# الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة: حالات مختارة

د. أحمد الباسوسي *

**مستخلص**

*مع تصاعد أهمية قطاع الطاقة، واعتباره القاطرة التي تقود كافة القطاعات التنموية الأخرى، ولما له من تأثير مباشر على تعزيز أو تهديد الأمن القومي لدى البلدان، أضحى هدفًا استراتيجيًا للمتسللين بكافة صورهم، سواء من الدول التي تستخدمه كسلاح سياسي لإضعاف خصومهم من الدول الأخرى، أو من الفاعلين من دون الدول مثل القراصنة الذين يستهدفون من وراء شن تلك الهجمات السيبرانية الحصول على مبالغ مالية كفدية في مقابل إعادة تشغيل أنظمة التحكم داخل منشآت الطاقة أو التنظيمات الإرهابية والسياسية التي تسعى من وراء هجومها لتحقيق أهداف ذات طبيعة سياسية أو إيديولوجية.*

*ولهذا، فقد واجهت البنى التحتية لقطاع الطاقة لهجمات شرسة في كافة القارات، بما في ذلك الأكثر تقدمًا لاسيما أمريكا الشمالية، وأوروبا، والشرق الأوسط. تفاوتت تلك الهجمات من حيث شدتها، وتأثيراتها، والنتائج المترتبة عليها. لكنها، في الوقت ذاته، كانت بمثابة جرس إنذار لمختلف دول العالم، دفعهم لضرورة إعادة النظر في استراتيجيات مواجهة الهجمات السيبرانية بشكل عام، والموجه منها لقطاع الطاقة على وجه الخصوص.*

*ومن هذا المنطلق، تسعى تلك الورقة للكشف عن أبرز الهجمات السيبرانية التي ضربت قطاع الطاقة على الصعيد العالمي، علاوة على رصد وتحليل أهم الجهود الدولية التي تم إتخاذها في إطار عمليات المكافحة، ناهيك عن أبرز العقبات التي واجهة التعاون الدولي في هذا الصدد.*

**كلمات مفتاحية:**

الهجمات السيبرانية– قطاع الطاقة– الأمن السيبراني– المتسللون– برامج الفدية

**Abstract:**

**With the rising significance of energy sector as engine of development, and its direct impact on enhancing or threating state's national security. It has become a strategic target for various intruders, whether from states that use it as a political weapon to weaken their opponents, or from other non-state actors such as hackers who seek to obtain money as ransom in exchange for restarting control systems within energy**

* مدرس العلوم السياسية – كلية الإدارة والاقتصاد وتكنولوجيا الأعمال –الجامعة المصرية –الروسية

- Email: Ahmed-elbassoussy@eru.edu.eg

**facilities, or terrorist and political organizations that seek to achieve political and ideological goals.**

**In this context, energy sector infrastructure faced a fierce attack on all continents and regions, including the most developed ones, especially in North America, Europe, the Middle East, and Latin America. These attacks varied in their intensity, effects, and consequences. However, it served as alarm to various states, that pushed them to reconsider their confrontation cyber-attacks strategies in general, and those directed at the energy sector in particular. From this standpoint, this paper seeks to reveal the most prominent cyber-attacks that hit the energy sector at the global level, in addition to monitoring and analyzing international efforts that have been taken in the framework of countering such operations. As well as shed light on the most prominent obstacles that faced international cooperation in this regard.**

**Key Words:**

**Cyber Attacks- Energy Sector- Cyber Security- Hackers- Ransomware**

**مقدمـة:**

شهد العقد الأخير دخول قطاع الطاقة بشكل واضح على خريطة الهجمات السيبرانية. فحيوية القطاع، وأهميته الاستراتيجية التى تتعدى حاجز البعد التنموي، لتشمل الأهمية السياسية، والأمنية، والمجتمعية جعلته هدفاً جديداً لمختلف أنماط المتسللين. فبعض الدول تستخدم تلك الهجمات كأداة لمواجهة خصومهم سواء بشكل مباشر أو عن طريق بعض الجماعات التى تعمل بتوجيهات منها. كما أنها باتت هدفاً أيضاً للتنظيمات التي تسعى من خلالها إلى تحقيق مكاسب مالية عن طريق إعاقة أنظمة التحكم والتشغيل للحصول على فدية. علاوة على الجماعات ذات الأهداف السياسية والإيديولوجية التى تسعى من جراء تلك الهجمات للانتقام من بعض أنظمة الحكم نتيجة مواقفهم السياسية لاسيما الإقليمية.

ولهذا، واجهت مختلف مناطق العالم موجه من الهجمات السيبرانية ضد منشآت قطاع الطاقة بدءً من عام ٢٠١٠، تجلت مع ظهور فيروس **Stunex** الذي أصاب المنشآت النووية الإيرانية، ثم تم رصده فى عدد من البلدان الأخرى. كما زادت التخوفات عام ٢٠١٢ مع ظهور فيروس شمعون **Shamoon**الذي أصاب شركات النفط السعودية، والذي ظهر منه إصدارات أخرى عام ٢٠١٦ و ٢٠١٧ أصابت العديد من القطاعات الحيوية فى المملكة العربية السعودية بما فيها قطاع النفط.

لم يتوقف الأمر عند منطقة الشرق الأوسط، بل إمتد إلى الولايات المتحدة الذي واجه قطاع الطاقة لديها واحدة من أخطر الهجمات السيبرانية بعد استهداف خط أنابيب كولونيال عام ٢٠٢١، والذي أسفر عن حدوث أزمة حقيقة فى توريدات الغاز والنفط بامتداد الساحل الشرقى الأمريكى. الأمر ذاته بدا متكرارً حينما واجه قطاع الطاقة الأوروبي أيضاً هجمات عديدة لاسيما في ألمانيا، وهولندا، وبلجيكا أثرت بشكل كبير على

إمدادات الطاقة الأوروبية. كما برزت الهجمات السيبرانية على قطاع الطاقة على الساحة الروسية–الأوكرانية بخاصة بعد عام ٢٠١٤ على خلفية ضم روسيا لجزيرة القرم، وإمتدت أيضاً خلال الغزو الروسى لأوكرانيا فى فبراير ٢٠٢٢.

دفعت كثافة وحده الهجمات السيبرانية الموجه لقطاع الطاقة العديد من دول العالم للبحث عن أدوات جديدة لمواجهة تلك الأخطار وتداعياتها، منها جهود فردية، مثل وضع استراتيجيات متكاملة لمواجهتها، ورفع ميزانيتها المتعلقة بالأمن السيبرانى، وتحديث البنية التشريعية لتسهيل عمليات تعقب المتسللين، علاوة على رفع كفاءة منظومات الأمن السيبرانى من خلال عقد دورات تدريبية، وتمارين لمحاكاة الهجمات السيبرانية للعناصر البشرية العاملة فى قطاع الطاقة. ذلك بالإضافة للتحركات والجهود الجماعية، والتي يتمثل أبرزها في زيادة معدلات التنسيق بين الدول، والعمل من خلال المنظمات الدولية والإقليمية. غير أن تلك الجهود لا تزال تواجه حزمة من العقبات التى تحول دول صياغة استراتيجية دولية شاملة لمواجهة التهديدات السيبرانية الموجهة لقطاع الطاقة.

## إشكالية الدراسة:

انطلاقاً من تزايد حده الهجمات السيبرانية، واتساع نطاقها، وتعدد مصادرها، وتأثيراتها الخطيرة التي تتجاوز الأبعاد الاقتصادية لتصل للتهديدات المباشرة للأمن القومي. فقد بدأت مختلف البلدان فى تطوير استراتيجيات لمكافحتها، والحد من آثارها. وفي هذا الصدد، فيمكن صياغة المشكلة البحثية فى تساؤل رئيسي، وهو كالآتي:-

ما هي أبرز ملامح الجهود الدولية لمكافحة التهديدات السيبرانية والحد من آثارها على قطاع الطاقة؟

## الأسئلة الفرعية:

للإجابة عن التساؤل الرئيسي، تستهدف الدراسة الإجابة عن عدد من الأسئلة الفرعية، وهي:

١- ما هو المقصود بالتهديدات السيبرانية، والفرق بينها بين الجرائم الإلكترونية، والحرب الإلكترونية؟

٢- ما هي أبرز خطوات التهديدات السيبرانية؟ وما هي أنواعها؟

٣- ما هو نطاق انتشار الهجمات السيبرانية على قطاع الطاقة؟

٤- لماذا يعد قطاع الطاقة جاذباً للتهديدات السيبرانية؟

٥- ما هي قطاعات الطاقة الأكثر تعرضاً للهجمات السيبرانية؟

٦- ما هي أبرز أنماط الهجمات السيرانية التي يتعرض لها قطاع الطاقة؟

٧- ما هي أوجه التشابة والاختلاف بين الهجمات السيبرانية على قطاع الطاقة؟

## منهجية الدراسة:

تعتمد الدراسة في إطار تناولها على منهجين: يتمثل الأول في المنهج الاستقرائي، والذي يعد الأكثر ملائمة لموضوع الدراسة، إذ يعتمد هذا المنهج على دراسة وتحليل

نقطة محددة للغاية– والتي تتمثل في جهود مكافحة التهديدات السيبرانية–، حيث تم اختيار الحالات وفقاً لعدد من المعايير، وهي: مراعاة شمولية التوزيع الجغرافي قدر الإمكان، واختيار حالات تتضمن هجمات لمختلف أنواع منشآت الطاقة بما في ذلك المنشآت النووية، وخطوط نقل الغاز والنفط، وشبكات توزيع الكهرباء، علاوة على حالات تتضمن الأنماط المختلفة للهجمات السيبرانية لاسيما هجمات الفدية، وتلك الموجهه بغرض تحقيق أهداف سياسية وإيديولوجية والتجسس، ذلك بالإضافة للمعيار الأهم والمتعلق باختيار حالات تتضمن الربط بين الهجوم من جانب، والسياق الجيوسياسي والاستراتيجي والاقصادي لوقوعها من جانب آخر. علماً بأن الباحث قد فضّل الاستعانة بهذا المنهج، حيث أن الهدف من الدراسة استقراء التوجه العالمي الشامل لمكافحة التهديدات الموجهه لقطاع الطاقة، مستدلًا على ذلك من خلال الحالات المتعددة التي تضمنتها الدراسة. أما الثاني، فهو المنهج المؤسسي لكونها ستتعرض لرصد الجهود المؤسسية سواء على مستوى الدول أو المنظمات الدولية والإقليمية لمكافحة الهجمات السيبرانية على قطاع الطاقة.

## أهداف الدراسة:

على الرغم من وجود العديد من الدراسات التي تناولت مفهوم التهديدات السيبرانية، إلا أن تلك الدراسات لم تتناول بشكل عميق تلك التهديدات على قطاع الطاقة. ولما كان لهذا القطاع من أهمية قصوى لكونه لا يرتبط بالأمن الاقتصادي فحسب، بل السياسي والأمني فقد بات هدفاً رئيسياً للعديد من المخترقين والمتسللين سواء من الفاعلين الرسميين، أو الفواعل من دون الدول.

لهذا، تسعى تلك الدراسة لمحاولة تفسير توجهات، وسلوكيات، ودوافع هؤلاء الفاعلين، علاوة على معرفة نقاط الضعف التي تجعل قطاع الطاقة أكثر عرضة للتهديدات ذات الطبيعية السيبرانية، فضلاً عن التعرف على مختلف الآليات التي تتبعها الدول للحد من تأثيراتها السلبية سواء بشكل منفرد أو جماعي.

