توظيف القوة السيبرانية في الصراعات الدولية: دراسة حالة هجوم ستوكسنت على المنشآت النووية الإيرانية

باحثة حوراء ثامر عبد الحسن جامعة بغداد /كلية العلوم السياسية بغداد، العراق
Hawraa.abd2201@copolicy.uobaghdad.edu.iq

أ.د. عباس هاشم عزيز جامعة بغداد/ كلية العلوم السياسية بغداد، العراق
Abbas.hashim@copolicy.uobaghdad.edu.iq

الملخص:

مع بروز الفضاء السيبراني تصاعدت أهمية القوة السيبرانية وتأثيره المباشر على العلاقات الدولية إذ أدت إلى تحولات جذرية وكبرى في حقل العلاقات الدولية، فقد أصبح الفضاء السيبراني واستخدام القوة السيبرانية من أدوات ممارسة القوة في الصراعات الدولية وإدارتها، فضلاً عن تحقيق الأهداف العليا والاستراتيجية للدول، إذ لم تعد الصراعات الدولية تقتصر على استخدام القوة الصلبة العسكرية المباشرة بل امتدت إلى توظيف عوامل القوة المتوفرة كافة بدءاً من ممارسة التأثير وصولاً الى المزج بين أدوات القوة عبر استخدام القوة الناعمة الى جانب استخدام مقومات القوة الجديدة المتمثلة بالإمكانات التقنية والتكنولوجية وذلك عبر استغلال واستخدام الفضاء السيبراني للقيام بتنفيذ هجمات عدائية بدقة عالية تؤدي الى تعطيل البنى التحتية الحيوية الحساسة للدول، ويمثل هجوم ستوكسنت على المنشآت النووية الإيرانية نقطة تحول الواضحة في استخدام إمكانيات الفضاء السيبراني والقوة السيبرانية، إذ أظهر قدرات الدول على إمكانية تنفيذ عمليات هجومية تكنولوجية معقدة لتعطيل البنى التحتية الحيوية بدون التدخل المباشر، مما يؤدي إلى التأثير على موازين القوى الدولية.

الكلمات المفتاحية: القوة، القوة السيبرانية، الصراعات الدولية، دودة ستوكسنت.

The Employment of Cyber Power in International Conflicts: A Case Study of The Stuxnet Attack on Iranian Nuclear Facilities

Master's Candidate
Hawraa Thamer Abdual Hassan
University of Baghdad
College of Political Science
Baghdad, Iraq

Prof.Dr.
Abbas Hashim Aziz
University of Baghdad
College of Political Science
Baghdad, Iraq

Hawraa.abd2201@copolicy.uobaghdad.edu.iq
Abbas.hashim@copolicy.uobaghdad.edu.iq

Abstract:

With the emergence of cyberspace, the significance of cyber power has grown, exerting a direct impact on international relations. This development has led to profound and major transformations within the field of international relations. Cyberspace and the use of cyber power have become key instruments for exercising power in international conflicts and managing them, as well as for achieving states' supreme and strategic objectives. International conflicts are no longer confined to the use of direct military hard power; rather, they have expanded to encompass the employment of all available power resources, ranging from exerting influence to combining various tools of power. This includes the use of soft power alongside the new elements of power represented by technological and technical capabilities. Cyberspace is exploited to carry out highly precise hostile attacks that can disrupt critical and sensitive national infrastructures. The Stuxnet attack on Iranian nuclear facilities marks a clear turning point in the use of cyberspace and cyber power, demonstrating states' abilities to conduct complex technological offensive operations capable of disabling vital

infrastructures without direct intervention, thereby influencing the balance of international power.
Keywords: power, cyber power, international conflicts, Stuxnet worm.

المقدمة:

إن العلاقات الدولية كما المجالات الأخرى شهدت تحولات كبيرة نتيجة التطورات التكنولوجية المتسارعة، إذ برز الفضاء السيبراني بوصفه ساحة جديدة للصراعات الدولية، ولم يعد مفهوم الصراع والنزاع يقتصر على استخدام الأسلحة التقليدية بل امتد ليشمل استخدام القوة السيبرانية خدمة للأهداف الاستراتيجية العليا للدول، وإن هجوم ستوكسنت Stuxnet على المنشآت النووية الإيرانية يمثل أحد أبرز الأمثلة على توظيف القوة السيبرانية في الصراعات الدولية، فهو عُد أول هجوم سيبراني معروف يقوم باستهداف البنية التحتية الحيوية الحرجة لدولة ما، مين ما أدى إلى تعطيل وتخريب أجهزة الطرد المركزي في منشأة نتنز النووية، إذ يوضح هذا النموذج أبعاد الظاهرة السيبرانية في الصراعات الدولية وتداعياتها على الأمن الدولي.

أهمية البحث: توضح الدراسة كيفية توظيف الدول للقوة السيبرانية كأداة لتحقيق أهدافها الاستراتيجية مما يؤدي إلى فهم متغيرات الأمن الإقليمي والدولي الجديد، ويعد هجوم ستوكسنت مثالا على تطور مفاهيم الحروب السيبرانية ودور القوة في الفضاء السيبراني وتأثيرها على البني التحتية الحيوية للدول، وتوضح الدراسة أحد الأساليب المستخدمة في تنفيذ الهجمات السيبرانية مما يساهم بمساعدة صانعي القرار على تطوير استراتيجيات وسياسات دفاعية أكثر فاعلية، كما تهدف هذه الدراسة إلى توضيح دور القوة السيبرانية في الصراعات الدولية عبر دراسة حالة هجوم ستوكسنت على المنشآت النووية الإيرانية، لإيضاح وتحليل كيف يتم توظيف

الهجمات السيبرانية بوصفها أداة استراتيجية تستهدف البني التحتية الحيوية الحساسة، وتستخدم للتأثير على الأمن القومي للدول.

إشكالية البحث: مع تزايد اعتمادية الدول على التكنولوجيا الرقمية في مختلف المجالات وظهور الفضاء السيبراني بوصفه الساحة الجديدة للصراعات الدولية أصبحت الهجمات السيبرانية تبعاً لذلك الأداة الفعالة لتحقيق الأهداف الاستراتيجية للدول دون الحاجة إلى التدخل العسكري المباشر. وبالتالي، تتمثل إشكالية هذه الدراسة في تساؤل رئيس وهو: كيف وظَفت القوة السيبرانية في الصراعات الدولية باستخدام هجوم ستوكسنت على البرنامج النووي الإيراني وكيف آثر على سياسات الأمن السيبراني في إيران؟

فرضية البحث: إن هجوم ستوكسنت يعد انموذجاً نوعياً لإمكانية توظيف القوة السيبرانية في الصراعات الدولية، إذ أظهر مدى قدرة الهجمات السيبرانية على إلحاق أضرار ملموسة بالبنى التحتية الحيوية للدولة المستهدفة دون الحاجة إلى التدخل العسكري التقليدي المباشر.

منهجية البحث: تم الاعتماد في هذه الدراسة على المنهج الوصفي، في وصف وتوضيح مفاهيم القوة والقوة السيبراني، وكذلك في تقديم وصف دقيق لهجوم ستوكسنت من حيث خلفيته، والجهة المنفذة، والأهداف المستهدفة، والتقنيات المستخدمة، كما اعتمدت هذه الدراسة على المنهج التحليلي، لتحليل دور القوة السيبرانية بوصفها إعداد جديدة في الصراعات الدولية وتغيير موازين القوى بين الدول، فضلاً عن تحليل نموذج الدراسة.

المبحث الأول

القوة السيبرانية في الصراعات الدولية

فتحت الثورة المعلوماتية وتأثير العولمة عصر جديد من التأثير السلبي والايجابي فضلاً عن التواصل والانفتاح (رزاق، ٢٠١٩، ٣٠١)، وإن ما يميز الصراعات المعاصرة في القرن الحادي والعشرين هو تراجع الخطوط الفاصلة بين حالتي الحرب والسلم، إذ لعبت عدة عوامل دوراً كبيراً في تصاعد وكثافة توظيف أدوات الحرب في اوقات السلم، مثل الحرب المعلوماتية، والحروب الاقتصادية، فضلاً عن دعم الجماعات الإرهابية، أو الميليشيات المسلحة بأسلحة متقدمة لتوظيفها ضد الدول المتصارعة، وهو الأمر الذي ساهم في تراجع الحاجة إلى اعلان الحرب، بل تعمد الدول أحيانًا على مبدأ الإنكار، خاصة إذا لم يتم تقديم أدلة حاسمة تؤيد حدوث هذا التورط (منصور، ٢٠١٩، ٢٠).

