا في البداية استهدفت المواقع الاستراتيجية الطاقوية ثم توسعت لتمس كافة المجالات, وكذا تبيان التحولات في أدوات الهجمات وأهدافها في نظام دولي غير مستقر يصعب تحديد الجهات المسؤولة عن الإستهداف, أين تبقى مشكلة الإسناد تعرقل طرق الاستجابة لمثل هذه التهديدات, لينتقل بعدها إلى عرض الهيكل المؤسساتي والتشريعي لمجال الأمن السيبراني الإيراني والذي خصصته للتعامل مع هذا النوع من التهديدات وتحليل واقع فعالية الاستراتيجية الرقمية الإيرانية في الاستجابة لمثل هذه التحديات في ظل العقوبات الدولية المفروضة عليها .

## المبحث الأول : ملامح البنية التحتية الطاقوية الإيرانية وأبعادها الاستراتيجية

يعتبر قطاع الطاقة في إيران من المجالات الحيوية التي تعكس تداخل الأبعاد الإقتصادية والتكنولوجية والأمنية بحيث لم يعد مصدرا للإنتاج والمداخيل المالية بل أصبح يشكل جزءا أساسيا من عقيدة الدولة الأمنية. وعلى إثر هذا, سيتناول المبحث من خلال مطالبه الأهمية الإستراتيجية للقطاع الطاقوي بالنسبة للجمهورية الإيرانية, دور البرنامج النووي من هذه الأحداث, أثر الرقمنة وكيف وسعت من سطح استهداف القطاع والمشاكل التي يواجهها بعد تبنيه النهج التكنولوجي.

### المطلب الأول : قطاع النفط والغاز كأصل استراتيجي

يعتبر القطاع الطاقوي أحد أعمدة القوة الهيكلية في الجمهورية الإسلامية الإيرانية, في نقطة تتقاطع فيها الإعتبارات السياسية والإقتصادية والأمنية ناهيك عن وفرة الموارد الهيدروكربونية وموقع منشآتها الجيواستراتيجي الحساس, الأمر الذي يجعل حمايته من أولويات السلطات العليا في البلاد.

في عام 2023 صنفت إيران رابع أكبر منتج للنفط الخام في منظمة الدول المنتجة والمصدرة للنفط (OPEC), إذ تمتلك 208,600,000,000 برميل من الاحتياطيات النفطية المؤكدة اعتبارا من 2025 , لتحتل بذلك المرتبة الثالثة عالميا وتمثل حوالي 11.82% من إجمالي احتياطيات النفط العالمية البالغة1,765,151,568,000.[1]

وفي عام 2022 كانت ثالث أكبر منتج للغاز الطبيعي الجاف في العالم بعد الولايات المتحدة وروسيا, كما بلغت احتياطياتها المؤكدة من الغاز الطبيعي نحو 1,200 تريليون قدم مكعب حتى ديسمبر 2023 وفقا لمجلة النفط والغاز(Oil & Gas Journal) , وتمتلك إيران

[1] نفط إيران ، في https://www.worldometers.info/ar/النفط/نفط-إيران /تاريخ الاطلاع 2 ماي 2026

نحو 16% من احتياطيات الغاز الطبيعي المؤكدة عالميا وحوالي 45% من احتياطيات دول منظمة الأوبك حسب ما أفاده تقرير وكالة إدارة معلومات الطاقة الأمريكية.[1]

وعمليا تترجم هذه المؤشرات في قدرة إنتاجها التصديري على التأثير في السوق الدولية , حيث أدى انسحاب الولايات المتحدة الأمريكية من الإتفاق النووي عام 2018 وإعادة فرض العقوبات على إيران إلى انخفاض صادراتها النفطية خلال أشهر, وارتفاع أسعار النفط عالميا مؤقتا ما أجبر بعض دول منظمة الأوبك إلى إعادة ضبط مستويات الإنتاج لتعويض النقص الحاصل . كما تشكل وفرة الموارد أداة تفاوض وضغط في البيئة الدولية, الأمر الذي برز خلال مفاوضات الإتفاق النووي عام 2015 أين كانت عودة النفط الإيراني إلى الأسواق العالمية من أبرز الأسباب التي جعلت بعض القوى الأوروبية تدعم رفع العقوبات نظرا لحاجتها إلى تنويع مصادر الطاقة خاصة بعد تأزم الأوضاع مع روسيا .[2]

كما يضيف موقع إيران الجغرافي بعدا حيويا استرايجيا ليتحكم بذلك في الإمدادات, إذ تقع على الساحل الشمالي لمضيق هرمز الذي يعتبر من أهم المنافذ البحرية ويربط منتجي النفط في الشرق الأوسط بأسواق آسيا وأوروبا وأميركا الشمالية وما وراءها. إذ يمر عبره ما يقارب خمس تجارة الغاز الطبيعي المسال, وأكثر من ربع تجارة النفط المنقول بحرا في العالم, مايجعل استقرار تدفقات الطاقة العالمية ترتبط بالحالة الأمنية لهذا المضيق البحري. هذا ويمنح السلطات الإيرانية نفوذا أكبر في المنطقة إذ هددت في العديد من المرات بغلقه ما أدى في كثير من الأحيان إلى تقلب الأسعار كاستجابة لأي تهديد محتمل له[3].

من جهة أخرى يمثل القطاع الطاقوي العمود الفقري للمالية العامة داخل البلاد, إذ تعد إيران من أكثر الدول استهلاكا وانتاجا للطاقة في العالم و الشرق الأوسط (حوالي 13.5

[1] U.S. Energy Information Administration, Country Analysis Brief: Iran, last updated October 10, 2024. p 3_10

[2] Ibid p 2_11

[3] عبد الرحمن أياس، "مضيق هرمز من الألف إلى الياء... شريان الطاقة والتجارة العالمي," في **majalla.com** , تاريخ الاطلاع 3 ماي 2026

كوادريليون وحدة حرارية بريطانية من الطاقة الأولية عام 2022 ) و رغم تنوع اقتصادها إلا أنها تعتمد على عائدات النفط والغاز بشكل كبير. في عام 2018 صدّرت إيران ما نسبته 47% من إنتاجها النفطي (2,197,396 برميل يوميا من أصل 4,711,351 تم إنتاجها) وبلغت إيرادات صادرات النفط نحو 53 مليار دولار عامي 2022 و2023 مقارنة بنحو 37 مليار دولار عام 2021, ما يعكس التأثر المباشر للإيرادات العامة بتقلبات الأسعار في الأسواق الطاقوية وحجم التصدير.[1] بحيث أدت العقوبات الإقتصادية المفروضة على طهران إلى تراجع صادراتها بعد عام 2018 ما خلق أزمة في سوق الصرف وأدى إلى تدهور قيمة العملة الإيرانية (الريال), كما فُرضت قيود على شركات الطاقة و أُلغيت العديد من المشاريع الإستراتيجية الأمر الذي يؤكد أن استقرار الميزانية مرهون باستمرارية التدفقات النفطية . لكن سرعان ماقامت إيران برفع انتاج النفط وحجم وتصديره تدريجيا متجاوزة بذلك قرارات الهيئات الدولية اتجاهها عبر قنوات بديلة إلى شركائها كالصين, ما أوضح من جانب آخر دور القطاع في توفير حد أدنى من الاستقرار المالي في ظل بيئة دولية ضاغطة.[2]

إضافة إلى هذا تزيد المنشآت الإنتاجية وحساسية مواقعها من أهمية البنية التحتية الطاقوية إذ تعتبر ركيزة الإنتاج الوطني, فحقل الأهواز وهو ثالث أكبر حقل نفطي في العالم ينتج حوالي 750 ألف برميل يوميا حسب بيانات وزارة النفط الإيرانية, وهناك أيضا حقل عجساران ثاني أكبر حقول النفط الإيرانية والذي ينتج 500 ألف برميل يوميا, وحقل مارون بإقليم خوزستان جنوب غرب طهران الذي ينتج مايقارب نصف مليون برميل يوميا أيضا وتبلغ احتياطاته 46 مليار برميل. وحقل آغاجاري بخوزستان خامس أكبر حقول النفط في البلاد وينتج مايقارب 200 ألف برميل يوميا وتقدر احتياطاته بـ 28 مليار برميل, بالإضافة إلى حقل بارس الجنوبي الذي يعد أكبر حقل غاز طبيعي في البلاد و العالم حيث يعد هو الآخر ركيزة لإمدادات الغاز الداخلية والصادرات ويجري إنشاء محطات أخرى تابعة له حسب مصادر

[1] U.S. Energy Information Administration,**op.cit**,p 3_11
[2] Ibid p 2_16

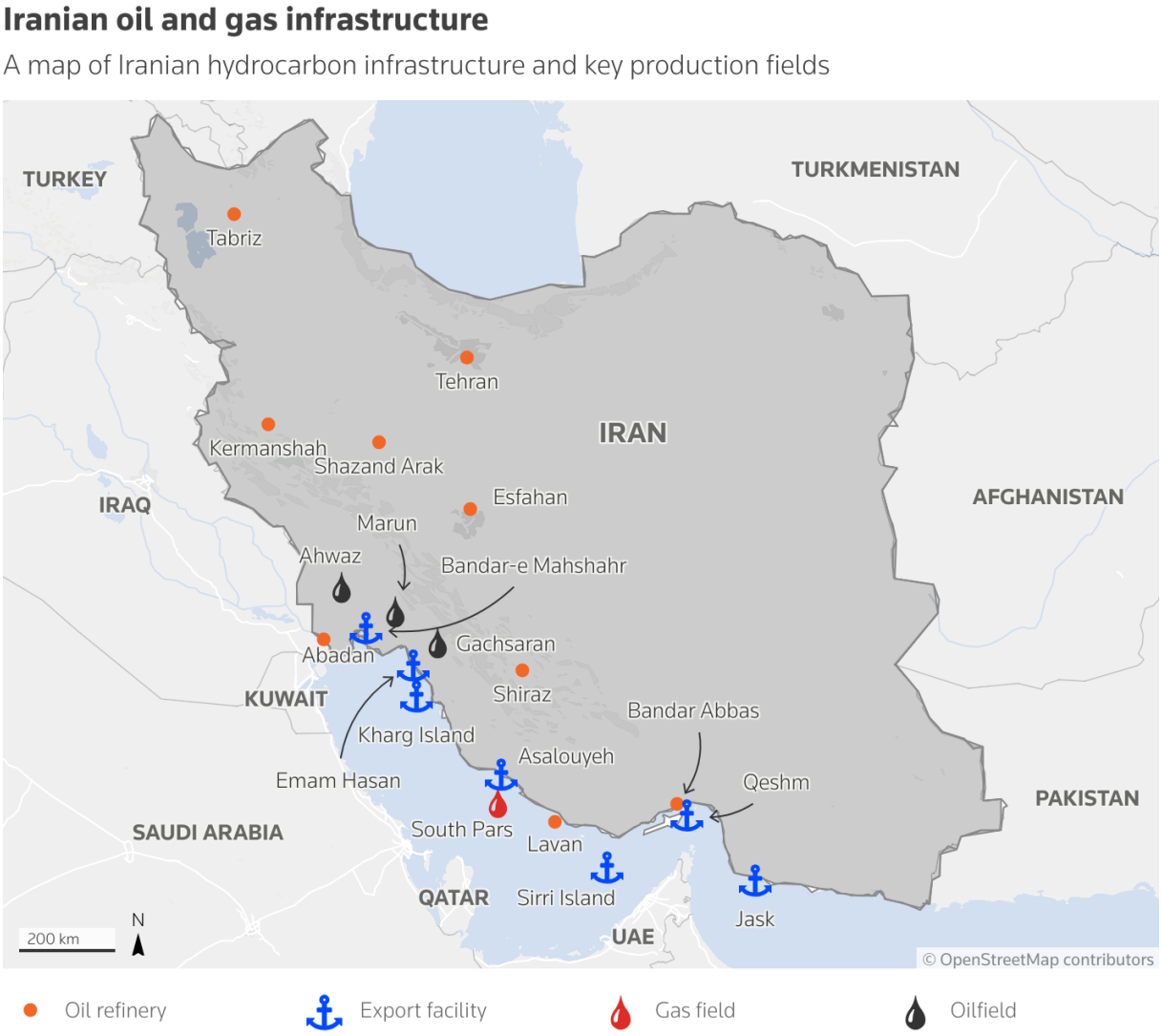
رسمية. كما تساهم المصافي الكبرى في تلبية الطلب المحلي المتزايد على المنتجات النفطية خاصة مع ارتفاع حاجة القطاعات الحيوية الأخرى لاستهلاك الطاقة داخليا. ففي مصفاة عبادان بخوزستان ينتج مايقارب 500 ألف برميل يوميا من 5 حقول نفطية بالمنطقة, إضافة إلى إنتاج حوالي 375 ألف برميل يوميا في مصفاة أصفهان, و250 ألف برميل في مصفاة العاصمة طهران التي تشمل 3 حقول, و مصفاة نجمة الخليج الفارسي للمكثفات التي تعالج المكثفات من حقل غاز جنوب فارس الإيراني, وهي أكبر مصفاة للمكثفات في إيران وتبلغ طاقتها الإنتاجية من النفط الخام 420 ألف برميل يوميا.[1]

أما مشاريع البنية التحتية المصرح بانشائها مثل خط أنابيب غور–جاسك حسب ماجاء في تقرير وكالة الطاقة الذرية حول إيران, فتترجم محاولة إيران تقليل الاعتماد على مضيق هرمز في تصدير انتاجها خصوصا عندما تكون هناك توترات جيوسياسية.

وفي مايلي خريطة توضح أبرز المنشآت الطاقوية في إيران :

[1]بينها ثالث أكبر حقل في العالم.. تعرف على منشآت النفط الإيرانية ، في https://www.aljazeera.net/ تاريخ الاطلاع 4 ماي 2026

**الشكل رقم (1) : خريطة المنشآت الطاقوية في إيران**




**المصدر : Youcef Saba . LSEG**

و صحيح أن هذه المنشآت لها دور كبير في العملية الإنتاجية إلا أن مسألة تأمينها يعد من أولويات الدولة باعتبارها محاور رئيسية داخل منظومة طاقوية متكاملة, بحيث أي أعطاب تقنية أو اضطرابات أمنية تطالها قد يمتد أثرها ليشمل سلسلة الإنتاج والتوزيع عامة, مما ينعكس مباشرة على القدرة الإنتاجية والاستقرار الإقتصادي والإجتماعي للدولة.

وعليه يعد القطاع الطاقوي في إيران ذات أهمية استراتيجية وحساسية أمنية عالية أي شيء يصيبه ينعكس بالسلب أو بالإيجاب على الدولة لذلك تحاول الأجندة الحكومية في طهران تطوير سياساتها لحمايته من أي خطر كان.

## المطلب الثاني: البنية النووية الإيرانية كأحد أبعاد الأمن القومي الإيراني

يُعد البرنامج النووي الإيراني من أكثر المشاريع الاستراتيجية إثارة للحساسية في الشرق الأوسط وهذا راجع لطبيعته التقنية ودلالاته السياسية والأمنية والرمزية, كما عرف أيضا تطورات عبر فترات زمنية جعلته يتحول من كونه مشروع علمي محدود إلى منظومة تكنولوجية متقدمة تعيد تأطير مفهوم السيادة الوطنية وتعزز المكانة الدولية للجمهورية الإسلامية الإيرانية. كما لم يعد وسيلة لإنتاج الطاقة أو البحث العلمي بل أصبح يعكس طموح الدولة نحو تحقيق الاستقلال التكنولوجي وتقليل التبعية للمنظومة الغربية, إلا أن التطور التقني الذي طال القطاع باعتماده على أنظمة التحكم الصناعية عالية الدقة كشف عن نوع جديد من المخاطر تتعلق بالهشاشة الرقمية مايسمح باستهدافها سيبرانيا. وعليه يهدف هذا المطلب إلى دراسة البرنامج النووي الإيراني من منظور السيادة التكنولوجية مع إبراز دوافعه والتحديات الرقمية التي يواجهها.