## تقسيم الدراسة:

على هذا النحو تُقسم الدراسة إلى ثلاثة أقسام رئيسية؛ إذ يقدم القسم الأول تأصيل نظري للمقصود بالهجمات السيبرانية، وأبرز خطواتها، علاوة على أنواعها. أما القسم الثاني، فيتناول بالتحليل أسباب جاذبية قطاع الطاقة للهجمات السيبرانية، والتأثيرات المتوقعة لتلك الهجمات على القطاع، فضلًا عن خريطة انتشار تلك الهجمات على الصعيد العالمي، وأبزر حالتها. والثالث، فيركز على استعراض أبرز الجهود والتوجهات الدولية لمواجهة الهجمات السيبرانية على قطاع الطاقة للحد من آثارها السلبية.

## أولًا: الإطار النظري التفسيري لظاهرة الهجمات السيبرانية (نظرية الأمننة)

### ١- ماهية نظرية الأمننة:

ترجع نظرية الأممنة Securitization بشكل أساسي لمنظري مدرسة كوبنهاجن للدراسات الأمنية في الثمانينيات من القرن العشرين، لاسيما أولي ويفيير Ole Weaver وباري بوزان Barry Buzan. فالأمننة هي عملية خطابية يقوم فيها كيان أو فرد بتصوير أي قضية عادية بـــأنها مسألة ذات طبيعة أمنية، وذلك بهدف استخدام وتبرير استخدام أدوات ووسائل أمنية غير عادية ضد الأفراد أو الكيانات استناداً على الأمن.[١]

### ٢- عناصر عملية الأمننة:

وانطلاقاً من هذا التعريف، وفقد وضع أولي ويفير Ole Weaver أربعة عناصر أساسية لابد من توافرها لتتم عملية الأمننة، وهي كالآتي:-

أ- الفاعل/ الوكيل: هو ذلك الكيان أو الشخص الذي يصنع الفعل المؤنن.

ب- التهديد الوجودي: ويقصد به الكائن أو النموذج الذي ينظر له باعتباره ضرراً محتملاً.

ج- الكيان أو الكائن المرجعي: يتمثل في الفكرة أو الموضوع الذي يتعرض للتهديد، وبالتالي فيحتاج إلى الحماية.

د- الجمهور: وهو الهدف الذي يحتاج إلى الإقناع وقبول فكرة أو قضية ما كتهديد أمني.[٢]

### ٣- قطاعات الأمننة:

أشار باري بوزان Barry Buzan لوجود خمسة قطاعات للأمن، وهي كالآتي:

أ- الأمن العسكري: والذي يتمثل في التهديدات الناتجة عن التفاعلات العسكرية المتبادلة بين الدول سواء الدفاعية أو الهجومية، وكذلك تلك الناتجة عن تصورات قادة الدول.

ب- الأمن السياسي: ويتعلق بالتخوفات الناتجة عن عدم استقرار الدولة أو نظام الحكم فيها أو التهديدات التي تواجه إيديولوجية الدولة.

ج- الأمن الاقتصادي: ويتمثل في تلك المخاوف الناتجة عن عدم القدرة على الوصول أو الوصول غير المتكافئ إلى الموارد الاقتصادية- بما في ذلك رأس المال أو الأسواق- اللأزمة للحفاظ على مستوى مقبول نسبياً من الرفاه الاجتماعية.

د- الأمن المجتمعي: وهي المخاوف التي تنتج عن التقيد المفرط أو التهديدات – سواء حقيقة أو متصورة- للأنماط التقليدية للغة والثقافة والهوية الدينية والوطنية والعادات.

٥- الأمن البيئي: وهي المخاوف التي تثيرها التهديدات التي يتعرض لها النظام البيئي المحلي أو الإقليمي أو العالمي، علاوة على التهديدات التي تصيب الموارد الطبيعية التي تعتمد عليها حياة الإنسان بشكل عام.[٣]

## ثانياً: التأصيل النظري لظاهرة الهجمات السيبرانية

### ١- تعريف الهجمات السيبرانية

لا يوجد ثمه اتفاق بين الباحثين حول مفهوم الهجمات السيبرانية، وذلك لتشابك أبعاده، وتعقيدها. ولهذا، فسيتم استعراض أهم تلك التعريفات. إذ يأتي في مقدمتها التعريف الذي قدمه، ريتشارد كلارك **Richard Clark**، والذي اعتبرها "مجموعة من الإجراءات التي تقوم الدول بإتخاذها بهدف التسلل إلى أجهزة أو شبكات الحاسوب لدولة أخرى بغرض إحداث ضرر أو إضطراب". لكن لعل ما يعيب هذا التعريف أنه يقصر تلك جهات التي تقوم بشن تلك الهجمات على الدول فقط، ويتجاهلها إذا صدرت عن إفراد أو منظمات، علاوة على أنه لم يوضح ماهية الإضطرابات التي تنتج عن تلك الهجمات[٤].

هذا، ويعرفها أيضاً مايكل هايدين **Michael Hayden**، بأنها "أي محاولة مقصودة لتعطيل أو تدمير شبكات الحاسوب لدولة أخرى". لكن يعيبه أيضاً شدة عمومية، فإنه لا يفرق بين تلك الهجمات، وبين بعض المصطلحات المشابهة مثل الجرائم الإلكترونية[١]، والحرب الإلكترونية[٢]، مما سيؤثر بالضرورة على الاستراتيجيات التي يُفترض أن يتبناها صانعي السياسات لمواجهة تلك الظاهرة[٥].

أما مارتن ليبكي **Martin Libicki**، فيرى أنها عبارة عن "هجمات رقمية تصيب أجهزة الحاسوب، لتجعلها تبدو طبيعية، لكنها في الحقيقة تصدر نتائج غير صحيحة". غير أن هذا النهج يستبعد نطاقاً واسعاً من التهديدات المحتملة للأمن القومي للدولة، وهي تلك التي تم استهداف بنيتها السيبرانية دون أن تصل إلى حد الهجمات الجسيمة.

وعلى صعيد التعريفات التي قدمتها الشركات الدولية المعنية بشأن الفضاء السيبراني والتهديدات التي تواجهه. فقد عرفتها مجموعة تالين **Tallinn Group**، بأنها "عملية هجومية إلكترونية سواء لأغراض -دفاعية أو هجومية-بغرض إصابة أو وفاة الأشخاص، أو التسبب في إتلاف أو إلحاق الضرر أو تدمير الممتلكات"[٦].

---

[١] الجرائم الإلكترونية ( السيبرالنية)، وهي عبارة أن إجراء سيبراني أو إلكتروني يتم بواسطة أنظمة الحاسوب من خلال متسللون غير حكوميين يؤدي لانتهاك قواعد القانون الجنائي.

[٢] الحرب الإلكترونية (السيبرالنية)، هي أعلى مستوى، وأكثر أنواع الهجمات الإلكترونية تعقيدًا، إذ يتم تنفيذها ضد المصالح السيبرانية الوطنية للدول، وعادة لها عواقب وخيمة.

## ٣- خطوات الهجمات السيبرانية

لا تتم الهجمات السيبرانية في أغلب الأحوال بشكل عشوائي، وإنما تكون نتيجة عملية تخطيط تأخذ عده مراحل، وخطوات. تبدأ من التخطيط، وتنتهي بالهجوم. وفي هذ الإطار، تجدر الإشارة إلى تلخيص تلك المراحل فيما يلي:-

أ- استطلاع الهدف المراد استهدافه **Reconnoitering a target for hacking**: وفيها يقوم المهاجمون باستكشاف الهدف أو القطاع المراد توجيه الهجمات إلية، والبحث عن نقاط الضعف في أنظمته السيبرانية، واستكشاف كيفية استغلالها.

ب- تسليح المعلومات ضد الهدف **Weaponizing information on a company**: يستخدم المخترق تلك المعلومات التي قام بجمعها بشكل مسبق لإنشاء طرق اختراق الشبكة، بحيث يتضمن ذلك العديد من الأدوات، منها: ارسال رسائل نصية احتيالية عبر البريد الإلكتروني **phishing e-mails**، أو إنشاء صفحات الكترونية احتيالية تبدو متطابقة تماماً مع صفحات رسمية لبنوك ومؤسسات كبرى، فيما يعرف بتقنية **watering holes**. ويهدف هذا النمط لجمع اسماء المستخدمين وكلمات المرور، لاستخدامها لتحميل مستندات مصابة ببرامج ضارة **Malware**. [٧]

ج- تنفيذ الهجوم **Delivering attack**: إذا نجحت التقنيات السابقة، واستطاع المتسلل الحصول على البيانات المطلوبة بعد أن قام أحد المتسهدفين بفتح الرسالة المزيفة، هنا تأتي مرحلة شن الهجمات، واستغلال ما تم جمعه من بيانات.

د- استغلال الخرق الأمني **Exploiting security Breach**: في تلك المرحلة يبدأ المخترق في عملية التحضير لجنى ثمار الهجوم، من خلال جمع البيانات المطلوبة بغرض تحقيق أهدافه. [٨]

ه- تثبيت الباب الخلفي **Installation of a Persistent Backdoor**: وهنا يقوم المتسلل بإنشاء حسابات خاصة به كمسئول داخل الشبكات **Administrator Accounts** ، بهدف توفير لنفسه القدرة على تعطيل جدار الحماية **Firewall**، مما يسهل له القيام بعملية تعطيل الخوادم والأنظمة الأخرى داخل الشبكات. بحيث يكون هدف المتسلل فى هذه المرحلة هو التأكد من البقاء داخل النظام، بما يساعده على تحقيق أهداف الهجوم.

و- ممارسة القيادة والسيطرة **Exercising Command & Control**: بعد ضمان المتسلل وجوده داخل الشبكة، يبدأ بالسيطرة عليها بشكل تام من خلال غلق حسابات المستخدمين الرسميين داخل القطاع المستهدف، واخراجهم خارج الشبكة تماماً، ثم يبدأ بعض المتسللون فى طلب فدية لإعادتهم مرة أخرى.

ز- تحقيق أهداف المتسلل **Achieving hacker's objectives**: وهنا يبدأ المتسلل بجنى ثمار العملية، وتحقيقه أهدافه، والتي قد تتضمن: سرقة بيانات العملاء والموظفين، والاستيلاء على تصميمات المنتجات، وتعطيل عمليات القطاع أو الشركة

المستهدفة. كما أنه إذا استطاع أحد المتسللين من الوصول إلى نظام التحكم الصناعي فيمكنه إيقاف تشغل المعدات، أو إدخال نقاط تعيين جديدة، علاوة على قدرته على تعطيل أجهزة الإنذار.[٩]

## ٣- أنواع الهجمات السيبرانية

تضم الهجمات السيبرانية عده أنواع، يمكن تلخيص أبرزها فيما يلي:

أ- البرمجيات الخبيثة **Malware**: تعد الأكثر شيوعاً بين كافة أنواع الهجمات الإلكترونية. وهي عبارة عن مجموعة من البرامج الضارة، تضم: الفيروسات المتنقلة Worms، وبرامج التجسسSpyware ، والبرامج الفديةRansomware ، وبرامج الإعلانات المتسللة Adware، وأحصنة طروادة Trojans. حيث تقوم تلك البرامج باختراق الشبكات عبر ثغرات أمنية عند قيام المستخدم بالنقر على رابط خطير، أو تحميل ملفات مرفقة في بريد إلكتروني أو عند استخدام ناقل بيانات مصاب.