المطلب الأول: الصراع السيبراني

ان التغير المستمر هو الصفة والعامل الثابت في العلاقات الدولية ويعود ذلك للتطورات السياسية والعسكرية والاقتصادية والتكنولوجية (الكعود والخفاجي، ٢٠٢١، ٢٨) أصبحت الصراعات اليوم معقدة ومتشابكة ومتداخلة أكثر من السابق والى حدً كبير، وهذا الامر يترتب عليه استحالة استخدام استراتيجية القوة الصلبة بمفردها (خلف، ٢٠١٥، ٢٢٧)، فبعد طرح مصطلحي القوة الناعمة والصلبة من قبل جوزيف ناي وضح حجم التأثير لهذه الأنواع من القوة على العلاقات الدولية فان مفهوم الصراع يتغير استناداً الى مبادى واساسيات تطور أساليب ووسائل وتقنيات المفهوم ذاته (العامري، ٢٠١٩، ٢٨٧)، ويعد العنصر المفاهيمي في أي دراسة علمية عاملاً محورياً ومهماً يساعد في استكشاف العلاقة بينة العنصر المتغير والثابت لتحليل وفك التفاعل وتحديد مدى الغموض في مفاهيم

الدراسة(Alwan, Manati.2024,1811)، ونقتبس مقولة فولتير الشهيرة " إذا أردت التحدث معي، فعرف مصطلحاتك أولاً" (Jasem,Ali.2024,434)، وان القدرة على اتخاذ قرارات سريعة في وقت قصير ضرورية لمنع حدوث الأزمات (Mutlak and Lahmood.2024,1964)، وان الصراعات الحروب ما هي الا اخطر تهديدات النظام العالمي وتخرق القوانين والأعراف الدولية ومبادئ الإنسانية (ياسين وكاظم، ٢٠٢٣، ٢٤٦) فالصراع السيبراني هو استخدام الاطراف المختلفة دولاً ام غير دول قدراتها في الفضاء السيبراني من اجل تحقيق اهدافها المتعارضة داخل او عبر البنية السيبرانية للفضاء السيبراني، اي هي ظاهرة صراعية مختلطة او هجينة تتداخل فيها الحسابات الانسانية مع الحسابات التكنولوجية، وتتشابك بها طبيعة واهداف وهويات الاطراف من الدول وغير الدول(علي، ٢٠١٧، ٣).

يشير الصراع في الفضاء السيبراني: إلى الإجراءات التي تتخذها أطراف النزاع للحصول على ميزة على خصومها في الفضاء السيبراني باستخدام مختلف الأدوات التكنولوجية والتقنيات القائمة على الأشخاص (Lin. 2012,515).

يتجه الصراع السيبراني اتجاهاً تنافسياً عن طريق السعي للسيطرة على عناوين المواقع وأسماء النطاقات والتحكم بالمعلومات ومحاولة اختراق الأمن القومي للدول، ولكن دون استخدام طائرات ومتفجرات ولا يتضمن انتهاك للحدود السيادية والتي تتمثل بهجمات قرصنة للكومبيوتر وتدمير المواقع والتجسس بما له من تأثير على امكانية تدمير الاقتصاد والبنية التحتية بالقوة مماثلة لتلك التي يحدثها تفجير تقليدي مادي مدمر، وقد اصبح الصراع السيبراني أحد اهم أوجه التفاعلات الدولية الجديدة شأنه شأن الهجمات السيبرانية والحرب السيبرانية إلا إنه يمتاز بخصائص أهمها (جيجان، ٢٠٢١، ٣٧):

اولاً: تنوع الفاعلين من دول وغير الدول.

ثانياً: غير مكلف من الناحية المادية.

ثالثاً: ليس من السهولة نزع سلاح الطرف الآخر أو تدميره كلياً أو احتلال إقليمه.
رابعاً: إمكانية استخدام الفضاء السيبراني في نوعي القوة الناعمة أو الصلبة.

ان التعاون الدولي قد يثري ويعزز الى حد بعيد الامن في الفضاء السيبراني، تبعاً ذكره تقرير اللجنة الدولية للتدخل والسيادة الدول إذ أكد التقرير على دور الفواعل الدولية دون غيرها بإشارته الى "إن النظام الدولي المتماسك والسلمي من المرجح أن يتحقق من خلال تعاون الدول المؤثرة الواثقة من مكانها في العالم وليس في بيئة من الكيانات الحكومية الهشة أو المنهارة او المجزئة والفوضوية بشكل عام (Ali,Qari and Alwan 2021,p.13)".

المطلب الثاني: القوة السيبرانية

إن القوة هي القدرة على التأثير في الآخرين لاستخلاص نتائج محددة، عن طريق سعي الطرف الذي يقوم بعملية التأثير للحصول عليها، إذ إن (هانز مورجنثاو) ربط القوة بفكرة التأثير أو التحكم في المكاسب، وقد تأثر عالم الاجتماع (روبرت دال) بأفكار مورجنثاو حول القوة وقدم تعريفاً أكثر وضوحاً للقوة، إذ عرفها بأنها "القدرة على جعل الآخرين يقومون بأشياء متناقضة مع أولوياتهم، ما كانوا يقوموا بها لولا ممارسة تلك القدرة " ومن الأمور الراسخة في العلاقات الدولية أن مكونات نفوذ الدولة ومصادر قوتها تتغير، وأن القوة العسكرية منفردة لم تعد تحقق الأهداف المطلوبة التي تسعى الدولة لتحقيقها، وأشكال هذه القوة متعددة فمنها القوة الصلبة المتمثلة بالقدرات العسكرية والاقتصادية، والقوة الناعمة المتمثلة بالعوامل غير المادية كالثقافة والقيم (خليفة، ٢٠١٧، ٤٢).

تتنوع أدوات ممارسة القوة في العلاقات الدولية تبعاً لإمكانيات وقدرات ورغبات القوى المشاركة فيه، فقد تكون القوة العسكرية هي أهم هذه الأدوات، اوقد تكون القوة الاقتصادية العامل الاساس للسيطرة على الخصم وممارسة القوة عليه، وقد تكون الأداة المعلوماتية اي استخدام وسائل الاتصال والتكنولوجيا الحديثة

والإنترنت هي العامل الرئيس لحسم صراع بين دولتين؛ وذلك لما للتكنولوجيا الحديثة من تأثير على مفهوم القوة وتحولاتها ادى بذلك إلى ظهور مفهوم القوة السيبرانية (Cyber Power) (خليفة، ٢٠٢١، ٦٥).

بقي مفهوم القوة السيبرانية موضع جدل الكثير من الباحثين، وفي أحدى المحاولات لتعريف القوة السيبرانية تركزت على إنها القدرة على استخدام الفضاء السيبراني من اجل خلق مزايا وتأثير في الأحداث لجميع البيئات، وعبر أدوات القوة، ويبقى مبدأ القوة الأكثر في قابلية التطبيق للدول الباحثة عن تفاعل استباقي في مجالها الدولي بمعنى (إنشاء الفرص الاستراتيجية عبر الفضاء السيبراني) وقد حدد جوزيف س.ناي مفردة القوة السيبرانية لفهم الدور الذي يؤديه الإنترنت في تشكيل القدرة للأطراف الدولية لتحقيق أهدافها، إن العصر الالكتروني قد قلل من الصعوبات، لكنه في الوقت نفسه فرض تحديات اكبر على الاطراف الدولية وبخاصة الولايات المتحدة الامريكية المحتكرة لمصادر القوة منذ نهاية الحرب (مهدي وصفاء، ٢٠٢٠، ١٥٢).