**أولا :** شهد البرنامج النووي الإيراني تطورا تاريخيا مر بعدة مراحل متمايزة في محاولة لامتلاك التقنية النووية.

بداية بخمسينيات القرن الماضي, أين كان هناك تعاون علمي بين الولايات المتحدة الأمريكية ونظام الشاه محمد رضا بهلوي في إطار ما يعرف ببرنامج **الذرة من أجل السلام** الذي يتيح الإستخدامات السلمية للطاقة الذرية كمجال للتنمية وانتاج الطاقة الكهربائية, حيث تم إنشاء مؤسسات بحثية أولية تهدف إلى تطوير الاستخدامات السلمية للطاقة النووية و التعاون مع عدة دول مثل فرنسا وألمانيا بهدف تبادل الخبرات وبناء المحطات.

غير أن نجاح الثورة الإسلامية في إيران عام 1979 بزعامة المرشد الأعلى آية الله الخميني, أعاد ترتيب أولويات الدولة وتوجيهها وتم على إثره توقيف المساعدات الأمريكية

وتوقف العمل بالمفاعلات النووية الفرنسية والألمانية, كما تم تجميد حصص مساهمات إيران في المشاريع النووية .

إلا أن الحرب العراقية–الإيرانية (1980–1988) غيرت الوضع ودفعت صانعي القرار الإيرانيين إلى إعادة تقييم أهمية امتلاك بنية علمية وتقنية متقدمة, خصوصا في مجالات الطاقة والتكنولوجيا الحساسة, وتم تفعيل البرنامج النووي من جديد واستقطاب علماء الذرة الأجانب وتطوير منشآت جديدة وتعزيز التعاون مع بعض الدول مثل روسيا و الصين وتزايد هذا الإهتمام كثيرا في تسعينات القرن الماضي, وهو ما أدى لاحقا إلى تصاعد الشكوك الدولية حول طبيعة هذا البرنامج وأبعاده المحتملة[1].

أما في بداية العقد الأول من القرن الحادي والعشرين, فقد برز البرنامج النووي الإيراني كقضية دولية مركزية خاصة بعد الكشف عن منشآت نووية حساسة ونصب أجهزة الطرد المركزي واتهامات حول تطوير أسلحة نووية, الأمر الذي أدى إلى فرض عقوبات دولية ومفاوضات مكثفة بشأن خفض نسبة تخصيب اليورانيوم انتهت بالتوصل إلى الإتفاق النووي حول سلمية الملف الإيراني عام 2015 بين إيران ومجموعة 5+1(الدول دائمة العضوية في مجلس الأمن + ألمانيا), قبل أن يتعرض لاحقا لتحديات كبيرة بعد انسحاب الولايات المتحدة الأمريكية منه سنة 2018.[2]

وبهذا يمكن القول إن البرنامج النووي الإيراني انتقل من كونه مشروعا علميا إلى كونه ملفا استراتيجيا معقدا يرتبط مباشرة بموازين القوى الإقليمية والدولية.

**ثانيا :** يعد البرنامج النووي الإيراني من جهة أخرى تجسيدا لمفهوم **السيادة التكنولوجية** بما معناه قدرة الدولة على امتلاك وتطوير وإدارة التقنيات الحساسة و المتطورة دون تبعية مباشرة للقوى الخارجية, ويُعد هذا المفهوم أحد أهم التحولات في الفكر الاستراتيجي للدول

[1] محمد سالمان الطايع، وهويدا عبد الله فتحي، "البرنامج النووي الإيراني وتأثيره على منطقة الشرق الأوسط"، المجلة العلمية لكلية الدراسات والسياسات الاقتصادية والسياسات السياسية، يناير 2024، ص 6_8.

[2] نفس المرجع ، ص9–12.

النامية التي تهدف إلى تعزيز مكانتها في النظام الدولي , إذ تكمن دوافع إيران على هذا الأساس في ما يلي:

فعلى المستوى الاقتصادي يعد النفط والغاز من الموارد النافذة وغير المتجددة الأمر الذي يخلق تحديا أمام إيران كون أن اقتصادها يرتكز بالأساس على هذه الموارد, لذلك كان في الطاقة النووية الخيار البديل الذي تستطيع أن توفر من خلاله مصدر مستقر لتوليد الكهرباء وتقليل الإعتماد على النفط والغاز محليا في محاولة لتوجيههما إلى التصدير وزيادة العائدات المالية ومنه توفق بين تلبية حاجياتها الداخلية والحفاظ على مواردها الطاقوية بشكل أكثر كفاءة وبكلفة أقل. [1]

أما على المستوى الأمني, فتنطلق دوافع الأجندة الإيرانية حول تطوير برنامجها النووي من فكرة أن محيطها الإقليمي مضطرب ويشهد حالة عدم استقرار ما يجعل مسألة التهديد في فكرها الإستراتيجي حالة بنيوية دائمة وليست مؤقتة, فإيران تنشط داخل فضاء جيوسياسي معقد إذ تربطها علاقات عدائية جد متوترة مع بعض القوى الإقليمية المدعومة من الولايات المتحدة الأمريكية كالكيان الصهيوني الذي يرتكز في عقيدته الأمنية على منع الخصوم من امتلاك قدرات استراتيجية متطورة, أو مع دول الخليج عامة إضافة إلى تشابك وتعقد الأزمات في العراق وسوريا ولبنان, أو في حدودها مع باكستان وأفغانستان التي تعرف تحديات مرتبطة بالجماعات المسلحة والتهريب, الأمر الذي يفرض على صانع القرار بناء عدة تصورات حول احتمالية التهديد من أي جهة كانت. ومنه تتشكل العقيدة الأمنية لإيران في اعتبار تطوير البرنامج النووي أداة ردع تعزز أمنها القومي وتراتبيتها في سلم القوى الإقليمي[2].

[1] عطا محمد زهرة، البرنامج النووي الإيراني بين إشكاليات الواقع واحتمالات المستقبل، مركز الزيتونة للدراسات والاستشارات، بيروت، ماي 2015، ص 5_6

[2] الطايع، مرجع سابق, ص14.

وعلى المستوى التكنولوجي يعكس البرنامج هدف البلاد إلى تقليص الفجوة العلمية مع الدول المتقدمة, من خلال انشاء قاعدة معرفية متطورة في مجالات الفيزياء النووية والتقنيات الدقيقة وهو ما يساهم في تطوير قطاعات علمية وصناعية مرتبطة بهذا المجال[1].

كما لا يمكن تجاوز البعد الرمزي أين جميع الماديات تربط بالجانب الروحي أو القيمي, إذ يُنظر إلى البرنامج النووي داخل الخطاب السياسي الإيراني باعتباره رمزا للاستقلال الوطني والكرامة السيادية والثورة الإيرانية الإسلامية, فالتهديد عند إيران يتعلق ببقائها كدولة إسلامية ذات ثقافة شيعية لذلك وجب حماية نظامها الإسلامي من أي تحديد كان وتسخير كافة السبل لتحقيق هذا الهدف[2].

ومنه فإن البرنامج النووي الإيراني لا يمكن فهمه فقط كعمل تقني, بل كجزء من مشروع استراتيجي أوسع يهدف إلى ترسيخ السيادة التكنولوجية ضمن نظام دولي شديد الحساسية.

غير أن هذا السعي نحو ترسيخ السيادة التكنولوجية لم يقتصر على تطوير القدرات العلمية فحسب, بل تجسد أيضا في بناء شبكة معقدة من المنشآت النووية تعتمد بشكل كبير على أنظمة رقمية متطورة لإدارة العمليات الطاقوية .

**ثالثا** :إذ تتكون البنية النووية الإيرانية بين منشآت تخصيب ومراكز بحث ومفاعل لإنتاج الطاقة الكهربائية, وتختلف من حيث تموقعها ووظيفتها ودرجة تحصينها الأمر الذي يعكس تشابك الإعتبارات التقنية والأمنية في نفس الوقت, أبرزها :

منشأة نطنز الواقعة بمحافظة أصفهان والتي تعد أكبر منشأة في البلاد و أساس المشروع النووي, تعمل في تخصيب اليورانيوم منذ فيفري 2007 وبُنيت على عمق 8 أمتار تحت الأرض, يُحيط بها جدار خرساني سميك يبلغ 2.5 متر وتحميها منظومة دفاع جوي وأسلاك شائكة وقوات من الحرس الثوري الإيراني. صممت لاستيعاب 50 ألف جهاز طرد مركزي(دعامة أساسية لأي برنامج نووي ) غير أنها تعتمد بشكل كبير على أنظمة تحكم

[1] زهرة , مرجع سابق, ص 7

[2] نفس المرجع , ص 8

صناعية عالية الدقة لاستمرار عملية التخصيب الأمر الذي يعكس هشاشتها التقنية و يجعلها عرضة للإختراقات السيبرانية[1].

تمثل منشأة فوردو بديلا لمنشأة نطنز وتضمن استمرارية البرنامج في الحالات التي تشهد تصعيدا عسكريا, فقد شُيّدت داخل مجمع أنفاق تحت جبل يبعد حوالي 32 كيلومترا شمال شرق مدينة قُم على عمق يُقدر بنحو نصف ميل تحت سطح الأرض في قاعدة عسكرية تابعة للحرس الثوري الإيراني, مايجعلها محصنة من الضربات الجوية التي تشهدها عدة مواقع نووية, كما تحتوي على أنظمة دفاع جوية متقدمة مايجعلها ذات وزن استرايجي جد مهم في إطار حماية المنظومة الطاقوية. إلا أن تموقعها تحت الأرض لا يُبعد اعتمادها على أنظمة تشغيل وأنظمة معلومات حساسة, خاصة ما يتعلق بالتهوية وأجهزة الطرد المركزي ما يجعلها هي الأخرى عرضة للتعطيل الوظيفي في حال تعرضت للإختراقات الإلكترونية[2].

أما محطة بوشهر فتقع على الساحل الجنوبي لإيران وتُعد المنشأة النووية الوحيدة العاملة لتوليد الكهرباء في البلاد (يوجد وحدات أخرى قيد الإنجاز), حسب ما أفاده تقرير وكالة الطاقة الذرية, وتجسد البعد السلمي للبرنامج النووي و تهدف إلى تلبية الطلب المتزايد على الكهرباء وتقليل الاعتماد على الموارد الأحفورية وتحقيق نمو اقتصادي مستدام وتنمية اجتماعية, بدأ تشغيلها عام 2013 و ساهمت بنحو 1.7% من إجمالي إنتاج الكهرباء الوطني في عام 2023, حيث تعمل بمفاعل من الماء المضغوط بقدرة تقارب 1024 ميغاواط, ويعتمد هذا النوع من المفاعلات على أنظمة تبريد معقدة لضمان استقرار درجة الحرارة داخل قلب المفاعل إذ يستمر الوقود النووي في إنتاج الحرارة حتى بعد إيقاف التشغيل, ما يجعل استمرارية هذه الأنظمة أمرا حيويا لتفادي أي مخاطر محتملة كما أن هذه الأنظمة لا تقوم فقط على

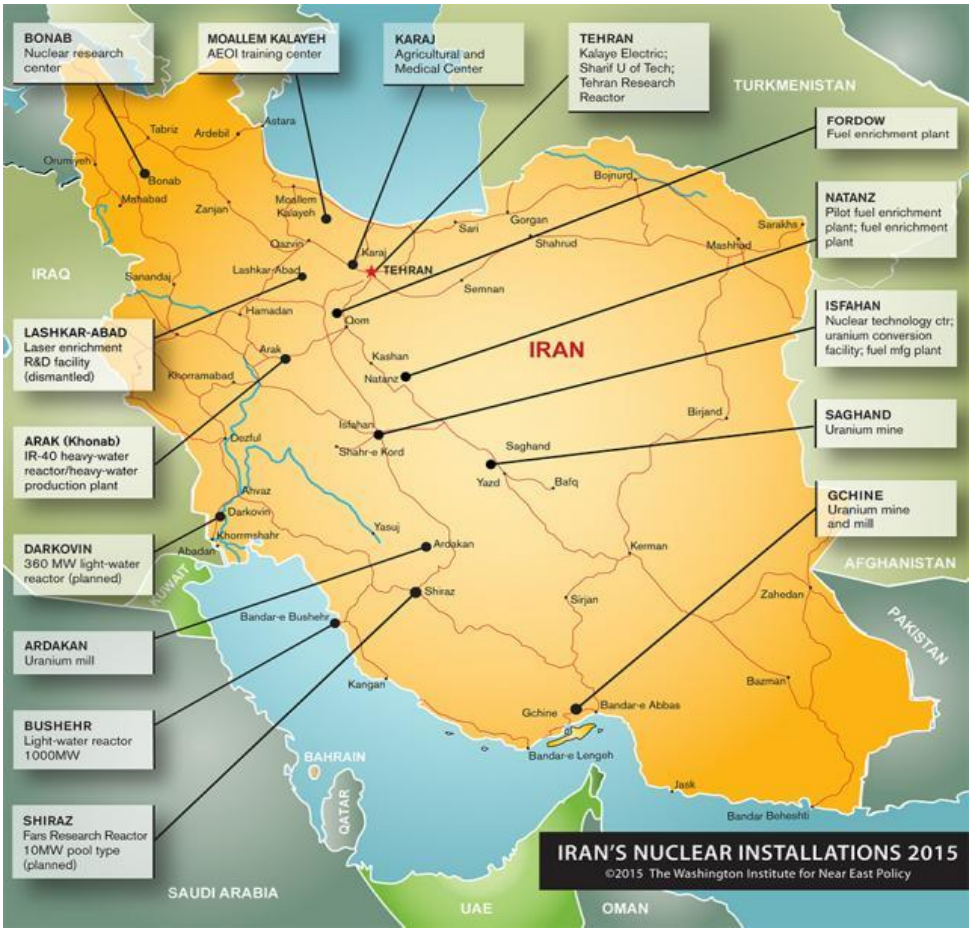
[1] "مفاعل نطنز النووي أكبر منشأة لتخصيب اليورانيوم في إيران, في https://www.aljazeera.net/ تاريخ الاطلاع 6 ماي 2026

[2] "محطة فوردو لتخصيب الوقود أحد أكبر المواقع النووية الإيرانية،" في https://www.aljazeera.net/ تاريخ الاطلاع 6 ماي 2026

مكونات ميكانيكية, بل تستند أيضا على تقنيات رقمية متقدمة وأنظمة تحكم صناعية دقيقة وهو ما يعزز كفاءتها التشغيلية, لكنه يطرح في الوقت ذاته إشكاليات تتعلق بالأمن التقني والهشاشة الرقمية .[1]

وفي مايلي خريطة توضح تموقع أبرز المنشآت النووية في البلاد :

**الشكل رقم (2) : خريطة منشآت إيران النووية**




**المصدر: The Washington Institute for Near East Policy 2015**

وعليه تكشف هذه المنشآت من خلال اختلاف مواقعها بين تحت الأرض وفوق الأرض, وتنوع وظائفها من إنتاج وردع ( إن أمكن القول ) واستخدام مدني عن منظومة نووية متطورة

[1] مفاعل بوشهر حجر الأساس للبرنامج النووي الإيراني،" في https://www.aljazeera.net/ تاريخ الاطلاع 6 ماي 2026

تسعى إلى تحقيق السيادة التكنولوجية وتحقيق الكفاءة الإنتاجية والتشغيلية, لكنها في الوقت نفسه تعتمد على أنظمة تقنية حساسة وسعت من سطح الهجوم التقليدي إلى السيبراني .

**رابعا** : ومع تزايد الاعتماد على الأنظمة الرقمية وأنظمة التحكم الصناعية في إدارة العمليات الحساسة داخل المنشآت النووية, ظهر نمط جديد من التهديدات لا يعتمد على القوة العسكرية المباشرة بل على الاختراق غير المباشر في الفضاء السيبراني.