ب- التصيد **Phishing**: يقوم المتسلل بانتحال صفة جهة موثوق منها، ومن ثم يرسل للضحية رسائل بريدية مزيفة. وفور فتح الرسالة والنقر على الرابط الضار المرفق، يتمكن المتسلل من الوصول إلى المعلومات السرية، والبيانات الخاصة بالحساب. علاوة على إمكانية تثبيت برامج ضارة على الشبكة.[١٠]

ج- هجوم الوسيط **Man in the Middle (MITM)**: يُعرف أيضاً باسم هجوم التنصت، وفيه يدخل المتسلل في اتصال بين العميل والمضيف. بحيث يمكنه ذلك من سرقة البيانات، والتلاعب بها.[١١]

د- هجوم كلمة المرور **Password Attack**: أحد أشكال الهجوم، الذي يقوم فيه المتسلل بسرقة كلمة المرور الخاصة بالمستخدمين، وذلك باستخدام العديد من البرامج مثل Aircrack، أو Abel وغيرها. علمًا بأن هناك العديد من أنواع هجمات كلمات المرور مثل Keylogger attack [١٢].

ه- هجوم حجب الخدمة **Denial of Service(DoS)**: يوجه هذا النوع للشركات بشكل أساسي، إذ يستهدف المتسللون مهاجمة الأنظمة، والخوادم، والشبكات عبر غمرها بالبيانات والحركات بغرض تشتيتها، واستنفاذ مواردها، بما يحول دون قدرتها على تلبية الطلبات الورادة إليها، مما يؤدئ لغلق الموقع الإلكتروني الذي يستضيفه أو إبطائه. [١٣]

و- هجوم حقن لغة الاستعلام الهيكلية **SQL Injection**: يقوم المتسلل بحقن رمز خبيث وسط لغة SQL في مربع بحث موقع الشبكة المستهدف، مما يجعل الخادم يكشف عن معلومات هامة. حيث يّمكن ذلك المتسلل من الحصول على أي بيانات يريدها من قاعدة البيانات، علاوة على تمكينه من حذفها، أو إعادة تحريرها مرة أخرى، مما يعطي المتسلل القدرة على تدمير الموقع، أو إيقافه عن العمل.[١٤]

ز- الهجوم الفوري **Zero-Day Exploit**: بعد الإعلان عن وجود ثغرة أمنية في الشبكة أو التطبيق، يقوم المتسللون باستغلالها قبل أن يستطيع المطورون التعامل معها

أو حلها. مما يمّكن المتسلل من استغلالها. وهو ما يجعل عملية سرقة هويات المستخدمين أمر وارد، ويجلعهم ضحايا محتملين لأشكال متعددة من الجرائم ذات الطبيعة الإلكترونية.[١٥]


أنواع الهجمات السيبرانية

أما على صعيد تصنيف الهجمات السيبرانية وفقاً لمعيار التوجية، فتنقسم إلى طائفتين. تتمثل الأولى في الهجمات الموجهة أو المستهدفة **Targeted Attacks:** وتكون مواجهه لقطاع أو صناعة بعينها لبنية تحتيه حيوية[١٦]. وتتطلب تلك الهجمات عملية تخطيط تفيصيلية، ومتقنة. ويستخدم فيها المخترق أو المتسلل أدوات وتقنيات متخصصة، وغير معروفة. وتتسم هذه الهجمات بما يلي:-

أ- ضرورة توافر قدرات فنية وتقنية متطورة للمتسلل.

ب- الاعتمام على منهجية جماعات التهديد المستمر **APTs**.

ج- قدرتها على استغلال واستهداف نقاط الضعف الموجودة بالأنظمة التكنولوجية. وبالتالي صعوبة التعامل معها أو مواجهتها.

د- تأثيراتها الشديدة ليس على القطاعات والشركات المستهدفة فحسب، ولكن على الدولة بأسرها فى حالة ما إذا كان القطاع المستهدف يتسم بقدر من الأهمية والحساسية، أو كان المنافس أو المتسلل يتسم بقدر كبير من العدائية.

أما الثانية، فتتمثل في الهجمات غير الموجهة أو غير المستهدفة **Non-targeted Attacks:** هى تلك الهجمات التي لا تستهدف جهة أو قطاع بعينه، بل يكون أحد

أهدافها توسيع قاعدة الأهداف قدر الإمكان. بحيث تستهدف الإضرار بنظام تكنولوجيا المعلومات Information Systems، أو أنظمة تكنولوجيا التشغيل Operating Systems، وتكون عادة عن طريق رسائل البريد الإلكتروني. [١٧]

## ثانياً: الهجمات السيبرانية على قطاع الطاقة

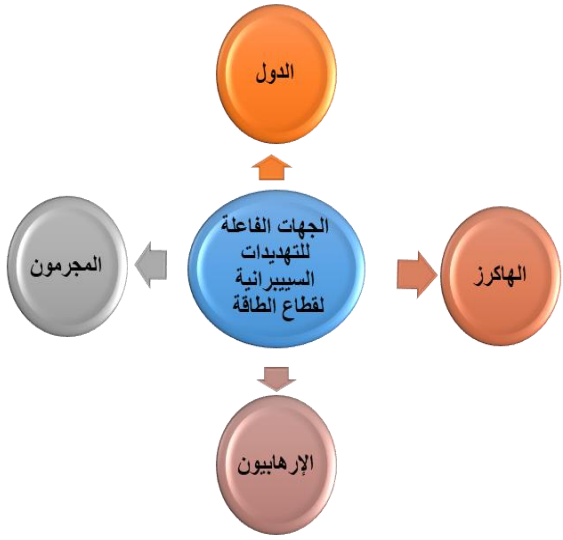
### ١- جاذبية قطاع الطاقة للتهديدات السيبرانية

يعاني قطاع الطاقة على الصعيدين العالمي والاقليمي من عدد من نقاط الضعف- مما يجعله أكثر عرضة للهجمات السيبرانية، وأكثر جذباً للمجرمين الإلكترونيين أياً كانت ماهيتهم- عن غيره من القطاعات الاقتصادية الأخرى. حيث يتسم هذا القطاع بما يلي:-

أ- الأهمية الاقتصادية لقطاع الطاقة: فقطاع الطاقة يعد بمثابة العمود الفقري لمعظم الأنشطة الاقتصادية للدول. وبالتالي فإن استهدافه وتعطيله من شأنه أن يحدث حالة من الشلل الكامل داخل الدولة، علاوة على الخسائر المادية الضخمة التي يمكن أن تسفر عنه في حال توقفه، مما يؤثر على الاستقرار السياسي والاجتماعي للدول.[١٨]

ب- تعدد الفواعل المستهدفة لقطاع الطاقة بين الفواعل الدولية ودون الدولية: فجاذبية قطاع الطاقة وأهميته جعلته هدفاً جيوسياساً للعديد من الفواعل. فهناك أربعة فواعل رئيسية تقوم كل منها بالهجمات السيبرانية، لكن بدوافع مختلفة. وهم:

- الدول Nation State: والتي تدفعها بشكل أساسي الرغبة في التخريب، والتجسس، وزعزعة الاستقرار السياسي والاقتصادي لدى الخصوم.
- المخترقون أو الهاكرز Hacktivists: الذين يتبنون أيديولوجيات وتوجهات طائفية سواء دينية أو سياسية يريدون فرضها، أو بهدف الإعلان عن مواقفهم لرفض سياسة أو فعل بعينة، أو بهدف تدمير سمعة جهة أو علامة تجارية.
- المجرومون Criminals: الذين يسعون نحو تحقيق مكاسب مالية.
- الإرهابيون Terrorists: والذين يستهدفون توسيع نطاق عمليات التبشير، وتدمير البيانات. [١٩]




الجهات الفاعلة للهجمات السيبرانية على قطاع الطاقة

ج- العمل المستمر لأنظمة الطاقة: فالبنية الرقمية التي تدعم قطاع الطاقة تعمل بشكل دائم ومستمر، دون توقف، مما يجعلها معرضة لتلك التهديدات بشكل شبه دائم.

د- تعقيد النظام الشبكي لقطاع الطاقة: فنظام إدارة الطاقة يعتبر معقد للغاية، فالبنية التحتية للطاقة تضم موزعين، وموردين، ومرافق للتخزين، علاوة على أصول، والتي غالباً ما تتداخل، وتنتشر في أكثر من دولة، مما يجعلها أكثر عرضه لمواجهة مخاطر الاستهداف السيبراني.[٢٠]

ه- غياب التدابير الكافية للأمن السيبراني: فأنظمة الإدارة، والتحكم في الشبكات، وأنظمة التوزيع والمراقبة، علاوة على الأنظمة المحاسبية تفتقر بشكل كبير لتدابير مواجهة التهديدات السيبرانية. ناهيك عن عدم توافر الكفاءات داخل قطاع الطاقة لمواجهة هذا النوع من التهديدات.[٢١]

## ٣- التأثيرات المتوقعة للهجمات السيبرانية على قطاع الطاقة

إن العمليات المتنوعة التي استهدفت قطاع الطاقة قد أسفرت عن عده تأثيرات. إذ يأتي في مقدمتها: اضطرابات الأسواق **Market disruption**، فعملية اختراق بيانات الشركة بخاصة المتعلقة بحجم الاحتياطات من شأنها أن تكشف حجم الاحتياجات المستقبلية للغاز والنفط، مما يؤثر على عمليات التسعير.

كما يمكن أن تؤدئ تلك التهديدات إلى تدمير البني التحتية للطاقة **Physical infrastructure damage**، بخاصة فى حالة استهداف السدود والحواجز التي تؤثر بدورها على إمدادات المياه، علاوة على إتلاف المعدات.

وتمتد التأثيرات أيضاً إلى إحداث أضرار بالأمن القومي National security، نظرًا لانها تستهدف بشكل أساسي البنية التحتية، والأنظمة الحيوية للدولة، مما يضر باقتصاد الدول، ويفقدها ميزتها التنافسية لحساب بعض الأطراف الدولية الأخرى. ناهيك عن تأثيراتها السلبية على معدلات السلامة، والأمن القومي.

كذلك، تطول التأثيرات الإضرار البشري Human harm، خصوصاً في الحالات التي يتم فيها استهداف المنشآت النووية، مما يؤدي إلى انتشار الأنشطة الإشعاعية، فضلاً عن إمكانية انقطاع الكهرباء، وإعاقة وصول الخدمات التي تعتمد عليها بخاصة وصول المياة الجارية للمنتفعين، أو التبريد، وغيرها من الخدمات التي تعتمد عليها. ليس هذا فحسب، بل أيضاً تؤدي تلك التهديدات إلى التأثير على الشبكات Network effects، فعملية اختراق نظام التحكم فى منشآت التوليد بمثابة نقطة وصول لمنشآت أخرى لها تأثيرات أكبر، مما يؤدي لفصل أجزاء كبيرة من الشبكة عن العمل.