يعرف دانيال كوهيل القوة السيبرانية بانها القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير على الأحداث في جميع البيئات التشغيلية وعبر أدوات السلطة، تتشكل أداة القوة السيبرانية من خلال عوامل متعددة، ففي حين أن الفضاء السيبراني كبيئة، فإن القوة السيبرانية هي دائما مقياس للقدرة على استخدام تلك البيئة، وإن التكنولوجيا هي أحد العوامل الواضحة، لأن القدرة على (دخول) الفضاء السيبراني هي ما يجعل من الممكن استخدامها، هذه التكنولوجيا تتغير باستمرار، وقد يكون بعض المستخدمين (الدول والمنظمات والجهات الفاعلة من غير الدول) قادرين على القفز فوق التقنيات القديمة لنشر واستخدام تقنيات جديدة للحصول على ميزة استراتيجية (Kramer, Starr, Wents.2009,75).

عرف جوزيف س.ناي القوة السيبرانية بانها "القدرة على الحصول على النتائج المرغوبة من طرف من خلال استخدام موارد المعلومات المترابطة إلكترونيا في المجال السيبراني"، ويمكن استخدام القوة السيبرانية لإنتاج نتائج مرغوبة للأطراف الحائزة على هذه القوة داخل الفضاء السيبراني، أو يمكنها استخدام الأدوات السيبرانية لإنتاج نتائج المرغوبة لها في مجالات أخرى خارج الفضاء السيبراني، ويعتمد سلوك القوة السيبرانية على مجموعة من الموارد المتعلقة بإنشاء المعلومات الإلكترونية والقائمة على الكمبيوتر والتحكم فيها والتواصل معها)البنية التحتية، والشبكات، والبرمجيات، والمهارات البشرية (ويشمل ذلك إنترنت أجهزة الكمبيوتر المتصلة بالشبكة، ولكن أيضا الشبكات الداخلية والتقنيات الخلوية والاتصالات الفضائية (Nye.2010,4) ، وهناك أنماط عدة لاستخدام القوة في الفضاء السيبراني وهي (مهدي وصفاء، ٢٠٢٠، ١٥٣):

اولاً: تأثير الفاعل أ على الفاعل ب: فعلى سبيل المثال فإن هجمات الحرمان من الخدمة وإدخال البرامج الضارة تعد (قوة صلبة) اما حملة المعلومات أو تجنيد أعضاء المنظمات الإرهابية فتعد (قوة ناعمة)

ثانياً: التحكم في الأجندة: وتتمثل في قدرة الفاعل أ على استبعاد إستراتيجيات الفاعل ب، وعلى سبيل المثال: الضغط على الشركات لاستبعاد بعض الأفكار تعد (قوة صلبة) اما معايير البرامج المقبولة فتعد (قوة ناعمة).

ثالثاً: قدرة الفاعل أ على إعادة ترتيب اولويات الفاعل ب: فعلى سبيل المثال إن تهديدات بمعاقبة المدونين الذين ينشرون مواد خاضعة للرقابة تعد (قوة صلبة)، اما المواقع الإباحية للأطفال فتعد (قوة ناعمة).

تؤثر القوة السيبرانية على العديد من المجالات من الحرب إلى التجارة، ويمكن التمييز بين (قوة الفضاء السيبراني الداخلية) و(قوة الفضاء السيبراني الإضافية)، يمكن استخدام أدوات المعلومات لإنتاج القوة الناعمة في الفضاء

السيبراني من خلال الجذب أو الإقناع، يمكن للموارد السيبرانية أيضاً إنتاج قوة صلبة داخل الفضاء السيبراني، على سبيل المثال، يمكن للدول أو الجهات الفاعلة غير الحكومية تنظيم هجوم موزع لرفض الخدمة باستخدام (شبكات الروبوتات) لمئات الآلاف أو أكثر من أجهزة الكمبيوتر التالفة التي تغمر نظام الإنترنت لشركة أو بلد (Nye.2010,5).

يوضح الجدول الاتي الاختلاف ما بين قوة الفضاء السيبراني الداخلية وقوة الفضاء السيبراني الاضافية لتحقيق اهداف القوة السيبرانية:

جدول ١ (الأبعاد المادية والافتراضية للقوة السيبرانية)

نوع الادوات	الفضاء السيبراني الداخلي	الفضاء السيبراني الاضافي
ادوات معلوماتية	القوة الصلبة: من امثلتها هجمات الحرمان من الخدمة القوة الناعمة: تتمثل بوضع القواعد والمعايير	القوة الصلبة: من امثلتها مهاجمة أنظمة سكادا SCADA (انظمة التحكم والمراقبة) القوة الناعمة: تتم مثلاً بواسطة حملة دبلوماسية عامة للتأثير على الرأي العام
ادوات فيزيائية	القوة الصلبة: وتتمثل بتشريع قوانين ضوابط حكومية توجه الى الشركات الخاصة القوة الناعمة: بتوظيف بنية تحتية لمساعدة نشطاء حقوق الإنسان	القوة الصلبة: باستخدام أجهزة توجيه القنابل أو قطع الكابلات القوة الناعمة: متمثلة باحتجاجات تمارس ضد مقدمي خدمات الإنترنت

الجدول من اعداد الباحثة استناداً إلى:

Joseph S. Nye Jr., Cyber Power: In the Future of Power in the 21st Century (Cambridge: Belfer Center for Science and International Affairs and Harvard Kennedy School, 2010), p.5.

المبحث الثاني

الأسلحة السيبرانية وتحول أنماط الصراع: دراسة حالة دودة ستوكسنت

إن الهجمات السيبرانية العسكرية هي الهجمات التي تتم باستخدام (أسلحة سيبرانية)، وتتعدد هذه الأسلحة السيبرانية التي إذ ما تم استخدامها فأنها ستلحق اضراراً مدمرة بالدول الَمستهدَفة، وأخطر أنواع هذه الأسلحة واهمها هي: **دودة ستوكسنت Stuxnet**

المطلب الاول: الأسس المفاهيمية والتقنية لدودة ستوكسنت

وُصفت دودة ستوكسنت بأنها "اول سلاح رقمي في العالم" إذ أدى هذا الهجوم السيبراني باستخدام دودة ستوكسنت إلى تغيير طريقة فهم المجتمعات للأمن السيبراني سواء على مستوى الدول او مستوى الشركات لنطاق التهديدات التي تمثلها الهجمات السيبرانية وأنواع الضرر المترتبة عليها (إبراهيم، ٢٠٢٤، ٨٠).

تُعد هذه الدودة أحد أكثر اشكال الأسلحة السيبرانية تهديداً وخطراً التي تم الكشف عنها، ومثلت طفرة نوعية في تصعيد اخطار الصراعات السيبرانية، إذ نقل مستوى التنفيذ من سرقة البيانات وتحطيمها، إلى تحطيم المكونات المادية ونظم التشغيل نفسها (خليفة، ٢٠٢١، ١١١). مثلت دودة ستوكسنت حدث مفصلي ونقطة تحول في المجال الأمني، إذ وصفت من العديد من الخبراء بكونها واحدة من أكثر البرامج الخبيثة فائقة التعقيد (شاكر، ٢٠٢٢، ٢٣٩) ، يعود السبب في ذلك إلى ظهورها ولأول مرة بوصفها سلاح سيبراني يستخدم بهدف الهجوم، والتدمير، وتخريب منظومة معلومات بشكل معين، وتكمن الأهمية الكبرى في تكامل برمجية الدودة، إذ تسللت بشكل سري إلى شبكة المراقبة الصناعية المنفصلة عن شبكة الأنترنت (Air Gap)، واستطاعت أن تعمل في بيئة محمية بشكل كامل، فالسرية والحماية مثلان دليلاً مباشراً على تدخل دولة ما وحمايتها لهذه

الدودة البرمجية الخبيثة، ولكن لم تعلن أي جهة عن مسؤوليتها عن هذا الهجوم بشكل مباشر (مجموعة مؤلفين، ٢٠١٨، ٦٧).