تعتمد المنشآت النووية الحديثة بما في ذلك الإيرانية على أنظمة تحكم صناعية متقدمة (Industrial Control Systems)تُستخدم لإدارة العمليات الحساسة مثل التخصيب, التبريد, إلى غير ذلك وفي إطار تحسين أمن هذه المنشآت يتم اعتماد ما يُعرف بالأنظمة المنعزلة ( Air-gapped Systems), وهي عملية العزل المادي للأنظمة الحاسوبية أو الشبكات بحيث لا يمكنها الاتصال فعليا بأي أنظمة أو شبكات حاسوبية أخرى بهدف تقليل احتمالية تعرضها للاختراقات السيبرانية, وتساعد النسخ الاحتياطية المعزولة (Air Gap Backups) , وهي نوع آخر من هذه الأنظمة في حماية المعلومات شديدة السرية بما في ذلك الأسرار العسكرية, والبيانات المالية, والأنظمة التي تتحكم في البنية التحتية الحيوية مثل تخزين المياه, والطاقة النووية.[1]

إلا أن هذا الطرح التقليدي لأمن البنى الطاقوية القائم على العزل الفيزيائي لا يكفي في ظل تطور تقنيات الهجوم السيبراني, حيث أثبتت الأبحاث العملية أن هذه الأنظمة رغم عزلها ليست محصنة بشكل كاف, إذ يمكن اختراقها بطرق غير مباشرة عبر إدخال برمجيات خبيثة مثلا وهو ما يجعل العزل الفيزيائي مجرد حل عابر , ويُعد الهجوم السيبراني المعروف بفيروس Stuxnetعلى منشأة نطنز النووية مثالا بارزا على هذا التحول النوعي في طبيعة التهديدات حيث استهدف بشكل مباشر أنظمة التحكم الصناعية داخل المنشأة, رغم أنها كانت تعتمد على أنظمة معزولة. وقد تم تصميم هذا الفيروس لاستهداف أجهزة الطرد المركزي عبر التلاعب

[1] "What Is an Air Gap?"available at **https://www.ibm.com/think/topics/air-gap** , accessed May 6, 2026

بسرعة دورانها ما أدى إلى إتلافها بشكل تدريجي, الأمر الذي يعكس مستوى التعقيد والدقة في الهجمات السيبرانية الحديثة. ومنه لم تعد المنشآت النووية تواجه مخاطر الهجمات العسكرية فقط بل أصبحت عرضة لتهديدات إلكترونية تستهدف بيئتها التقنية, إذن فالهشاشة الرقمية في المنشآت النووية الإيرانية ناتجة عن تعقد الأنظمة وتداخلها

وفي الختام يتبين أن البرنامج النووي للجمهورية الإسلامية الإيرانية رغم سعيه نحو تعزيز السيادة التكنولوجية بالإعتماد على الرقمنة والأتمتة, أصبح في الوقت نفسه أكثر انكشافا أمام التهديدات الرقمية نتيجة تعقد بنيته التقنية. كما يعد هذا التحول مرتبطا بالبيئة الدولية بالحديث عن العقوبات التي جعلت من تحديث البرمجيات والأنظمة التشغيلية أمرا صعبا, ما أزم مشكلة التقادم التقني داخل المنشآت النووية الإيرانية.

وبناء على هذا سيتم في المطلب الموالي إلى تحليل أثر التحول الرقمي ومشكلة التقادم التقني في ظل القيود والعقوبات الدولية باعتبارها أحد أهم العوامل المفسرة لارتفاع مستوى الهشاشة السيبرانية في البنية النووية الإيرانية.

## المطلب الثالث : التحول الرقمي في إدارة الطاقة الإيرانية

شهدت البنى التحتية الطاقوية لدول العالم خلال العقود الأخيرة تحولا سريعا نحو الرقمنة, إذ تم اعتماد التقنيات التكنولوجية الحديثة في إدارة العمليات الإنتاجية والتشغيلية في المنشآت الطاقوية. غير أن هذا التحول لم يتم في بيئة تقنية مستقرة بالنسبة للدولة الإيرانية, إذ شكلت القيود الدولية الصارمة والعقوبات حاجزا أمام قدرة إيران على تحديث برمجياتها وأنظمتها التشغيلية بشكل دوري بسبب كلفتها التي تفوق ميزانيتها. وعلى إثر هذا ظهرت مشكلة قدم الأنظمة التقنية التقنية كتحدي في القطاع الطاقوي الإيراني , حيث أدى الاعتماد على أنظمة قديمة أو غير محدثة بسبب مافرضته عليها القيود الدولية إلى خلق ثغرات أمنية قابلة للاستغلال خاصة وأن التهديدات السيبرانية تواكب هذا التطور.

وعليه يهدف هذا المطلب إلى تحليل العلاقة بين التحول الرقمي والعقوبات الدولية والتقادم التقني باعتبارها عوامل مترابطة تفسر تنامي الهشاشة الرقمية في البنية الطاقوية الإيرانية.

أصبحت البنية الطاقوية الإيرانية تعتمد بشكل متزايد على أنظمة التحكم الصناعي (ICS)كأنظمة SCADA ,وأنظمة التحكم الموزع ( DCS) وغيرها التي تم التطرق إليها بالتفصيل في الفصل الأول وذكر وظائفها وأهميتها في تسيير مختلف الجوانب الفيزيائية للعمليات الصناعية كالضغط في خط الأنابيب, درجة الحرارة في المفاعل الكيميائي, سرعة المحرك في خط الإنتاج. وقد ساعد هذا الشكل الحديث من الإعتماد في تنظيم العمليات الإنتاجية بالمنشآت الطاقوية بطريقة أكثر دقة, حيث أصبحت عمليات المراقبة والتحكم والإدارة تتم بشكل آني ومستمر بعد أن كانت تعتمد الأساليب التقليدية كالتدخل البشري المباشر وطول الوقت في جمع البيانات وتحليلها[1].

مستوى الكفاءة التشغيلية داخل القطاع تعزز أيضا نتيجة الانتقال إلى تطبيق أحدث التقنيات, من خلال تحسين قدرة إدارة موارد البنية التحتية الطاقوية بشكل مرن بالإعتماد على أنظمة التشغيل (OT) وتقليل نسب الأخطاء والأعطال المرتبطة بالعمليات الفيزيائية أو غير المؤتمتة مثلا : تكتشف المستشعرات وأنظمة رؤية الماكينة العيوب في الوقت الفعلي, وتوقف العملية أو تصححها فور حدوث خطأ. إضافة إلى هذا ساعد إدماج الأنظمة الرقمية على تحليل البيانات التشغيلية في الزمن الحقيقي وهو ما جعل إمكانية اتخاذ القرارات في وقت قصير و أكثر دقة ممكنة داخل مراكز التحكم والإدارة, خصوصا بعد دمج أنظمة التشغيل

[1] Industrial Control Systems (ICS). Available at https://searchinform.com/articles/cybersecurity/type/industrial-control-systems/ accessed May 6, 2026.

(OT) مع أنظمة المعلومات (IT) لتسهيل عملية تحليل البيانات ونقلها بين المستخدمين واتخاذ القرارات في نفس الوقت[1].

كما جعل هذا التطور المؤسسات تُقلص الاعتماد على التدخلات البشرية ( نسبيا ) في بعض العمليات التشغيلية الدقيقة نتيجة تعاظم دور الأنظمة الرقمية في ضبط سيرورة العمليات الصناعية, وهو ما أدى في الأخير بالبنية الطاقوية الإيرانية (العالمية بصفة عامة) إلى الإرتباط أكثر بالبنية التكنولوجية التي تقوم عليها هذه الأنظمة سواء كان ذلك من حيث التشغيل أو من حيث الاستمرارية[2].

وعليه يعد التحول الرقمي داخل القطاع الطاقوي للدولة الإيرانية ليس فقط تحديث تقني مرحلي عابر, بل إعادة هيكلة لنمط إدارة الموارد الطاقوية في زمن أصبح للأنظمة الرقمية فيه جزءا مركزيا من آلية تشغيل وتوجيه القطاع.

إلا أن مسار التحول الرقمي في القطاع الطاقوي الإيراني لم يتم ضمن بيئة تكنولوجية مستقرة, فالجمهورية الإسلامية الإيرانية تخضع منذ عدة سنوات لعقوبات دولية أو كما يطلق عليها **بالجزاءات الإقتصادية الدولية** فرضتها قوى دولية ومؤسسات رسمية بسبب برنامجها النووي, حيث تجسدت هذه العقوبات في سلسلة من القرارات الصادرة عن مجلس الأمن الدولي أين دعى إلى توقيف (تعليق) جميع أنشطة إيران النووية المتصلة بالتخصيب والتجهيز, إضافة إلى عمليات البحث والتطوير والتعاون التقني مع الدول الأخرى كما وضع أنشطتها تحت مراقبة المنظمة الدولية للطاقة النووية, إضافة إلى هذا تم فرض حظر مالي على الأصول المالية والموارد الإقتصادية والأشخاص والكيانات التي تشترك في الأنشطة الحساسة لإيران, وكلما رفضت التسليم بالقرارات كلما تم توسيع نطاق العقوبات خصوصا بعد انسحاب الولايات

[1] "Information Technology (IT) vs. Operational Technology (OT) Cybersecurity," available at https://www.fortinet.com/resources/cyberglossary/it-vs-ot-cybersecurity accessed May 7, 2026

[2] "ما هي الأتمتة الصناعية؟ الأنواع والفوائد الرئيسية"، في https://www.omch.com/ar/what-is-industrial-automation/ تاريخ الاطلاع 7ماي 2026

المتحدة الأمريكية من الاتفاق النووي سنة 2018 ما جعل الدولة غير قادرة على استيراد البرمجيات الحديثة, فأنظمة التحكم الصناعي مثلا بحاجة إلى تحديث دوري لتحسين كفائتها التشغيلية إضافة إلى أن التجهيزات الصناعية تعتمد على خدمات مابعد البيع التي تقدمها الشركات المصنعة كالصيانة الدورية والتي قطعت بدورها تعاملاتها مع إيران بموجب الأوامر الدولية, ومع غياب هذا الدعم واجهت المنشآت الطاقوية العديد من التعقيدات كونها تعتمد الأنظمة التقليدية, الأمر الذي عزز الفجوة التقنية للقطاع أو المعروفة أيضا في الأوساط الأكاديمية بالتقادم التقني أين يصبح الإتصال بوحدات التحكم المركزية صعبا نظرا لقدم الأنظمة وحاجتها للتحديثات الجديدة, كذلك يتم فقدان البرامج المرخصة وملفات التفعيل وغيرها من المشاكل. الأمر الذي دفع بالحكومة إلى البحث عن حلول بديلة كالإعتماد على الكفاءات المحلية لتغطية النقائص وتشجيع البحث العلمي داخل البلاد[1].

وعليه شكل التحول الرقمي الذي طال البنية التحتية الطاقوية الإيرانية فرصة لتحسين المنظومة التشغيلية ودعم العمليات الصناعية, إلا أنه أنتج نوعا من الهشاشة في الأنظمة الرقمية خصوصا في ظل القيود الدولية المفروضة على البلاد, والتي حدت من إمكانية إدخال التعديلات اللازمة وجعلت القطاع بأكمله عرضة للتهديدات السيبرانية .

[1] منى حبيب أحمد، "العقوبات الاقتصادية كوسيلة ضغط في السياسة الدولية: إيران أنموذجًا"، مجلة قضايا سياسية، العدد 72 (2023)، ص 296_299

## المبحث الثاني: تطور الهجمات السيبرانية التي استهدفت البنية التحتية الطاقوية الإيرانية

يستعرض هذا المبحث تحليل أول هجوم سيبراني في العالم من حيث الخطورة Stuxnet 2010, أين ستفهم حيثياته وأسباب اختراعه لينتقل بعدها إلى إبراز وتفسير أغلب الهجمات بعد 2010 لغاية 2025 والتي عرفت تحولا في أساليب الهجوم وحتى الأهداف.

### المطلب الأول: هجوم (2010) Stuxnet كنقطة تحول في المدركات الإيرانية

يعد هجوم Stuxnet عام 2010 على منشأة نطنز النووية بإيران نقطة تحول في الأدبيات الدولية حول طبيعة التهديدات, فبعد أن كانت تقليدية مباشرة وعلى أرض الواقع أصبحت غير مرئية وفي الفضاء السيبراني, أين يتم استهداف الشبكة الرقمية للبنى التحتية الطاقوية عبر برمجيات خبيثة واختراقات إلكترونية في ظرف وجيز تختصر الجهد والتكلفة وتتجاوز أضرارها مايلحقه الهجوم المادي أو أكثر, كما لايمكن تتبع الفواعل المسؤولين عن الهجومات نظرا لصعوبة الإسناد في الفضاء الرقمي وكذا المحاكمة القانونية. وعليه سيحاول هذا المطلب توضيح السياق التقني والسياسي للهجوم ودوافعه وآثاره على البرنامج النووي بصفة خاصة والبيئة الدولية بصفة عامة.

تم اكتشاف Stuxnet لأول مرة من قبل الباحث **سيرغي أولاسن** في شركة VirusBlokAdaببيلاروسيا عام 2010 أثناء تلقي أخبار عن سلسلة من الأعطال التقنية في أجهزة الطرد المركزي بإيران. وهو عبارة عن دودة كمبيوتر (فيروس في مصادر أخرى) متطورة للغاية تستغل الثغرات الأمنية غير المستكشفة في نظام التشغيل Windows لإصابة أنظمة معينة فقط والانتشار إلى أخرى لتغطي الأعطال عددا أكبر من الأجهزة[1] .

ويستهدف Stuxnet وحدات التحكم القابلة للبرمجة (PLC) المسؤولة عن أتمتة وإدارة العمليات الفيزيائية في المنشآت الطاقوية في الوقت الحقيقي, إذ يعمل بالأساس على ايجاد الفجوات التقنية في برنامج Siemens Step 7 الذي تنتجه شركة Siemens (شركة رائدة في انتاج البرامج

[1] Harshad Katikar, Stuxnet: Analysis and Implications of the World's First Cyber-Weapon (n.p., n.d.),p 10.

المتطورة والأنظمة الرقمية المخصصة لتشغيل العمليات الصناعية) والذي تستخدمه وحدات التحكم المنطقية القابلة للبرمجة (PLCs) في أدائها لوظائفها. وكيفية تغلغل الفيروس تكمن في أن وحدات (PLCs) في برمجتها تشترط أن تكون متصلة بنظام Windows عبر أقراص USBالتي ينتقل من خلالها الفيروس إلى هذه الوحدات, وبعد أن تنفصل عنه تشرع هذه البرمجية الخبيثة في التلاعب بالبيانات والتعليمات, فترسل أوامر مزيفة تبدو وكأنها حقيقية للمستخدمين والوحدات المركزية توهمهم بنجاح العمليات, في إطار ما أسماه المختصين **الرجل في الوسط** مايجعل اكتشافه أمرا في غاية الصعوبة. بالإضافة إلى هذا تستعمل أغلب المعدات الصناعية محركات التردد المتغير المسؤولة عن ضبط سرعة تشغيل هذه المعدات, حيث يساهم Stuxnet في التلاعب بها بتغيير قيمها أثناء الهجوم ما يجعل أجهزة الطرد المركزي تدور بسرعة خارجة عن نطاقها تؤدي إلى اتلافها وتعطيل قدرتها الإنتاجية, كما أن الفيروس لايعمل إلا بعدما يتم التأكد أن هذه المحركات من تصنيع شركات معينة كالشركة الإيرانية Fararo Paya مايدعم فرضية تخصيص هذه البرمجية الخبيثة لأغراض تخريبية بالمنشآت الإيرانية, حيث كل التفسيرات التي قدمتها الدراسات ربطت بنية الفيروس ببنية المنظومة النووية الإيرانية, وسط إدعاءات بأن كل من الولايات المتحدة الأمريكية والكيان الصهيوني اشتركا في تطوير هذه الدودة الإلكترونية لاستهداف البرنامج النووي الإيراني ومنعه من التطور, ويرجع هذا إلى عام 2005 أين تم فرض قرارات على إيران بشأن توقيف مشروعها, الأمر الذي رفضته الأجهزة الحكومية الإيرانية وشرعت المراكز المتخصصة على إثر هذا في انشاء الفيروس, للحد من طموحات إيران ومر بعدة مراحل لغاية يوم اكتشافه في 2010, وسميت العملية المشتركة بين الدولتين للإطاحة بإيران بعملية الألعاب الأولمبية Olympic Games operation, هذا ولم يتم التصريح بشأن انتساب الهجوم إليهما . حيث قامت شركة الأمن السيبراني Symantec بتتبع حوالي 100,000 جهاز مصاب حتى 29 سبتمبر 2010 , كان حوالي 60,000 منها في منشأة نطنز النووية, وحسب بعض المصادر دمر ما يقارب خُمس

أجهزة الطرد المركزي, وأصيب أكثر من 200000 جهاز كمبيوتر, و تلُف 1000 جهازا ماديا[1] .