ويضاف لذلك، الخسائر المالية Financial loss، بما في ذلك تكلفة استبدال المعدات المدمرة، وأنظمة الترقية المتأثرة بالهجوم، وفقدان الفرص التجارية، وخسائر مقدمي الخدمات فى حالة استمرار انقطاع الأعمال أوتأخير عودتها.[٢٢]

### ٣- توزيع الهجمات السيبرانية داخل قطاع الطاقة.

يواجه قطاع الطاقة تباين ملحوظ في نسبة الهجمات الموجهة لمختلف مكوناته. ففي الفترة ما بين ٢٠١٧ وحتى يوليو ٢٠٢٢، تعرض قطاع الطاقة عالمياً لـــ٤٥ هجوم سيبراني، منها ١٣ هجوم وقع بحلول يوليو ٢٠٢٢، وهو المعدل الأعلى لحدوث الهجمات خلال الستة أعوام. حيث تم توجيه ثلث الهجمات للأصول النفطية، والبني التحتية لخطوط الغاز والنفط والمنشآت النووية، وجاءت شبكات الكهرباء في المرتبة الثانية بأكثر من ربع تلك الهجمات، ويشترك قطاعا الغاز والشحن في الحوادث المتبقية. علمُاً بأن ربع تلك الهجمات قد تم توجيهها للولايات المتحدة الأمريكية وحدها، بينما شهدت أوروبا ١١ واقعة، أما الباقي فيتوزع على باقى دول العالم.[٢٣]

### ٤- خريطة انتشار الهجمات السيبرانية على قطاع الطاقة

لم يعد من الممكن لأي دولة مهما بلغت من تقدم تكنولوجي وتقني تجنب الهجمات السيبرانية لاسيما الموجه منها لقطاع الطاقة. وفي هذا الإطار، ستتعرض الدراسة لعدد من أشهر نماذج الهجمات السيبرانية في مختلف المناطق الجغرافية، بما في ذلك بلدان الشرق الأوسط، والولايات المتحدة الأمريكية، وأوروبا، وغيرها من المناطق. إذ يأتي في مقدمتها ما يلي:-

١- استهداف المنشآت النووية الإيرانية: مثلت المنشآت النووية هدفاً محورياً للهجمات السيبرانية، من أهمها: هجوم ستونكس ٢٠١٠ STUNEX 2010 ، هو عبارة عن هجوم فيروسي تم توجيه عام ٢٠١٠ إلى أجهزة الطرد المركزي بمحطة تخصيب اليورانيوم في منشآة نطنز الإيرانية، حيث تمكن الفيروس من الانتشار فيما

يقرب من ١٠٠ ألف مضيف. إذ استهدف الفيروس أنظمة التحكم الإشرافي والحصول على البيانات SCADA [٣]، مما أسفر عن حدوث شلل وتوقف كامل لـــ ١٦٤ جهاز طرد مركزي مستخدم في علميات تخصيب اليورانيوم[٢٤].

وعلى الرغم من أن هوية المخترقين ظلت غير معروفة إلا أن عدة تقارير قد أشارت لتورط الجانبين الأمريكي والإسرائيلي في هذا الهجوم. علماً بأنه ومن المرجح أن يكون الاستهداف قد تم من داخل المنشأة نظراً للطبيعة التقنية التي تعتمد عليها.[٢٥]

أما على صعيد تأثيرات انتشار ستونكس على الداخل الإيراني، فقد تجاوزت فكرة الأثر المباشر، والذي يتعلق بتعطيل تقدم البرنامج النووي الإيراني، بل امتدت لجوانب أخرى تتعلق بشكل رئيسي بإظهار الدولة الإيرانية ضعيفة غير قادرة على تأمين البنى التحتية الحيوية بشكل كاف. ذلك علاوة على التأثيرات الاقتصادية السلبية حيث اضطرت السلطات الإيرانية لإنفاق موارد مادية ضخمة للتعامل مع تلك التأثيرات لا سيما إنشاء أجهزة طرد مركزي جديدة، فضلاً عن تخصيص موارد أكبر لتوفير أدوات تكنولوجية متقدمة لمكافحة التهديدات السيبرانية المستقبلية للحيلولة دون تكرارها فى المستقبل.[٢٦]

ودوليًا، أن الفيروس لم يصب إيران فحسب بل امتد لعدد من البلدان. ففي الوقت الذي أصاب فيه ٦٢،٨٦٧ جهاز حاسوب في إيران، فقد أصاب أيضاً ١٣،٣٣٦ جهاز فى أندونسيا،و ٦،٥٥٢ في الهند، و٢،٩١٣ في الولايات المتحدة، و ٢،٤٣٦ في أستراليا، و١،٠٣٨ في بريطانيا، و١،١٠٣ في ماليزيا، و٩٩٣ جهاز في باكستان.[٢٧]

وبالنظر للسياق الجيوسياسي لتلك الهجمات، فأنها وقعت بعد أشهر قليلة من إعادة انتخاب الرئيس الإيراني الأسبق، محمود أحمدي نجاد، والمعروف ليس فقط بمواقفه المتشددة تجاه إسرائيل، وإنما إصراره على المضي قدمًا في استكمال البرنامج النووي الإيراني، علاوة على تعثر مفاوضات الملف النووي الإيراني مع الوكالة الدولية للطاقة الذرية. الجدير بالذكر، أن تلك الهجمات التي استهدفت أجهزة الطرد المركزي جاءت بالتزامن مع عملية اغتيال لاثنين من العلماء النوويين الإيرانيين، وهما: مسعود محمدي في ١٢ يناير ٢٠١٠، ومجيد شهرياري في نوفمبر من العام ذاته. كما تكررت عمليات اغتيال العلماء النوويين الإيرانين في عام ٢٠١١ بعدما تم اغتيال كل من داريوش رضائي نجاد، ومصطفى أحمدي. وبالتالي، فإنها نُسبت لإسرائيل والولايات المتحدة باعتبارهما العدو الرئيسي لإيران.

---

[٣] أنظمة التحكم الإشرافي والحصول على البيانات SCADA هي عبارة عن بنية نظام تحكم تشمل أجهزة كمبيوتر واتصالات بيانات شبكية وواجهات مستخدم رسومية للإشراف عالي المستوى على الآلات والعمليات.

وفي أبريل ٢٠٢١، أعلنت السلطات الإيرانية عن تعرض شبكة الطاقة الكهربائية بمفاعل ناتنز النووي لهجوم سيبراني أدى إلى شلل جزئي- ذكرت الصحافة الإسرائيلية عن ضلوع الموساد لاسيما الوحدة التكنولوجيا العسكرية ٨٢٠٠ في تلك العمليات-، وهو الحدث الذي جاء مباشرة بعد قيام الرئيس الإيراني، حسن روحاني، بتدشين عدد من أجهزة الطرد المركزي الجديدة المسئولة عن عملية تخصيب اليورانيوم داخل المنشأة.[٢٨]

كما تكررت الهجمات مرة أخرى في أكتوبر ٢٠٢٢، عندما أعلنت مننظمة الطاقة الذرية الإيرانية عن اختراق خادم البريد الإلكتروني بمنشآة بوشهر للطاقة النووية، إلا أن فريق تكنولوجيا المعلومات بالمحطة قد استطاع إتخاذ حزمة من الإجراءات الوقائية فى أعقاب الحادثة. علماً بأن المنظمة قد أكدت على وقوف دول أجنبية وراء محاولة القرصنة، إلا أن جماعة إيرانية تُدعى Black Reward قد أعلنت مسئوليتها عن الاختراق.[٢٩]

يبدو أن السياق الجيوسياسي لتلك الهجمات مرتبط بمدى التقدم الذي تحرزه إيران فى برنامجها النووي من جانب، والتعثر الذي تشهده المفاوضات الخاصة بالملف من جانب آخر، وهو مبرر بالنظر للموقفان الإسرائيلي والأمريكي من البرنامج، حيث يراه مهدداً حقيقياً لأمنهما القومي، وبالتالي، فإن الغرض منها هو تحقيق أهداف سياسية واستراتيجية تتمثل في عرقلة البرامج النووي الإيراني، وتكبيد النظام الإيراني مزيداً من الخسائر المادية لاقتصاد يعاني من أزمة اقتصادية نتيجة العقوبات المفروضة عليه منذ سنوات.

٢- هجوم شمعون Shamoon Malware: يُعرف برنامج شمعون الخبيث أيضًا باسم " Disttrak أو W32.Disttrack.B،[٣٠] حيث يقوم هذا الفيروس بتدمير سجل التمهيد الرئيسي (MBR)[٤] System's master boot record.[٣١]

ففي ١٢ أغسطس ٢٠١٢، تم ادخال فيروس شمعون في شبكات شركة النفط الوطنية المملوكة للدولة السعودية " أرامكو". مما أسفر عن إصابة أكثر من ٣٠ ألف جهاز حاسوب تابع للشركة. إذ تسبب الفيروس في محو بيانات ما يقارب من ثلاثة أرباع أجهزة الحاسوب للشركة لاسيما المستندات، وجدوال البيانات، والبريد الإلكتروني، والملفات الأخرى المهمة.

---

[٤] سجل التمهيد الرئيسي MBRهو المعلومات الموجودة في القطاع الأول من القرص الثابت أو محرك الأقراص القابل للإزالة. إذ يحدد كيف وأين يوجد نظام تشغيل النظام Operating Systemليتم تحميله في وحدة التخزين الرئيسية للكمبيوتر أو ذاكرة الوصول العشوائي RAM .

وخلافًا للفيروسات الاخرى، كان لهذا الفيروس طبيعة مدمرة، فبدلًا من القيام بسرقة البيانات، فإنه أصابة الأجهزة بحالة من الشلل، مما عطلها عن العمل تمامًا. فقد تم تصميم فيروس شمعون للقيام بخطوتين: الاولى: تتمثل في محو البيانات الموجودة على الأقراص الصلبة، ثم استبدالها بصورة لعلم أمريكا محترق.

وفي إطار هذه العملية يقوم الفيروس بالكتابة فوق الملفات التالفة بحيث لا يمكن استعادتها مرة أخرى. وقد دفع ذلك الشركة إلى إغلاق شبكتها الداخلية، وتعطيل البريد الإلكتروني للموظفين، ومنع دخولهم على الأنترنت للحيلولة دون انتشار الفيروس. غير أن الشركة قد أعلنت عن عدم تأثر الأعمال الأساسية الخاصة بعمليات التنقيب عن النفط وإنتاجه، وذلك لكون تلك العمليات تعتمد على شبكة معزولة أو مغلقة.[٣٢]

هذا، وأعلنت جماعة تُدعى "سيف العدالة" مسئوليتها عن هجوم شمعون، إلا أن الأجهزة الأمنية والمخابراتية لم تعلن عن اسماء المتورطين في الهجوم. غير أن المسئولين فى المخابرات الأمريكية اعتبروا أن الجاني الحقيقى هو إيران دون تقديم أي أدلة لدعم تلك الأدعاءات.[٣٣]

أما عن دوافع هجوم شمعون، فقد أعلنت الجماعة عبر الأنترنت أن الهجوم يعد بمثابة عمل إنتقامي ضد نظام آل سعود لما اقترفوه من جرائم وفظائع في مختلف بلدان الشرق الأوسط بخاصة سوريا، والبحرين، واليمن، ولبنان، ومصر. [٣٤]

الجدير بالذكر، أن فيروس شمعون عاد للظهور مرة أخرى فى شهر نوفمبر عام ٢٠١٦ عندما قام بتعطيل بعض المنشآت الهامة فى السعودية بخاصة النقل، ثم بعد ذلك مرة أخرى في يناير ٢٠١٧ بعد استهداف موقع وزارة الاتصالات والعمل والمعلومات.[٣٥]

وبالنظر للسياق الجيوسياسي للهجمات، فعلى الرغم من عدم التأكد من وقوف إيران وراء تلك الهجمات، إلا أن حالة العداء بين إيران والمملكة العربية على خلفية المواقف المتعارضة بينهم في العديد من القضايا وفي مقدمتها الحرب في سوريا يمكن أن يفسر شن تلك الهجمات بعد أقل من عام على اندلاع الصراع بين نظام بشار الأسد- المدعوم من إيران-، وبعض فصائل المعارضة -المدعومة من السعودية-، ولعل ما يصب في الاتجاه ذاته، أن تلك الهجمات قد تكررت أيضاً في نوفمبر ٢٠١٦ بعد أقل من عام من بداية الحرب في اليمن، والذي تتشابه ظروفها مع الحرب في سوريا، حيث بدا بشكل واضح تناقض المواقف بين طهران من خلال دعمها للحوثيين، والرياض الداعم الرئيسي للنظام، وقائد التحالف العسكري. لكن يبدو أن الواقع السياسى الجديد بعد توقيع اتفاق عودة العلاقات بين طهران والرياض، ومما سيسفر عنه من تهدئه للأجواء بينهم، فمن المرجح أن تنحسر الهجمات السيبرانية على قطاع الطاقة السعودي.