فدودة ستوكسنت تمثل جزء متقدم من رمز حاسوبي Code تهدف بشكل أساس إلى الانتشار مستخدماً ميزة التشغيل التلقائي Auto Run في نطاق الشبكة العالمية العنكبوتية، وتم تصميمها حتى تستطيع القيام بعدة وظائف، وبمجرد تثبيتها يتم تحديد النظام المضيف ويقوم بتطوير خرائط الشبكة المضيفة ، وبعد ذلك تعطي نسخاً عنها، كما تمتلك القدرة على القيام بالإبلاغ عما تجده (إبراهيم، ٢٠٢٤، ١٦٤).وبشكل عام، تقوم دودة ستوكسنت باستهداف أنظمة التحكم الصناعية المطبقة على نطاق واسع في المنشآت ذات الأهمية الكبرى، مثل محطات توليد الطاقة الكهربائية، وخطوط نقل النفط، فضلاً عن المفاعلات النووية، وغيرها من المرافق الاستراتيجية الأساسية الهامة، وتقوم بالتنقل بين أجهزتها بواسطة أجهزة USB اختصاراً لـ (Universal Serial Bus)* مستغلة واحد او أكثر من نقاط الضعف في نظام تشغيل ويندوز (Windows OS)* (خليفة، ٢٠٢١، ١١٢).

مثلت دودة ستوكسنت تطبيق معقد ومتقدم للغاية الهدف منه القيام بإعاقة عمل مفاعلات تخصيب اليورانيوم في الجمهورية الإسلامية الايرانية التي تشغل

* يو اس بي USB، أو الناقل التسلسلي العالمي Universal Serial Bus، هو آلية تستخدم لتوصيل الأجهزة الطرفية بأجهزة الحاسوب.. للمزيد يرجى الاطلاع على: Chiradeep BasuMallick, "What Is USB (Universal Serial Bus)? Meaning, Types, and Importance," Spiceworks, January 10, 2023, available at:]Cited 13, Jan, 2025, 01:43 pm [https://www.spiceworks.com/tech/tech-general/articles/universal-serial-bus/.

* نظام التشغيل ويندوز من مايكروسوفت (Windows Operating System) هو نظام تشغيل رسومي، يمكن للمستخدمين استخدامه لقراءة الملفات وتخزينها وتشغيل التطبيقات ولعب الألعاب ومشاهدة مقاطع الفيديو بالإضافة إلى الاتصال بالإنترنت، وتم توفيره للاستخدام الشخصي والمهني على حد سواء.. للمزيد يرجى الاطلاع على: Bhumika, "What is Windows Operating System?" GoSeeko, April 9, 2022, [Cited 13, Jan, 2025, 01:53 pm], available at: https://www.goseeko.com/blog/what-is-windows-operating-system/.

بواسطة محولات فائقة السرعة توظف في منشآت تخصيب اليورانيوم في نتنز (مجموعة مؤلفين، ٢٠١٨، ٦٧).

للوصول الى العتبة النووية تتم عن طريق عملية متراكمة ومعقدة من الاجراءات في المفاعلات المتخصصة ، وهذا يعني إن تخصيب اليورانيوم إلى النقاء اللازم لصنع سلاح نووي تدميري هو عملية معقدة بشكل كبير، إذ إن خام اليورانيوم، عندما يكون على سطح الأرض، تتكون في الغالب من هذه النظائر النادرة تسمى اليورانيوم-٢٣٨، يحتوي على أقل من ١ في المائة من اليورانيوم-٢٣٥، وهو الشكل الأخف من المعدن الفضي الذي يمكن استخدامه للانشطار النووي الذي يطلق الطاقة اللازمة لتشغيل أو تدمير مدن بأكملها، وإن الطاقة النووية تتطلب يورانيوم يبلغ حوالي نسبة ٣ إلى ٥ في المائة من اليورانيوم-٢٣٥، ولكن الأسلحة النووية تتطلب نواة من اليورانيوم تصل إلى ٩٥ في المائة تتكون من هذا النظائر النادرة (Greenberg.2019,113).

وللوصول إلى هذه النسبة يأتي عمل أجهزة الطرد المركزي؛ لإثراء اليورانيوم إلى مادة يصنع منها السلاح النووي، يجب إن يتم تحويله إلى غاز وضخه في أسطوانة الألمنيوم الطويلة للطرد المركزي، ويتم تدويره داخل طول تلك الاسطوانة بواسطة محرك في أحد الطرفين، وتدور بعشرات الآلاف من الدورانات في الدقيقة، بحيث تتحرك الحافة الخارجية بما يتجاوز سرعة الصوت، وتصل قوة اجهزة الطرد المركزي التي تدفع من المركز نحو جدران غرفة الغزل تلك إلى ما يصل إلى مليون مرة من قوة الجاذبية، مما يفصل اليورانيوم-٢٣٨ الأثقل بحيث يمكن سحب اليورانيوم-٢٣٥ للوصول إلى تركيزات درجة الأسلحة، ويجب تكرار العملية مراراً وتكراراً عبر (سلسلة) من أجهزة الطرد المركزي (Greenberg.2019,113).

بدأ اكتشاف دودة ستوكسنت بعد إن وجدت شركة فايروس بلوكادا (VirusBlokAda)، وهي شركة للأمن السيبراني لمكافحة الفيروسات مقرها في مينسك في بيلاروسيا، أذ أن جهاز الحاسوب لأحد عملائها في إيران كان عالقاً في حلقة من الأعطال المتكررة وإعادة التشغيل. حقق الباحثون لتلك الشركة عن مصدر تلك الحوادث ووجدوا شيئاً أكثر تطوراً بكثير مما كانوا يتخيلون، وله امكانية فائقة التخفي، وهو من البرامج الضارة المعروفة باسم الجذور الخفية (Rootkit) التي تستطيع دفن نفسها في أعماق نظام تشغيل الحاسوب، وعندما حللوا تلك الجذور الخفية، وجدوا شيئا أكثر أخطر بكثير، إذ تمت أصابه الجهاز بمجرد إدخال عصا يو اس بي USB المصابة في منفذ الكمبيوتر، إذ ظهرت البرامج الضارة لتثبيت نفسها على الجهاز دون أي إشارة للمستخدم على الإطلاق(Greenberg.2019,115) ، في وقت لاحق، قام الباحث الألماني رالف لانغنر (Ralph Langner) بفك مفصل للبرمجية الخبيثة وساعد في تحديد أن هدفه من المعدات التي تنتجها شركة سيمنز الالمانية المستخدمة في منشأة نتنز النووية الإيرانية(Deibert.2013,223).

اكتشف الباحث رالف لانغنر أن دودة ستوكسنت كانت موجهة فقط إلى وحدة تحكم صناعية محددة، تصنعها شركة سيمنز، تم تكوينها لتشغيل سلسلة من أجهزة الطرد المركزي النووية، ولكن ليس فقط أي أجهزة طرد مركزي نووية قديمة قد تكون غير مستعملة، ولكن موجهة فقط لسلسلة من أجهزة الطرد المركزي ذات حجم وعدد معينين تحمل الرقم (٩٨٤) مرتبطة ببعضها البعض، وكان هذا العدد الدقيق تحمله أجهزة الطرد المركزي في منشأة نتنز النووية (Singer,Friedman.2014,177).

المطلب الثاني: التطبيق العملي لدودة ستوكسنت في استهداف البرنامج النووي الايراني

ان محور الصراع بين الولايات المتحدة واسرائيل من جهة وايران من جهة اخرى يتمحور حول الملف النووي ومحاولة ايران الحصول على السلاح النووي كما يتهم الغرب ايران، بدأت الأزمة من بعد العقوبات على قطاع البتروكيمياويات الإيراني التي فرضتها إدارة الرئيس الأمريكي الأسبق باراك اوباما في شهر حزيران من عام ٢٠١٠، تبعها اسقاط ايران لطائرة استطلاع أمريكية بالقرب من مضيق هرمز، بادرت الولايات المتحدة الامريكية بشن هجمات سيبرانية استهدفت بها شبكة تجسس إيرانية فضلاً عن استهدافها لأنظمة الكترونية إيرانية تستخدمها لأطلاق الصواريخ (شاكر، ٢٠٢٢، ٢٣٨)، وعلى إثرها قامت ايران بإسقاط طائرة دون طيار أمريكية سيبرانياً، اتهمت الولايات المتحدة الامريكية ايران بدورها في تصعيد الصراع باستخدامها الهجمات السيبرانية، ففي عام ٢٠١٠ أدى الفضاء السيبراني دوراً محورياً بكونه مجال جديد يستخدم في العمليات العدائية، فايران والولايات المتحدة الامريكية و(إسرائيل) تبادلتا الاتهامات مع تصعيد الصراع سيبرانياً في ذروة الازمة القائمة بين الاطراف حول الملف النووي الإيراني (شاكر، ٢٠٢٢، ٢٣٩).

