الأمن السيبراني ودوره في رفع مستوى الأمن العام للدولة
"المملكة العربية السعودية أنموذجاً"

دراسة في الجغرافيا السياسية

Cyber security and its role in raising the level of public security of the state
The Kingdom of Saudi Arabia as a Model
Studies in political geography

بحث مشترك

إعداد
دكتورة. سمية مشرف عبد الله العمري
أستاذ الجغرافيا السياسية المساعد
قسم الجغرافيا والإستدامة البيئية-كلية العلوم الإنسانية والإجتماعية
جامعة الأميرة نورة بنت عبد الرحمن
Email: Smalamry@pnu.edu.sa

أستاذة. أفنان عبدالله عثمان التركي

محاضر نظم المعلومات الجغرافية

قسم الجغرافيا والإستدامة البيئية-كلية العلوم الإنسانية والإجتماعية
جامعة الأميرة نورة بنت عبد الرحمن
Email: afaalturki@pnu.edu.sa

إصدار يناير لسنة ٢٠٢٤م

شعبة البحوث الجغرافية

الملخص

اهتم البحث بقضية الهجمات الإلكترونية كنوع من الحروب الجديدة على صعيد النزاعات الدولية، وذلك بهدف الكشف عن مخاطرها وأبعادها المستقبلية، وكيفية تصدي المملكة العربية السعودية لها. وقد اعتمدت الدراسة على بيانات المركز الوطني للأمن السيبراني، فضلاً عن بعض دراسات جامعة الأمير نايف للعلوم الأمنية، بإستخدام المنهج الوصفي التحليلي. وخلصت الدراسة إلى أنه توجد علاقة بين الأمن الوطني للمملكة والأمن السيبراني في ظل تعرض المصالح الإستراتيجية للمملكة لأخطار وتهديدات سيبرانية متواصلة، كما أظهرت الدراسة بعض الهجمات التي تعرضت لها المملكة، وشن حرباً الكترونية عليها مثل إرسال شمعون ٢ الذي عمل على تعطيل ٣٠ ألف جهاز في شركة أرامكو السعودية القطاع الرئيس للنفط في المملكة، وهجماتها على المنشآت النفطية "خريص وبقيق" التابعتين لشركة أرامكو السعودية، ، وتوصلت أيضا إلى أن هناك قضايا شائكة ذات ارتباط وثيق الصلة بالهجمات الإلكترونية كالتهريب والتسول والإرهاب والإتجار بالبشر. كما أبرزت الدراسة دور نظم المعلومات الجغرافيةGIS في تحليل الأنظمة التي يحتمل أن تكون معرضة للخطر، واكتشاف قيمة الخاصية المكانية والجغرافية في تحليل وحل المشكلات المتعددة في الأمن السيبراني.

وأوصت الدراسة بأهمية دعم المصالح الوطنية من خلال بناء القدرات، ونقل وتوطين التقنيات التي يمكن استخدامها بشكل آمن لحماية البيانات، وتحقيق أمن المعلومات، والتعرف على أساسيات القوانين المتعلقة بالجرائم الإلكترونية ضمن إطار قانوني يوضح العقوبات والتهديدات التي تتعرض لها المملكة.

الكلمات الدالة: الأمن السيبراني، الحرب السيبرانية، الجغرافيا السياسية

Abstract

The research focused on the issue of cyber-attacks as a kind of new war in the field of international conflicts, to reveal its dangers and future dimensions, and how the Kingdom can address them. The study relied on the data of the National Cyber Security Center and some studies of Prince Nayef University for Security Sciences, using a descriptive-analytical approach. The study concluded that there is a relationship between the Kingdom's national security and cybersecurity, in light of the Kingdom's strategic interests being exposed to continuous cyber dangers and threats. The study also showed some of the attacks the Kingdom was subjected to, and the cyber war launched against it, such as sending Shamoon 2, which disabled 30,000 devices in Saudi Aramco, the main oil sector in the Kingdom, and attacks on oil facilities, the Khurais and Abqaiq facilities of Saudi Aramco. The study also concluded that there are thorny issues closely related to cyberattacks, such as smuggling, begging, terrorism, and human trafficking. The study also highlighted the role of GIS in analyzing systems that are potentially at risk and discovering the value of spatial and geographic property in analyzing and solving multiple problems in cybersecurity .

The study recommended the importance of supporting national interests through capacity building, transfer, and localization of technologies that can be used securely to protect data, achieve information security, and identify the basics of laws related to cybercrimes within a legal framework that clarifies the penalties and threats to the Kingdom is exposed to.

Keywords: Cyber security, cyber war, political geography.

أولاً: المقدمة:

تعتبر الحروب الإلكترونية أو الحرب السيبرانية مفهوماً جديداً على صعيد النزاعات الدولية في القرن الحادي والعشرين، التي تهتم بها الجغرافيا السياسية للدولة، إذ يعد الفضاء الالكتروني، وتعقيداته التكنولوجية من أهم وسائل الصراعات المستقبلية. وظهر مؤخراً بشكل متزايد مقابل مصطلح الحرب السيبرانية مصطلح آخر مضاد له وهو الأمن السيبراني، ولاقى اهتماماً من الدول المتقدمة نتيجة ازدياد الجرائم والهجمات الالكترونية العابرة للحدود. إن تنوع وضخامة حجم وسائل الاتصالات والتطبيقات الذكية سهل زيادة تبادل المعلومات حول العالم، مما أدى إلى زيادة العبء المالي على الدول من أجل تحقيق الأمن بمفهومه الشامل، لأن أمن المعلومات بشكل خاص سرعة تناميه في إزدياد لذلك قامت المملكة العربية السعودية بتأسيس صناعة وطنية تهتم بمجال الأمن السيبراني، لتحقق ريادة عالية استنادًا على ما تضمنته رؤية ٢٠٣٠ وإنطلاقًا من مبدأ سيادة الدولة على إقليمها وحفظ الأمن العام للوطن، وتسهم نظم المعلومات الجغرافية في الحماية من تلك الهجمات من خلال الخدمات المتعددة التي تقدمها من خلال تحديد المواقع الجغرافية التي تنطلق منها الهجمات الالكترونية، كما يمكن لنظم المعلومات الجغرافية تصور وتمثيل الموقف لاستيعاب الخطر بالتالي اتخاذ أفضل القرارات في مواجهة الهجمات.

ثانياً: مشكلة البحث:

استفادت الجريمة المنظمة بكافة أنواعها من الفضاء السيبراني وتقنية الاتصالات والمعلومات، وأدى تحول المجتمع إلى الفضاء السيبراني، تحديات خطيرة، نتج عنه الجريمة المنظمة، والإرهاب، والتجسس الصناعي، والتهريب، ومن ثم عرضت استقرار الدول، وعلاقاتها، وأمنها للخطر، كما يمكن أن يقوم بأنشطة الجرائم السيبرانية والمعلوماتية مجموعات صغيرة أو أفراد ذات مهارة تقنية حتى لو كانت محدودة ، أو من قبل الجماعات العالمية عالية التنظيم الإجرامي، وقد تسببت هذه الأنشطة الكثير من الخسائر سواء خسائر سرقة معلومات حساسة أو مالية، وقد وصل أثر هذا النوع من الأنشطة إلى التأثير مباشرة على الأمن القومي للدولة.

وتتعرض المملكة العربية السعودية لمحاولات مستمرة للهجوم على أمنها السيبراني؛ إذ احتلت المرتبة ٤٢ من بين الدول الأكثر تعرضاً للمخاطر في هذا الشأن، إضافة إلى أن التوترات الإقليمية في المنطقة تفرض على حكومة المملكة اتخاذ كافة الإجراءات التي تضمن بقاء الفضاء الالكتروني للمملكة آمناً (الشمري، ٢٠١٥).

ثالثاً: أهمية البحث:

تأتي أهمية البحث الحالي من أهمية الأمن السيبراني في نطاق العلوم الإنسانية والاجتماعية، وكذلك انطلاقه من تخصص مختلف عن تخصص علوم الحاسب الآلي، وهو تخصص الجغرافيا السياسية، لما للتخصص من اهتمام واسع بالأمن الداخلي والخارجي للدولة، والعوامل الجغرافية التي أدت إلى ذلك بشقيها الطبيعي والبشري، فبناء جهاز وقطاع قوي لصد الهجمات الالكترونية أصبح طلبًا ملحًا وضروريًا لتصدي الهجمات بإختلاف أهدافها السياسية والأمنية والاقتصادية.

رابعاً: أهداف البحث:

١. عرض أهداف الأمن السيبراني في المملكة العربية السعودية.
٢. توضيح العلاقة بين الأمن السيبراني وأمن الدولة عامة.
٣. التعرف على أشكال التهديدات السيبرانية التي تعرضت لها المملكة العربية السعودية.
٤. عرض التدابير الأمنية لرفع مستوى الأمن السيبراني في المملكة العربية السعودية.
٥. توضيح أهمية دمج أنظمة المعلومات الجغرافية الحديثة مع الأمن السيبراني.