كانت تداعيات هذا الهجوم على إيران كارثية استمرت لأعوام فيما يتعلق بعملية تخصيب اليورانيوم, إضافة إلى كشف تقادم بنيتها التقنية خصوصا بعد عزوف الشركات المصنعة بيعها أحدث التقنيات لتحسين كفائتها التشغيلية وتعزيز أمنها بعد قرار العقوبات الدولية, الأمر الذي فتح على إيران باب جديد من التهديدات عبر الفضاء الرقمي وأكد صحة النظريات أنذاك في امكانية انتقال الصراع من بيئته التقليدية إلى بيئته السيبرانية, من خلال احتكار التكنولوجيا المتقدمة واستعمالها كورقة ضغط للتأثير في النظام الدولي .

هذا ولا تكمن أهمية وثقل هجوم stuxnet في حجم الأضرار التي ألحقها بالبرنامج النووي, وإنما في كونه غير الإدراك الاستراتيجي لطبيعة التهديدات التي تواجه الدول, لأنه أثبت أن امتلاك القدرات العسكرية أو حماية الحدود الجغرافية لم يعد كافيا لضمان الأمن القومي, في ظل امكانية اختراق البنية التحتية الحيوية عن بعد باستخدام تقنيات رقمية متطورة, وهذا ما يترجم مكانة الأمن السيبراني واعتباره جزءا من الأمن القومي الشامل خاصة للدول التي تعتمد على الرقمنة في تشغيل قطاعاتها الحيوية.

كما سارع المجتمع الدولي على إثر هذا الهجوم إلى إطلاق مشاريع بحثية لتطوير تكنولوجيا القطاع العسكري استعداد لجيل جديد من الحروب, الأمر الذي خلق بعد ذلك جدالا واسعا حول أخلاقيات الحرب السيبرانية, ودعوات إلى وضع قواعد دولية من شأنها تنظيم استخدام الأسلحة الإلكترونية للحد من مخاطر التصعيد في المجال السيبراني[2].

وعليه أشار هذا المطلب إلى أن هجوم Stuxnet لايكشف عن أضرار تقنية بحتة, بل في كونه أيضا يبين كيف يمكن توظيف الفضاء الرقمي بشكل غير مباشر, كأداة لتحقيق

[1] Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," Small Wars Journal, April 14, 2011, p 2_5.
[2] United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (New York: United Nations General Assembly, July 22, 2015), p.5_16

أهداف استراتيجية كانت في السابق تستوجب استخدام أدوات عسكرية مباشرة لردع الخصوم أو الدخول في الحروب, هذا إلى جانب أنه أوضح أن البنية التحتية الطاقوية أصبحت محور الاستهداف في هذه البيئة الصراعية الجديدة, ما يعني إعادة تعريف مفاهيم الردع والقوة في العلاقات الدولية .

إلا أن الهجمات لم تتوقف عند هذا العام إذ تلته عدة هجمات طالت مختلف قطاعات الدولة الإيرانية.

## المطلب الثاني: هجمات سيبرانية لاحقة على البنى التحتية للقطاعات الحيوية الإيرانية من 2010 إلى 2025

لقد كان هجوم Stuxnet عام 2010 تجسيدا فعليا لانتقال الصراع من شكله التقليدي إلى نمط جديد يعتمد على الفضاء الرقمي كساحة رئيسية لهجوم أكثر فعالية. إذ أصبحت المنظومة التقنية للبنى التحتية الطاقوية الهدف المباشر لاستهداف الدول بعد رقمنتها ودمج الأنظمة التكنولوجية بالمعدات الفيزيائية لتحسين كفائتها التشغيلية والإنتاجية, وبالنسبة لإيران لم تتوقف الهجمات عند هذا الحدث, إذ استمرت سلسلة الهجومات وتوسعت لتشمل باقي القطاعات الحيوية .

هذا ماسيتطرق له المطلب من خلال عرض أبرز هذه الهجمات وتحليلها وتوضيح أهدافها في ظل غموض الأطراف التي تقف خلفها .

ويوضح الجدول التالي أغلب الهجمات التي تعرضت لها البنية الحيوية الإيرانية :

**ملاحظة :**

توجد عدة هجمات على البنية التحتية الحيوية الإيرانية لم تصرح بها الحكومة, أشارت أغلب المواقع والمراجع التي تم الإطلاع عليها إلى أن إيران عمدت إلى إخفاء الهجمات لأسباب يرجح أنها أمنية .

**الجدول رقم (2) : الهجمات السيبرانية على البنية التحتية الحيوية من 2010 إلى 2025**

| الأثر | نوع الهجوم | القطاع المستهدف | الحادثة | السنة |
|---|---|---|---|---|
| تعطيل أجهزة الطرد المركزي | ICS Malware | نووي (نطنز) | Stuxnet | 2010 |
| تعطيل الأنظمة ومسح بيانات | Wiper Malware | النفط والغاز | هجوم وزارة النفط الإيرانية | 2012 |
| تجسس /اختراق طويل المدى للبيانات | APT Intrusion | حكومي / طاقوي | حملات اختراق سيبرانية متفرقة | 2015 |
| اختراقات مستمرة منخفضة الظهور | Cyber Espionage (APT) | الطاقة والبنية الحكومية | هجومات متقدمة مستمرة APT | 2018–2019 |
| شلل واسع في محطات الوقود | Operational Disruption | توزيع الطاقة | هجمات على محطات الوقود | 2021 |
| تسريب / اختراق بيانات | Cyber Espionage | النفط والغاز | حملات APT مستمرة | 2022–2024 |
| تعطيل خدمات تشغيلية | DDoS / Wiper / Sabotage | طاقة + خدمات | هجمات على البنية التحتية | 2023–2025 |

**المصدر** : من إعداد الباحثة

كان تركيز الهجمات (Stuxnet) واضح على المنشآت النووية, ما يثبت أن تطور الهجمات ضد إيران لم يكن عشوائيا, وإنما اتسم بالتدرج في طبيعة الأهداف والأساليب المستخدمة. أين تم استهداف أنظمة التحكم الصناعية في البداية بمنشأة نطنز وبشكل خاص أجهزة الطرد المركزي, في محاولة لإيقاف إيران عن استمرار برنامجها النووي, حيث صممت البرمجية الخبيثة بشكل يسمح لها بالتسلل إلى المعدات التقنية دون أن يلاحظ نشاطها, لتقوم بتعطيل المعدات الفيزيائية وإلحاق أقصى ضرر بها بغية إبطال برنامجها النووي. وعليه كان هذا الهجوم تجسيدا لفرضيات إمكانية نجاح الحرب السيبرانية وفهم أبعادها والغاية منها, خصوصا في بيئة رقمية اندمجت فيها المنظومة التقنية مع المنظومة الفيزيائية أين أصبحت كل العمليات الصناعية مؤتمتة, وهذا أحد أسباب نقل الصراع إلى الفضاء الرقمي .[1]

إلا أن هذا النمط اختلف بعد هذا العام, حيث بدأت ترصد الحكومة الإيرانية هجمات إلكترونية في مختلف قطاعاتها الحيوية خصوصا قطاع النفط والغاز الذي يعد المصدر الأساسي لعائداتها المالية وركيزة اقتصادها, تهدف إلى تعطيل أنظمتها التشغيلية أو الإدارية إضافة إلى التأثير على توافر المعلومات داخل المؤسسات الطاقوية, ما يؤثر بالسلب على الدورة الإقتصادية في البلاد. فمثلا عام 2012 تم الإعلان عن أن فيروسا أصاب أنظمة الكمبيوتر والاتصالات في منشآت تصدير النفط الرئيسية بإيران في جزيرة خارك, بالإضافة إلى الشبكة الداخلية ومواقع وزارة النفط والمنظمات التابعة لها عام 2012.[2]

ومع الثورة التقنية بدأت تظهر هجمات أكثر تطورا لاتعتمد على الإختراق المباشر أو الضربات السريعة, بل تتخذ طابعا أكثر تعقيدا أين تتسلل تدريجيا إلى الأنظمة وتبقى داخلها لفترات طويلة دون اكتشافها بهدف جمع المعلومات أو التأثير على العمليات التشغيلية بشكل

[1] Katikar, Stuxnet: Analysis and Implications of the World's First Cyber-Weapon .
[2] Saeed Kamali Dehghan, "Iranian Oil Ministry Hit by Cyber-Attack," available at https://www.theguardian.com/world/2012/apr/23/iranian-oil-ministry-cyber-attack accessed May 8 ,2026

غير مباشر, عرفت باسم التهديدات المتقدمة المستمرة (APT) والتي تقف ورائها جهات تتمتع بموارد وفيرة وتنخرط في هذه الأنشطة الإلكترونية الخبيثة. بعض الأبحاث والتقارير صنفت هذه الهجمات بكونها مدعومة من قبل دول بهدف تصفية الحسابات الدولية, وتقوم المنظمات العاملة في مجال الأمن السيبراني والتي تُجري أبحاثا حول التهديدات المتقدمة المستمرة بتسمية هذه الجهات بأسماء وأرقام فور اكتشافها. ونظرا لمشاركة أكثر من منظمة في هذا النوع من الأبحاث واحتمالية وجود تداخلات بينها, فقد يُطلق على جهة تهديد متقدمة واحدة عدة أسماء. وعليه لا يوجد معيار نهائي لتسمية هذه الجهات منها ALLANITE , Aoqin Dragon وغيرها[1].

وفي هذا السياق يظهر أن نطاق الاستهداف قد توسع أيضا ليشمل البنية التحتية الخدماتية المرتبطة بالطاقة مثل محطات الوقود وشبكات التوزيع. حيث لم تعد الأهداف مقتصرة على المنشآت الإستراتيجية والحيوية الكبرى, بل تشمل الخدمات اليومية المرتبطة بالشعب الإيراني ما يوسع دائرة تأثير هذه الهجمات بما قد يؤدي إلى خلق حالة من الضغط الداخلي[2].

وعليه يمكن القول أن الهدف الرئيسي لهذه الإستهدافات لم يعد يقتصر على إحداث أضرار تقنية, بل تجاوزه ليقوم بتعطيل الوظائف الحيوية للبنية التحتية الحيوية للجمهورية الإسلامية الإيرانية وخلق حالة من عدم الإستقرار التشغيلي داخلها, ما انعكس سلبا في إدارة الدولة لمواردها خاصة في مايخص القطاع الطاقوي الذي يعد مركز ثقل للدولة. هذا بالإضافة إلى صعوبة اسناد الهجمات أين يتعذر على الدولة تحديد الفواعل أو الجهات الرئيسية لهذه

[1] Cybersecurity and Infrastructure Security Agency (CISA), "Nation-State Cyber Actors," U.S. Department of Homeland Security, availabale at, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors accessed May 9, 2026

[2] "Iran petrol stations hit by cyberattack, oil minister says,"available at https://www.reuters.com/world/middle-east/software-problem-disrupts-iranian-gas-stations-fars-2023-12-18/ accessed May 9 ,2026

الهجمات فقط شكوك واتهامات تزيد من تعميق المشهد الأمني, ويجعلها تجد صعوبة في كيفية الرد ( الإستجابة) .

وختاما, نستنتج أن الهجمات على البنية التحتية الطاقوية الإيرانية توسعت من حيث طبيعتها (أنواعها) ونطاق استهدافها ودرجة تعقيدها, إذ انتقلت من استهداف المنشآت النووية إلى باقي القطاعات الحيوية التي تمس سير الدولة يعكس تحولا في الاستراتيجية الهجوميةمن إحداث ضرر تقني مباشر إلى ممارسة ضغوط اقتصادية وحتى اجتماعية تؤثر في قدرة إيران على إدارة مواردها الحيوية, إلى جانب أنها كشفت أن النجاح في الانتقال إلى الأنظمة المتطورة لا يتم قياسه بزيادة الكفاءة التشغيلية والإنتاجية, وإنما في قدرة الدولة على إدارة المخاطر الناتجة عنه. هذا وتطرح عدة تساؤلات حول الجهات المسؤولة والدوافع التي تحركها .

## المطلب الثالث : الفاعلون وإشكالية اسناد الهجمات السيبرانية

لم تعد الهجمات السيبرانية الموجهة ضد البنى التحتية الطاقوية للدول مجرد حوادث تقنية عادية, بل تحولت إلى أدوات يتم الاعتماد عليها في الصراع الدولي الحديث نظرا لصعوبة تحديد الفواعل فيها, ما جعل الدول تواجه صعوبات في كيفية بناء سياساتها الحمائية وهو ما يعرف في الدراسات الأمنية بإشكالية الإسناد .

إن مسألة تعدد الفواعل في العلاقات الدولية من البديهيات إذ نظر لها منذ السبعينيات , أين تم تجاوز فكرة الدولة هي الفاعل الوحيد في المشهد الدولي لتشمل المنظمات الحكومية وغير الحكومية, الشركات متعددة الجنسيات, الأفراد, الجماعات الإرهابية وغيرها. إلا أن الإشكال اليوم يكمن في الفضاء الرقمي أين يصعب تحديد الفواعل الحقيقية المسؤولة عن الهجمات أو إثبات وجودها من الأساس, إذ تستطيع الإختباء خلف جدران تقنية عديدة تسمح باخفاء هوية المسؤول أو تغيير مسار الهجوم عبر خوادم وسيطة خصوصا مع استخدام أحدث التكنولوجيات في هذا المجال, إضافة إلى أن الفواعل لا يندرجون ضمن فئة معينة بل ينشطون في أشكال مختلفة, فقد يكون المسؤول عن الهجوم دول بشكل غير مباشر من خلال تجنيد جهات متخصصة في العمليات السيبرانية مثل APT أو مجموعات قرصنة مستقلة أو شبه

مستقلة عن الدول, أو في غالب الأحيان حتى جهات وسيطة بهدف تضليل عملية الإسناد الحقيقية للهجمات ما يخلق حالة من الغموض ويعقد نمط الفهم و التحليل لدى المستهدفين, كما يكلفهم الأمر الكثير من الوقت والمجهود في جمع الأدلة فالمهاجم يقوم بزرع أدلة مضللة لخداع أفراد الأمن السيبراني بالرغم من استخدام تقنيات مثل الأدلة الجنائية وإعادة الهندسة العكسية, وتتبع المصدر, وفخاخ الحواسيب, وتقنيات تحويل المسارات للعثور على أدلة يمكن أن تقود إلى الجناة .[1]

في هذا السياق وُجد محللون آخرون يرون في هذا الطرح نوع من المبالغة, فحسبهم مسألة الإنكار والإخفاء لم تعد ذات فعالية, لأن الضحايا هم من أصبحوا يحددون عتبة الإثبات بأنفسهم. فالصراع بالأساس وجد بين الدول تغيرت فقط طبيعته وبيئته وأشكاله, فمسألة وجود فاعلين آخرين غير الدول يستهدفون البنى الحيوية للدول ماهي إلى حجة اخترعتها الدول لتبرير أفعالها عند الصراعات, ومن تقول عنها جهات اجرامية ماهي إلا وكلاء تقوم بتجنيدهم وتوظيفهم لتحقيق أهدافها وكذا تجنب المواجهة المباشرة و العقوبات الدولية. ففي الفضاء السيبراني أصبح من السهل تتبع الهجمات حتى لو أخفت الدولة ذلك بالنظر إلى وجود أحدث التقنيات في المجال, إضافة إلى السياق السياسي الذي تستطيع الدول أن تحدد فيه الأطراف التي تربطها معها علاقات توتر واحتكاك وتبني قرارها بالإعتماد عليه, فالسياسة الدولية قائمة في الأخير على مبدأ الشك ومنه تستطيع توجيه ضربات عكسية ما يعني أن خطر التصعيد مازال قائما .[2]

وبالنظر إلى الحالة الإيرانية يمكن فهم استهداف منظومتها الطاقوية ضمن سياق جيوسياسي واستراتيجي شامل, يهدف إلى إعادة هيكلة ميزان القوى في المنطقة من خلال شل أهم مصادر قوتها وهو القطاع الطاقوي مستخدمة تقنيات التطور التكنولوجي في هذا المجال.

---

[1] Paulo Shakarian et al., "An Argumentation-Based Framework to Address the Attribution Problem in Cyber-Warfare," arXiv preprint arXiv:1404.6699 (2014), p. 1.

[2] Canfil, Justin Key. " The Illogic of Plausible Deniability: Why Proxy Conflict in Cyberspace May No Longer Pay." Journal of Cybersecurity 8, no. 1 (2022). https://doi.org/10.1093/cybsec/tyac007

وعليه, يمكن القول أن قضية الإسناد في الفضاء الرقمي لا تتمحور حول صعوبة تحديد الفواعل الرئيسية, بل تشمل أيضا بنية هذا المجال المعقدة التي تسمح بتداخل الأدوار بين الدول والفواعل الوسيطة الأمر الذي يجعل مسألة تحديد المسؤولية عملية نسبية تقوم على الشك أكثر من اليقين .