أما عن نمط الهجمات، فإنها موجهة بشكل أساسي للمنشآت النفطية، نظراً لكون المملكة تمثل نموذج للدولة الريعية التي تعتمد على الصادرات النفطية كمصدر لدخلها

القومي. وبالتالي، توجيه الهجمات لهذا القطاع تحديداً يمكن أن يكون له تأثيرات اقتصادية واجتماعية سلبية عليها.

٣- هجوم خط أنابيب كولونيال ٢٠٢١ Colonial Pipeline Attack: تعرض خط أنانيب كولونيال الأمريكي في ٧ مايو ٢٠٢١ لهجوم سيبراني عن طريق برامج الفدية Ransomware، حيث قام المتسللون بسرقة ما يقارب ١٠٠ جيجا من البيانات قبل إغلاق أجهزة الحاسوب، وطلب الفدية التي قدرت ما يقارب٤,٤ مليون دولار بالعملة الرقمية "بيتكوين".

ينقل هذا الخط الضخم ما يقارب ٢,٥ مليون برميل من البنزين، والديزل، وزيت التدفئة، ووقود الطائرات يومياً لما يزيد عن ٥٥٠٠ ميل من تكساس وحتى نيوجيرسي. علماً بأن هذا الخط يوفر حوالي نصف إمدادات الوقود في الساحل الشرقي للولايات المتحدة الأمريكية، مما يؤثر إغلاقه لفترة طويلة ليس على أسعار الوقود فحسب، وإنما في التأثير السلبي على صناعة النفط بشكل عام. [٣٦]


مسار شبكة خطوط أنابيب كولونيا

الجدير بالذكر، أن المتسللين قد استخدموا حساب شبكة خاصة إفتراضية virtual private network account للتسلل إلى شبكة الحاسوب الخاصة بالشركة، وإيقاف نظمتها. حيث تم اكتشاف كلمة مرور هذا الحساب من ضمن مجموعة من كلمات المرور المسربة من الويت الخفي Deep Web[٥]. [٣٧]

[٥] يعتبر جزء الشبكات العالمية، والتي لا يتم فهرستها في محركات البحث. ويعد مايكل بيرجمان من رواد هذا المصطلح .

أما عن الجهة المسئولة عن الهجوم، فقد أعلن مكتب التحقيقات الفيدرالي الإمريكي في ١٠ مايو ٢٠٢١، أن مجموعة " دارك سايد" Dark Side، هي المسئول عن شن الهجوم، وهي مجوعة إجرامية تقيم داخل الحدود الروسية دون أن يكون لها علاقة رسمية بالحكومة الروسية، إذ تحترف تلك المنظمة ما يطلق عليه Ransomware as a Service (RaaS)، .[٣٨]

وفي ١٣ مايو٢٠٢١، قامت شركة كولونيال المشغلة للخط بدفع الفدية للمتسللين، بما يتناقض مع التصريحات السابقة لمسئولي الشركة، التي كانت تؤكد على أنها لا تنتوي الخضوع لعملية الإبتزاز التي يمارسها عليها القراصنة، مما أدى إلى إعادة تشغيل الخط مرة أخرى.[٣٩]

وعلى صعيد السياق الجيوسياسي المحيط بالهجمات السيبرانية على خط أنابيب كولونيال، فتلك الهجمات جاءت في خضم حالة من التنافس الحاد بين الولايات المتحدة والصين، فلم يعد التنافس اقتصادي وعسكري فحسب، وإنما تكنولوجي أيضاً. فالمواجهات العسكرية المباشرة مستبعدة، وبالتالي فإن تلك الهجمات يمكن أن تكون أحد الأدوات الجديدة للمواجهة. كما أنها أيضاً حدثت بالتزامن مع زيادة حدة التنافس الأمريكي–الروسي، فالسياسيين الروس وفي مقدمتهم الرئيس فلاديمير بوتين قد أعلن عن نيته للسعى للتحول بالعالم إلى نظام دولي متعدد الأقطاب، كما أنها تزامنت أيضاً مع زيادة معدلات تصدير الغاز الصخري الأمريكي إلى أوروبا لتقليل الاعتماد الأوروبي على روسيا. وهو الأمر الذي أجج حالة التنافس الأمريكي–الروسي.

أما عن نمط الهجمات السيبرانية ضد الولايات المتحدة، فإن أغلبها هجمات بهدف الحصول على فدية مقابل إعادة تشغيل الأنظمة، سواء عن طريق القراصنة أصحاب الأجندات السياسية والمدعومة من المنافسين الدوليين، أو هؤلاء الساعين للحصول على أموال من جراء تلك العمليات.

وبالتالي، فمن المتوقع استمرار تعرض الولايات المتحدة لهذا النمط من الهجمات، ليس فقط بسبب تعدد الخصوم وشراستهم، بل أيضاً بسبب استجابة السلطات الأمريكية لمطالب القراصنة، ودفعهم للفدية، بما يشجعهم على إطلاق المزيد من الهجمات السيبرانية على قطاع الطاقة الأمريكي.

٤- الهجمات السيبرانية ضد قطاع الطاقة في أوروبا: واجه قطاع الطاقة الأوروبي مجموعة من الهجمات السيبرانية، من أبرزها: في مايو ٢٠٢١ تعرضت شركة Volue Technology النرويجية لتكنولوجيا الطاقة، والبنية التحتية لهجوم فدية، باستخدام Ryuk ransomware، مما أدى لتعطيل منصات العملاء الأمامية، وجعلها غير قابلة للقراءة. وأجبر الهجوم الشركة، وعملاءها لإغلاق التطبيقات التي توفر البنية التحتية اللازمة لتوفير مرافق المياه التي تخدم ٨٥% من النرويج[٤٠].

والحقيقة أن استهداف منشآت الطاقة النرويجية يأتي في إطار سياق جيوساسي مضطرب، لكنه في الوقت ذاته مبرر، وذلك لأمرين: يتثمل الأول في أن النرويج تعتبر مورد أساسي لمصادر الطاقة لأوروبا بخاصة الغاز والنفط، خصوصاً مع إعلان الاتحاد الأوروبي سعيه للبحث عن بدائل لمصادر الطاقة الروسية.

كما أنها تعتبر من البلدان المؤسسة لحلف شمال الأطلنطلي (الناتو)، ومن أبزر الداعمين لتوسعة الحلف، علماً بأن تلك الهجمات جاءت في ظل دعوات نرويجية حثيثة بضرورة سرعة ضم باقى الدول الأسكندنافية لاسيما فنلندا والسويد، وهو الأمر الذي دفع روسيا- وفقاً للعديد من التقارير- لاستهداف منشآت الطاقة لديها كأداة للضغط عليها. ومع استمرار الحرب الروسية- الأوكرانية، يبدو أن مزيداً من الهجمات ستحدث بخاصة بعد زيادة النرويج لانتاجها من مصادر الطاقة، وهو ما انعكس على زيادة قدرتها التصديرية نحو بلدان الاتحاد الأوروبي.

واجهت أيضًا اثنان من كبرى مصافي النفط الأوروبية في يناير وفبراير ٢٠٢٢هجمات فدية وهما: Mabanaft/Oiltanking ألالمانية، و Amsterdam–Rotterdam–Antwerp (ARA) في هولندا وبلجيكا، مما أسفر عن تعطيل ما يقارب من ١٧ محطة تكرير نفط. حيث منع الهجوم تحميل ناقلات النفط، وتفريغها لكونها تتم بشكل آلي. وقد أجبر ذلك الشركات على تحويل الناقلات إلى موانئ أخرى، مما أدى إلى خنق تدفق وقود التدفئة والديزل والبنزين. وقد نُسب الهجوم لمنظمة تدعى Black Cat تستهدف المنشآت الصناعية.[٤١]

وبخصوص الواقع الجيوسياسي والاستراتيجي لوقوع تلك الهجمات، فأنها جاءت بالتزامن مع حشد روسيا لقواتها على الحدود تمهيداً لشن الحرب على أوكرانيا، وهي المرحلة التي اتسمت بموقف أوروبي صارم رافض للتحركات الروسية مدعوم من الولايات المتحدة. كما أنها جاءت في نهاية فترة المستشارة الألمانية أنجيلا ميركل –التي كانت بمثابة الأمل في وجود علاقات جيدة بين روسيا وألمانيا على الرغم من وجود مساحة من الاختلاف بين الطرفين، ووصول أولاف شولتس لمنصب المستشارية الألمانية، بموقف أكثر تشدداً إزاء روسيا. ويضاف لذلك، أنها جاءت في الوقت الذي أعلن فيه المستشار الألماني عن إيقاف مشروع خط غاز " نورد ستيريم ٢" الذي كان من المفترض أن ينقل الغاز الروسي عبر بحر البلطيق إلى ألمانيا، ثم إلى باقي البلدان الأوروبية. علاوة على أنها وقعت في الوقت الذي بدأت فيه البلدان الأوروبية بوضع عقوبات اقتصادية على روسيا. وبالتالي، فإن تلك الهجمات يمكن اعتبارها أداة للضغط على تلك البلدان وفي مقدمتها ألمانيا بهدف التقليل من حده موقفها تجاه روسيا. ولهذا، فمن المتوقع استمرار هذا النمط من الهجمات ضد منشآت الطاقة الأوروبية طالما ظل الموقف المتشدد ضد روسيا.

٥- الهجمات السيبرانية الروسية ضد منشآت الطاقة الأوكرانية من ٢٠١٥ حتى ٢٠٢٢: شهدت الفترة ما بعد عام ٢٠١٤، وتحديداً بعد ضم روسيا لجزيرة القرم كثافة شديدة للهجمات السيبرانية الروسية الموجهة ضد أوكرانيا، وخصوصاً ضد قطاع الطاقة الأوكراني . ولعل أهم أمثلة ذلك: الهجوم الإلكتروني الذي وقع خلال عامي ٢٠١٥-٢٠١٦ الذي استهدف شبكة الكهرباء الأوكرانية، والذي تم عن طريق التسلل لشبكة الحاسوب، علاوة على اختراق أنظمة التحكم الإشرافية للشبكة SCADA.

ففي أواخر عام ٢٠١٥ تم فصل ما يقرب من ٣٠ محطة فرعية لمدة ثلاث ساعات، مما أسفر عن انقطاع الكهرباء في ثلاث من كبرى الشركات الإقليمية في توزيع الكهرباء وهي:

Kyivoblenergo، Prykarpattyaoblenergo، Chernivtsioblenergo، وهو الأمر الذي أدي لانقطاع التيار الكهربائي عن مائتي ألف عميل. علماً بأنه قد تم التعرف على المتسللين، وهي مجموعة قرصنة روسية تُدعى Sand Worm، تستهدف بشكل أساسي حلف شمال الأطلنطي، والحكومات الأوروبية.[٤٢] إذ استخدم المتسللون تقينات متعددة، ومتقدمة، ومركبة مرت بعدة مراحل، تتمثل فيما يلي:-

أ- قيام بعمليات التصيد الاحتيالي Phishing من أجل الوصول الشبكات.

ب- الاختراق بهدف بث البرامج الخبيثة داخل الشبكات لاسيما برامج Black Energy 3 الذي تستخدمه حركات القرصنة الروسية.

ت- العمل على سرقة البيانات من داخل الشبكات عن طريق الشبكات الافتراضية بغرض إصدار الأوامر عن بعد.

ث- محو البيانات من الأقراص الصلبة للأجهزة التي تم مهاجمتها باستخدام برامج Kill Disk.