خامساً: تساؤلات الدراسة:

١. ما أهداف الأمن السيبراني في المملكة العربية السعودية؟
٢. ما أبعاد العلاقة بين الأمن السيبراني وأمن الدولة عامة؟
٣. ما أشكال التهديدات السيبرانية التي تعرضت لها المملكة العربية السعودية؟
٤. ما التدابير الأمنية لرفع مستوى الأمن السيبراني في المملكة العربية السعودية؟
٥. ما هي كيفية دمج أنظمة المعلومات الجغرافية الحديثة مع الأمن السيبراني؟

سادساً: الإطار النظري:

١. مفهوم الأمن الشامل:

يعرف الأمن الشامل بقدرة الدولة على تأمين أدنى مستوى من الأمن تجاه كل ما من شأنه يقوم بتهديد سلامة المجتمع وأمنه، فكل دولة حريصة على تحقيق الأمن تجدها تسعى ضمن هذا الإطار إلى المحافظة على سير الحياة العلمية والإجتماعية والسياسية والإقتصادية والمعلوماتية والتقنية، لكافة مرافق الدولة ومنشأتها، ولقد دعت الحاجة إلى ظهور هذا المفهوم لأن العالم مر أثناء العقدين الأخيرين بالعديد من الكوارث والقضايا والتهديدات والأسلحة المدمرة، إضافة إلى ما يواجهه العالم اليوم بعد أزمة جائحة كورونا، مما نتج عنها أزمات اقتصادية ومالية وفقد العديد من المواطنين وظائفهم في عدة دول.

وهذا يفسر لنا الإهتمام بالأمن الشامل الحديث بدلًا عن الأمن التقليدي الذي يركز فقط على المخاطر دون التعمق في وضع الحلول والاستراتيجيات وكيفية معالجتها (عبدالصادق، ٢٠١٦).

ولعل أهم ما يؤرق المتخصصين في تقنية المعلومات هو أمن هذه الشبكات المهمة نظرًا لاحتوائها على قاعدة معلومات وبيانات ضخمة، يعتمد عليها اعتماداً كلياً في سير العمل والإنتاج، مما يعني أن توقفها عن العمل يسبب أزمة، ومثال للإعتماد العالي على تقنيات المعلومات يمكن أخذ الحكومة الالكترونية التي تقدم خدمات للمواطنين والمقيمين والمنظمات والهيئات الداخلية والخارجية، (القحطاني، ٢٠١٥). وفي كل مجالات الحياة الاجتماعية برزت أهمية المنظومة الأمنية الشاملة، والهدف منها هو تأهيلهم لمواجهة ظروف عيشهم وكرامتهم والحصول على حقوقهم الأساسية لذا من أهم عناصر الأمن القومي للدول هو الأمن السيبراني ووضع إستراتيجيته ورؤيته للمستقبل (عبدالصادق، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، ٢٠١٧).

٢. العلاقة بين التطور التكنولوجي والأمن:

دعى الإستخدام غير السلمي للفضاء الالكتروني إلى تنامي العلاقة بين الأمن الوطني للدول والتكنلوجيا حيث أنه يؤثر في رخاء الدولة واستتباب أمنها الداخلي والخارجي، ومما لا شك فيه أن الواقع الحالي يثبت إرتباط الأمن السيبراني بجميع مناحي الحياة خاصة في مجال الأعمال وقطاع التجارة والإقتصاد والسياسة، أي أن هناك ارتباط وثيق الصلة بين أمن هذه المصادر وبين كافة البيانات والمعلومات التي تندرج ضمنها والتي تعد جزء من منظومة الأمن السيبراني، والتي يترتب على استقرارها القدرة على الإنتاج وسير العمليات اليومية بمسارها السليم.

تُستخدم التكنولوجيا في جميع أنواع الجريمة المنظمة ، يستغل المجرمون أدوات الذكاء الاصطناعي لإرتكاب الجرائم، فهي مصادر للتهديدات الإجرامية

والأمنية الجديدة، ولا شك أن تطور التكنولوجيا ساهم بشكل أو آخر في تعزيز وتطوير الذكاء الاصطناعي، من خلال إنشاء جرائم جديدة لم تكن معروفة من قبل أهمها الجرائم الإلكترونية التي يمكن أن تكون لها عواقب كارثية، بما في ذلك سرقة البنوك من خلال الإختراق الإلكتروني لحسابات العملاء، وسرقة المعلومات، وتدمير الأنظمة الإلكترونية التي تدير المرافق الحيوية مثل محطات المياه ومحطات الطاقة، الدفاع، بالإضافة إلى الهجمات ضد أجهزة الكمبيوتر الشخصية، والشركات، والبشر، وغسيل الأموال عبر الإنترنت، وما إلى ذلك.

ويتضح مما سبق أن التطور التكنلوجي والذكاء الإصطناعي سلاح ذو حدين فهي ساعدت كثيرًا على سرعة كشف الجرائم ومحاصرتها ومنعها، ومن جانب آخر خدمة الجريمة من خلال سهولة التخطيط للجرائم عن بعد من عدة دول مختلفة وسهولة تطبيقها. (السويدي، ٢٠١٨).

ومن جهة أخرى تساعد التقنيات الحديثة على منع الكثير من الجرائم قبل وقوعها والكشف عن المجرمين والجرائم والمواد المحظورة، وقد أدت التكنولوجيا إلى الحد من بعض الجرائم؛ على سبيل المثال جرائم سرقة السيارات تراجعت إلى أقل حد بل اختفت من بعض الدول، بفضل التكنولوجيا الحديثة الموجودة في السيارات، وساهم التطور التكنولوجي إضافة إلى ذلك في سرعة الإستجابة للكوارث الطبيعية والأمنية وهذه أمثلة بسيطة عن الجانب السلمي والإيجابي عن التطور التكنلوجي لأن القائمة تطول .

إن الأضرار الناجمة عن جرائم الإنترنت ستكلف العالم ١٠,٥ تريليونات دولار سنويًا بحلول عام ٢٠٢٥ - أي أكثر بكثير من الأضرار التي لحقت بالكوارث الطبيعية خلال عام، وأكثر ربح من التجارة العالمية لجميع أنواع المخدرات. وقد كشفت دراسة أجرتها شركة Frost & Sullivan بتكليف من مايكروسوفت أن الخسارة الاقتصادية في العالم بسبب حوادث الأمن السيبراني قد وصلت إلى ٨ تريليون دولار في السنه (Morgan, 2019).

ونلخص العلاقة بين التطور التكنولوجي والأمن فيما يلي:

أ. خلق جرائم ومصادر تهديد أمنية جديدة.
ب. زيادة خطورة التهديدات والجرائم التقليدية.
ت. زيادة معدلات البطالة.
ث. المساعدة في سرعة الكشف عن التهديدات والسيطرة عليها.

٣. نظريات الأمن الشامل:

لا توجد نظريات متخصصة في أمن المعلومات نظراً لكونه فرع من منظومة الأمن الشامل، يوجد مدرستان تناولت موضوع الأمن الوطني الشامل بطريقة مختلفة لكل مدرسة وهما:

أ- **المدرسة الإستراتيجية:** تهتم بكيان الدولة ونسيجها الاجتماعي الداخلي وعلاقتها الدولية وكل ما من شأنه يهدد وحدة الدولة الداخلية، تهتم كذلك بمفهوم القوة من خلال أي معيار يمكنها فيه إثبات قوتها. (الشهري،٢٠٢٠)

ب – المدرسة المعاصرة (التنموية): يرى أصحاب هذه المدرسة أن التهديدات الداخلية لا تقل شأن عن التهديدات الخارجية، وأن مجال الأمن القومي يشمل على أبعادًا ثقافية واجتماعية واقتصادية وسياسية، وتهتم بإتجاهين رئيسة هما التنمية الاقتصادية وأمن الموارد الاستراتيجية الحيوية، وفي هذا الشأن نجد الدولة تستطيع مواجهة جميع التحديات والتهديدات إذا كانت مؤمنة ضد الأخطار الداخلية والخارجية ولديها جهاز أمني قوي وتعير منظومة الأمن الشامل اهتمامًا واسعًا. (شيبي، ٢٠٠٩).

سابعاً: الدراسات السابقة:

تطرقت دراسة (العلوان،٢٠٢٣) إلى أدوار وتحديات الأمن السيبراني المعتمد على الذكاء الإصطناعي من خلال أربعة مراحل تمر بها، ولتحقيق أهداف الدراسة استخدم منهج دراسة الحالة متدرجًا من منظومة أمن المعلومات وصولًا إلى منظومة الأمن السيبراني والذكاء الإصطناعي، وتوصلت دراسته إلى أن هناك علاقات معقدة ومترابطة بين كل مرحلة وأخرى تواجهها تحديات متجددة وسريعة تتطلب بناء مؤهلات بشرية على اطلاع دائم ومستمر لمستجدات الفضاء الإلكتروني بكافة فروعه وتخصصاته الدقيقة.