وإنطلاقا من هذا يمكن تلخيص الدوافع وراء هذه الهجمات فيما يلي :

- ✓ إعادة هيكلة ميزان القوى من خلال استهداف البنى الحيوية للدول خاصة القطاع الطاقوي باعتباره ركيزة الإقتصاد .
- ✓ الردع غير المباشر والذي يجعل الدول تحقق أهدافها بدون مواجهة عسكرية في اختصار للوقت والتكلفة المادية والبشرية .

وختاما, يتضح أن الهجمات السيبرانية على البنى التحتية لاتفسر من زاوية التطور الرقمي أو توسع نطاق استهدافها بل تأخذ بعين الإعتبار مسألة انكار الفاعلين وحدود المسؤولية في البيئة الدولية, فإشكالية الإسناد أصبحت من أبرز التحديات التي تواجه الأمن الدولي الحالي, لأنها لاتؤثر فقط في تحديد المسؤولية القانونية عن الهجمات, وإنما تمتد للتأثير في خيارات الدول المتعلقة بالردع وإدارة الأزمات وصياغة القرارات. وبالنسبة لإيران فرض هذا الواقع عليها أن تتبنى مقاربة أمنية شاملة تقوم على تعزيز القدرات السيبرانية وانشاء الهياكل والمؤسسات المتخصصة لحماية بنيتها التحتية الحيوية .

## المبحث الثالث : حماية البنية التحتية الحيوية الإيرانية : المحددات وواقع الفعالية

يعرض هذا المبحث الإطار المؤسسي والتشريعي للأمن السيبراني في إيران, وتقييم فعالية استراتيجيتها في حماية قطاعاتها الحيوية من التهديدات الرقمية في ظل بيئة سياسية وأمنية متوترة وضغوطات خارجية, اللذان فرضا عليها تشكيل هذا النوع من النماذج لإدارة مجالها الإفتراضي .

### المطلب الأول : الهيكل المؤسساتي لمجال الأمن السيبراني الإيراني

يتم التعامل مع الفضاء السيبراني في إيران على أساس أنه جزء لا يتجزأ من أمنها القومي وليس مجرد مجال تقني بحت خصوصا بعد الهجمات التي استهدفت بنيتها الطاقوية, إذ برز نشاطها واهتمامها بهذا المجال مع نهاية العقد الأول من الألفية الثالثة, عملت من خلاله على تكوين منظومة مكلفة بحماية مجالها السيبراني بما يخدم أهدافها الإستراتيجية. وهو ما سيتطرق إليه هذا المطلب من خلال توصيف بنية القوة السيبرانية الإيرانية.

قامت إيران بانشاء مجموعة من القوى والهيئات التي تضطلع بمهام الدفاع السيبراني عن قطاعاتها الحيوية والإستراتيجية, وقوى أخرى مدربة لخوض الحروب السيبرانية, كما تخضع هذه الأجهزة لقيادة وإشراف كبرى المؤسسات بالبلاد : **كحرس الثورة الإسلامي** والذي يُعنى بمهام حماية الثورة والنظام الجديد من التهديدات الداخلية والخارجية, أُنشئ كقوات مستقلة عن وحدات الجيش السابق. **وزارة الإستخبارات والأمن القومي** والتي تتولى وظيفة جمع وتحليل المعلومات داخليا وخارجيا, ومكافحة التجسس, وحماية النظام الإسلامي. **ووزارة الاتصالات** المسؤولة عن الخدمات البريدية والهواتف وتكنولوجيا المعلومات في البلاد[1] .

ويمكن تعداد أهم هذه الأجهزة المكلفة بمهام الدفاع والهجوم السيبراني فيما يلي:

- **المجلس الأعلى للفضاء السيبراني** والذي أُنشئ عام 2012 بأمر من المرشد الأعلى علي خامنئي و هو الهيكل المسؤول عن وضع السياسات العامة في الفضاء الرقمي,

[1]أنيس عبد الوهاب بن أحسن، " القوة السيبرانية الإيرانية وأثرها على الاستقرار الإقليمي"، مجلة السياسة العالمية، المجلد 6، العدد 2 (2022)، ص 735 .

يترأسه رئيس البلاد ويعمل بالتنسيق بين مختلف الجهات الحكومية بما في ذلك الحرس الثوري, وزارة الاتصالات, ووكالات الاستخبارات لضمان التنسيق في وضع استراتيجيات الدفاع والهجوم السيبراني[1] .

- **الشرطة الإيرانية المكلفة بالجرائم الإلكترونية (FATA)** المختصة بمراقبة وتحليل الأنشطة عبر الإنترنت داخل البلاد, من خلال تتبع أنشطة معارضي النظام والمنشقون عنه وفرض رقابة صارمة عليهم واعتقالهم, بالإستعانة بتقنيات مراقبة متقدمة لرصد لكل من يروج للأفكار المعارضة أو ينشر محتوى يُعتبر تهديدا للنظام الإيراني[2].
- **قوات الباسيج** : وتعني التعبئة بالفارسية أو رسميا منظمة تعبئة المستضعفين, تأسست نهاية عام 1979 بأمر من الخميني الذي طالب بإنشاء جيش من 20 مليون رجل لحماية الثورة ونظامها السياسي والديني. تختص بحماية الجبهة الداخلية و احباط أي تحركات معارضة للنظام, أما وقت السلم تضطلع بإنفاذ الأعراف الاجتماعية في البلاد وتعمل كشرطة أخلاق على المعابر ونقاط التفتيش والمتنزهات, كما تنتشر وقت الكوارث الطبيعية. وفي الفضاء الرقمي فتقوم بمراقبة النشاط الإلكتروني والقبض على الخونى الموالين لأعداء إيران. في سبتمبر 2019 أعلن قائد الباسيج غالم رضا سليماني عن تعزيز قدرات قوة الباسيج السيبرانية عبر استحداث كتائب جديدة تماشيا مع التحديات التي تواجه بلادهه في الفضاء الإلكتروني[3]
- **الجيش السيبراني** : تم إنشائه بقيادة قائد الحرس الثوري الإيراني محمد علي جعفري وإلحاقه بجهاز الاستخبارات التابع للحرس الثوري من مهامه : مواجهة المواقع الإلكترونية الأجنبية واتخاذ تدابير ضدها ومراقبة التهديدات الإلكترونية التي تستهدف

---

[1] حسن سلمان خليفة البيضاني، " الحرب السيبرانية في المواجهة العسكرية الإيرانية (الإسرائيلية): الإمكانيات وحدود التأثير"، في https://www.hcrsiraq.net تاريخ الاطلاع 10 ماي 2026

[2] "Iranian Cyber Police," available at, https://www.opensanctions.org/entities/NK-JuSFjNaaxPpNk3kwMpaSGT accessed May 10, 2026

[3] "من يقاتل في الشوارع ومن يقود الحرب؟ الفرق بين الباسيج والحرس الثوري"، في https ://www.aljazeera.net/ تاريخ الاطلاع 11 ماي 2026

النظام داخل إيران والتصدي لها. تُخصص له ميزانية ضخمة ويقدر عدد أفراده حوالي 2500, في حين يدعم أعضاء مجلس الشورى (البرلمان) التابع للنظام الديني علنا الأعمال غير القانونية التي يقوم بها الجيش السيبراني, حيث قالت فاطمة عليا عضو لجنة الأمن في المجلس في 28 أكتوبر 2010 : فيما يتعلق بالحرب السيبرانية نحتاج في ظل الظروف الراهنة إلى تخصيص ميزانية كافية لشراء المعدات اللازمة لهذا النوع من الحروب حتى نتمكن من تكريسها للحرب السيبرانية والجيش السيبراني. من بين العمليات أقر بها الجيش السيبراني الإيراني : اختراقه ل 500 موقع في وقت واحد بالإضافة إلى تعطيله شبكات الاستخبارات والمواقع الإلكترونية الخاصة في دول أخرى بتاريخ 20 نوفمبر 2010 كما تبنى الهجمات التي استهدفت موقع تويتر ومحرك البحث الصيني بايدو[1].

في حين وافق قائد الحرس الثوري الإيراني العام أنذاك محمد علي جعفري على خطة جعل الجيش السيبراني القوة السادسة للحرس الثوري للعمل داخل إيران بالتعاون مع قوات الباسيج لقمع الاحتجاجات والانتفاضات الاجتماعية , بالإشتراك مع فيلق القدس خارج الحدود للتدخل في شؤون الدول الأخرى لخدمة أهداف النظام الإيراني خارجيا[2].

- **منظمة الدفاع السلبي** والتي تم انشائها في أكتوبر 2003 بعد **عملية حرية العراق** حسب عدة باحثين يرجع سبب قيامها لاحتراز إيران من قيام تحالف عسكري دولي ضدها. وتتلخص مهامها في : وضع السياسات والتخطيط والتوجيه والتنظيم والتنسيق والمراقبة والرصد والتشغيل فيما يخص أنشطة الدفاع السلبي والدفاع المدني التي تمارسها الوكالات المنافسة والمعارضة لإيران, تتعامل أيضا مع التهديدات البيولوجية

[1] Staff Writer, "NCRI Publishes Report on Iran's Cyber Army," National Council of Resistance of Iran (NCRI), available at https://www.ncr-iran.org/en/news/iran-protests/ncri-publishes-report-on-iran-s-cyber-army/ accessed May 11 2026

[2] Ibid .

والإشعاعية والكيميائية. ومع بروز التهديدات السيبرانية, تم إضافة خطط بشأن التعامل مع الهجمات الإلكترونية من خلال تسخير كافة الموارد الرقمية وغير الرقمية الوطنية للاستجابة لأي هجوم إلكتروني على البنية التحتية الحيوية في إيران من قبل جهات معادية . هذا وتم ترقيتها في السنوات الماضية إلى وزارة للحرب الإقتصادية و بلغت ميزانيتها الخاصة 34 مليون دولار خلال السنة المالية الماضية ومن المتوقع زيادتها في المرحلة المقبلة .[1]

كما تقوم الحكومة الإيرانية على تنفيذ عدة تدريبات سيبرانية شاملة سنويا بمشاركة مختلف قطاعات الدولة, بهدف تعزيز قدرة المؤسسات العسكرية والمدنية على مواجهة الهجمات الإلكترونية الخطيرة وتطوير آليات اكتشاف الهجمات السيبرانية والتقنيات المتقدمة لحماية الأنظمة الحساسة من أي تهديدات خارجية[2].

هذا وعملت إيران أيضا على تجنيد مجموعة من الفواعل غير النظامية في إطار التوتر الذي تعيشه مع القوى الدولية والإقليمية, لحماية مصالحها الوطنية وكرد فعل عن الهجمات السيبرانية التي تتعرض لها, الأمر الذي عبر عنه عدة قادة إيرانيين, وحسب عدة تقارير دولية مختصة في هذا المجال يُعتقد أنها تعمل تحت إشراف الحرس الثوري الإسلامي ووزارة الاستخبارات والأمن. نذكر منها:

- **مجموعة APT35** تعرف أيضا باسم Magic Hound أو Charming Kitten أو Educated Manticore بدأت نشاطها منذ عام 2014 , يُزعم أنها مدعومة من قبل الحكومة الإيرانية. قامت بتنفيذ عدة عمليات تجسس إلكتروني استهدفت فيها وكالات حكومية ومنظمات عسكرية وشركات طاقة خاصة في الولايات المتحدة الأمريكية

[1] Farzin Nadimi, Iran's Passive Defense Organization: Another Target for Sanctions, available at **https://www.washingtoninstitute.org/policy-analysis/irans-passive-defense-organization-another-target-sanctions** accessed May 11, 2026

[2] National Council of Resistance of Iran (NCRI) **op.cit**

والكيان الصهيوني. تعتمد على هجمات التصيد الاحتيالي من خلال استغلال الهندسة الإجتماعية لتخدع الضحايا وتجبرهم على فتح ملفات خبيثة وروابط مزيفة بهدف سرقة بيانات إعتماد المستخدمين, كما استغلت أيضا ثغرات أمنية وقامت باستهداف مواقع التوزيع وسلاسل التوريد[1].

- **مجموعة APT42** : والتي يزعم ارتباطها بالحرس الثوري الإيراني تنشط منذ عام 2015 على الأقل, تستهدف الأفراد والمنظمات ذات الأهمية بالنسبة لإيران كالدبلوماسيين والمسؤولين العسكريين والصحفيين من مختلف البلدان, خصوصا الولايات المتحدة والكيان الصهيوني وإيران نفسها ( المعارضين). تقسم عملياتها عبر ثلاث فئات : جمع بيانات الاعتماد وعمليات المراقبة ونشر البرمجيات الخبيثة, يشاع أيضا أنها تتشارك التقنيات والأدوات مع **مجموعةAPT35** في حين يختلفان من حيث الأهداف والمهارات[2].
- **شركة Emennet Pasargad الإيرانية** : في السابق عرفت باسم Eeleyanet Gostar و Net Peygard Samavat ويرجع نشاطها حسب عدة مصادر إلى عام 2020, تنفذ عمليات رقمية ضد مؤسسات في الولايات المتحدة وأوروبا والكيان الصهيوني ودول أخرى في الشرق الأوسط. تركز في نشاطها على عمليات الاختراق والتسريب كأسلوب أساسي, حيث تتسلل إلى البنى التحتية للمؤسسات من أجل استخراج معلومات حساسة لتتمكن من تسريبها لاحقا. ضحاياها أغلبهم موسسات ضخمة ذات قاعدة عملاء واسعة, خصوصا تلك المؤسسات التي تستخدم خدمات الويب وتعتمد لغة PHP أو قواعد بياناتMySQL , والتي يمكن تحليلها بسهولة باستخدام أدوات اختبار الاختراق المتاحة للجميع .[3]

[1] "The Iranian Cyber Capability," available at **https://www.trellix.com/blogs/research/the-iranian-cyber-capability** accessed May 11. 2026
[2] Ibid
[3] Ibid

- **فريق Ashiyane للأمن الرقمي :** وهو عبارة عن مجموعة إيرانية للقرصنة والأمن السيبراني تأسس عام 2002, بدأ ببضعة قراصنة ماهرين ثم تطور ليصبح من أكبر وأهم المجموعات في إيران, تقوم أعماله على تشويه المواقع الإلكترونية خاصة مواقع الحكومات الأجنبية المعارضة لإيران بالإضافة إلى تحديد الثغرات الأمنية في المواقع الإيرانية ومعالجتها. مع مرور الوقت تم انشاء مركز تدريب خاص به و شركة أمنية وخدمات استضافة مواقع إلكترونية,كما قدم الفريق دورات في القرصنة والأمن السيبراني في جامعة شريف للتكنولوجيا.كما احتل المرتبة الثانية عالميا في مجال تشويه المواقع الإلكترونية على منصة Zone-H وحصل على لقب أفضل فريق قرصنة. وحسب بحث أجرته مؤسسةHRA حافظت المجموعة على صلات مع الحرس الثوري الإيراني وشرطة الأمن السيبراني الإيرانية, الأمر الذي مكنها من تجنب القيود التي استهدفت مجموعات القرصنة الأخرى في البلاد[1].

ومن خلال هذا يتضح أن إيران عملت على تطوير منظومتها الرقمية باستحداث هيئات ومراكز نظامية وغير نظامية متخصصة لإدارة المجال السيبراني من أجل الإستجابة لأي نوع من التهديدات وكذلك حماية بنيتها الحيوية إدراكا منها أن التهديدات لا تمس قطاعا بعينه وإنما كافة القطاعات, الأمر الذي يدل على أن الفضاء الرقمي أصبح محور أساسي من محاور الأمن القومي للبلاد إلى جانب أنه يطرح تساؤل حول إمكانية التنسيق بين هذه الفواعل المتعددة وعدم تداخل أدوارها, خصوصا وكلها أدوار ذات طابع أمني عسكري هدفها في المقام الأول حماية النظام الإيراني من الإعتداءات الداخلية والخارجية,

إلى جانب هذا, وضعت تشريعات وسياسات وطنية تدعم هذا الطرح .