ج- قطع التواصل بين العميل، والشركة المقدمة للكهرباء من خلال برامج Denial of Service(DoS) حتى لا يتمكن العميل من الاتصال بخدمة العملاء للإبلاغ عن المشكلة.[٤٣]

كما زادت حده تلك الهجمات بعد الغزو الروسي لأوكرانيا مع بدايات عام ٢٠٢٢. ففي ١٢ أبريل أعلن باحثين من شركة ESET لأمن المعلومات، بالتعاون مع فريق الاستجابة للطوارئ الحاسوبية الأوكراني عن أحباط محاولة جديدة لاستهداف شبكة الكهرباء الأوكرانية باستخدام الإصدار الثاني من فيروس Indestroyer 2. كما أكدوا أيضاً على أن جماعة Sandworm الروسية هي المسئولة عن تلك الهجمات.[٤٤]

والجدير بالذكر، أن السياق الجيوسياسي بدا جلياً في حالة استهداف منشآت الطاقة الأوكرانية لاسيما وأنها جاءت بعد عام ٢٠١٤، فحالة العداء بين روسيا وأوكرانيا على خليفة التحالف الأوكراني مع الغرب، وسعى أوكرانيا للانضمام لحلف الناتو، فضلاً عن سعي روسيا لتأمين نطاق الجيوساسي بخلق منطقة عازلة بينها وبين

الناتو، كانت دافعاً مركزياً لشن روسيا هجماتها السيبرانية على أوكرانيا كجزء من استراتيجيتها االشاملة لتقويض أوكرانيا. ولهذا، فان الهجمات السيبرانية الروسية ضد أوكرانيا كان أغلبها على شبكات الكهرباء، وذلك بهدف شل حركة الدولة، وإظهار فشل الحكومة–الموالية للغرب– بأنها غير قادرة على مواجهة التهديدات الخارجية. وبالتالي، إضعاف موقفها أمام الشعب الأوكراني، وهو ما يصب بالضرورة في مصلحة روسيا.

ومع استمرار الواقع الجيوسياسي المعقد، وعدم القدرة على التوصل لتسوية سياسية للأزمة الروسية–الأوكرانية حتى بعد الوساطة الصينية، فمع المرجح استمرار الهجمات السيبرانية على قطاع الطاقة الأوكراني.

وبعد استعراض أبرز حالات الهجمات السيبرانية على قطاع الطاقة في مختلف مناطق العالم وسياقها الجيوسياسي، تجدر الإشارة لوجود ثلاثة أنماط رئيسية للهجمات والغرض منها، وهما كالآتي:

أ- الاستهداف بغرض الحصول على الفدية Ransomware، حيث يقوم المتسللون باختراق شبكات التشغيل وتعطيلها أو إحداث شلل بها لفترة زمنية محددة، ومن ثم المطالبة بالحصول على فدية أو أموال مقابل إعادة تشغيلها، وهو النمط الذي انتشر على إثر التطورات التكنولوجية الهائلة بخاصة مع انتشار العملات الإلكترونية التي لا يمكن تتبع مسارها.

ب- الاستهداف السياسي، حيث يقوم فيه متسللون لهم أغراض سياسية محددة–قد يكونون دول أو جماعات أو أفراد يعملون بتوجيهات من مسئولين في دول– للضغط على دول أخرى لتحقيق مصالح بلادهم.

ج- الاستهداف بغرض التجسس: يقوم المتسللون باختراق أنظمة الحاسوب بغرض الحصول على معلومات والتجسس على الخصوم السياسيين.

أما عن مدى التشابه بين الهجمات السيبرانية على قطاع الطاقة من حيث طبيعتها وتكتيكاتها، فعلى الرغم من التشابه بين تلك الحالات إلا أنه لا يزال هناك فوارق بينها. فعلى صعيد التشابة، فإن جميع الهجمات تبدأ بإجراء عملية استطلاعية عن الهدف المراد توجيه الهجمة ضده، ثم تمر بعملية تسليح المعلومات التي تم جمعها، ثم استغلال الخرق الأمني، علاوة على تنفيذ الهجوم.

وعلى صعيد الاختلافات، فتتعلق بشكل أساسي بالتكتيكات المستخدمة في تنفيذ الهجوم، والتي يمكن توضيحها فيما يلي:-

أ- هجمات بسيطة، وهى تلك التي تعتمد على تكتيك مبسط كسرقة كلمات المرور أو عمليات التصيد بالرمح بهدف سرقة بعض البيانات أو إحداث شلل مؤقت بنظام التشغيل.

ب- هجمات مركبة، فهي التي تعتمد على أكثر من تكتيك، التي تبدأ بعملية تصيد من خلال إرسال صفحات تبدو رسمية بهدف الحصول على كلمات المرور، ثم اختراق

الشبكات وبث برامج خبيثة وفيروسات، ثم سرقة البيانات، ومحوها تماماً من على الأقراص الصلبة، علاوة على قطع التواصل بين المستفيد أو العميل للحيلولة دون قدرته على التواصل مع الشركات مقدمة خدمات الطاقة.

## ثالثًا: استراتيجيات مكافحة الهجمات السيبرانية لقطاع الطاقة

وانطلاقاً من كونها باتت ظاهرة عالمية، فقد بدأت العديد من البلدان بتطوير استراتيجيتها، وتكثيف جهودها للتعامل مع آثارها السلبية سواء بشكل منفصل أو مجتمعة. وفي هذا الصدد، يمكن الإشارة لأبرز تلك الجهود، وهي كالآتي:-

١- أعتلاء الأمن السيبراني قائمة الأولويات الحكومية:_فعلى خلفية هجمات خط كولونيال الأمريكي في منتصف عام ٢٠٢١، أعلن الرئيس الأمريكي، جو بايدن، أن "إدارته ستعطى قضية الأمن السيبراني أولوية قصوى على كاف مستويات الحكومة، مؤكدًا على أنه لن يقف مكتوف الأيدي أمام الهجمات الإلكترونية التي تواجهه أمتنا". وقد تمخض عن ذلك توقيع بايدن أمراً تنفيذياً بغرض تعزيز معايير الأمن السيبراني للحكومة الفيدرالية لخدمات البرمجيات التي تستخدمها، وهو الأمر الذي تم وصفه بأنه تحول كبير في نهج الحكومة الفيدرالية إزاء حوادث الأمن السيبراني باعتباره يقدم حلاً دائماً بعيداً عن الحلول المؤقتة.[٤٥]

٢- تطوير المنظومات التشريعية الإقليمية الخاصة بالأمن السيبراني: وهو النمط الذى أعتمد عليه الاتحاد الأوروبي. فعلى الرغم من أن الاتحاد كان قد وضع تشريعات لتعزيز الأمن السيراني في ٢٠١٦، والمعروفه باسم " توجيه أمن الشبكات والمعلومات Network and Information Security Directive إلا أن الهجمات الأخيرة التي ضربت البنية التحتية لقطاع الطاقة لاسيما في النرويج، وألمانيا، وهولندا، وبلجيكا قد دفعت الاتحاد لإدخال تطورات جديدة على تلك التشريعات، وهو ما تجلى في نوفمبر ٢٠٢٢ عندما وافق كل من البرلمان الأوروبي، والمجلس الأوروبي على تنفيذ سياسة جديدة تعرف باسم توجيه أمن الشبكات والمعلومات ٢ (NIS 2.0) Network and Information Security Directive 2 . وفقًا للاتحاد فأن هذا التشريع سيساعد ما يقارب ١٦٠ ألف كيان على إحكام قبضته على الأمن الأوروبي، وجعل أوروبا مكانًا آمنًا للحياة، والعمل[٤٦].

وفي هذا السياق، ركز التشريع الجديد على ضرورة تحسين ما يطلق عليه تطبيق "المرونة الإلكترونية" للكيانات العامة والخاصة في سبعة قطاعات محددة نظراً لاهميتها الاقتصادية والاجتماعية، وهي: الطاقة، والمصارف، والبنى التحتية للأسواق المالية، والنقل، والرعاية الصحية، والبنى التحتية الرقمية، وإمدادات مياه الشرب وتوزيعها. ذلك بالإضافة إلى ثلاث خدمات رقمية وهي: الأسواق عبر الأنترنت، ومحركات البحث، وخدمات الحوسبة السحابية. فقد ألزم التشريع الجديد الدول بمطالبة مقدمي الخدمات الأساسية بضرورة وضع متطلبات الأمن السيبراني، والإبلاغ عن الحوادث[٤٧].

٣- صياغة استراتيجيات شاملة للأمن السيبراني: سعت العديد من الدول لصياغة رؤي واستراتيجيات شاملة –وليس مجرد إجراءات مؤقتة- لتحقيق معدلات عالية من الكفاءة في مجال الأمن السيبراني. فعلى سبيل المثال: الإمارات، حيث اطلقت " الاستراتيجية الوطنية للأمن السيبراني" وتم تحديثها عام ٢٠١٩، إذ تهدف لتطوير منظومة متكاملة للأمن السيراني، وتضم خمسة محاور أساسية، علاوة على تبنيها لـــ٦٠ مبادرة لتحقيق الهدف ذاته. علماً بأن تلك الاستراتيجية قد تم تطويرها بناء على تحليل ما يزيد عن ٥٠ مؤشراً عالمياً، بالإضافة إلى التعاون مع فريق من الخبراء الدوليين في مجال الأمن السيبراني، علاوة على اعتمادها على منهج المقارنة المعيارية مع قرابة ١٠ بلدان من الأكثر تطوراً في العالم في هذا المجال[٤٨].

٤- تخصيص ميزانيات ضخمة لتعزيز القدرات التقنية للردع السيبراني: أجبرت حده الهجمات وخطورتها، وتعدد مصادرها العديد من البلدان لرفع مواردها المالية المخصصة لهذا الغرض في ميزانيات عام ٢٠٢١ . إذ يأتي في مقدمتها: الولايات المتحدة التي خصصت ١٨,٧ مليار دولار للاستثمار فى مجال الأمن السيبراني، وكذلك فرنسا التي خصصت وفقًا لتصريحات الرئيس الفرنسي إيمانويل ماكرون ١,٢ مليار دولار للغرض ذاته، وبريطانيا أيضاً خصصت حكومتها ١٦,٥ مليار دولار، علاة على الحكومة الكندية التي حددت ٨٠ مليون دولار للغرض ذاته، وإيران ٧١,٤ مليون دولار، بالإضافة إلى ماليزيا بـــ٢٧ مليون دولار[٤٩].

٥- رفع كفاءة أنظمة الأمن السيبراني فى منشآت قطاع الطاقة:_فمع اتساع نطاق الهجمات الموجهه لقطاع الطاقة، بدأت بعض القوى الدولية الكبرى بخاصة الولايات المتحدة إدراك وجود ثغرات تقنية يتم استغلالها من قبل المتسللين، وهو ما قد دفع الرئيس الأمريكي، جو بايدن، للإعلان عن خطة لتطوير البنية التحتية بقيمة ٢ تريليون دولان تتضمن ١٠٠ مليار لتحديث شبكة الكهرباء، وتضمينها إجراءات محسنة للأمن السيبراني.[٥٠]

٦- زيادة معدلات التعاون والتنسيق بين الشركات العالمية المعنية بالطاقة: كان للهجوم السيبراني على خط كولونيال الأمريكي، وما تبعه من هجمات ضد منشآت الطاقة الأوروبية أثر الصدمة، مما دفع ١٨ من كبرى الشركات العالمية العاملة في قطاع النفط والغاز- منها أرامكو، ودراجس، أوكسيدنتال بتريليوم- للاتفاق على إتخاذ تدابير جماعية تتعلق بما يطلق عليه " المرونة الإلكترونية" **Cyber resilience**، إذ تخطط المنظمات لاعتماد ستة مبادئ قائمة على العمل الجماعي، وتبادل الدروس المستفادة. وهو الأمر الذي أعلن عنه، ألكسندر كليمبورغ، رئيس مركز الأمن السيبراني في المنتدى الاقتصادي العالمي[٥١].