هدفت دراسة (الشهري،٢٠١٩) إلى التعرف بطبيعة وأسباب الجرائم الإلكترونية، وتطرق إلى جميع المخاطر التي من الممكن أن تعترض الأمن السيبراني في المملكة، وهدفت الدراسة إلى رسم استراتيجية هدفها العمل على الحد من الجرائم الإلكترونية، ورفع مستوى الأمن السيبراني، وتوصلت الدراسة إلى أنه لا يوجد حدود مكانية ولا زمانية للجرائم الإلكترونية وأن التقنيات الحديثة وتوفر الأنترنت هيأت فرص أوسع للجرائم، وأكدت الدراسة على أن أهم تهديد يواجه الفضاء السيبراني في المملكة العربية السعودية هو انتهاك السياسات الأمنية الخاصة بأهمية إنفاذ التشريعات والأنظمة في مواجهة الجريمة الإلكترونية.

تناولت دراسة (المقصودي، ٢٠١٧) صفات الجريمة المعلوماتية التي تميزها عن غيرها، وضح في دراسته أن هناك اختلاف بين الجرائم الإلكترونية والجرائم التقليدية، منها اشتمالها على جوانب فنية وتقنية، كما أن التسجيلات الإلكترونية هي غالبية موضوعات الجريمة الالكترونية والتي تتم من خلال

شبكات الفضاء والإتصال السيبراني، وقد توصلت الدراسة أنه ليس هناك قانون دولي يحرم ويجرم هذه الأفعال، كما بينت الدراسة ضرورة التعاون بين الدول للحد من انتشارها، وأوضح أن هذه الجرائم تمتاز بأنها عابرة للحدود وعادة ما يكون التخطيط في بلد والفاعلون في بلد آخر والمتضررون في بلد مستهدف، مما يؤكد صعوبة الملاحقة القضائية.

وهدفت دراسة (الشمري، ٢٠١٥) إلى بيان مفهوم الفضاء الإلكتروني، وحدوده وخصائصه وتعريف الفجوة الإلكترونية، واستعراض واقع وحماية الفضاء الإلكتروني في المملكة العربية السعودية، وبيان مخاطر الفضاء الإلكتروني، ومدى وعي المسؤولين عن أمن المعلومات واستجلاء كل ما من شأنه أن يحد من مواجهة أخطار الفضاء الالكتروني.

١. أهداف الأمن السيبراني في المملكة العربية السعودية:

هدفت رؤية المملكة (٢٠٣٠) لتطوير البنية التحتية الرقمية؛ وحددت المملكة أهدافها المتعلقة بأمنها السيبراني **في الآتي:**

أ. تطوير صناعة المعرفة التقنية الحديثة.
ب. إعداد وتهيئة قدرات شباب الوطن في تخصص الأمن السيبراني.
ت. التوسع في الشراكات ما بين القطاعين العام والخاص كوسيلة لتطوير قطاع الإتصالات وتقنية المعلومات.
ث. تعزيز قوة حماية الشبكات والتحقق من فاعلية أنظمة تقنية المعلومات.
ج. تشجيع الإستثمار والإبتكار في كل ما يخص مجال الأمن السيبراني.
ح. الكشف المبكر عن الهجمات في وقتها وحماية الأنظمة من الإختراق.
خ. وضع الخطط الإستراتيجية لإنشاء بيئة سحابية آمنة ولحماية الفضاء الإلكتروني في المملكة.
د. سن الأنظمة والقوانين التشريعية التي تنظم استخدام التكنلوجيا والتقنية.

إن قوة الجهاز الإلكتروني والتقني في المملكة العربية السعودية من حيث تطوره وقوة أنظمته ساهم في تعظيم النفوذ والمنفعة الدفاعية والأمنية والعسكرية والاقتصادية ، بدليل أنه أصبح لها مؤشر عالمي يقاس من خلالها مدى تقدم الدولة أو تأخرها في التقدم التقني، لذلك حرصت المملكة عند رسم استراتيجيتها في مجال الأمن السيبراني التركيز على جذب الفرص الإستثمارية المتميزة وتم رصد لها ميزانية بقيمة ٧٥ مليار ريال، وتعمل على تدريب وتوطين أكثر من ٢٠ ألف ما بين متخصص وخبير في الذكاء الإصطناعي والأمن الإلكتروني، عملت كذلك على تحفيز الشركات الناشئة وريادة الأعمال بحدود ٣٠٠ قطاع متخصص في أنظمة الفضاء الإلكتروني، كما شجعت البحث والإبتكار العلمي وقد وصلت ضمن أعلى ٢٠ دولة في المنشورات والأبحاث العلمية، وتسعى المملكة العربية السعودية لأن تكون مركزًا دوليًا عالميًا ضمن أعلى ١٥ دولة في منظومة الأمن الذكاء الإصطناعي. (المطيري،٢٠٢٣)

العلاقة بين الأمن السيبراني وأمن الدولة:

بسبب الإستخدامات غير السلمية للفضاء الإلكتروني تنامت العلاقة بين الأمن الوطني والتكنولوجيا، لأنه يؤثر في الرخاء لكافة مناحي الحياة لكافة الدول (عبد الصادق، ٢٠١٦). ويشمل الأمن السيبراني جميع المسائل الاقتصادية، والاجتماعية، والسياسية، والإنسانية، حيث يرتبط الأمن السيبراني في العصر الحالي بسلامة مصادر الثروة ، من القدرة على الإتصال والتواصل لكافة البيانات، والمعلومات، وهو الأساس الذي يتكون حوله القدرة على المنافسة، والإنتاج، والإبداع، ثم إن الأمن الوطني الشامل للدولة بما يحتويه من أمن سياسي، واقتصادي، واجتماعي، فإن الأمن السيبراني يمسها ويتداخل معها بطريقة مباشرة، نظراً لإعتماد كل جانب من هذه الجوانب على نظم المعلومات والشبكات، وهذا مصدر رئيس من مصادر المخاطر تجب معاملته كخطر أمني (السويدي، ٢٠١٨).

لذلك يعد موضوع الأمن الوطني إحدى الموضوعات الهامة في الجغرافية السياسية، لكونه يحتاج إلى ربط وتحليل العوامل والتفاعلات البشرية عظيمة التأثير مثل (الأنماط والعلاقات السياسية والأحداث العسكرية) مع دراسة العوامل الجغرافية طبيعة وبشرية، ومن خلال معنى لفظ الدولة يتضح لدينا ترابط منظومة الأمن بما فيها أمن المعلومات وحماية الفضاء الإلكتروني بمهام الجغرافيا السياسية، إذ أن الهجمات الإلكترونية التي تستهدف المملكة العربية السعودية الفاعل فيها لا يخرج عن كونها حكومات دول معادية ومنفذين من المختصين في شبكات المعلومات التي تستخدمهم الدولة لتحقق أهدافها في محاولة للنيل من أمن المملكة المعلوماتي، وهنا لا بد من الوقوف على الخلفية الطبيعية والبشرية والتاريخية كمؤشر لقياس الظاهرة وتحدياتها وتحديد أيضاً خطرها والتنبؤ بمستقبلها، فالجيوبوليتك في الجغرافيا السياسية تركز على الدور السياسي الفاعل الذي يمكن أن تؤديه في حالة مثل – المملكة العربية السعودية – تجاه خطر ما، يمس سيادتها وأمنها أو يقف حائلًا دون استقرارها (سعودي، ٢٠١٠).

كما تهدف الجغرافيا السياسية إلى تحويل المعلومات الجغرافية إلى بيانات ومعلومات علمية يستفيد منها قادة الدولة في سياساتهم، ومن هنا بدأ الإهتمام الحديث بنظم المعلومات الجغرافية، ويبرز من خلاله أهمية أمن المعلومات لسببين، أولهما تعتمد المجتمعات اليوم اعتمادًا كليًا على الإتصالات وتقنية المعلومات في كافة أنشطتها، والثاني أي ضرر يستهدف المنظومة العالمية لشبكات الإتصالات وتقنية المعلومات سيؤثر حتمًا على حياة المجتمعات فجميع أنشطة مرافق الدولة والمجتمع قائمة على تقنية الإتصالات الحديثة. (رياض، ٢٠١٤).

إذًا يتضح مما سبق تحول المسؤولية الأمنية لكل قطاع من قطاعات الدولة على الأمن السيبراني، ويخصص كل قطاع وحدة للأمن المعلوماتي

بالدفاع عن نظام أمنها. من أجل ذلك تولي المنظمات والهيئات المسؤولة عن قطاع الإتصالات على نشر أهمية الأمن السيبراني وتحذر المجتمعات بصورة مستمرة من المخاطر التي تحدث، ويتبع الهجمات السيبرانية قضايا متعددة فهناك محتويات غير مشروعة انتشارها يؤثر تأثيرًا سلبيًا على أخلاقيات المجتمع خاصة فئة الشباب والأطفال، من أجل ذلك لا بد من تجهيز المجتمع ليكون مسؤلًا ومدركًا لمخاطر الفضاء السيبراني (جبور، ٢٠١٥).

وعلى الصعيد الاقتصادي يتطلب تحقيق الأمن السيبراني لهذا القطاع تفادي خسارة المال والأزمات الاقتصادية، وليس كسبه، فعلى سبيل المثال: تعرض نظام شبكة شركة أرامكو إلى هجمة سيبرانية تعطلت على أثرها ٣٠ ألف جهاز مما أدى إلى إعاقة وتهديد حوالي ٩ مليون برميل تنتج للسوق العالمية يوميًا فترة التعطيل (مؤتمر حلول أمن المعلومات لمنطقة الشرق الأوسط وشمال أفريقيا، ٢٠١٨).