في كانون الثاني/يناير عام ٢٠١٠ بدأ المسؤولون في الوكالة الدولية للطاقة الذرية، وهي هيئة تابعة للأمم المتحدة مكلفة بمراقبة البرنامج النووي الإيراني، في ملاحظة شيء غير عادي يحدث في مصنع تخصيب اليورانيوم خارج مدينة نتنز في وسط ايران داخل قاعة الطرد المركزي الكبيرة في المنشأة، المدفونة في القبو على بعد أكثر من خمسين قدماً تحت سطح الارض، كانت الآلاف من أجهزة الطرد المركزي المصنوعة من الألمنيوم تدور بسرعة تفوق سرعة الصوت، مما يؤدي لنشر غاز سداسي فلوريد اليورانيوم في المكان، وفي وقت ماضي على

هذه الملاحظة، كان العمال في المصنع يزيلون دفعات كبيرة جداً من أجهزة الطرد المركزي التالفة ويستبدلونها بأخرى جديدة (Zetter.2014,6).

إذ إن المهندسون العاملون في مشروع نتنز واجهوا مشكلة غامضة وفي أوقات عشوائية، إذ بدأت بعض أجهزة الطرد المركزي في الخروج عن نطاق السيطرة، وتتحرك غرفته الداخلية بشكل أسرع حتى من محاملها المصممة بعناية للتعامل معها، وفي حالات أخرى، ازداد الضغط داخل الغرفة الداخلية للأسطوانة لدرجة إن يتم دفعها خارج مدارها، فتصطدم أسطوانة الغزل بعد ذلك بأطرافها بسرعة تفوق سرعة الصوت، مما يؤدي إلى تمزيق الماكينة من الداخل ولم يتمكن المشغلون من رؤية أي علامة أو تحذير في مراقبتهم الرقمية لأجهزة الطرد المركزي لشرح حالات العطل المفاجئة للآلات، ومع ذلك استمر العطل في الحدوث(Greenberg.2019,113).

من الجدير بالملاحظة ، كان لدى ايران في تشرين الثاني/ نوفمبر عام ٢٠٠٩، حوالي ثمان الاف وسبعمائة جهاز طرد مركزي مثبت في نتنز، لذلك كان من الطبيعي تماماً أن نرى الفنيين يوقفون حوالي ثمان مئة منها على مدار العام لفشل الأجهزة لسبب أو لآخر، ولكن عندما احتسب القائمين على ادارة الوكالة الدولية للطاقة الذرية أجهزة الطرد المركزي التي تمت إزالتها على مدى عدة أسابيع في كانون الأول/ ديسمبر ٢٠٠٩ وأوائل كانون الثاني/يناير من عام ٢٠١٠، أدركوا أن إيران كانت تتخلص من أجهزة الطرد المركزي المتعطلة بمعدل غير عادي(Zetter.2014,6).

في خضم التصعيد بين الاطراف ، تم الكشف عن دودة ستوكسنت عام ٢٠١٠ عندما اصابت أجهزة الطرد المركزية الإيرانية وتسببت في إيقاف العديد منها واخراجها عن الخدمة، إذ هاجمت نظم التشغيل لأجهزة الطرد المركزي التي كانت تشغل عبر نظام التحكم الصناعي SCADA اختصاراً لـ (supervisory

(control and data acquisition التحكم الإشرافي والحصول على البيانات وهو نظام تحكم صناعي لإدارة ومراقبة العمليات الصناعية بشكل حاسوبي من صنع شركة سيمنز الألمانية (Siemens)(خليفة، ٢٠٢١، ١١٢).

عد الهجوم من الهجمات السيبرانية التي كان لها دور على المستوى الدولي، وعرف بكونه برنامج دودي كشفه المحققون الجنائيون وأطلق عليه اسم ستوكسنت، ويرجع سبب تسميته إلى ظهور اسم ملف يحمل اسم ستوكسنت في تكوين البرنامج، وما تفعله هذه الدودة هو التسبب في جعل أجهزة الحاسوب للمنشأة النووية تدخل في دورة غير منتهية من إعادة التشغيل والتي تؤدي إلى تعطيل النظم المعلوماتية للمنشأة بشكل كبير، وتم وصف هذا البرنامج الدودي من المختصين والخبراء في علوم الحاسوب الآلي بكونه من أكبر البرمجيات الخبيثة التي تمت ترقيتها في التاريخ من حيث التعقيد والتطور التكنولوجي فضلاً عن وصفه بكونه (صاروخ سيبراني عسكري)(شاكر، ٢٠٢٢، ٢٥٩).

إذ كانت دودة ستوكسنت تقوم بتسجيل مؤشرات ترتبط بعملية تخصيب اليورانيوم، ومن ثم قامت بالتلاعب بآليه عمل أجهزة الطرد المركزي وتدميرها، واستغلت الدودة بذلك أكثر من عشرين ثغرة صفرية، وكان من بينها أربع ثغرات غير مكتشفة في نظام الويندوز، فضلاً عن ستة عشر ثغرة كانت غير مكتشفة في برنامج التحكم الصناعي نفسه(خليفة، ٢٠٢١، ١١١).

فقد استطاعت الدودة إن تقوم بإعادة برمجة وحدة التحكم المنطقي القابلة للبرمجة، واخفت التغييرات التي قامت بصنعها وتنفيذها، وفي الوقت نفسه قامت بعرض المعلومات السابقة التي قامت بتسجيلها امام شاشات المراقبين والفنيين؛ وذلك ليظهر الامر بان كل شيء على ما يرام ويسير بصورة طبيعية، حتى نجحت دودة ستوكسنت في إنهاء مهمتها التي صنعت من اجلها(خليفة، ٢٠٢١، ١١٢).

المبحث الثالث

الانعكاسات الاستراتيجية والقانونية لهجوم دودة ستوكسنت في الصراع السيبراني الدولي

المطلب الاول: الانعكاسات الاستراتيجية والسياسية لهجوم دودة ستوكسنت

إن الهجوم العنيف الذي مورس ضد منشآت تخصيب اليورانيوم الإيرانية باستخدام دودة ستوكسنت كان له الدور الكبير في إحداث تحولات جذرية في سياسة واستراتيجية الامن المعلوماتي للنظام الإيراني، وطال التأثير الساحة الدولية؛ وذلك لممارسة التهديدات السيبرانية في النطاق الجغرافي بأكمله؛ الذي يغطيه الفضاء السيبراني العالمي، إذ لم يتم إطلاق الدودة دفعة واحدة، بل مرت العملية بسلسلة مراحل متطورة حتى تمت الهجمة، تخللت الدودة إلى باطن وحدات التحكم المشغلة لأجهزة الطرد المركزي لمشروع نتنز النووي الإيراني(الرزو، ٢٠٢٠،٣٤١)

على الرغم من إن الجهة التي صنعت دودة ستوكسنت كانت قد خصصتها بشكل خاص لإصابة أجهزة الطرد المركزية الإيرانية وبالخصوص أجهزة التحكم التي تمت صناعتها من شركة سيمنز الألمانية دون غيرها، ألا إن أحد الباحثين العامل في البرنامج النووي الإيراني أوصل حاسوبه المصاب مباشرة مع شبكة الإنترنت العالمية مما تسبب ذلك الفعل بتسريب الدودة وتغلغلها عبر شبكة المعلومات الدولية (الإنترنت) مما أدى إلى انتقالها لمشاريع أخرى في ايران نفسها، فضلاً عن وصولها إلى بلدان العالم الأخرى منها ألمانيا، الهند، وباكستان واندونيسيا، حتى بلوغها الولايات المتحدة الأمريكية(الرزو، ٢٠٢٠، ٣٤٢).