[1] Spreading Justice, available at **https://spreadingjustice.org/group-violator/** accessed May 12, 2026

## المطلب الثاني : الهيكل التشريعي لحماية البنية التحتية الحيوية الايرانية :

عملت إيران على انشاء مؤسسات مختصة لحماية فضائها الرقمي, لكن هذا وحده لايكفي ما لم يدعم بإطار قانوني وتنظيمي يضفي الشرعية على هذه الأجهزة ويحدد قواعد التعامل مع التهديدات وكيفية الإستجابة لها, الأمر الذي جعل إيران تسن قوانين و تشريعات تنظم بها مجالها وتحمي من خلالها بنيتها الحيوية كافة دون تفضيل قطاع على آخر, فهي تدرك جيدا أهمية الفضاء السيبراني كأداة للقوة الوطنية وعنصر أساسي في صياغة الأمن القومي الإيراني

بعد التهديدات السيبرانية المتكررة التي شهدتها الدولة الإيرانية خصوصا هجوم Stuxnetعام 2010, زاد اهتمامها بالمجال السيبراني وبدأت في سن قوانين تضبط من خلالها فضائها الرقمي لتوفير حماية أكبر لمنظومتها الحساسة. ويمكن أن نلتمس أول قوانينها عام 2000 حيث منحت الحماية القانونية لمُنتجي و مبدعي البرمجيات الحاسوبية , ونظمت حقوق الملكية المتعلقة بها, إذ حرص القانون أيضا على تسجيل البرمجيات رسميا وفرض عقوبات على من يحاول انتهاك هذه الحقوق, في انعكاس واضح لبداية تبلور رؤية إيران التنظيمية لفضائها الرقمي.[1]

كما أصدرت عام 2009 / 2010 قانون الجرائم الإلكترونية والتابع للمادة 123 من دستور الجمهورية الإسلامية الإيرانية الذي وُضع ليتعامل خصيصا مع التهديدات التي لها صلة بالأمن القومي كالاختراقات والوصول غير المصرح به إلى البيانات أو أنظمة الكمبيوتر أو الاتصالات المحمية بإجراءات أمنية أو التجسس الحاسوبي .[2]

هذا بالإضافة إلى إنشاء المجلس الأعلى للفضاء السيبراني عام 2012 الأمر الذي كشف عن جدية إيران واهتمامها بتطوير منظومتها أكثر, حيث يقوم المجلس بمهمة تنسيق

[1] Act on the Protection of Rights of Computer Software (Iran, 2000).
[2] Islamic Consultative Assembly, Computer Crimes Law (Tehran: Islamic Republic of Iran, 2009), available at, **https://rc.majlis.ir/fa/law/show/135717** accessed May 13, 2026

السياسات السيبرانية ورسم التوجهات العامة المرتبطة بالأمن الرقمي كما يشرف على مركز الأبحاث وتطوير القدرات التكنولوجية ويتعاون مع عدة هياكل حساسة بالدولة.[1]

مايعني أن الجمهورية الإيرانية لم تعتمد مقاربة دفاعية رقمية وحدها بل اتجهت إلى الربط بين البعد القانوني والبعد المؤسساتي.

وعليه يمكن القول أن إيران وُفقت في استحداث أرضية تنظيمية ووقائية, لكن هذا وحده لا يكفي ولا يعني بالضرورة تحقيق نتائج فعالة لأن نجاح تشريعاتها مرهون بمدى ترجمة هذه القوانين إلى ممارسات ملموسة.

إضافة إلى صياغة التشريعات والقوانين عملت الدولة الإيرانية على تطوير سياسات لحماية البنى التحتية الحيوية لكونها تعتبرها عنصرا من عناصر أمنها القومي, خاصة قطاع الطاقة الذي يعد ركيزة الإقتصاد الوطني الإيراني ومدى مساهمة عائدات النفط والغاز في الخزينة العامة الأمر الذي جعله يتعرض لتهديدات إلكترونية كثيرة تزداد عاما بعد عام . لكن إيران لم تعمل على سن قوانين تخص حماية المنشآت الطاقوية وحدها حسب الاطلاع على سياساتها السيبرانية, لأن القطاع الطاقوي لا ينفصل في عقيدتها الاستراتيجية عن باقي القطاعات الحيوية التي وجب حماية منظومتها المادية والتقنية حسب عدة مصادر رسمية, خصوصا مع هجوم Stuxnet الذي كشف أن استهداف أنظمة التحكم الصناعية رغم عزلها الشبكي يؤدي مباشرة إلى خسائر مادية تستمر لأعوام, ومع تصاعد موجة الاستهدافات في الأعوام اللاحقة لتشمل باقي القطاعات كان لابد من الاهتمام بتطوير أنظمة التحكم الصناعي وأنظمة المعلومات والتشغيل وتوسيع استخدام العزل الشبكي في بعض الأنظمة الحساسة وتقليل نقاط الانكشاف المحتملة, أين تم الإستعانة بالخبرات المحلية واستقطاب أخرى أجنبية ودعم

[1] Luigi Toninelli, "Forward Defense in Cyberspace: Iran's Hybrid State-Hacking Doctrine," ISPI (Istituto per gli Studi di Politica Internazionale) available at https://www.ispionline.it/en/publication/forward-defense-in-cyberspace-irans-hybrid-state-hacking-doctrine-229198 , accessed May 13 ,2026

مشاريع بحثية وزيادة نسب تمويل هذا المجال للعمل ليس فقط على صد الهجمات وإنما الإستجابة لها واستمرار العمليات الصناعية دون أن يتعمم الضرر .

ومن أبرز ما حققته إيران في هذا المجال نذكر :

- ✓ في عام 2012 أثبت المسح الميداني لمؤسسة Scopus أن الإنتاج العلمي لإيران بلغ المرتبة 17 عالميا بعد أن بلغ عدد البحوث المنشورة 34,155 بحثا متفوقة بذلك على كل من السويد وتركيا . أما في عام 2022 فقد وصلت البلاد إلى المركز الـ 15 عالميا بأكثر من 78 ألف إنتاج علمي. في حين بلغت نسبة النمو في الإنتاج العلمي خلال السنوات 1996_2004 400% وحصدت المرتبة الأولى , تليها الصين في المركز الثاني.[1]
- ✓ كما تعد شركة Raspina NetPars من أكثر الشركات مهارة في العالم وتتمثل وظيفتها في الاستفادة من المعرفة والمعايير الحالية في العالم لحل المشكلات وزيادة مستوى المعرفة التقنية والوعي لدى الشركات والمؤسسات في مجال أمن المعلومات[2]
- ✓ إضافة إلى شركة إيران سايت Iran Site وهي أول شركة تصميم مواقع إلكترونية في إيران تروج لأنواع عديدة من خدمات التسويق الرقمي في عام 2025[3]

فهي تنظر إلى الهجمات السيبرانية كجزء من القدرات العسكرية غير المتكافئة التي تحتاجها لمواجهة خصومها, لذلك تسعى دائما إلى تطوير منظومتها الخاصة .

إلا أن هذه السياسات واجهت تحديات كبيرة نتاجا لتقادم بعض الأنظمة التقنية وصعوبات في تحديث البرامج المتطورة بسبب العقوبات المفروضة على إيران, ما جعل أغلب السياسات الحمائية تواجه عقبات تحد من فعاليتها العملية.

---

[1] حسن مظفر الرزو, التهديد السيبراني الإيراني : الملف المضاف إلى برنامجه النووي ودوره المحتمل في تأجيج صراع من نمط جديد ( برلين: المركز الديموقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية , 2022) , ص 74

[2]," TechBehemoths, availabale at, https://techbehemoths.com/company/raspina-net-pars accessed May 13, 2026

[3]"IRANSITE Company Profile," TechBehemoths, available at https://techbehemoths.com/company/iransite accessed May 13 ,2026

ومنه إذا كان التشريع يمثل الإطار القانوني وسياسات الحماية والوقاية تمثل الجانب الإجرائي, فإن مفهوم **السيادة الرقمية** يعد الخلفية الفكرية والسياسية التي ترتكز عليها هذه التوجهات .

إذ يرى صناع القرار في إيران أن **السيادة الرقمية** هي امتداد للسيادة الوطنية مايفسر رغبة وسعي الدولة في تطوير قدارتها من أجل التحكم ببنيتها التقنية و تقليص اعتمادها على المنظومة الغربية في المقام الأول, ثم الإعتماد عليها داخليا من خلال ضبطها وتنظيمها لأغراض رقابية حفاظا على النظام والأمن العام خصوصا بعد احتجاجات 2009 أو مايعرف **بالحركة الخضراء**, أين تم استغلال الفضاء الرقمي في تعبئة سياسية خارج نطاق الدولة ما هدد استقرارها الداخلي, وعليه تبلور لدى الحكومة الإيرانية فكرة انشاء إنترت وطني المعروف **بمشروع الشبكة الوطنية للمعلومات** وترتكز على مجموعة واسعة من مراكز البيانات الوطنية والمحلية Data Centers لحماية المجتمع الإيراني من التأثير الخارجي الغربي خصوصا في فترة الأزمات. كما عملت على استحداث شبكة وطنية علمية أخرى تقوم بالتنسيق بين الجامعات ومراكز البحث والتطوير العلمي في كل أنحاء للبلاد وتعد جزءا من الشبكة الوطنية للمعلومات, بدأت الشبكة عمليا كتجربة عام 2011 ثم تحولت إلى العمل فعليا عام 2012[1].

ومن خلال هذا يتضح أن حماية البنية التحتية الحيوية عامة والطاقوية خاصة ليست مسألة تقنية منفصلة عن مفهوم حماية السيادة الإيرانية ما يسمح بتداخل وتعدد مستويات الأمن القومي الإيراني, إلا أن هذا الإطار الصارم لايلغي وجود ثغرات أو فجوات تحد من تحقيق كفاءة عالية.

وختاما, يتضح أن استراتيجية إيران لحماية بنيتها الحيوية جمعت بين بناء مؤسسات واستحداث سياسات حمائية وقائية, ضمن مقاربة أوسع تجمع كل مقومات أمنها القومي بالاعتماد على كفاءاتها المحلية وخبراتها السابقة مع الهجمات السيبرانية .

[1] الرزو, مرجع سابق, ص 76_77

## المطلب الثالث: تحليل واقع فعالية الحماية السيبرانية في القطاع الطاقوي الإيراني

عملت إيران على بناء وتطوير منظومة مؤسساتية وتشريعية لحماية بنيتها التحتية الحيوية عامة والطاقوية بصفة خاصة وهو ما تم التفصيل فيه في المطلبين السابقين, الأمر الذي يجعل من تقديم تحليل أو تقييم لمدى فعاليتها أمرا ضروريا, فمسألة أن يكون هناك هياكل و أجهزة حكومية وسياسات وقوانين لا ينم عن الكفاءة و الحماية الكلية لهذه القطاعات. ومنه سنحاول في هذا المطلب تحليل جاهزية وفعالية السياسة الحمائية الإيرانية بالوقوف عند مواطن القوة والقصور واستخلاص النتائج.

في إطار خلق طبقة حماية لبنيتها التحتية عملت إيران على استحداث هيكل مؤسسي متعدد الأبعاد أين نرى وجود مراكز وهيئات عسكرية وأمنية وتكنولوجية تعمل في إطار شامل ومتكامل تخضع فيه لكبرى المؤسسات الحكومية في إيران لاتخاذ أهم القرارات وتوجيهها, ما يوضح أن هناك تنظيم وتوزيع في المهام ويبرز غاية الدولة وجديتها في التعامل مع هذا المجال الحساس, وقد أظهر تقييم مؤسسة e-Governance Academy Foundation المختصة بتطوير وإدارة مؤشر الأمن السيبراني الوطني National Cyber Security Index - NCSI لعام 2021 , أن الجمهورية الإيرانية تعمل على تحسين مقدراتها لتصل إلى النتيجة المطلوبة من الحماية, إذ جائت في المرتبة 54 في الأمن السيبراني العالمي وهي نسبة متوسطة مقارنة بدول أخرى, أما من ناحية تطوير تكنولوجيا المعلومات فاحتلت المرتبة 81 وهذا شيء إيجابي ومن حيث جاهزية شبكتها المرتبة 79[1]

هذه المؤشرات عند تحليلها نستلخص أن إيران وسط الضغط الدولي عليها استطاعت الاستفادة من خبرائها المحليين وتجاربها السابقة لتصيغ لنفسها استراتيجية فعالة تغطي النقص التقني الذي تعاني منه وهو ما تُرجم في المؤشرات السابقة .

[1] e-Governance Academy Foundation, National Cyber Security Index: Iran (Islamic Republic of) (Tallinn: e-Governance Academy Foundation, 2023), p 1.

التقييم أظهر أيضا أن إيران تشهد تطورا في سياساتها السيبرانية بنسبة 75 % ما يعني فعالية استراتيجيتها ومؤسساتها. كذلك قدراتها في الإستجابة للهجمات الإلكترونية بلغت 50% و عملياتها العسكرية السيبرانية بلغت 33%, ما ينم على وجود اهتمام بالجانب العملياتي والأمني أكثر من الجوانب الأخرى المتعقة بالتحديثات الجديدة. أما في مايخص التعليم والتطوير المهني فقد بلغت نسبتها 22% فرغم وجود برامج أكاديمية وبحثية مكثفة إلى أنها لم تبلغ المعايير الدولية المناسبة[1].

ومن خلال هذه المؤشرات والنسب الإيجابية لا يمكن الجزم بأن إيران حققت فعالية كاملة إذ لا زالت تواجه عدة صعوبات تعيق مسارها التطوري. حيث بلغت المرتبة 133 بنسبة 19% فيما يخص مؤشر الأمن السيبراني الوطني وهي نسبة قليلة باعتبارها من أوائل الدول التي عملت على الاهتمام بالفضاء الرقمي وادراجه في أجندتها الحكومية[2] .

هذا بالإضافة إلى التشريعات والقوانين التي سنتها لحماية فضائها الرقمي وبيانات مستخدميها وخدماتها الحيوية الأساسية فوصلت لنسب جد متدنية, كما أنها لاتنشر بيانات وتقييمات سنوية لتمكن الأخصائيين من التحليل ودراسة سياساتها مايطرح التساؤل حول مدى شفافية الحكومة, كذلك مسألة هل عدم نشر البيانات الدورية راجع لأسباب أمنية تتعلق بكون إيران تربطها علاقات متوترة مع كثير من الفواعل الإقليمية الأخرى ونشر مثل هذه البيانات يساعد أعدائها حسب اعتقاد صفوة المجتمع الإيراني في الكشف عن استراتجيتها ويمكن أن تستخدم لاحقا ضدها أم هناك أسبابا أخرى .

مساهمتها في الأمن السيبراني العالمي أيضا محدودة جدا, حيث بلغت 17% , في ما يخص اتفاقيات الجرائم السيبرانية والتمثيل في أطر التعاون الدولي بما فيه دعم دول أخرى وهذا راجع لتوتر العلاقات مع غالبية الدول وانغلاقها على ذاتها وحتى بسبب القيود المفروضة عليها التي من شأنها تقويض مساهمتها في مثل هذه المجالات .[3]

[1] Ibid p 2
[2] Ibid p 2
[3] e-Governance Academy Foundation ,**op. cit** p 1

إذ تتعامل أكثر مع روسيا والصين باعتبارهم حلفائها لتشارك بعض المصالح الاستراتيجية, أين أعلنت عن أولى صفقاتها الإلكترونية مع روسيا عام 2015 , وفي عام 2017 وقع الحليفان مذكرة تفاهم للتعاون بشأن القضايا المتعلقة بتكنولوجيا المعلومات والاتصالات وأيضا حوكمة الإنترنت وأمن الشبكة والاتصال الدولي بالإنترنت. أما في عام 2018 بادرت إيران بانشاء لجنة ثنائية للتعاون الإعلامي الأمر الذي رحبت بيه روسيا و هدفت المبادرة إلى مكافحة الإرهاب الإلكتروني .[1]

هذا وتواجه قيودا أخرى تقنية تتعلق بالبنية التحتية الحيوية خصوصا الطاقوية, مثل التقادم التقني أين لازالت تعتمد على الأنظمة والبرامج القديمة غير المحدثة في إدارة العمليات الصناعية نظرا لكلفتها الباهضة وعزوف الشركات المصنعة التعامل معها بسبب العقوبات الدولية المفروضة عليها, ما يخلق نوع من الهشاشة الرقمية والذي يصعب التعامل معه ويزيد من احتمالية التعرض للاستهداف. وقد أظهرت الهجمات السيبرانية ذلك, أين كانت أولى الهجمات"Stuxnet " الذي كشف عن وجود ثغرات رقمية في الأنظمة الصناعية يمكن استغلالها لاحداث ضرر متعدد المستويات, مادفع بالبلاد إلى تطوير سياساتها الحمائية التي بقيت رهن القدرة على التكيف والاستجابة, ما كشفت عنه الهجمات اللاحقة التي مست باقي القطاعات الحيوية الأخرى .