ويتضح أن هناك علاقة وثيقة بين الأمن السيبراني والأمن الاجتماعي بمفهومه الواسع، فقد ترتب على التطور الذي حققته وسائل الإتصالات من امكانيات التواصل السريع والكبير بين البشر أنهم في أثناء انفتاح آفاق المجتمعات وتعزيز القبول والتسامح لم يخلوا من الآثار السلبية وهي ظهور حروب الجيل الرابع التي تعتمد على استخدام الفايروسات الإلكترونية وكذلك نشر الأوبئة والفايروسات المعدية وهدفهم هو خلق نوع من الخوف وعدم استقرار المجتمعات وإثارة الفتن والطائفية والعرقية، مما يؤكد أن هناك علاقة وثيقة الصلة بين الأمن السيبراني والأمن الاجتماعي(السويدي، ٢٠١٨).

ويجب الإشارة إلى الآتي:

- أصدرت وزارة الطاقة بيانًا رسميًا معلن جاء فيه أن إحدى الدول قامت بإرسال هجمات سيبرانية في منتصف سبتمبر ٢٠١٩ على منشأتي خريص وبقيق التابعتين لأرامكو السعودية مما أدى إلى توقف ما يقارب ٥٠٪ من الإنتاج بشركة أرامكو (وزارة الخارجية، ٢٠١٩).
- حصلت العديد من المتغيرات الأمنية والسياسية خاصة في الدول العربية بعد عام ٢٠١١ تحديدًا كان للمجال السيبراني دورًا واضحًا خاصة على المجتمعات وحكوماتهم عن طريق محاولة إنهيار وإفشال مؤسسات الدولة، وقد تم استغلال الدول التي تعاني من تراجع في مسيرة التنمية وإنتشار الفقر والبطالة وعدم الاستجابة لمطالب الشعوب- حالة اليمن وليبيا وأدت في أخرى دورًا سياسيًا حالة- تونس ومصر وسوريا، فقد استهدف المجال السيبراني الجانب النفسي لتلك الشعوب خاصة فئة الشباب عن طريق شبكات التواصل الاجتماعي، وقد استغل الاختلاف الديني والطائفي والمذهبي والسياسي من خارج تلك البلدان واستغلت مطالبهم لتكون مدخلًا لهم في تفرقة الشعوب وبث روح التفرقة والكراهية (خليفة، ٢٠١٧).

- دفع تزايد هجمات القرصنة الإلكترونية خاصة على دول الخليج العربي، إلى زيادة الإستثمار والإنفاق في الأمن السيبراني وإنتشار هيئات مختصة بالأمن فقد أمرت حكومة المملكة العربية السعودية في ٢٠١٧ بإنشاء الهيئة الوطنية للأمن السيبراني ويكون مجال اختصاصها بناء استراتيجية تعمل على مواجهة المخاطر الإلكترونية وصد الهجمات. (الهيئة الوطنية للأمن السيبراني،٢٠١٨).

<u>ونستطيع تلخيص علاقة الأمن السيبراني بالأمن الوطني العام للدولة من خلال قدرة الأمن السيبراني على تحقيق ما يلي:</u>

١- التصدي للمخاطر الإلكترونية.
٢- تعزيز "القوة المؤسسية" في السياسة الدولية.
٣- سعياً لدرء تهديدات أمن الفضاء الإلكتروني، أصبح الآن بالإمكان عسكرة الفضاء الإلكتروني وبرز في هذا الإطار عدة اتجاهات منها، تصاعد القدرات في سباق التسلح السيبراني، والتطور في مجال سياسات الدفاع والأمن الإلكتروني.
٤- الفضاء الإلكتروني جزء لا يتجزأ من الأمن القومي للدول، وذلك عبر، تحديث أساليب الحروب القديمة، وإنشاء وحدات متخصصة مهمتها متابعة مستجدات الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني.
٥- الحروب في المستقبل، هي حروب المعلومات لذا لا بد من رفع كفاءة الجاهزية بالتدريب المستمر وتبني المواهب.

٦- تحديث القدرات الدفاعية والهجومية. (عبدالصادق ع.، أسلحة الانتشار الشامل في عصر الفضاء الالكتروني، ٢٠١٢).

٢. التهديدات السيبرانية التي تعرضت لها المملكة العربية السعودية:

إن ما تتعرض له المملكة العربية السعودية من هجمات الكترونية، لا يمكن تسميتها بـهجمات القرصنة الإلكترونية الإعتيادية، بل هي حروب سيبرانية، مثال على هذه الهجمات تصدت الهيئة السعودية للبيانات والذكاء الإصطناعي بكوادرها الشابة السعودية المؤهلة ل٢,٣٠٠٠٠٠٠ هجمة الكترونية أثناء انعقاد قمة مجموعة العشرين الإفتراضية. (موقع الهيئة السعودية للبيانات والذكاء الاصطناعي،٢٠٢٣)

وواجهت ٣٠٠,٠٠٠ هجمة في عام ٢٠٢١ استهدفت بشكل خاص البيانات الحكومية لغرض تعطيلها وتوقف نشاطها وسرقة بياناتها.

وفي عام ٢٠٢٠ تصدى العاملون في مجال الأمن السيبراني إلى ٢٢٤٤ هجمة يوميًا أي بمتوسط ٩٣,٥ هجمة في الساعة (مركز المعلومات الوطني، ٢٠٢٠)، وهذا دليل على قوة الجهاز الدفاعي فمما لا شك فيه أن الإهتمام

بالكوادر الوطنية والأمن المعلوماتي يعد قوة استراتيجية، ويتطلب في المقابل الانفاق المتسارع والمتزايد من الأموال.

وبلغ عدد ما تعرضت له المملكة العربية السعودية في عام٢٠١٧- ٥٤ ألف هجوم الكتروني، ومن بين الدول التي تعرضت للهجوم حازت المملكة بالمرتبة الثالثة على مستوى العالم أي بمعدل ١٥٠ هجومًا الكتروني في اليوم، ونحو ٦ هجمات في الساعة، على جميع مرافقها الحكومية، وفي عام ٢٠١٥ تعرضت المملكة إلى ٦٠ مليون هجمة الكترونية بمعدل ١٦٤ ألف هجمة يومية (الربيعة، ٢٠١٨).

فقد استهدفت أنظمة المملكة الحاسوبية في عدداً من الوزارات، والمؤسسات الحكومية، والمنشآت الحيوية، وبعض الشركات، حيث شهدت هجمات الكترونية عملت على تعطيل مصالحها، وألحقت بها ضررًا، استخدمت فيها القرصنة وتوظيف الفيروسات (الشمري، ٢٠١٥).

وفي عام ٢٠١٨ أعلنت وزارة الداخلية في المملكة عن أنه تم رصد عدة هجمات من دول مختلفة ومئات العناوين الخارجية وقد تصدت المملكة لهذه الهجمات واستطاعت إعادة المواقع للعمل في أقل من ساعتين. (وكالة الأنباء السعودية، ٢٠١٨)

وفي عام ٢٠١٣ أعلنت وزارة الداخلية عن تعرض موقعها لهجمة سيبرانية تسببت في حجب خدمات موقعها بالإضافة إلى عدد من المنشآت الحكومية تعرضت مواقعها لهجمات مكثفة تعطلت على أثرها لساعات بسيطة . (الملتقى العلمي لأمن المعلومات،٢٠١٦)

وتبدأ معظم الهجمات الإلكترونية بسرقة بيانات الدخول للمستخدمين بطرائق احتيال مختلفة، وتتفاوت الهجمات التي تتعرض لها المملكة العربية السعودية ما بين هجمات تستهدف أفراد – وهجمات تسعى خلف البيانات البنكية – وأخرى تستهدف الشركات، والدوائر الحكومية وما يهمها هو الاستحواذ على بيانات الدخول السرية للولوج إلى أنظمة، وقواعد بيانات القطاعات السعودية خاصة المهم منها، بغية العبث بها وطلب فدية مالية.