ولم تتوقف الهجمة عند هذا الحد التي أصابت فيه أكثر من مئة ألف نظام حاسوبي ضمن حدود إيران وحدها، بل أخذت بالتوسع باتجاه توليد المزيد من السلالات التي نسخ فيها المبرمجون الهندسة البرمجية لدودة ستوكسنت، وعظمت

المزيد من الآثار ذات الضرر الأكثر، فضلاً عن توسيع نطاق دائرة التأثير على حقول القطاعات الأخرى المتعددة(الرزو، ٢٠٢٠، ٣٤٣).

لم تربط أي دولة نفسها بشكل رسمي بدودة ستوكسنت لكن أصابع الاتهام والشكوك دارت حول الولايات المتحدة الأمريكية و(إسرائيل) وإن الهجوم ما هو الا ثمرة تعاون بينهما، إذ أغنى هذا الهجوم والاستخدام الناجح له عن القيام بهجوم تقليدي عسكري على منشآت إيران النووية مما قد يسبب بانتقام تصعيدي، وقد يفسر ذلك بأن الولايات المتحدة الأمريكية قادرة على التسلل والوصول إلى منشآت محمية جداً وحساسة وتضم أسلحة دمار شامل(مجموعة مؤلفين، ٢٠١٨، ٦٨).

ما زاد من تأكيد الشكوك حول الولايات المتحدة الامريكية و(إسرائيل) هو حدثين، الاول ، في حفلة تقاعد الفريق الإسرائيلي غابي أشكنازي (الرئيس السابق لجيش الدفاع الإسرائيلي)، عندما بدا أن المحتفلين يدعون أن ستوكسنت هو أحد نجاحاته الرئيسة، فقد كان هناك إعلان تجاري إسرائيلي لشركة تلفزيون الكابل يظهر ما يبدو أنه ثلاثة عملاء موساد متخفيين بزي الحجاب في إيران يفجرون جهاز الطرد المركزي بعد الضغط عن طريق الخطأ على زر على جهاز لوحي من سامسونج، والثاني، في كانون الأول/ديسمبر ٢٠١٠، قال غاري سامور، منسق البيت الأبيض للحد من الأسلحة وأسلحة الدمار الشامل والأمن ومراقبة الأسلحة الاسبق، لمؤسسة الدفاع عن الديمقراطيات في واشنطن: "نحن سعداء لأنهم يواجهون مشكلة في آلة الطرد المركزي الخاصة بهم وأننا (الولايات المتحدة الامريكية وحلفائها)، نفعل كل ما في وسعنا للتأكد من أننا نعقد الأمور بالنسبة لهم"(Deibert.2013,223).

بعد التسريبات الإعلامية الكبيرة والتغطية الواسعة التي نالها هجوم دودة ستوكسنت على أنظمة الحاسوب التي كانت تتحكم في وحدات تخصيب اليورانيوم في إيران ومحاولة تخريبها، وما نسب من مسؤولية إلى الولايات المتحدة الأمريكية

و(إسرائيل)، ساهم هذا الهجوم إلى حد كبير في تعزيز ميزة الردع الإسرائيلي والامريكي على حد سواء، فنسب الهجوم اليهما مثل نقلة نوعية فيما يتعلق بالقدرة الهجومية السيبرانية لهما، فضلاً عن قوتهما ونفوذهما في الفضاء السيبراني(مجموعة مؤلفين، ٢٠١٨، ١٨).

علاوة على ذلك ، إنه بعد التعرض لدودة ستوكسنت ازداد الوعي داخل (إسرائيل) بأهمية حماية أنظمة التحكم الصناعية حتى لا تستغل الفواعل الأخرى هذه الثغرات وتقوم بإنشاء برمجيات خبيثة قادرة على الإضرار بتلك الأنظمة(مجموعة مؤلفين، ٢٠١٨، ٨٤).

تشير التقارير إلى إن الهندسة البرمجية لدودة ستوكسنت تمت المباشرة بإنشائها وتطويرها وتطوير خوارزميتها منذ عام ٢٠٠٥، وذلك باشتراك فريق من وكالة المخابرات المركزية في الولايات المتحدة الأمريكية وفريق تابع للوحدة الخاصة ٨٢٠٠ في (إسرائيل) إذ تم إنشاء مصنع تجريبي (Pilot Plant) مشابه لمنظومة أجهزة الطرد المركزية الإيرانية، وكانت عبارة عن أجهزة طرد مركزي تم صناعتها في باكستان وتم استخدامها في إحدى وحدات ليبيا النووية، وتمت هذه العملية لاختبار مستوى نجاح السلوك الخبيث لدودة ستوكسنت، فضلاً عن محاولة إجراء العديد من التعديلات البرمجية للوصول إلى مستوى مثالي من الإداء حتى يتم تنفيذ المهام التي أوكلت بالهندسة والمنطق البرمجي لدودة ستوكسنت(الرزو، ٢٠٢٠، ٣٤٢).

وفي سياق القدرات ، فإن هجوم دودة ستوكسنت تطلب إمكانيات لا تملكها فواعل من غير الدول، ولو تمت المقارنة بين البديل التقليدي العسكري لمهاجمة المفاعل والبديل السيبراني الذي لجأت إليه الأطراف سنلاحظ حتماً إن الهجوم السيبراني كان أكثر إنجازاً لمصالح كل من الولايات المتحدة الأمريكية و(إسرائيل) ، لاسيما فيما يتعلق في درجته التدميرية، ناهيك عن الميزة الأخرى فيما يتعلق سعر

التكلفة التي تم بها تطوير دودة ستوكسنت والتي قدرت بحوالي عشرة ملايين دولار بينما تقدر التكلفة المالية للضربة العسكرية التقليدية بأضعاف ذلك، فضلاً عن نتائجه المدمرة على صعيد الخسائر البشرية، وصولاً إلى ما يؤديه من رد فعل انتقامي من ايران، فقد قامت دودة ستوكسنت بتنفيذ الهدف نفسه ولكن بتكلفة أقل في تخريب البرنامج النووي الإيراني ودون أحداث خسائر بشرية أو إيقاع حرب واسعة النطاق في منطقة الشرق الأوسط إذ اظهر هجوم دودة ستوكسنت التأثير الإستراتيجي للأسلحة السيبرانية(شاكر، ٢٠٢٢، ٢٤٠-٢٤١).

المطلب الثاني: الإشكاليات القانونية وبناء القدرات السيبرانية في مرحلة ما بعد ستوكسنت

إن وصف دودة ستوكسنت بأنها سلاح سيبراني استخدمت في هجوم سيبراني يرجع سبب ذلك لأنها توفر معظم توصيفات السلاح ، لاسيما النية من استخدامه، ولكن الصعوبة التي تواجهها بوصفها سلاح هو التصنيف القانوني له؛ وذلك لان الأسلحة التقليدية القانونية لا تمتلك خاصية التناسخ الذاتي، ولا تمتلك القدرة على استقلالية الانتشار، فضلاً عن عدم امتلاكها ميزة التشغيل التلقائي التي تمتاز بها دودة ستوكسنت (إبراهيم، ٢٠٢٤، ١٦٤).

ومن الجدير بالذكر، ما ذكره هنري كيسنجر في كتابه (التكوين- Genesis) انه، حتى لو توقفت دولة مهيمنة عن الحرب، فإن الذكاء الاصطناعي فائق الذكاء يمكن أن يقوض ويمنع برنامجاً منافساً، فمثلاً دور الذكاء الاصطناعي بتعزيز الفيروسات التقليدية بقوة غير مسبوقة وتمويهها بدقة مماثلة. مثل دودة الحاسوب ستوكسنت – السلاح السيبراني الذي يقال إنه دمر خمس أجهزة الطرد المركزي لليورانيوم في إيران قبل الكشف عنه – إذ يمكن لوكيل الذكاء الاصطناعي أن

يخرب تقدم المنافس بطرق تحجب وجوده، وبالتالي يقود علماء العدو إلى مسارات التحقيق غير المجدية (Kissinger,Mundie,Schmidt.2024,122).