هذا ويزداد الفضاء الرقمي تعقيدا بكون الهجمات الإلكترونية في تطور مستمر من ناحية الوسائل والأساليب ما يجعل الدول وفي طليعتهم إيران في سباق مستمر نحو بناء منظومة دفاعية تواكب هذا التطور.

وعليه لايمكن الحكم على فعالية الإستراتيجية الإيرانية بشكل مطلق, إذ تعد محصلة لمجموعة من العوامل التي تحمل مؤشرات قوة و تحديات. حيث نجحت في خلق بيئة مؤسساتية

[1] د. محمد فريد عزي، "النشاط السيبراني الإيراني: ما بين السرية والعلن"، في https://trendsresearch.org/ar/insight/النشاط-السيبراني-الإيراني-ما-بين-السر تاريخ الاطلاع 14 ماي 2026

وقانونية وعملت على تطوير امكانياتها السيبرانية حتى في أصعب الظروف استجابة لواقع المجال الرقمي دون تفضيل قطاع على آخر, إلا أن تطور التهديدات مع القيود المفروضة عليها وحدود التعاون الدولي وقفت حاجزا أمام قدرتها على التقدم, ومنه تتلخص امكانية الدولة الإيرانية في هذا الميدان على التكيف مع التهديدات أكثر من سعيها لتحقيق حماية شاملة تستجيب فيها للمخاطر الناتجة عن هذه التهديدات.

**خلاصة الفصل**

من خلال ما تم التطرق إليه في هذا الفصل, يتضح أن البنية التحتية الطاقوية الإيرانية مثلت أحد أبرز نماذج الإستهداف في الفضاء السيبراني المعاصر, نظرا لوزنها الإستراتيجي وارتباطها بالأمن القومي بجميع مستوياته خصوصا بعد اعتمادها أحدث التقنيات التكنولوجية في دعم كفائتها الإنتاجية والتشغيلية, الأمر الذي يعد أرضية خصبة لنشاط الإختراقات الإلكترونية .

هذا وأظهر تحليل الفصل خلال الفترة الممتدة من 2010 إلى 2025 أن الهجمات الرقمية تطورت من ناحية طبيعتها وأهدافها, فمن استهداف لمنشآت نووية إلى باقي القطاعات الحيوية الأخرى التي تسير الدولة, الأمر الذي برهن على أن الصراع هو الآخر انتقل لمستويات أعلى أصبح فيه احتكار التكنولوجيا يمثل ورقة ضغط غير مباشرة مع صعوبة اسناد الهجمات إلى فواعل معينة مايعني استحالة مواجة التهديدات بالوسائل التقليدية وغياب المحاكمة الدولية, الأمر الذي زاد من تعميق المشهد الأمني لإيران خاصة و العالم عامة.

هذا وعرض الفصل أبرز استراتيجيات وسياسات الجمهورية الإسلامية الإيرانية السيبرانية التي تهدف إلى حماية بنيتها الحيوية من خلال طرح وتفسير هيكلها المؤسساتي والتشريعي والذي يشهد هو الآخر تطورا يجمع بين عدة مؤسسات وهياكل في توزيع واضح للمهام والتنسيق, وأيضا حلل جاهزية الدولة في مواجهة التهديدات الرقمية التي تعد في نفس الوقت تحديات تعرقل مسارها التنموي .

# خاتمة

وختاما, يمكن القول أن الاعتماد المتزايد على التقنيات المتقدمة داخل القطاعات الحيوية خاصة قطاع الطاقة أدى إلى تقليل التدخلات البشرية في العمليات, ما رفع من طبيعة التهديدات لتصبح موجهة ضد الأنظمة الرقمية التي تدير هذه العمليات, مشكلة بهذا تحديا للدول حول كيفية حماية بنيتها التحتية الطاقوية, وانطلاقا من هذا هدفت الدراسة إلى تحليل طبيعة الهجمات السيبرانية التي استهدفت البنية التحتية الطاقوية في إيران من 2010 إلى 2025 والبحث في سياساتها واجراءاتها المتبعة في مجال الأمن السيبراني, وكيف انتقل مفهوم حماية البنية التحتية من كونه قضية تقنية إلى كونه أحد مكونات الأمن القومي الإيراني, وهذا لإدراكها أن استهداف قطاع الطاقة يمكن أن ينعكس على مكانتها الإقليمية, وقدرتها على الصمود في مواجهة الضغوط الخارجية. وقد توصلنا في الأخير إلى النتائج التالية :

- ✓ تبين أن البنية التحتية للقطاع الطاقوي باتت من أكثر البنى الحيوية عرضة للتهديدات السيبرانية في ظل الانتقال نحو أتمتة العمليات الصناعية, وهذا راجع لارتباطه المباشر مع بقية القطاعات الأخرى وأهميته في استمرارية عملها, فالتهديد هنا لا يقتصر على الجانب التقني فحسب بل يمتد ليشكل تهديدا للأمن القومي للدول.
- ✓ أوضحت الدراسة أن التطور التكنولوجي كان عاملا أساسيا في نقل الصراع بين الفواعل الدولية إلى بيئة جديدة أكثر تعقيدا وهي الفضاء الرقمي, أين تتم تصفية الحسابات في وقت وجيز وكلفة منخفضة مقارنة بالسابق, والأهم من هذا دون عقوبات قانونية أو مساءلة دولية نظرا لصعوبة اسناد الهجمات وتحديد الجهات المسؤولة عنها.
- ✓ إدراج الأمن السيبراني كأحد المقومات الأساسية للأمن القومي كان ضرورة حتمية نتيجة التحولات الرقمية المعاصرة, فهو يهدف إلى دراسة الهجمات الإلكترونية, تطور أساليبها, طبيعتها وحتى أهدافها ووضع استراتيجيات تواكب كل جديد بخصوصها.
- ✓ يعد هجوم Stuxnet عام 2010 نقطة التحول في طبيعة التهديدات الموجهة ضد المنشآت الحيوية الإيرانية, ومنه تأكدت فرضية انتقال الصراع إلى الفضاء الرقمي لتمتد

بعد ذلك سلسلة الهجمات الإلكترونية وتشمل باقي البنى التحتية للقطاعات الحيوية, في إشارة واضحة إلى زعزعة الاستقرار والأمن القومي الإيراني وتحجيم دورها في المنطقة خاصة بعد مساعيها الرامية لإكتساب السلاح النووي.

- ✓ نتيجة للهجمات المتكررة تحتم على الدول عامة وإيران بصفة خاصة تطوير الخبرات والكفاءات المتخصصة في ميدان الأمن السيبراني, بالإضافة إلى تحديث البنية التكنولوجية وأنظمة الحماية الرقمية المستخدمة سواء في قطاع الطاقة أو باقي القطاعات .
- ✓ تأكد من خلال الدراسة أن التقنيات الحديثة والأنظمة الرقمية المتقدمة التي تحتاجها القطاعات لتحسين كفائتها التشغيلية والإنتاجية وكذا تعزيز الإجراءات الحمائية تتطلب تحديثات دورية, الشيء الذي لم تستطع إيران تحمله بسبب كلفتها الباهضة خاصة وأنها عانت من موجة عقوبات دولية متتالية أنهكت خزينتها العامة لإرتباط إقتصادها بشكل كبير على عائدات قطاع المحروقات .
- ✓ رغم الضغوطات والفترات الحرجة التي عاشتها إيران استطاعت الاستفادة من تجاربها السابقة والإعتماد على قدراتها الذاتية, وهذا ببناء منظومة دفاعية من شأنها حماية بنيتها الحيوية الرقمية من خلال استحداث قوانين وهياكل ومؤسسات متخصصة وتشجيع البحث العلمي في مجال الأمن السيبراني, إلا أنها ركزت على تعزيز قدراتها العسكرية في المجال السيبراني من أجل ردع خصومها في سياق جيوسياسي مضطرب, أكثر من تطوير سياسات تستجيب فيها للهجمات التي تصيب منشآتها الحيوية فيما يعرف بالمرونة السيبرانية.
- ✓ كشفت تجربة إيران أن بناء منظومة فعالة لحماية البنى الحيوية لايتوقف عند إنشاء المؤسسات وسن التشريعات, بل يتطلب تطويرا مستمرا للقدرات التقنية والبشرية وتعزيز التعاون الدولي متى سمحت البيئة السياسية بذلك .

بعد دراسة الموضوع واستنتاج أن تبني التقنيات الحديثة والسير على نهج التطور التكنولوجي ساهم في تحسين الوظائف الحيوية في شتى الميادين, إلا أنه خلق تهديدات جديدة كانت الدول في غنى عنها, جعلنا نتساءل هل هذه الدعوة إلى رقمنة كافة المجالات نعمة أم نقمة؟ وباعتبار أن الدول تسعى للحفاظ على أمنها القومي وبقائها بالدرجة الأولى فالاحتمال الوحيد الذي يضمن هذا هو فصل البيئة الواقعية عن البيئة الافتراضية, لأن كل الملفات الأمنية والحساسة والسرية تكون مكشوفة للطرف الآخر في الفضاء الرقمي.

# قائمة المراجع

## المراجع العربية

### أولا: الكتب

1) الرزو مظفر، التهديد السيبراني الإيراني: الملف المضاف إلى برنامجه النووي ودوره المحتمل في تأجيج صراع من نمط جديد. برلين: المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، 2022.

2) زهرة عطا محمد، البرنامج النووي الإيراني بين إشكاليات الواقع واحتمالات المستقبل. بيروت: مركز الزيتونة للدراسات والاستشارات، 2015.

### ثانيا: المقالات العلمية المحكمة

3) بن أحسن، أنيس عبد الوهاب، "القوة السيبرانية الإيرانية وأثرها على الاستقرار الإقليمي." **مجلة السياسة العالمية** 6، العدد 2 (2022): 735.

4) حبيب أحمد منى، "العقوبات الاقتصادية كوسيلة ضغط في السياسة الدولية: إيران أنموذجًا." **مجلة قضايا سياسية**، العدد 72 (2023): 296–299.

5) سالمان الطايع محمد، وهويدا عبد الله فتحي، "البرنامج النووي الإيراني وتأثيره على منطقة الشرق الأوسط." **المجلة العلمية لكلية الدراسات والسياسات الاقتصادية والسياسية**، يناير 2024.

6) قانصو محمد إبراهيم، "الحرب السيبرانية: التهديدات، الاستراتيجيات، وتحديات الردع في الفضاء الرقمي." **مؤشر للدراسات الاستطلاعية**، المجلد 7، العدد 20، 2025.

### ثالثا: الدراسات والتقارير البحثية

7) البيضاني حسن، سلمان خليفة، "الحرب السيبرانية في المواجهة العسكرية الإيرانية (الإسرائيلية): الإمكانيات وحدود التأثير." حمورابي للدراسات الاستراتيجية، 30 يونيو 2025.

8) عزي محمد فريد، "النشاط السيبراني الإيراني: ما بين السرية والعلن TRENDS Research & Advisory"، 5ديسمبر 2021.

**رابعا: المواقع الإلكترونية والمقالات الصحفية**

9) أبو الخير خالد، "أبراج حفر آبار النفط : 5 مكونات أساسية لنجاح عمليات الحفر ". Petro News، 19يوليو 2022https://petro-news.com/43138/ .

10) أبو الخير محمد، "مكونات آبار النفط : 8 عناصر أساسية من الحفر إلى الإنتاج، " Petro News، 17أبريل 2025https://petro news.com/112811/ .

11) أياس عبد الرحمن، "مضيق هرمز من الألف إلى الياء... شريان الطاقة والتجارة العالمي"، المجلة ، 18 مارس 2026 **https // :www.majalla.com**

12) الجزيرة نت، "بينها ثالث أكبر حقل في العالم: تعرف على منشآت النفط الإيرانية،" تم الاطلاع 10 أبريل 2026 **https// :www.aljazirah.net**

13) الجزيرة نت، "محطة فوردو لتخصيب الوقود أحد أكبر المواقع النووية الإيرانية،" 15 يونيو 2025**https// :www.aljazirah.net** .

14) الجزيرة نت، "مفاعل بوشهر حجر الأساس للبرنامج النووي الإيراني،" 15 يونيو 2025**https // :www.aljazirah.net** .

15) الجزيرة نت، "مفاعل نطنز النووي أكبر منشأة لتخصيب اليورانيوم في إيران،" 13 يونيو 2025**https// :www.aljazirah.net** .

16) الجزيرة نت، "من يقاتل في الشوارع ومن يقود الحرب؟ الفرق بين الباسيج والحرس الثوري،" 16 مارس 2026.**https// :www. aljazirah.net**

17) الجزيرة نت، "هجوم عين أميناس،" 2 فبراير 2016**https// :www.aljazirah.net** .

18) Aras Energy" مراحل تشغيل مصفاة النفط : من استقبال النفط الخام إلى إنتاج الوقود،" 28 أبريل 2025arasenergy.co/ar/blog/the-stages-of-an-oil-refinerys-operation/ .

19) Come-Star"كيفية تواصل نظام SCADA مع وحدات التحكم المنطقية القابلة للبرمجة: تحويل البروتوكول وتوافق الواجهة"، 22 أغسطس 2025 **https //www.comstar.com.**

20) Decowell"ما هو نظام التحكم الموزع(DCS) ؟" تم الاطلاع 2 أبريل 2026.

21) Delixi Electric"المكونات الرئيسية لنظام نقل الكهرباء،" 10 نوفمبر 2023. https://www.cn delixi.com/ar/news/key

22) Emirates Nuclear Energy Corporation (ENEC)"مكونات الحلقة الأولية في توليد الكهرباء بمحطة الطاقة النووية،"

2024 https://www.enec.ae/ar/discover/how-nuclear-energy-works/ .

23) Key Time Solutions"أنواع التهديدات السيبرانية للشركات وكيفية الوقاية منها،" تم الاطلاع 15 مايو 2026. **https://www.key time solutions**

24) Omch"ما هي الأتمتة الصناعية؟ الأنواع والفوائد الرئيسية" ،تم الاطلاع 2026 **https://www.Omch.com.**

25) Worldometer "نفط إيران" ،تم الاطلاع 21 مايو 2026 . https://www.worldometers.info/ar/النفط/نفط-إيران/

**دروس ومحاضرات**

26) قطينة فهد، الهجمات السيبرانية: دليل أشهر أنواع الهجمات السيبرانية الشامل Cyber Course.

**Foreign References**

**First: Journal Articles**

27) Bellamkonda, Srikanth. "Ransomware Attacks on Critical Infrastructure: A Study of the Colonial Pipeline Incident." International Journal of Research in Computer Applications and Information Technology 7, no. 2 (2024): 1423–1433.

28) Canfil, Justin Key. "The Illogic of Plausible Deniability: Why Proxy Conflict in Cyberspace May No Longer Pay." Journal of Cybersecurity 8, no. 1 (2022).

29) Dhanaraj, Anandan. "The Evolution of Cyber Threats: From Traditional Attacks to AI-Powered Challenges." European Journal of Computer Science and Information Technology 13, no. 36 (2025).

30) Sahnoune, Nor El Imen. "The Strategic Importance of Pipelines between Geopolitics and Cooperation Opportunities." Journal of Comprehensive Security and Strategic Affairs 1, no. 3 (2024): 61–62.

31) Schmitz, Richard, et al. "Energy Security and Resilience: Reviewing Concepts and Advancing Planning Perspectives for Transforming Integrated Energy Systems."

32) Shakarian, Paulo. "Stuxnet: Cyberwar Revolution in Military Affairs." Small Wars Journal, April 14, 2011.

33) Shakarian, Paulo, Jana Shakarian, Andrew Ruef, and Gerardo I. Simari. "An Argumentation-Based Framework to Address the Attribution Problem in Cyber-Warfare." arXiv preprint arXiv:1404.6699 (2014).

**Second: Reports, Technical Guides, and Institutional Publications**

34) Congressional Research Service. Critical Infrastructure: Emerging Trends and Policy Considerations for Congress. Report R48878. Washington, DC: Congressional Research Service, 2026.