أ ـ القطاعات التي استهدفتها التهديدات الإلكترونية:

بالنظر إلى شكل ١ يتبين مايلي:

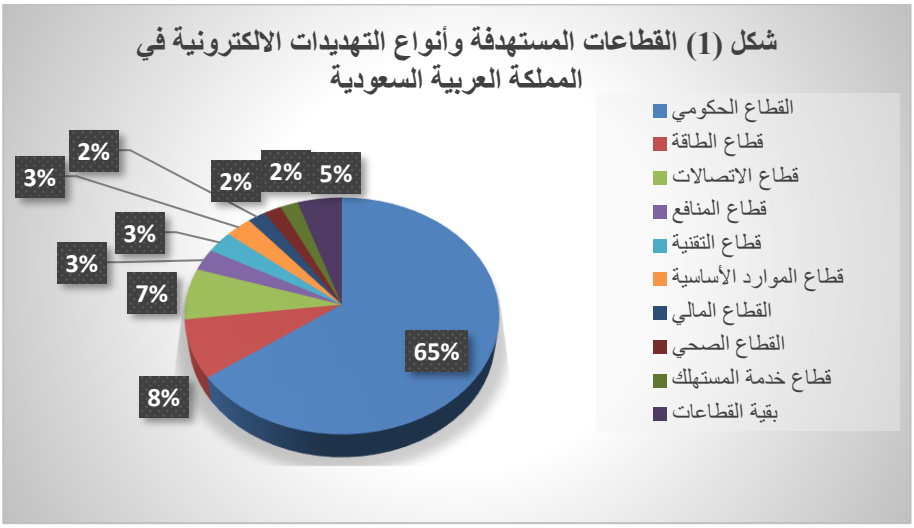
١. يعد القطاع الحكومي هو أكثر القطاعات المستهدفة ٦٥٪، وذلك لما يشمله القطاع من معلومات مهمة اقتصادياً وسياسياً وخدمياً.

٢. استهداف قطاع الطاقة بنسبة ٨٪ لإرتباطه بسوق النفط العالمي ومن ثما يؤثر مباشرة على بقية القطاعات في الدولة.

٣. استهداف قطاع الإتصالات بنسبة٧٪ كونه الرابط بين جميع القطاعات.

٤. ٣٪ من التهديدات لكل من قطاع التقنية والموارد والمنافع.

٥. استهداف قطاع الخدمات الصحية والمالية وخدمات المستهلك بمقدار ٢٪ لكل قطاع ، وتتوزع الخمسة بالمائة المتبقية على باقي القطاعات.



المصدر: الهيئة العامة للأمن السيبراني، تقرير الربع الأخير من عام ٢٠١٧ (الهيئة الوطنية للأمن السيبراني، ٢٠١٨).

ب - أنواع التهديدات الإلكترونية التي وجهت للمملكة العربية السعودية:

١- المحاولات بنسبة ٥٩٪ من التهديدات.

٢- البرمجيات الخبيثة بنسبة ١٩٪

٣- الرسائل التهديدية بنسبة ١٠٪

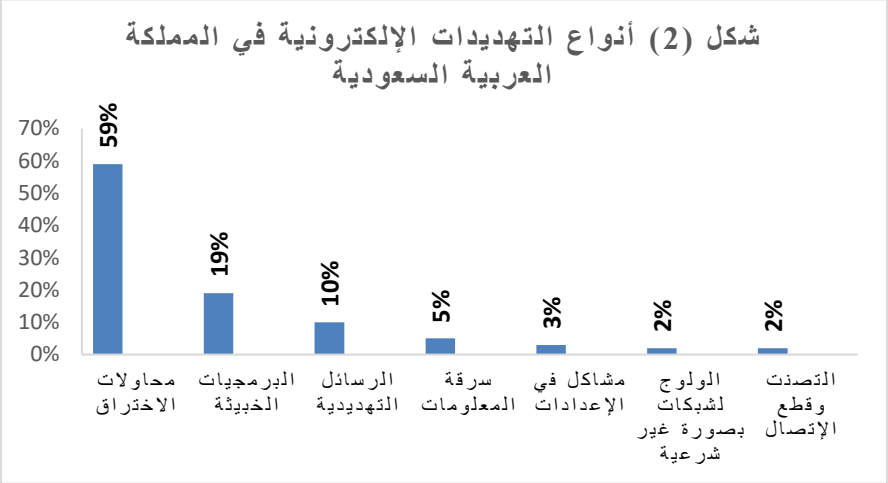
٤- سرقة البيانات ومنظومة المعلومات وذلك بنسبة ٥٪

٥- التهديدات في هيئة استخدام مشاكل في الإعدادات أو غير صحيح وذلك بنسبة ٣٪

٦- محاولات الدخول غير المصرح به، ومحاولات غير شرعية للولوج إلى الشبكات بنسبة ٢٪

٧- ومن اجمالي التهديدات الإلكترونية التي تعرضت لها المملكة في الربع الاخير من عام بلغت محاولات التنصت وقطع الاتصالات نسبة ٢٪

(الهيئة الوطنية للأمن السيبراني،٢٠١٨)



المصدر: الهيئة العامة للأمن السيبراني، تقرير الربع الأخير من عام ٢٠١٧ (الهيئة الوطنية للأمن السيبراني، ٢٠١٨).

ونستنتج من شكل (١) وشكل (٢) أن تكرار الهجمات وتنوعها يدل على أن أهدافها هو، تدمير قواعد البيانات والمعلومات، أو سرقتها والعمل على نشرها بغرض أهداف سياسية، وتركز الهجمات على قطاع التقنية وقطاع الصناعة بغرض تخريب البنية التحتية الحيوية وهو بشكل أو آخر يعمل على شل حركة الدولة في القطاع الإنتاجي مما يؤثر بدوره على الإنتاج العالمي وليس فقط المحلي، بالتالي يتضح عمق الخطر الاستراتيجي لهذه الهجمات، وهذا ما دفع المملكة العربية السعودية لحماية شبكات المعلومات وضمه وجعله من أولويات الأمن الوطني وجزء لا يتجزأ منه.

٣. التدابير الأمنية للرفع من مستوى الأمن السيبراني في المملكة العربية السعودية:

من أهم التدابير الأمنية التقنية التي يتم تنظيمها في المملكة العربية السعودية والعالم مؤتمر أمن المعلومات، فهو ملتقى عالمي يجمع أفضل خبراء التقنية لمناقشة التحديات الأمنية والثقافية والاجتماعية التي تواجهها دول العالم.

كان التحول الرقمي مطلبًا ملحًا وضروريًا أدرج ضمن رؤية ٢٠٣٠ للحفاظ على أمن المملكة وجميع قطاعاتها فعملت على عقد الشراكات مع أكبر المنظمات والشركات المختصة بتقنية المعلومات لتأمين البنية التحتية خاصة لشركة الإتصالات السعودية حتى تتمكن من تقديم بيئة رقمية آمنة لكافة العملاء. بلغ حجم سوق الأمن السيبراني في المملكة العربية السعودية ٩,١٠ مليار ريال سعودي في عام ٢٠١٩

وواصل نموه حتى بلغ ٥٩,١٦٪ عام ٢٠٢٣ أي بما يقدر ٢١ مليار ريال سعودي (مؤتمر أمن المعلومات بمنطقة الشرق الأوسط وشمال أفريقيا،٢٠٢٣)

ولقد تفهمت المملكة بعد حدوث عدة هجمات الكترونية على أهم قطاعاتها بأن لهذه الهجمات تأثير **على ما يلي:**

أ. الشعب وثقتهم بحكومتهم.
ب. العلاقات السياسية العالمية.
ت. أدوات الحرب لتعزيز الدور الدولي.
ث. مجال للصراع بين الدول.
ج. الإحتقان الدبلوماسي لإتهام الدول المتضررة من الهجمات دول مرسلة للهجمات عبر الفضاء الالكتروني بالتدخل في شؤونها الداخلية.

لذا **وجب أن يكون للمملكة إستراتيجيات دفاع حديثة** لردع تلك الهجمات حال حدوثها. وهذا حقيقة بعض ما يتضمنه مفهوم الجيبولتيك في الجغرافيا السياسية الذي يهدف إلى تحليل وفهم النزاعات، والخلافات الدولية بكافة أشكالها خاصة في عصرنا الحالي المعروف بعصر الأزمات والنزاعات، ليبني صانع القرار إستراتيجيات الدفاع المناسبة، وتصوراته السياسية المستقبلية لسياسته الخارجية في ضوء تفاعلات المكان الجغرافي.

ولقد أسفرت الدراسات التي تهتم بدراسة العلاقة بين وعي المستخدمين وأمن المعلومات بنتيجة ايجابية أذ أن العلاقة طردية بين مستوى الوعي الأمني لدى المستخدمين وبين نسبة نجاح تأمين المعلومات .

على الرغم من الجهود العظيمة التي تبذلها الجهات المختصة بالأمن المعلوماتي الا أنه لا يمكن تحقيق أمن معلومات من طرفها فقط فالمجتمع شريك نجاح هذه العملية.

ويمكن القول أنه لن نستطيع تحقيق أمن معلوماتي بشكل متكامل من طرف واحد فقط كالجهات المختصة في أمن المعلومات فعلى الرغم من أهمية ما تقدمه من حلول تقنية والكترونية الا أن المستخدم لهذه التقنية يمثل حجر الزاوية في منظومة أمن المعلومات، فالمخترقين والمهاجمين يستهدفون الحلقة الأضعف وهي المستهدف، مستغلين ضعف الوعي والادراك لأمن المعلومات و عدم الحفاظ على معلوماتهم السرية لحساباتهم، ومن ثما يعملون على تنفيذ اختراقاتهم وشن هجماتهم الالكترونية.