لقد كان لهذا الهجوم انعكاسات واضحة على اعادة بناء البنية السيبرانية الايرانية، فبعد أن مرت خمسة أشهر على الهجمة المدمرة لدودة ستوكسنت على المنشآت النووية الإيرانية، قامت كل من مؤسسة الحرس الثوري الإيراني* ومنظمة الباسيج* بتدريب الف وخمسمائة مقاتل سيبراني Cyber Warrior وارتفع الطلب على قراصنة المعلومات والمختصين بممارسة اختراق المواقع والتشجيع على التوجه للالتحاق بنوادي للقرصنة السيبرانية، مما دفع الكثيرين لمحاولة تنمية القدرات على الاختراق واكتشاف ثغرات أمنية في الشبكات أسند ذلك توفر الدعم الحكومي مع إعطاء إمكانية نيل فرصة عمل لدى أكثر من مؤسسة حكومية داخل ايران، وفي عام ٢٠١٣ توجهت الحكومة الإيرانية إلى رفع حجم التخصيصات الاستثمارية وزيادتها لتطوير أمن الفضاء السيبراني بالقدر الذي يتناسب مع ارتفاع حجم التهديدات فازدادت بذلك نسبة التخصيصات بنسبة ١٢٠٠% خلال السنوات المالية الثلاثة اللاحقة ٢٠١٤ – ٢٠١٥ – ٢٠١٦ (الرزو، ٢٠٢٠، ٢٤٤).

* الحرس الثوري الإيراني، أحد اهم مؤسسات الجمهورية الإسلامية الإيرانية، يعرف باللغة الفارسية باسم "سباه باسدران إنقلابي إسلامي"، اي "فيلق الحرس الثوري الإسلامي"، تأسس بأمر من مرشد الثورة الإيرانية (روح الله الخميني)؛ وذلك لحراسة الثورة، وللحرس الثوري نفوذ سياسي واسع وحضور في قطاعات عديدة في إيران، منها الأمنية، والاستخباراتية، وفضلاً عن القطاعات الصناعية والاقتصادية، ناهيك عن القطاعات الثقافية والاجتماعية. للمزيد يرجى الاطلاع على: موقع الجزيرة، "الحرس الثوري.. حارس ثورة إيران المتوغل في مفاصل الدولة"، "، تمت الزيارة بتاريخ ٢٠٢٥/١/١٤، ٥:٥٥ مساءاً، متاح على : https://www.aljazeera.net/encyclopedia/2014/11/6/الحرس-الثوري-الإيراني.

* "الباسيج" هي منظمة عقائدية مسلحة إيرانية، تضم بين اعضاء من ملايين المتطوعين ومولة بشكل مباشر من الدولة، وتعد من الكيانات الأكثر تأثيراً في الحياة الامنية والسياسية والمجتمعية في ايران، فضلاً عن انها أداة عسكرية لحماية مصالح النظام السياسي داخلياً وخارجياً، وتأسست (قوات التعبئة الشعبية شبه العسكرية) المعروفة بـ"الباسيج" أي (المتطوعون) نهاية عام ١٩٧٩ على إثر نجاح الثورة الإسلامية في ايران. للمزيد يرجى الاطلاع على:موقع الجزيرة، "الباسيج.. درع تحمي نظام الثورة الإيرانية"، تمت الزيارة بتاريخ ٢٠٢٥/١/١٤، ٥:٥٥ مساءاً، متاح على: https://www.aljazeera.net/encyclopedia/2016/6/26/الباسيج-الدرع-الحصينة-لنظام-الثورة .

ووفقاً لبعض اراء محللي الاستخبارات الأمريكيين، أعادت دودة ستوكسنت البرنامج النووي الإيراني للوراء لمدة عام أو عامين او أكثر، مما أعطى إدارة الرئيس الأمريكي الأسبق باراك أوباما وقتاً كافياً لجلب إيران إلى طاولة المساومة، وبلغت ذروتها في اتمام الاتفاق النووي عام ٢٠١٥ (Greenberg.2019,118).

وفي الوقت نفسه، ان القدرة على اتخاذ قرارات سريعة في وقت قصير ضرورية لمنع حدوث الأزمات (Mutlak,Lahmood.2024,1964) ، تنبه القادة السياسيون والدبلوماسيون في جميع أنحاء العالم بإنشاء قاعدة جديدة في الفضاء السيبراني؛ بسبب دودة ستوكسنت، ليس فقط في تقدمها التقني، ولكن في الجغرافيا السياسية ايضاً، إذ تمكنت الولايات المتحدة الامريكية من استخدام شكل من أشكال الأسلحة التي لم يكن لدى أي بلد منها من قبل، فأصبح التدمير المادي باستخدام الفضاء السيبراني قاعدة جديدة ومقبولة للعبة العالمية(Greenberg.2019,119).

وان التعاون الدولي قد يثري ويعزز الى حد بعيد الامن في الفضاء السيبراني، تبعاً ذكره تقرير اللجنة الدولية للتدخل والسيادة الدول إذ أكد التقرير على دور الفواعل الدولية دون غيرها بإشارته الى "إن النظام الدولي المتماسك والسلمي من المرجح أن يتحقق من خلال تعاون الدول المؤثرة الواثقة من مكانها في العالم وليس في بيئة من الكيانات الحكومية الهشة أو المنهارة او المجزئة والفوضوية بشكل عام"(Ali,Qati,Alwan.2021,13)

الخاتمة:

بما إن القوة هي القدرة على التأثير فإن التحولات التكنولوجية الكبرى أدت إلى ظهور نوع جديد من أنواع القدرة على ممارسة التأثير باستخدام الفضاء السيبراني وهي القوة السيبرانية التي أصبحت أداة فعالة في الصراعات الدولية توظفها الدول خدمة لمصالحها العليا وتحقيقا لها، كما إن هجوم ستوكسنت على

المنشآت النووية الإيرانية مكنة الجهات الفاعلة في تنفيذه بإلحاق أضرار ملموسة بالبنى التحتية الحيوية النووية لإيران وتأخير البرنامج النووي الإيراني وصولاً إلى الدخول في الاتفاق النووي عام ٢٠١٥م، وكل ذلك تم بدون اللجوء إلى استخدام القوة العسكرية التقليدية بشكل مباشر، من ما يوضح تصاعد أهمية الفضاء السيبراني في الاستراتيجيات الأمنية للدول و ضرورة تطوير سياسات دفاعية فاعلة لمواجهة التهديدات والأخطار المتزايدة في الفضاء السيبراني، وفي ختام الدراسة تم التوصل إلى **الاستنتاجات** الآتية:

١. أصبحت القوة السيبرانية أداة فعالة توظف في الصراعات الدولية عبر تنفيذ عمليات هجومية فعالة عن بعد.
٢. يعد هجوم ستوكسنت أول هجوم باستخدام سلاح السيبراني استهدفه بشكل مباشر البنية التحتية الحيوية الحرجة لدولة سيادية.
٣. تزايد أهمية الأمن في الفضاء السيبراني للدول إذ أصبح ضرورة ملحة لحماية المنشآت الحيوية عبر تطوير الدفاعات السيبرانية الفعالة.
٤. ينطوي الفضاء السيبراني على مستوى عالي من الغموض فضلاً عن عدم القدرة على إسناد الهجمات السيبرانية مما يعقد آليات الردع والمسؤولية القانونية على الجهات الفاعلة في القانون الدولي.

وعلى وفق ما خرجت به هذه الدراسة، يمكن تقديم مجموعة من **المقترحات** إلى الجهات المعنية الاتية:

١. **صانعو القرار العراقي:** ضرورة تعزيز التشريعات والقوانين المتعلقة بالفضاء السيبراني لضمان حماية البنية التحتية الرقمية الحيوية للمعلومات، وإدخال ودمج مفاهيم الأمن السيبراني في السياسات الدفاعية والأمنية للدولة بما يتناسب مع التحديات الرقمية المتزايدة في الفضاء السيبراني.

٢. **وزارة الداخلية العراقية/مركز الأمن السيبراني:** ضرورة تطوير برامج تدريبية متخصصة لمنتسبي وزارة الداخلية حول طرق وأساليب الكشف عن الهجمات السيبرانية فضلاً عن تقنيات الاستجابة لها، فضلاً عن تطوير وتعزيز تقنيات الامن السيبراني للبنية التحتية للمعلومات داخل المؤسسات الأمنية لضمان حماية المعلومات والبيانات السرية والحساسة.