٧- عقد قمم دولية وإقليمية لمناقشة سبل التعاون في مواجهة الأمن السيبراني: استضافت الأردن في الفترة ما بين ١٥-١٦ أغسطس ٢٠٢٢ "القمة العالمية للأمن السيبراني" بحضور العديد من الخبراء الدوليين، حيث تناولت القمة مناقشة العديد من

الموضوعات، من أبرزها: الثورة الرقمية، والكشف عن التهديدات، وأمن البريد الإلكتروني، علاوة على أساليب نشر الوعي بمفهوم الأمن السيبراني.[٥٢]

في السياق ذاته، شهدت البحرين في الفترة ما بين ٦-٨ ديسمبر ٢٠٢٢ إنعقاد القمة العربية الدولية الأولى للأمن السيبراني تحت شعار " تمكين التعاون فى مجال الأمن السيبراني". إذ شارك فيها العديد من خبراء الأمن السيبراني من مختلف دول العالم. وفي هذا الصدد، سعت القمة لمناقشة وضع استراتيجيات لمواجهة تحديات الأمن السيبراني لاسيما سبل تعزيز حماية شبكات وبيانات القطاعات الهامة[٥٣].

٨- التعاون من خلال المنظمات الدولية: بدأت الأمم المتحدة جهودها فى مواجهة الهجمات السيبرانية في ٢٠٠٩، حينما قامت بإنشاء ما يطلق عليه " الشراكة التعددية ضد الهجمات السيبرانية" Impact.[٥٤] وفي العام التالي، وتحديدًا في أبريل ٢٠١٠، قامت لجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية بتكوين فريق دولي من الخبراء الحكوميين مهمته بحث مشاكل الهجمات السيبرانية، وكيفية التعامل معها.[٥٥]

وعلى صعيد المنظمات الإقليمية، فقد أولى مجلس التعاون الخليجي أهمية معتبرة لقضية الأمن السيبراني، وهو الأمر الذي تجلى في إنعقاد الاجتماع الأول للجنة الوزارية للأمن السيبراني بمجلس التعاون الخليجي في العاصمة السعودية، الرياض في ٢٣ أكتوبر ٢٠٢٢. فخلال الاجتماع تم بحث سبل التعاون المشترك بين دول مجلس التعاون في مجال تحقيق الأمن السيبراني، والتي تتضمن: تنسيق السياسات والإجراءات لمواجهة الهجمات السيبرانية، ورفع كفاءة التعاون بين الاتحاد والمنظمات الدولية المعنية بالأمن السيبراني، وتبادل الخبرات، والمعرفة، والمعلومات، والبحوث، والدراسات، علاوة على تدريب كوارد وطنية مؤهلة لمواجهة تلك التحديات، وذلك لتوفير فضاء إلكترونياً يتسم بقدر واسع من الأمن[٥٦].

٩- إطلاق مبادرات لصياغة اتفاقات دولية خاصة بمواجهة الجرائم السيبرانية: وكنتيجة لغياب التشريعات، والاتفاقات الدولية في مجال مكافة الأمن السيبراني، وزيادة معدلات استهداف القطاعات الحيوية لاسيما قطاع الطاقة. فقد دعا وزير الطاقة السعودي، الأمير عبد العزيز بن سلمان، إبان مشاركته فى المنتدى الدولي للأمن السيبراني، الذي أنعقد في الرياض خلال شهر نوفمبر ٢٠٢٢ إلى ضرورة سرعة عقد اتفاقاً دولياً لمواجهة الهجمات السيبرانية مثل ما حدث مع الاتفاقات الدولية الخاصة بمواجهة الإرهاب. كما طالب بن سلمان ليس فقط بضرروة إجبار مختلف الدول على الانضمام إليه، وإنما أيضاً بالمشاركة بكافة المعلومات التي تتعلق بالهجمات السيبرانية[٥٧].

١٠- إطلاق نماذج لمحاكاة مواجهة التهديدات السيبرانية: اعتمدت بعض البلدان على آلية إطلاق تمارين، وتدريبات لمحاكاة لكيفية مواجهة تلك التهديدات. فقد أعلنت الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية بالتعاون مع وزارة الطاقة عن تنظيم ما يطلق عليه " تمرين الأمن السيبراني لمنظومة الطاقة"، وذلك بمشاركة ما يزديد عن

٤٤ هيئة وطنية مختصة بقطاع الطاقة، علاوة على أكثر من ١٦٠ تقني ومختص بالأمن السيبراني.

فقد تضمن التمرين إجراءات محاكاة لمختلف أنواع الهجمات السيبرانية، وكيفية مواجهة التهديدات الطارئة، بما في ذلك الاستعداد، والكشف، مروراً بالتحليل، ثم إجراءات الأحتواء والتعافي، وانتهاء بالإجراءات التي يجدر أتباعها بعد الحادثة. ويأتي التمرين الذي تم إطلاقه يناير ٢٠٢٣ في إطار البرنامج الوطني للتمارين السيبرانية، الذي يهدف لاعتماد حماية متكاملة للفضاء السيبراني السعودي بغية الحفاظ على المصالح الحيوية، وبالتالي الأمن القومي للمملكة.[٥٨]

## الخاتمة والتوصيات

لا شك أن حيوية قطاع الطاقة باعتباره عصب الأمن القومي قد جعلته أحد أبرز أهداف الهجمات السيبرانية بمختلف أنواعها، وهو ما دفع مختلف دول العالم لإعادة النظر في آلياتها، واستراتجيتها لتحجيمها، والتقليل من آثارها، تمهيداً لمنعها نهائياً مستقبلاً. وهو الأمر الذي يتطلب مزيد التعاون بين مختلف الأطراف الدولية-سواء من الفواعل الدولية أو دون الدولية-، فلم يعد من الممكن خوض غمار معركة مكافحة الهجمات السيبرانية، أو تحقيق معدلات أفضل من الأمن السيبراني بشكل منفرد.

لكن، تظل عملية التعاون الدولي لمواجهة التحديات السيبرانية تواجه العديد من العقبات، من أبرزها:-

١- عدم وجود تنسيق قانوني كاف بين مختلف الدول، وتضارب الاختصاصات القضائية بين القضاء المحلي، والدولي.

٢- تضارب المصالح بين مختلف الدول، مما يتضح فى قيام بعضها باستخدام الهجمات السيبرانية كسلاح ضد البعض الآخر لاسيما في أوقات الحروب، والنزاعات.

٣- غياب استراتيجية دولية شاملة أو اتفاقاً دولياً ملزماً للكافة لمواجهة التهديدات السيبرانية على الصعيد العالمي.

٤- أنه على الرغم من زيادة حصة الأمن السيبراني في موازانات بعض البلدان، إلا أن تلك المخصصات لا تزال أقل من المطلوب، مما يعيق عملية المواجهة.

٥- ضعف البنية التشريعية الداخلية لمواجهة التهديدات السيبرانية في العديد من دول العالم.

٦- غياب الشفافية لدى بعض الحكومات، وعدم أعترافها بتعرض منشآتها للهجمات السيبرانية خوفاً من أن ينال ذلك من شرعيتها أمام شعوبها لعدم قدرتها على مواجهة تحديات أمنها القومي.

وانطلاقًا من تلك الحقائق، فإن عملية المواجهه باتت أمراً حتمياً لا يمكن التراجع عنه أو التهاون معه. وفي هذا الإطار توصي الدارسة بما يلي:-

**١- استحداث جهازاً شرطياً دولياً – يضم عناصر أمنية، وخبراء في مجال الأمن السيبراني- تقتصر مهمته على متابعة وتتبع التنظيمات التي تقوم بشن الهجمات السيبرانية.**

**٢- استحداث جهازاً دائماً لدى منظمة الأمم المتحدة تكون مهمته الأساسية التعامل مع تهديدات الأمن السيبراني-على غرار مجلس الأمن الدولي-يكون قادراً على اتخاذ قرارات ملزمة لفرض السلم والأمن الدوليين فى مجال الأمن السيبراني.**

**٣- ضرورة الإسراع في عقد مؤتمر دولي ضخم تحت رعاية الأمم المتحدة بهدف التفاوض بشأن إبرام إتفاقية دولية متكاملة، ومتطورة، وملزمة لجميع دول العالم لمواجهة التهديدات السيبرانية. بحيث تتضمن إجراءات وآليات محددة للتعاون، والتنسيق، والشفافية، وتبادل المعلومات.**

**٤- زيادة الميزانيات الموجهه للأمن السيبراني لاسيما مع ارتفاع التكلفة التي تخلفها تلك الهجمات. بعبارة أخرى، الاستثمار في قطاع الأمن السيبراني.**

**٥- عقد دورات بشكل دائم لتوعية العاملين في القطاعات الحيوية التي تعد هدفاً للهجمات السيبرانية لا سيما قطاع الطاقة بأنماط الهجمات السيبرانية، والطرق التي يستخدمها المتسللون، علاوة على الإجراءات التي يمكن أن يقوموا بها للتقليل من فرص نجاح تلك الهجمات.**

**٦- رفع مستوى التعاون بين الحكومات، والقطاع الخاص نظراً لما يملكه هذا القطاع من كفاءات، وخبرات تؤهله لمواجهة التهديدات السيبرانية.**

**٧- التوسع في تنظيم التدريبات والتمارين على مستوى الدولي الخاصة بمحاكاة التهديدات السيبرانية، وهو ما يساهم فى رفع كفاءة منظومة الأمن السيبراني داخل المؤسسات الهامة.**

**٨- عقد مؤتمرات دورية تحت رعاية المنظمات الإقليمية لعرض آخر المستجدات، والأساليب التي يتبعها المتسللون، وكيفية مواجهتها.**

## هوامش الدراسة

[١] سيد أحمد فوجيلي، "فهم الأمننة: مقاربة نقدية للدراسات الأمنية"، ***شؤون الأوسط***، العدد ١٥٣، نوفمبر ٢٠١٨، ص. ٧١.

[٢] ضحى هوام، نظرية الأمننة، الموسوعة السياسية، ٧ أكتوبر ٢٠١٨، منشور على الرابط الإلكتروني التالي:

https://political-encyclopedia.org/dictionary/%D9%86%D8%B8%D8%B1%D9%8A%D8%A9%20%D8%A7%D9%84%D8%A3%D9%85%D9%86%D9%86%D8%A9 (Accessed on 5 April 2023)

[3] Barry Buzan, Ole Weaver, and Japp de wilde, **Security: A New Framework of Analysis**, London: Lynne Rinner Publishers, 1st edition, 1998, PP- 21 23.

[4] Yuchong Li, and Qinghui Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", ***Energy Reports***, 7 (2021), P. 8177.

[5] Michael Robinson, Kevin Jones, and Helge Janicke, "Cyber warfare: Issues and challenges, **Computers *& Security***, 49 (2015). P. 70.

[6]Yuchong Li, and Qinghui Liu, ***Op. Cit***, P. 8179.