لذلك لا يمكن فصل أمن المعلومات والفضاء السيبراني عن الأمن القومي لأي دولة، وقد أدركت المملكة العربية السعودية أهمية هذا الجانب فأطلقت أول مشروع وطني يهتم بالتوعية بأمن المعلومات "آمن" في عام ٢٠١٦ ويهدف إلى الحد من مخاطر الهجمات والإختراقات الإلكترونية، وتوعية جميع قطاعات الدولة بضرورة بناء جهاز أمن سيبراني قوي لصد الهجمات وتتبع التصيد والاختراق، وتثقيف المجتمع وتوعيتهم بضرورة الحفاظ على هوية المستخدم وأرقامه السرية، وقد أقيم مؤتمر الأمن الإلكتروني كأول نشاط للبرنامج كان من أهم توصياته "ضرورة التأكيد على أهمية تعزيز التوعية

الوطنية لأمن المعلومات كمطلب قومي" وبهذا الشأن صدر بموجب الأمر الملكي رقم (أ/٤٧١) وتاريخ ١٤٤٠/١٢/٢٩هـ ،الهيئة السعودية للبيانات والذكاء الإصطناعي (سدايا) وترتبط مباشرة برئيس مجلس الوزراء، ويرتبط بها تنظيمياً: مكتب إدارة البيانات الوطنية، والمركز الوطني للذكاء الإصطناعي، ومركز المعلومات الوطني مما يترجم الأهمية القصوى لأمن المعلومات وعلاقته المباشرة بأمن الدولة، ثم توالى إنشاء الهيئات والمراكز المختصة التابعة للهيئة السعودية للبيانات والذكاء الإصطناعي وجميعها تهدف بالحفاظ على أمن الدولة وأنظمتها التقنية والمعلوماتية. (المطيري،٢٠٢٣)

إضافة إلى هذه التطورات في هذا المجال يذكر أن هناك مجموعات غير ربحية تطوعية نشيطين جدًا تشمل على مجموعة من التقنيين المختصين والمحبين لهذا المجال يقومون بنشر ثقافة ومفهوم الأمن الإلكتروني ورفع مستوى وعي المجتمع من خلال وسائل التواصل الاجتماعي، وإدراكًا من حكومة المملكة العربية السعودية من أنه لا بد من مواكبة جميع التطورات التقنية التي تحقق الأمن المعلوماتي للمجتمع والفرد والمنشآت، وحتى يكون هناك نظام صارم لكل من يسيء استخدام التقنية، ورغبة في مواكبة الدول التي أخذت بمثل هذه الاحترازات صدر مرسوم ملكي بتاريخ ٨-٣-١٤٢٨هـ بالموافقة على "نظام مكافحة الجرائم المعلوماتية وتحديد عقوبات مقررة لكل جريمة وجهات الاختصاص التي تهتم بها"

وبناء على المؤشر العالمي للأمن السيبراني المعروفة بـ «الاتحاد الدولي للإتصالات» احتلت المملكة المرتبة الثانية عالميًا منذ إطلاق رؤية ٢٠٣٠ والأولى على مستوى الشرق الأوسط. (الهيئة السعودية للبيانات والذكاء الاصطناعي،٢٠٢٣)

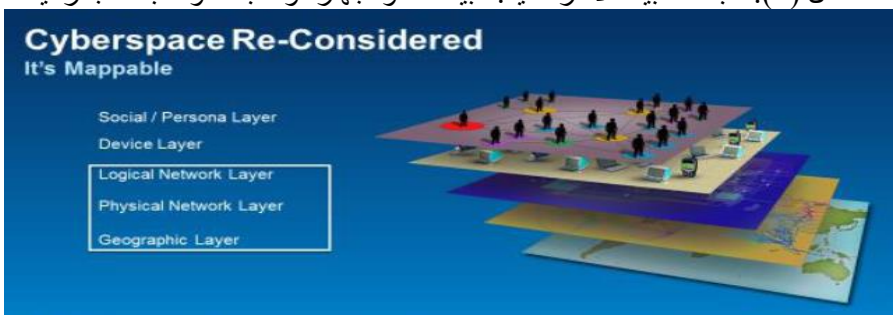
٤. النظم الجغرافية الحديثة والأمن السيبراني:

في عصر التقنية والإنترنت أصبح التحول الإلكتروني في كافة القطاعات الحكومية والخاصة لذا أصبح الأمن المعلوماتي ضرورة ملحة لحماية ذلك الكم من البيانات الهامة والسرية أحيانا. ومما سبق تبين أن الهجمات الإلكترونية والإختراقات تكلف المؤسسات خسائر مادية طائلة بالإضافة إلى توقف الخدمة وسرقة البيانات وغيرها من الأخطار لذلك يلجأ الأمن السيبراني إلى استخدام استراتيجيات وأدوات لتفادي تلك الخسائر. ولا يمكن تجاهل التهديدات الأمنية أو توكيل إدارة التقنية بتولي الناحية الأمنية لا بد من دمج الأمن السيبراني بالأنظمة الالكترونية.

إن **نظم المعلومات الجغرافية GIS** توفر أدوات يمكن أن تساعد المؤسسات على تحليل الأنظمة التي يحتمل أن تكون معرضة للخطر وتطوير دفاعات أقوى، ومع اكتشاف الكثير من القطاعات قيمة الخاصية المكانية والجغرافية في تحليل وحل المشكلات المتعددة يستمر دور نظم المعلومات

الجغرافية بالتوسع في الأمن السيبراني لإيقاف مجموعة متطورة من الأخطار. باستخدام نظم المعلومات الجغرافية، يمكن للإدارات الاستفادة من بيانات الموقع في توقع الهجمات السيبرانية واكتشافها والرد عليها واستعادة الأنظمة بشكل أفضل. تمتلك نظم المعلومات الجغرافية قدرات تساعد على تصور وتمثيل الموقف لاستيعاب الخطر بالتالي اتخاذ القرار بشكل أفضل.

شكل (٣): طبقات البيئة الافتراضية: البيانات، والجهاز، والشبكة، والطبقة الجغرافية



المصدر:(Esri, 2015)

ذكرت إزري Esri الأمريكية أن الفضاء السيبراني يتكون من مزيج معقد من البيانات والأجهزة والأشخاص، بالتالي **للجغرافيا** دور مهم في ربط الفضاء السيبراني ببقية البيانات، وأن البيئة الافتراضية تتكون من أربعة أنواع مختلفة من طبقات الشبكة كما يظهر في شكل (٣)، ولكل منها عقد يمكن تحديد موقعها في الزمان والمكان، وتشمل هذه البيئة: البيانات والجهاز والشبكة والطبقات الجغرافية. وغالبًا ما يتم تعيين طبقات البيانات وفقًا لنوع العقدة المستخدمة، سواء أكان ذلك الشخص أو الجهاز، وتخدم الطبقة الجغرافية كإطار تكامل مشترك لجميع الطبقات. ويتم تحقيق التكامل من خلال تحديد الموقع الجغرافي لجميع العقد، بما في ذلك الأشخاص وأجهزة المستخدم وأجهزة البنية التحتية، والروابط بينهم داخل طبقة وبين الطبقات. يوفر تعيين جميع الطبقات للطبقة الجغرافية خط الأساس المشترك الذي يمكن من خلاله تحقيق الوعي الشامل. كذلك يمكن استخدام النظام الأساسي لنظم المعلومات الجغرافية لدمج بيانات الموقع والنشاط الإلكتروني والمعلومات الأخرى لتوقع الحوادث السيبرانية واكتشافها والرد عليها والتعافي منها على نحو أفضل، وفي وقتنا الحالي أصبحت أغلب القطاعات الحكومية الخاصة تستخدم الأنظمة الجغرافية وبعضها لديها إدارات خاصة بنظم المعلومات الجغرافية لذا يسهل دمج نظامها مع نظام الأمن السيبراني لإتخاذ قرارات أفضل وتوفير الحماية الأمنية. وتظهر أهمية الموقع المكاني بأنه الأساس الذي يمكن من خلاله تنظيم جميع الأنشطة وتصورها ومشاركتها من أجل اتخاذ القرارات الفعالة، حيث يوفر النموذج الجغرافي حلاً لدمج هذه الجهود، ومواءمتها مع التخصصات الأمنية الأخرى، والتركيز على كلاهما بناءً على تدفق البيانات ذات الأولوية التي أنشأتها المنظمة.

أي إطار يمكنه إنجاز ذلك يجب أن يكون له أساس جغرافي مكاني قوي، حيث تتضمن أي منصة قوية لنظم المعلومات الجغرافية GIS: الأجهزة والبرمجيات والبيانات وأفراد العمل ويمكن بالطبع دمج هذه المنصة مع بيانات وتقنيات الأمن السيبراني الموجودة في المؤسسة لتحسين **ما يلي:**

أ. إدارة البيانات
ب. التحليل
ت. تصور وضع الحالة
ث. تبادل المعلومات

كما أوضح (Peters, 2018) بأن تكنولوجيا نظام المعلومات الجغرافية (GIS) ستساعد على تحسين الدفاع السيبراني وتمكين منهج متعدد التخصصات الأمنية في توفير ضمان تنظيم المهمة الأمنية عبر المساعدة في إعطاء الأولوية. ومن خلال الجمع بين المؤشرات السيبرانية التقليدية ومنصة جغرافية مكانية، يمكن للمنظمات أن تكتشف بسرعة وتحدد جميع أنواع التهديدات السيبرانية المقصودة منها أو العرضية، من خلال إنشاء نموذج شامل يدمج جميع البيانات المتاحة. ويمكن أن توفر مجموعات البيانات الجغرافية المكانية التقليدية، مثل الطقس وأنماط الجريمة والتهديدات الأمنية قيمة لمشغلي الفضاء الإلكتروني عند تقييم المخاطر على شبكات الإتصالات الخاصة بهم. بغض النظر عن سبب التعطل، يجب أن يكون مشغلو الإنترنت قادرين على توقع أخطار الفشل في بعض الأجهزة الهامة، ومن ثم تحديد تأثير فشل تلك الأجهزة(Esri, 2015).