35) e-Governance Academy Foundation. National Cyber Security Index: Iran (Islamic Republic of). Tallinn: e-Governance Academy Foundation, 2023.

36) International Energy Agency. Digitalization and Energy. Paris: International Energy Agency, 2017.

37) International Energy Agency. World Energy Outlook 2023. Paris: International Energy Agency, 2023.

38) International Energy Agency (IEA). 2022 Energy Crisis: The Crises and Global Responses.

39) Katikar, Harshad. Stuxnet: Analysis and Implications of the World's First Cyber-Weapon. N.p., n.d.
40) National Institute of Standards and Technology (NIST). Glossary of Key Information Security Terms. NISTIR 7298 Rev. 3. Gaithersburg, MD: U.S. Department of Commerce, 2019.
41) Schweikert, Amy, et al. Resilience and Critical Power System Infrastructure: Lessons Learned from Natural Disasters and Future Research Needs. Policy Research Working Paper No. 8900. Washington, DC: World Bank Group, 2019.
42) Stouffer, Keith, Joe Falco, and Karen Scarfone. Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82 Rev. 2. Gaithersburg, MD: National Institute of Standards and Technology, 2023.
43) U.S. Energy Information Administration. Country Analysis Brief: Iran. Last updated October 10, 2024.
44) United Nations. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174. New York: United Nations General Assembly, 2015.

**Third: Laws and Official Documents**

45) European Parliament and Council of the European Union. "Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive)." Official Journal of the European Union L 333, December 27, 2022.
46) Iran. Act on the Protection of Rights of Computer Software. 2000.
47) Iran. Computer Crimes Law. Tehran: Islamic Republic of Iran, 2009.

**Fourth: Official Institutions and Government Agencies Websites**

48) Cyber Security Agency of Singapore. "Cybersecurity Act." Last modified April 2, 2025. **https://www.csa.gov.sg/legislation/cybersecurity-act/**
49) Cybersecurity and Infrastructure Security Agency (CISA). "Cyber Attack against Ukrainian Critical Infrastructure." Last revised July 20, 2021. **https://www.cisa.gov/topics/cybersecurity-best-practices**
50) Cybersecurity and Infrastructure Security Agency (CISA). "Cybersecurity Best Practices." Accessed April 1, 2026. **https://www.cisa.gov/topics/cybersecurity-best-practices**

51) Cybersecurity and Infrastructure Security Agency (CISA). "Nation-State Cyber Actors." Accessed April 17, 2026. **https://www.cisa.gov/topics/cybersecurity-best-practices**

52) Cybersecurity and Infrastructure Security Agency (CISA). "Securing the Internet of Things (IoT)." February 1, 2021. **https://www.cisa.gov/topics/cybersecurity-best-practices**

53) European Union Agency for Cybersecurity (ENISA). "What We Do." Accessed April 1, 2026. **https://www.enisa.europa.eu/about-enisa/what-we-do**

54) International Atomic Energy Agency (IAEA). "International Nuclear Information System (INIS)." Accessed May 28, 2026. https://www.iaea.org/resources/databases/inis

55) National Cyber Security Centre (NCSC). "What Is Cyber Security?" Accessed March 24, 2026. **https://www.ncsc.gov.uk/section/about-ncsc/what-we-doaccessed**

56) National Cyber Security Centre (NCSC). "What We Do at the NCSC." Accessed April 1, 2026. **https://www.ncsc.gov.uk/section/about-ncsc/what-we-doaccessed**

**57)** National Protective Security Authority (NPSA). "Critical National Infrastructure." Last modified March 25, 2026. **www.npsa.gov.uk/about-npsa/critical-national-infrastructure**

**Fifth: Technical and Specialized Websites**

58) Awati, Rahul. "Remote Terminal Unit (RTU)." WhatIs/TechTarget, July 16, 2024.**https// : www.TachTarget.com**

59) Burgess, Monica. "Halliburton Ransomware Attack: Impact, Victims, Recovery." Huntress, November 21, 2025. **https// :www.Halliburton.com**

60) Caballar, Rina Diane, and Cole Stryker. "What Is Secure Coding?" IBM Think, March 17, 2026.

61) Darktrace. "DCS Security." Accessed April 1, 2026. **https// :www.Dartrace.com**

62) Dashlane. "What Is Network Segmentation & How Does It Work?" Accessed May 7, 2026. **https// :www.Dashlane.com**

63) DataGuard. "Cyber Security Threats: What to Defend Against and How." Accessed March 25, 2026. **https// :www.DataGuard.com**

64) Finio, Matthew, Amanda Downie, and Nick Douglas. "What Is OT Security?" IBM Think, Accessed April 1, 2026. **https// :www.IBM.com**

65) Flinders, Mesh, and Ian Smalley. "What Is Network Security?" IBM Think, Accessed April 1, 2026. **https// :www.IBM.com**
66) Fortinet. "Information Technology (IT) vs. Operational Technology (OT) Cybersecurity." Accessed April 19, 2026. **https//www.Fortinet.com**
67) Fortinet. "SCADA and SCADA Systems." Accessed April 1, 2026. **https//www.Fortinet.com**
68) Fortinet. "SolarWinds Cyber Attack: An Overview." Accessed March 27, 2026. **https//www.Fortinet.com**
69) Fortinet. "What Is a Firewall? Definition and Types of Firewall." Accessed March 30, 2026. **https//www.Fortinet.com**
70) Fortinet. "What Is DLP (Data Loss Prevention)?" Accessed March 31, 2026. **https//www.Fortinet.com**
71) Fortinet. "What Is OT Security? An Operational Technology Security Primer." Accessed April 1, 2026.**https//www.Fortinet.com**
72) Group IB. "Intrusion Detection and Prevention Systems (IDS/IPS)." Accessed March 30, 2026.**https// :www.GroupIB.com**
73) Holdsworth, Jim, and Matthew Kosinski. "What Is Information Security?" IBM Think, Accessed April 1, 2026. **https// :www.IBM.com**
74) IBM. "What Is a Cyberattack?" Accessed March 25, 2026. **https// :www.IBM.com**
75) IBM. "What Is an Air Gap?" Accessed April 13, 2026. **https// :www.IBM.com**
76) IBM. "What Is Backup and Restore?" Accessed May 7, 2026. **https// :www.IBM.com**
77) IBM. "What Is Cloud Security Posture Management?" Accessed May 15, 2026. **https// :www.IBM.com**
78) IBM. "What Is Cloud Security?" Accessed April 1, 2026. **https// :www.IBM.com**
79) IBM. "What Is Encryption?" Accessed March 31, 2026. **https// :www.IBM.com**
80) IBM. "What Is Identity & Access Management?" Accessed April 1, 2026. **https// :www.IBM.com**
81) IBM. "What Is MFA (Multifactor Authentication)?" Accessed May 7, 2026. **https// :www.IBM.com**
82) IBM. "Zero Day (Explained)." Accessed March 27, 2026. **https// :www.IBM.com**

**83)** Inductive Automation. "What Is a PLC? Programmable Logic Controller." Last updated October 9, 2025. **https// :www. Inductive Automation.com**

84) Kirvan, Paul, and Michael Cobb. "What Is Data Masking?" TechTarget SearchSecurity, October 22, 2025. **https// : www.TachTarget.com**

85) Kosinski, Matthew. "What Is Phishing?" IBM Think, Accessed May 15, 2026. **https// :www.IBM.com**

86) ScienceDirect Topics. "Industrial Control System." Accessed May 28, 2026.**https// :www.ScienceDirectTopics.com**

87) ScienceDirect Topics. "Information Technology." Accessed April 1, 2026. **https// :www.ScienceDirectTopics.com**

88) SearchInform. "Industrial Control Systems (ICS) Security." Accessed April 1, 2026.**https// :www.SearchInfo.com**

89) Senstar. "Physical Infrastructure Security." Accessed March 30, 2026.**https//:www.Senstar.com**

**90)** TechBehemoths. "IRANSITE Company Profile." Accessed April 27, 2026.**https//:www.Senstar.com**

91) TechBehemoths. "Raspina Net Pars Company Profile." Accessed April 27, 2026.**https// :www. TechBehemoths.com**

92) Toninelli, Luigi. "Forward Defense in Cyberspace: Iran's Hybrid State-Hacking Doctrine." ISPI, February 5, 2026.**https// :www. ISPI.com**

93) Trellix. "The Iranian Cyber Capability." March 5, 2026.**https//.www.Trellix.com**

**94)** Williment, Chloe. "How Will the Energy Crisis Affect Global Supply Chains?" Supply Chain Magazine, March 25, 2026.**https// :www.Supply ChainMagazine**

**Sixth: News Sources and Press Articles**

95) Kamali Dehghan, Saeed. "Iranian Oil Ministry Hit by Cyber-Attack." The Guardian, April 23, 2012.

96) National Council of Resistance of Iran (NCRI). "NCRI Publishes Report on Iran's Cyber Army." April 4, 2016.

97) Reuters. "Iran Petrol Stations Hit by Cyberattack, Oil Minister Says." December 18, 2023.

98) "Group Violator." Spreading Justice, November 20, 2025.

99) "Iranian Cyber Police." OpenSanctions. Accessed April 22, 2026.

100) "Northeastern Blackout of 2003." EBSCO Research Starters. Accessed April 1, 2026.

# الفهرس العام

| العنوان | الصفحة |
|---|---|
| **الشكر و التقدير** ..... | **4** |
| **الإهداء** ..... | **5** |
| **ملخص الدراسة بالعربية** | **6** |
| **ملخص الدراسة بالإنجليزية** | **7** |
| **خطة البحث** | **8** |
| **مقدمة**..... | **11** |
| **الإطار المنهجي** ..... | **14** |
| **الفصل الأول : الإطار النظري لأمن البنية التحتية الطاقوية في ظل التهديدات السيبرانية** | **26** |
| **المبحث الأول** : البنية التحتية الطاقوية المفهوم والأبعاد الاستراتيجية | **28** |
| **المطلب الأول** : تعريف البنية التحتية الطاقوية ومكوناتها | **28** |
| **المطلب الثاني** : الأهمية الاستراتيجية للبنية التحتية الطاقوية | **39** |
| **المطلب الثالث** : هشاشة البنية التحتية الطاقوية في عصر الرقمنة | **41** |
| **المبحث الثاني** : التهديدات السيبرانية وتأثيرها على البنية التحتية الطاقوية | **45** |
| **المطلب الأول:** الإطار المفاهيمي للأمن السيبراني | **45** |
| **المطلب الثاني:** طبيعة الهجمات السيبرانية التي تستهدف قطاع الطاقة | **49** |

| | |
|---|---|
| **المطلب الثالث:** التحول من التهديدات التقليدية إلى التهديدات السيبرانية | **54** |
| **المبحث الثالث:** ممارسات وسياسات حماية البنية الطاقوية | **57** |
| **المطلب الأول:** مبدأ حماية البنية التحتية الحيوية وتطبيقاته في الأجندة الحكومية | **57** |
| **المطلب الثاني:** أدوات وأساليب حماية البنية التحتية الطاقوية | **62** |
| **الفصل الثاني : التهديدات السيبرانية وأمن البنية التحتية الطاقوية الإيرانية** | **67** |
| **المبحث الأول** : ملامح البنية الطاقوية الإيرانية وأبعادها الاستراتيجية | **69** |
| **المطلب الأول** : قطاع النفط والغاز في إيران كأصل استراتيجي | **69** |
| **المطلب الثاني** : البنية النووية الطاقوية كأحد أبعاد الأمن القومي الإيراني | **74** |
| **المطلب الثالث** : التحول الرقمي في إدارة الطاقة الإيرانية | **81** |
| **المبحث الثاني** : تطور الهجمات السيبرانية التي استهدفت البنية الطاقوية الإيرانية | **85** |
| **المطلب الأول** : هجوم Stuxnet 2010 كنقطة تحول في المدركات الإيرانية | **85** |
| **المطلب الثاني** : هجمات سيبرانية لاحقة على قطاع الطاقة من 2010 إلى 2025 | **88** |
| **المطلب الثالث** : الفاعلون و إشكالية اسناد الهجمات السيبرانية | **92** |
| **المبحث الثالث** : حماية البنية التحتية الإيرانية : المحددات وواقع الفعالية | **95** |
| **المطلب الأول** : الهيكل المؤسساتي لمجال الأمن السيبراني الإيراني | **95** |
| **المطلب الثاني** : الهيكل التشريعي لحماية البنية التحتية الحيوية الإيرانية | **101** |

| | |
|---|---|
| **المطلب الثالث** : تحليل واقع فعالية الحماية السيبرانية في القطاع الطاقوي الإيراني | **105** |
| **خاتمة** ..... | **110** |
| **قائمة المراجع** ..... | **114** |
| **الفهرس العام**..... | **124** |
| **فهرس الأشكال**..... | **128** |
| **فهرس الجداول**..... | **130** |
| **فهرس المختصرات**..... | **132** |

# فهرس الأشكال

| الرقم | العنوان | الصفحة |
|---|---|---|
| (1) | خريطة المنشآت الطاقوية في إيران | 73 |
| (2) | خريطة منشآت إيران النووية | 79 |

# فهرس الجداول

| الرقم | العنوان | الصفحة |
|---|---|---|
| (1) | مقارنة بين التهديدات التقليدية والتهديدات السيبرانية | 55 |
| (2) | الهجمات السيبرانية على البنية التحتية الحيوية من 2010 إلى 2025 | 89 |

# فهرس المختصرات

| الاختصار | الاسم باللغة الأصلية | الاسم بالعربية |
|---|---|---|
| **ICS** | Industrial Control System | أنظمة التحكم الصناعي |
| **SCADA** | Supervisory Control And Data Acquisition | أنظمة التحكم الإشرافي وجمع البيانات |
| **DCS** | Distributed Control System | أنظمة التحكم الموزعة |
| **PLCs** | Programmable Logic Controller | وحدات التحكم القابلة للبرمجة |
| **RTUs** | Remote Terminal Unit | الوحدات الطرفية البعيدة |
| **OT** | Operational Technology | أنظمة التشغيل |
| **IT** | Information Technology | أنظمة المعلومات |
| **VPN** | Virtual Private Network | الشبكة الافتراضية الخاصة |
| **InfoSec** | Information Security | الأمن المعلوماتي |
| **IoT** | Internet of Things | إنترنت الأشياء |
| **IAM** | Identity and Access Management | إدارة الهوية والأصول |

| | | |
|---|---|---|
| **DDoS** | Distributed Denial of Service | هجوم حجب الخدمة الموزع |
| **CIP** | Critical Infrastructure Protection | حماية البنية التحتية الحيوية |
| **CISA** | Cyber and Infrastructure Security Agency | وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية |
| **NIS** | Directive on Security of Network and Information Security | توجيه أمن الشبكات ونظم المعلومات |
| **NCSC** | National Cyber Security Center | المركز الوطني للأمن السيبراني البريطاني |
| **GCHQ** | Government Communication Headquarters | مقر الاتصالات الحكومي البريطاني |
| **MI5** | Military Intelligence Section 5 | الاستخبارات العسكرية القسم الخامس ( جهاز الأمن الداخلي البريطاني ) |
| **CSA** | Cyber Security Agency of Singapore | وكالة الأمن السيبراني في سنغافورة |

| | | |
|---|---|---|
| **MDDI** | Ministry of Digital Development and Information | وزارة التنمية الرقمية والمعلومات بسنغافورة |
| **SingCERT** | Singapore Computer Emergency | فريق الاستجابة لطوارئ الحاسوب في سنغافورة |
| **IDS/ IPS** | Intrusion Detection System / Intrusion Prevention System | نظام كشف التسلل / نظام منع التسلل |
| **DLP** | Data Loss Prevention | حماية البيانات من الفقدان |
| **CSPM** | Cloud Security Posture Management | إدارة وضعية أمن الحوسبة السحابية |
| **MFA** | Multi-Factor Authentication | المصادقة متعددة العوامل |
| **OPEC** | Organisation of the Petroleum Exporting Countries | منظمة الدول المنتجة والمصدرة للنفط |
| **USB** | Universal Serial Bus | الناقل التسلسلي العام |
| **APT** | Advanced Persistent Threat | التهديدات المتقدمة المستمرة |
| **FATA** | Federally Administrered Tribal Areas | المناطق القبلية الخاضعة للإدارة الفيدرالية بإيران |
| **NCSI** | National Cyber Security Index | المؤشر الوطني للأمن السيبراني |