[7] Joseph Raczynski, "Kill chain: The 7 stages of Cyberattacks", Thomson Reuters, 12 October 2018. Available at: **https://tax.thomsonreuters.com/blog/kill-chain-the-7-stages-of-a-cyberattack/** (Accessed on 17 January 2023)

[8] Chrissy Kidd, "Cyber Kill Chains Explained: Phases, Pros/Cons & Security Tactics", 11 November 2022. Available at: **https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html** (Accessed on 18 January 2023)

[9]"Recognizing the seven stages of Cyber-attack," DNV, 2020. **https://www.dnv.com/cybersecurity/cyber-insights/recognizing-the-seven-stages-of-a-cyber-attack.html** (Accessed on 20 January 2023)

[10] Shruti M., 10 Types of cyber-attacks you should be aware in 2023, 8 February 2023. Available at: **https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks** (Accessed on 1 March 2023)

[11]Andrew Magnusson, **"Man-in-the-Middle (MITM) Attack: Definition, Examples & More"**, Strongdm, 12 February 2023. Available at: https://www.strongdm.com/blog/man-in-the-middle-attack (Accessed on 20 February 2023)

[12] "11 Password Cracker Tools (Password Hacking Software 2023), Software Testing Help, 13 February 2023. Available at: **https://www.softwaretestinghelp.com/password-cracker-tools/** (Accessed on 20 February 2023)

[13] "What is a denial of service attack (DOS)?", Paloalto networks. Available at: **https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos** ( Accessed on 20 February 2023)

[14] "What is SQL Injection & how to prevent SQL Injection?. Simplilearn, 14 February 2023. Available at: **https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-sql-injection** (Accessed on 1 March 2023)

[15] "What is a Zero-day Attack? - Definition and Explanation, Kaspersky. Available at: **https://www.kaspersky.com/resource-center/definitions/zero-day-exploit** (Accessed on 10 February 2023)

[16] Joe Franscella, "Targeted Attack Vs. Untargeted Attack", The Anomali Blog. Available at: **https://www.anomali.com/blog/targeted-attack-vs-untargeted-attack-knowing-the-difference** (Accessed on 10 May 2022)

[17] Pierre Jeanne and Olivier Jamart, "Report on Cyber Threats to Operational Technologies in the Energy Sector", GE Steam Power & Thales, 2020. P.18 Available at: **https://www.ge.com/content/dam/gepower-new/global/en_US/downloads/steam-new-site/services/automation-controls/ge-thales-cybersecurity-report-2020.pdf** (Accessed on 10 June 2020)

[18]"Energy is the Top Target for Cyberattacks. How Can the Sector Respond?", International Energy Forum, 25 August 2022. Available at: **https://www.ief.org/news/energy-is-the-top-target-for-cyberattacks-how-can-the-sector-respond**

[19]Pierre Jeanne and Olivier Jamart, "Report on Cyber Threats to Operational Technologies in the Energy Sector", ***Op.cit***, P. 20.

[20] Jonathan Nelson and Alejandro Romero, "Why Europe's energy industry is vulnerable to cyber-attacks", ***European Council On Foreign Relations***, 7 March 2022. Available at: **https://ecfr.eu/article/why-europes-energy-industry-is-vulnerable-to-cyber-attacks/** (Accessed on 7 January 2023)

[21] Nicholas Newman, Why is the energy sector so vulnerable to hacking?, ITPRO, 7 October 2021. Available at: **https://www.itpro.co.uk/security/cyber-attacks/361142/why-is-the-energy-sector-so-vulnerable-to-hacking** (Accessed on 10 January 2023)

[22] World Energy Council, The Road to Resilience: Managing Cyber Risks, 2016. P.17. Available at: **https://www.worldenergy.org/assets/downloads/The-road-to-resilience_Financing-resilient-energy-infrastructure_Report.pdf** (Accessed on 15January 2023)

[23] Luke James, Energy sector: More Cyber-attacks in 2022 than ever before, Power & Beyond, Available at: **https://www.power-and-beyond.com/energy-sector-more-cyber-attacks-in-2022-than-ever-before-a-a53dfeb9e1a85d8a0710a010c7a7e7d3/**

[24] Tomas Plėta, Manuela Tvaronavičienė, Silvia Della Casa, Konstantin Agafonov. Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. ***Insights into Regional Development***, 2020, 2 (3), pp.707 - 708. Available at: **https://hal.science/hal-03271856/document** (Accessed on 15 February 2023)

[25] Ahmad Mohee, "A Realistic Analysis of the Stuxnet Cyber-attack", 1 March 2022.P. 3 Available at: **https://preprints.apsanet.org/engage/api-gateway/apsa/assets/orp/resource/item/621e416fce899b8848a85f0b/original/**

**a-realistic-analysis-of-the-stuxnet-cyber-attack.pdf** (Accessed on 15 February 2023)

[26]Marie Baezner and Patrice Robin, "Hotspot Analysis: Stuxnet", Center for Security Studies (CSS), ETH Zürich, 2017, P. 4. Available at: **https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf** (Accessed on 10 April 2022)

[27] John Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield", ***Journal of Computer & Information Law***, Vol. 29, No.1, 2011. P.6.

[٢٨] منشأة نطنز النووية الإيرانية: ما هي وما سر الحوادث المتكررة فيها؟، بي بي سي نيوز عربي، ٢١ أبريل ٢٠٢١، منشور على الرابط الإلكتروني التالي:

**https://www.bbc.com/arabic/middleeast-56721332** (Accessed on 10 April 2023)

[29]Apurva Venkat, "Iran's nuclear energy agency confirms email server hacked", 24 October 2023. Available at: **https://www.csoonline.com/article/3677849/irans-nuclear-energy-agency-confirms-email-server-hacked.html** (Accessed on 6 April 2023)

[30] European Union Agency for cybersecurity, "Shamoon Campaigns with Disttrack", 7 January 2019. Available at: **https://www.enisa.europa.eu/publications/info-notes/shamoon-campaigns-with-disttrack** (Accessed on 9 October 2022)

[31] The BlackBerry Cylance Threat Research Team, "Threat Spotlight: Disttrack Malware", 21 February 2017. Available at: **https://blogs.blackberry.com/en/2017/02/threat-spotlight-disttrack-malware** (Accessed on 17 October 2022)

[32] Shamoon (2012), Cyber Law. Available at: **https://cyberlaw.ccdcoe.org/wiki/Shamoon_(2012)#cite_note-NYT-1** (Accessed on 5 December 2022)

[33] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. sees Iran Firing Black", ***New Times***, 23 October 2012. Available at: **https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html** (Accessed on 10 December 2022)

[34] Shamoon (2012), ***Op. Cit***,

[٣٥] تعرف على تاريخ فايروس " شمعون" في السعودية، العربية، ٢٤ يناير ٢٠١٧. منشور على الرابط الإلكتروني التالي:

**(Accessed on 7 August 2022)https://cutt.ly/z82TJhr**

[36] Sara Morrison, How a major oil pipeline got held for ransom?, VOX, 8 June 2021. Available at: **https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices** (Accessed on 20 December 2022)

[37] William Turton and Kartikay Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password", ***Bloomberg***, 4 June 2021. Available at: **https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?leadSource=uverify%20wall** (Accessed on 25 December 2022)

[38] Claudia Piccirilli, "How the Colonial Pipeline attack occurred", WTW, 21 May 2021. Available at: **https://www.wtwco.com/en-US/Insights/2021/05/how-the-colonial-pipeline-attack-occurred** (Accessed on 5 December 2022)

[39] Joe Panettieri, "Colonial Pipeline Cyberattacks: Timeline and Ransomware attack recovery details", 9 May 2022. Available at: **https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/** (Accessed on 7 February 2023)

[40] Eduard Kovacs, "Green Energy Company Volue hit by Ransomware, Security Week", 13 May 2021. Available at: **https://www.securityweek.com/green-energy-company-volue-hit-ransomware/** (Accessed on 27 December 2022)

[41] "Ransomware Attacks in the Energy Industry", CDW, 5 May 2022. Available at: **https://www.cdw.com/content/cdw/en/articles/security/ransomware-attacks-energy-industry.html** (Accessed on 20 February 2023)

[42] Tomas Plėta, Manuela Tvaronavičienė, Silvia Della Casa, Konstantin Agafonov, Op. ***Cit***, P. 710

[43] E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case".28 March 2016. Available at: **https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf** (Accessed on 15 January 2023)

[44] Shaun Nichols, "Ukraine energy grid hit by Russian Industroyer2 malware", Tech Target, 12 April 2022. Available at: **https://www.techtarget.com/searchsecurity/news/252515899/Ukraine-energy-grid-hit-by-Russian-Indestroyer2-malware** (Accessed on 20 January 2023)

[45] Sara Morrison, **Op. *Cit***.

[46]"From stricter reporting rules to new cyber threat hub, the EU is upgrading its cybersecurity law", ***World Economic Forum***, 2 February 2022. Available at: **https://www.weforum.org/agenda/2022/12/cybersecurity-european-union-nis/** (Accessed on 10 February 2023)

[47] The NIS 2 Directive, 2022. Available at: **https://www.nis-2-directive.com/**. (Accessed on 10 January 2023)

[٤٨] السلامة السيبرانية والأمن الرقمي، البوابة الرسمية لحكومة دولة الأمارات العربية المتحدة، ٢٠ يناير ٢٠٢٣، منشور على الرابط الإلكتروني التالي:

**https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security** (Accessed on 10 February 2023)

[49] Ritika Sagar, Top cybersecurity budget around the world, ***Analytics India Mag***, 10 June 2021. Available at: **https://analyticsindiamag.com/top-cybersecurity-budgets-around-the-world/** (Accessed on 5 January 2022)

[50] Sara Morrison, **Op*. Cit***.

[51] David Jones, "Oil and gas industry pledges cyber cooperation at World Economic Forum", Cybersecurity dive, 26 May 2022. Available at: **https://www.cybersecuritydive.com/news/oil-and-gas-industry-cyber-world-economic-forum/624460/** (Accessed on 10 January 2022)

[52] Race against cyber threats in 2022 and beyond, ***Trescon global***, 1 August 2022. Available at: **https://tresconglobal.com/conferences/cyber-sec/jordan/** (Accessed on 1 January 2023)

[٥٣] قمة عربية دولية للأمن السيبراني في البحرين، ***روسيا اليوم***، ٤ ديسمبر ٢٠٢٢، منشور على الرابط الإلكتروني التالي:

(Accessed on 5 January 2022)**https://cutt.ly/l8F6DLm**

[٥٤] هبه جمال الدين، "الأمن السيبراني والتحول في النظام الدولي"، ***مجلة كلية الاقتصاد والعلوم السياسية***، المجلد الرابع والعشرون، العدد الأول، يناير ٢٠٢٣، ص. ٢٠٧.

[٥٥] مراد مشوش، "الجهود الدولية لمكافحة الإجرام السيبراني"، ***مجلة الواحات للبحوث والدراسات***، المجلد الثاني عشر، العدد الثاني، ٢٠١٩، ص. ٧٣٠.

[٥٦] "خلال انعقاد الاجتماع الأول للجنة الوزارية للأمن السيبراني بدول مجلس التعاون ... إطلاق التمرين الخليجي الأول للأمن السيبراني" ، المركز الإعلامي لمجلس التعاون الخليجي، ٢٣ أكتوبر ٢٠٢٢. منشور على الرابط الإلكتروني التالي:

**https://www.gcc-sg.org/ar-sa/MediaCenter/NewsCooperation/News/Pages/news2022-10-23-4.aspx**

(Accessed on 28 October 2022)

[٥٧] " وزير الطاقة السعودي يدعو إلى اتفاق دولي لمواجهة الهجمات السيبرانية"، ***الشرق اقتصاد***، ١٤ نوفمبر ٢٠٢٢، منشور الرابط الإلكتروني التالي:

(Accessed on 27 November 2022) **https://cutt.ly/48Z8EUV**

[٥٨] " الهيئة الوطنية للأمن السيبراني تنفذ تمرين الأمن السيبراني بالتعاون مع وزراة الطاقة"، ***وكالة الأنباء السعودية***، ٨ يناير ٢٠٢٣، منشور على الرابط الإلكتروني التالي:

**https://www.spa.gov.sa/viewfullstory.php?lang=ar&newsid=2415807**

(Accessed on 10 January 2023)