قام Hui وآخرون في جامعة نورث فلوريدا باستخدام المنظور الجغرافي المكاني في الأمن السيبراني لرصد وتحليل الهجمات الإلكترونية. ففي قسم تكنولوجيا المعلومات بجامعة نورث فلوريدا يستخدم برنامج الكشف عن تهديدات الأمن السيبراني ويقوم برصد كميات كبيرة من الهجمات ومحاولات الاقتحام في كل دقيقة. كانت أنماط وعلاقات أصل الهجوم السيبراني ليست واضحة حتى تم عرض البيانات في خرائط واختبارها باستخدام النماذج الإحصائية، **وقد تم الاستعانة بالخطوات التالية:**

- اكتشاف مواقع أصول الهجوم الإلكتروني بواسطة برنامج بروتوكول الإنترنت الجغرافي (GEO-IP).
- استخدام نظم المعلومات الجغرافية لرسم خريطة لمواقع منشأ الهجمات الإلكترونية.
- استخدام التحليل الإحصائي المكاني المتقدم لوظائف تحليل البيانات المكانية الاستكشافية وتحليل نمط النقطة المكانية وقد تم الاستعانة ببرنامج R لاستكشاف أنماط الهجوم السيبراني.

فمن خلال تحديد الموقع الجغرافي للهجمات الإلكترونية على شبكة الحاسوب التابعة لجامعة نورث فلوريدا استنادًا إلى عناوين المصدر IP، تم الكشف عن أنماط مكانية عالمية لأصول الهجوم، وحددت البلدان التي لها معظم أصول الهجوم وأصول الهجوم في المناطق الساخنة في الولايات المتحدة الأمريكية. إن توظيف العامل المكاني لن يساعد فحسب في معالجة تهديدات الأمن السيبراني التي تتعرض لها جامعة نورث فلوريدا بشكل أفضل، بل يمكن أن يكون نموذجاً للأنظمة الجامعية الحكومية الأخرى والمنظمات الخارجية. حيث يعد المنظور المكاني اتجاهاً جديداً نظراً لوجود عدد قليل من الدراسات التي تستخدم تحليلات الموقع والإحصاءات المكانية في أبحاث الكشف عن الهجمات الإلكترونية والوقاية منها (Hui, Baynard, Hu, & Fazioi, 2015). وعلى الوجه الآخر الإستعانة بالأمن السيبراني في تطبيقات وقواعد نظم المعلومات الجغرافية على شبكة الانترنت أساسي ومهم للغاية لحماية البيانات من الاختراق والحفاظ على سرية البيانات المكانية خاصة الحساسة منها والسرية.

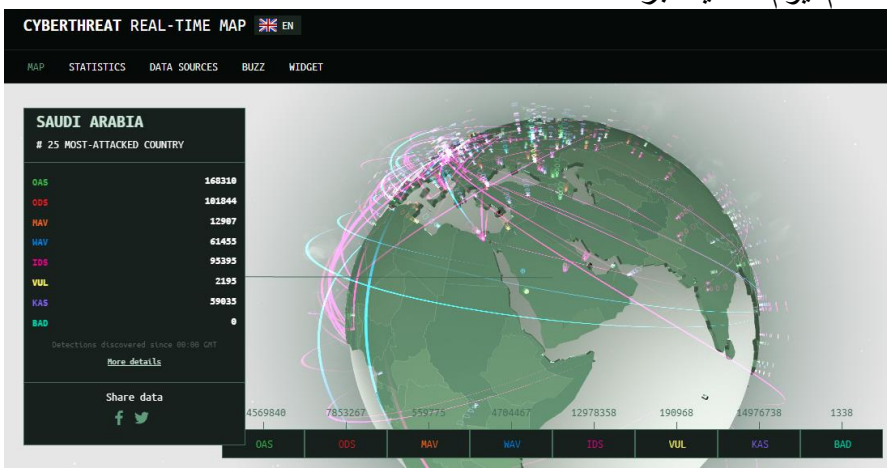
إن شبكة نظم المعلومات الجغرافية عبرالإنترنت GIS Web هي وسيلة فعالة لنشر البيانات الجغرافية المكانية وأدوات المعالجة الجغرافية عبر الإنترنت، وتتضمن بعض طرق تحليل أمان قاعدة البيانات **وتطبيقها ما يلي:**

أ. تقييد الوصول والإستخدام غير المصرح به.
ب. اختبار الضغط واختبار سعة قاعدة البيانات لضمان عدم تعطلها في حالة الهجوم أو التحميل الزائد للمستخدم.
ت. تأمين خادم قاعدة البيانات والمعدات الاحتياطية من السرقة والكوارث الطبيعية.
ث. فحص النظام الحالي لأي نقاط ضعف معروفة أو غير معروفة وتحديد وايجاد طريق للتخفيف منها. (Giribabu, et al., 2018)

و في السنوات الأخيرة نشأ تحالف تهديدات الإنترنت Cyber Threat Alliance، وهو منظمة غير ربحية تعمل على تحسين الأمن السيبراني للنظام الرقمي العالمي من خلال تمكين مشاركة معلومات تهديد الإنترنت للحظة الحالية وهي معلومات عالية الجودة من الشركات والمؤسسات في مجال الأمن السيبراني. ويتيح هذا التحالف لممارسي الأمن السيبراني مشاركة معلومات موثوق بها عن تهديدات الإنترنت، وبالتالي تساعد في اكتشاف الهجمات المباشرة عند إطلاقها (CTA, 2019). وعلى سبيل المثال، من أشهر خرائط التهديدات السيبرانية الحية خريطة شركة Kaspersky الأمنية والتي تملك العديد من برمجيات الحماية الشهيرة. ويضم الموقع خريطة تفاعلية توضح الهجمات السيبرانية العالمية حيث تعرض من أي تأتي الهجمة وأين تنتهي. ويمكن استعراض الهجمات لكل دولة على حدة وتتوفر كذلك مع الخريطة الكثير من الاحصائيات للهجمات السيبرانية العالمية والأشكال البيانية

الاحصائية. فعلى سبيل المثال حين تم تحديد دولة المملكة العربية السعودية تبين لنا أنها على المرتبة ٢٥ في الدول المتعرضة للهجوم السيبراني كما يظهر في شكل (٤).

شكل (٤) صورة من موقع Kaspersky توضح الهجمات السيبرانية على العالم ليوم ١٣ديسمبر ٢٠١٩



المصدر:(Cyber Map, Kaspersky, 2019)

وحسب الاحصائيات المرفقة في الموقع ظهرت أعلى أنواع التهديدات التي تعرضت لها المملكة في من شهر نوفمبر حتى ديسمبر ٢٠١٩ **على النحو التالي:**

١ Trojan.Multi.Preqw.gen ٪٢٥,٨٨
٢ Trojan.Script.Generic ٪١٩,٢٩
٣ Virus.Boot.Stoned.PC-AT ٪١٤,٦٢
٤ Trojan.BAT.Miner.gen ٪٩,١٦
٥ Trojan-Downloader.Script.Generic ٪٦,٢٥
٦ Hoax.Script.Loss.gen ٪٥,٨٣
٧ Trojan.Script.Miner.gen ٪٤,١٥
٨ Trojan.Win32.Nion.gen ٪١,٧٨
٩ Trojan.MSOffice.Badur.gen ٪١,٢٧
١٠ Trojan-PSW.Script.Generic ٪١,٢٣(Cyber Map, Kaspersky, 2019)

تاسعاً: نتائج البحث:

١. توجد علاقة بين الأمن السيبراني والأمن الوطني للمملكة في ظل تعرض المصالح الإستراتيجية للمملكة إلى تهديدات سيبرانية وأخطار متواصلة.
٢. يؤثر الإستخدام غير السلمي للفضاء الإلكتروني على الرخاء السياسي والاقتصادي والاجتماعي لكافة الدول.
٣. تطور أساليب الجرائم بسبب اعتمادهم على التقنية الإلكترونية مثل جرائم التهريب والتزوير والإرهاب وغسيل الأموال.
٤. نالت الحروب الإلكترونية من زعزعة استقرار بعض المجتمعات عن طريق تصعيد حدة الخلاف بين الطوائف الدينية.
٥. أدى تحول الحروب الافتراضية إلى حروب سيبرانية وتزايد القرصنة الالكترونية على دول الخليج من زيادة الإنفاق والاستثمار في الأمن السيبراني.
٦. رصدت وزارة الداخلية السعودية هجمات منظمة مستمرة متزامنة مع مئات العناوين الخارجية من دول مختلفة.
٧. يمكن استخدام الميزة المكانية في الاكتشاف المبكر وسرعة الاستجابة على مستوى الحكومة عند التصدي للهجوم الإلكتروني وحماية أمنها الإلكتروني من خلال نظم المعلومات الجغرافية.
٨. باستخدام نظم المعلومات الجغرافية، يمكن للإدارات الاستفادة من بيانات الموقع في توقع الهجمات السيبرانية واكتشافها والرد عليها واستعادة الأنظمة بشكل أفضل.