٣. **جهاز الأمن الوطني العراقي:** إنشاء وحدات متخصصة في الأمن في الفضاء السيبراني من ضمنها جهاز الأمن الوطني العراقي لضرورة مراقبة وتحليل التهديدات السيبرانية التي تستهدف الأمن القومي العراقي، فضلاً عن تطوير قدرات الرصد والاستخبارات السيبرانية ليه تفعيل الدفاع السيبراني والكشف المبكر عن الهجمات الرقمية وإمكانية التعامل معها بفاعلية.

٤. **فريق الاستجابة للحوادث السيبرانية العراقي CERT:** تحسين آليات الاستجابة الفورية للحوادث والهجمات السيبرانية عبر تحديث بروتوكولات التعامل مع الهجمات وتطوير أنظمة التحذير المبكر> وإطلاق منصة وطنية للإبلاغ عن التهديدات السيبرانية وتبادل المعلومات مع مختلف الجهات المعنية.

٥. **مستشارية الأمن القومي العراقي:** إنشاء مراكز أبحاث مختصة لدراسة تطوير القدرات السيبرانية في الفضاء السيبراني فضلا عن التطورات الحاصلة فيه وتقديم توصيات استراتيجية مستمرة لصناع القرار، وتوجيه الاستثمارات نحو تطوير تكنولوجيا محلية في مجال الأمن السيبراني للحد من الاعتماد على الحلول الخارجية الأجنبية.

المصادر:

اولاً: المصادر باللغة العربية:

١. إبراهيم، أحمد محمود أبو الحسن. ٢٠٢٤. التهديدات السيبرانية وأثرها على حماية البنى التحتية والخدمات الحيوية. كفر الشيخ: دار العلم والإيمان للنشر والتوزيع.
٢. اسراء شريف الكعود واحمد كامل الخفاجي. ٢٠٢١. "تطبيق القوة الذكية في صراع القوى الإقليمية في الشرق الأوسط بعد ٢٠١١"، مجلة العلوم السياسية، العدد ٦٢: ٢٧-٥٤.
٣. إسراء شريف جيجان. ٢٠٢١. "الأمن السيبراني الصيني: دراسة في الدوافع والتحديات." مجلة قضايا سياسية، مجلة صادرة عن كلية العلوم السياسية بجامعة النهرين، العدد ٦٥.
٤. حيدر زاير العامري. ٢٠١٩. العلاقات الدولية ما بين توازن القوى وتوازن التهديد (إطار نظري) مجلة العلوم السياسية، العدد ٥٣: ٢٨٥-٢٩٨.
٥. خالد حنفي علي. ٢٠١٧. "إشكاليات تداخل الصراعات السيبرانية والتقليدية." في الصراع السيبراني: التنازع العالمي على قوة الفضاء الإلكتروني. مجلة السياسة الدولية، المجلد ٥٢، العدد ٢٠٨.
٦. خلف، حسين مزهر. ٢٠١٥. "الاستراتيجية الأمريكية في إدارة الصراع: بين القوة الصلبة والقوة الناعمة." مجلة العلوم السياسية، العدد ٤٩: ٢٠٥-٢٣١.
٧. خليفة، إيهاب. ٢٠٢١. الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس. أبو ظبي: المستقبل للأبحاث والدراسات المتقدمة.
٨. خليفة، إيهاب. ٢٠١٧. القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت. القاهرة: العربي للنشر والتوزيع.
٩. الرزو، حسن مظفر. ٢٠٢٠. التهديد السيبراني الإيراني: الملف المضاف إلى برنامجها النووي ودوره المحتمل في تأجيج صراع من نمط جديد. برلين: المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية.
١٠. شاكر، فراس جمال. ٢٠٢٢. السيبرانية وتحولات القوة في النظام الدولي. عمان: دار أمجد للنشر والتوزيع.
١١. عبد الوهاب منصور، شادي. ٢٠١٩. حروب الجيل الخامس: أساليب التفجير من الداخل على الساحة الدولية. القاهرة: العربي للنشر والتوزيع.

١٢. عمار حميد ياسين وزهراء جاسم كاظم. ٢٠٢٣. " مستقبل الحرب الروسية–الأوكرانية ومدى انعكاساتها على امن دول شرق اوربا بعد ٢٠٢٢"، مجلة العلوم السياسية، العدد ٦٦: ٢٤٥–٢٧٣.

١٣. فاتن محمد رزاق. ٢٠١٩. مقومات التسامح العالمي وتأثيرها على السلام، مجلة العلوم السياسية، العدد ٥٢: ٣٠١–٣٣٤، ص ٣٠١.

١٤. مجموعة مؤلفين. ٢٠١٨. السلاح السيبراني في حروب إسرائيل المستقبلية. إعداد رندة حيدر. بيروت: مؤسسة الدراسات الفلسطينية.

١٥. مهدي، لبنى خميس، وتغريد صفاء. ٢٠٢٠. "أثر السيبرانية في تطور القوة." مجلة حمورابي، العدد ٣٣–٣٤، السنة ٨.

١٦. موقع الجزيرة. ٢٠١٦. "الباسيج.. درع تحمي نظام الثورة الإيرانية". https://www.aljazeera.net/encyclopedia/2016/6/26/الباسيج-الدرع-الحصينة-لنظام-الثورة.

١٧. موقع الجزيرة. ٢٠١٤. "الحرس الثوري.. حارس ثورة إيران المتوغل في مفاصل الدولة". https://www.aljazeera.net/encyclopedia/2014/11/6/الحرس-الثوري-الإيراني.

ثانياً: المصادر باللغة الإنكليزية:

1. Ali, Inass A., Sana K. Qati, and Batool H. Alwan. 2021. "Iraqi Women's Leadership and State-Building." *Journal of International Women's Studies* 22, no. 3: 13-27.
2. Alwan, Saad Obaid, and Tamara Kadim Manati. 2024. "Transformations of the World Order after the Corona Pandemic COVID-19: The Role of Culture, Science, and the Environment." *Journal of International Crisis and Risk Communication Research* 7, no. S10: 1810-1824.
3. BasuMallick, Chiradeep. 2023. "What Is USB (Universal Serial Bus)? Meaning, Types, and Importance." Spiceworks, January 10, 2023 https://www.spiceworks.com/tech/tech-general/articles/universal-serial-bus/.
4. Bhumika.2022. "What is Windows Operating System?" GoSeeko, April 9, 2022. https://www.goseeko.com/blog/what-is-windows-operating-system/.

5. Deibert, Ronald J. 2013. Black Code: Surveillance, Privacy, and the Dark Side of the Internet. Toronto: McClelland & Stewart.
6. Greenberg, Andy. 2019. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Doubleday.
7. Jasem, Faieq Hassen, and Inass Abdulsada Ali. 2024. "Sub-National Governments' Interactions in International Affairs: An Arab Perspective on Paradiplomacy." IASR International Area Studies Review 27, no. 4: 434–447.
8. Kissinger, Henry A., Craig Mundie, and Eric Schmidt. 2024. Genesis. New York: Little, Brown and Company, Hachette Book Group.
9. Kramer, Franklin D., Stuart H. Starr, and Larry Wentz. 2009. Cyberpower and National Security. Washington, DC: National Defense University Press.
10. Kushner, David. 2013. "The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program." IEEE Spectrum, February 26, 2013. https://spectrum.ieee.org/the-real-story-of-stuxnet.
11. Lin, Herbert. 2012. "Cyber Conflict and International Humanitarian Law." International Review of the Red Cross 94, no. 886.
12. Mutlak, Donia Jawad, and Flras Ammar Lahmood. 2024. "Early Warning System Means and Tools in the African Union and the Organization of American States: An Analytical Study." Journal of Ecohumanism 3, no. 4: 1964–1971.
13. Nye, Joseph S. Jr. 2010. Cyber Power: In the Future of Power in the 21st Century. Cambridge: Belfer Center for Science and International Affairs and Harvard Kennedy School.
14. Singer, P. W., and Allan Friedman. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press.
15. Zetter, Kim. 2014. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown Publishing.