عاشراً: توصيات البحث:

١. إعداد إستراتيجية واضحة وشاملة لأمن المعلومات في كافة القطاعات.
٢. تشجيع جهود الباحثين في مجال أمن المعلومات، والتركيز على ما يخص المصالح الوطنية وبناء القدرات، وتوطين ونقل التقنيات التي تساعد على الاستخدام الأمن لحماية البيانات.
٣. التركيز على تحليل المخاطر والتهديدات الأمنية المحتملة.
٤. التعامل مع الشركات الوطنية المتخصصة في إدارة تقنية المعلومات وصيانة الأجهزة لديها بدلًا من الشركات الخارجية وهو ما يُسمى (Outsourcing).
٥. تنظيم المؤتمرات والندوات التي من شأنها أن تعمل على مواكبة المستجدات، والتهيؤ للأخطار وإدارتها بفاعلية.
٦. دمج نظم المعلومات الجغرافية التي تمكن التصور الشامل والمحاكاة لمختلف الأنشطة المرتبطة بالأمن السيبراني وتحديدها هدف الهجمة بدقة.

الحادي عشر: مراجع البحث:

أ. المراجع العربية

إيهاب خليفة. (٢٠١٧). القوة الإلكترونية. أبو ظبي: مركز المستقبل للأبحاث والدراسات المتقدمة.

الملتقى العلمي لأمن المعلومات –التحديات، الرؤى والتوجهات. (٢٠١٦). الرياض: الفترة ٤ – ٥ أكتوبر ٢٠١٦، جامعة نايف العربية للعلوم الأمنية.

الهيئة الوطنية للأمن السيبراني. (٧ ٩, ٢٠١٨). تم الاسترداد من https://www.my.gov.sa/wps/portal/snp/pages/agencies/agencyDetails/AC403

إيهاب خليفة. (٢٠١٧). *القوة الإلكترونية*. أبو ظبي: مركز المستقبل للأبحاث والدراسات المتقدمة.

جعفر أحمد العلوان. (٢٠٢٢). أدوار وتحديات الأمن السيبراني المعتمد على الذكاء الاصطناعي: دراسة حالة: المجلة الأردنية في إدارة الأعمال المجلد ١٨ العدد٣ الأردن.

جمال سند السويدي. (٢٠١٨). التغيير والأمن تعدد مصادر الخطر وآليات المواجهة الجديدة. *مجلة المركز العربي لأبحاث الفضاء الالكتروني*.

حامد قنيفذ الشمري. (٢٠١٥). رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية. *رؤية إستراتيجية لحماية الفضاء الالكتروني للمملكة العربية السعودية*، الرياض.

ذيب عايض القحطاني. (٢٠١٥). *أمن المعلومات*. الرياض: مدينة الملك عبد العزيز للعلوم والتقنية، مكتبة الملك فهد الوطنية للنشر.

رياض محمد الشهري. (٢٠٢٠). رؤية استشرافية للأمن الوطني للمملكة العربية السعودية في ضوء رؤية ٢٠٣٠. *رسالة دكتوراه غير منشورة، جامعة الأمير نايف للعلوم الأمنية*.

صادق عبدالصادق. (٢٠١٦). *أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني*. الاسكندرية: مكتبة الاسكندرية.

صالح علي الربيعة. (٢٠١٨). لأمن الرقمي وحماية المستخدم من مخاطر الإنترنت. *لاتحاد السعودي للأمن السيبراني والبرمجة*. الرياض.

صحيفة الرياض. (١٤ ١١ ,٢٠١٨) تم الاسترداد من

http://www.alriyadh.com/1506873

عادل عبدالصادق. (٢٠١٢). أسلحة الانتشار الشامل في عصر الفضاء الالكتروني. *مجلة السياسية الدولية، العدد ١٨٨*.

عادل عبدالصادق. (٢٠١٧). أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي. *مجلة السياسية الدولية، العدد ١٩٠*.

عادل محمد القحطاني. (٢٠١٥). تصور استراتيجي لتطوير أمن المعلومات تعزيزًا للأمن الوطني في المملكة. *رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، الرياض*.

علي زايد الشهري. (٢٠١٩). رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية. *رسالة دكتوراه غير منشورة، جامعة الأمير نايف للعلوم الأمنية*، الرياض.

لخميسي شيبي. (٢٠٠٩). *الأمن الدولي والعلاقات بين منظمات حلف شمال الأطلسي والدول العربية – فترة ما بعد الحرب الباردة*. القاهرة: جامعة الدول العربية، معهد البحوث والدراسات العربية.

محمد أحمد المقصودي. (٢٠١٧). الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونيا. *المجلة العربية للدراسات الأمنية*، المجلد (٣٣)، العدد (٧٠).

محمد رياض. (٢٠١٤). *الأصول العامة في الجغرافيا السياسية والجيوبولتيكا*. القاهرة: مؤسسة هنداوي للتعليم والثقافة والنشر.

محمد عبدالغني سعودي. (٢٠١٠). *الجغرافيا السياسية المعاصرة*. القاهرة: مكتبة الأنجلو المصرية.

منى الأشقر جبور. (٢٠١٥). أهمية الاتفاقية العربية للأمن السيبراني. *اللقاء السنوي الرابع للمختصين في أمن وسلامة الفضاء السيبراني*. جامعة الدول العربية, بيروت: المركز العربي للبحوث القانونية.

مؤتمر حلول أمن المعلومات لمنطقة الشرق الأوسط وشمال أفريقيا. (٢٠١٨). الرياض: الاتحاد السعودي للأمن السيبراني، الفترة ٦ – ٧ نوفمبر ٢٠١٨.

مؤتمر حلول أمن المعلومات لمنطقة الشرق الأوسط وشمال أفريقيا. (٢٠٢٣). الرياض: الاتحاد السعودي للأمن السيبراني، الفترة ١٢ – ١٣ سبتمبر ٢٠٢٣.

مركز المعلومات الوطني. (٢٩ ١٠ ,٢٠٢٣). تم الاسترداد من https://www.my.gov.sa/wps/portal/snp/agencies/agencyDetails/AC344

الهيئة السعودية للبيانات والذكاء الإصطناعي. (٢٥ ١١ ,٢٠٢٣). تم الاسترداد من

https://sdaia.gov.sa/ar/Sectors/Nic/Pages/default.aspx

هيئة الاتصالات وتقنية المعلومات. (١٠ ١٠, ٢٠١٨). تم الاسترداد من http://www.citc.gov.sa

وزارة الخارجية. (٢٧ ١١, ٢٠١٩). *موقع وزارة الخارجية على شبكة الإنترنت*. تم الاسترداد من http://www.mofa.gov.sa/aboutkingdom/kingdomforeignpolicy/Pages/ForeignPolicy24605.aspxhttp://www.mofa.gov.sa

وكالة الأنباء السعودية. (٢٢ ٩, ٢٠١٨). *موقع وكالة الأنباء السعوديةالإلكتروني*. تم الاسترداد من https://www.spa.gov.sa

ب. المراجع الأجنبية

Cyber Map, Kaspersky. (2019). Retrieved from Kaspersky: https://cybermap.kaspersky.com/stats/

CTA. (2019). *HOW OUR SHARING WORKS*. Retrieved from CYBER THREAT ALLIANCE: https://www.cyberthreatalliance.org/

Esri. (2015). The Geospatial Approach to Cybersecurity: Implementing a Platform to Secure Cyber Infrastructure and Operations. *An Esri® White Paper*.

Giribabu, D., Pandey, K., K.R.M, R., Rao, S., Udayraj, Bothale, V., et al. (2018). Cybersecurity in WebGIS Environment. *International Journal of Computer and Internet Security*, 11-34.

Hui, Z., Baynard, C., Hu, H., & Fazioi, M. (2015). GIS Mapping and Spatial Analysis of Cybersecurity Attacks on a Florida University. *2015 23rd International Conference on Geoinformatics* (p. 5). https://doi-org.sdl.idm.oclc.org/10.1109/GEOINFORMATICS.2015.7378714.

Morgan, S. (2019, Feb 6). *2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics.* Retrieved from Cyber Security Ventures: https://cybersecurityventures.com/cybersecurity-almanac-2019/

Peters, J. (2018, April 12). *Putting the geospatial in cybersecurity*. Retrieved from Federal News Network: https://federalnewsnetwork.com/commentary/2018/04/putting-the-geospatial-in-cybersecurity/