Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Journal of University Studies for Inclusive Research

Vol.11, Issue 35 (2024), 15502- 15527

USRIJ Pvt. Lt

فاعلية استخدام المنصات التفاعلية في التحليل المكاني للكشف عن الهجمات السيبرانية على المملكة العربية السعودية

The effectiveness of using interactive platforms in spatial analysis to detect cyber-attacks on the Kingdom of Saudi Arabia

إعداد: د. فاطمه موسى يحيى مطاعن

Dr: Fatmah Mousa Yahya Motaen

أستاذ مشارك- قسم العلوم الفيزيائية- برنامج نظم المعلومات الجغرافية- كلية العلوم- جامعة جدة

Associate Professor

Department of Physical Sciences-Geographic information systems program

College of Science

University of Jeddah

fmmotaen@uj.edu.sa

966-565550737

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

فاعلية استخدام المنصات التفاعلية في التحليل المكاني للكشف عن الهجمات السيبرانية على المملكة العربية السعودية

إعداد: د. فاطمه موسى يحيى مطاعن

أستاذ مشارك- قسم العلوم الفيزيائية- برنامج نظم المعلومات الجغرافية- كلية العلوم- جامعة جدة

الملخص:

تناولت الدراسة موضوع فاعلية استخدام بيانات المنصات التفاعلية في الكشف عن الهجمات السيبرانية على المملكة العربية السعودية. بهدف التعرف على الدول الأكثر استهدافاً للفضاء السيبراني للمملكة، وتوضيح القطاعات الأكثر استهدافا بالهجماتً. ولتحقيق أهداف الدراسة تم الاعتماد على المنهج الوصفي التحليلي. كما تم جمع البيانات من خلال التقارير الأمنية الصادرة من منصتي sonic wall security center & nets cout cyber threat horizon. وتم تحليل البيانات من خلال استخدام برنامج Spss & Arc Gis، وتم الاعتماد على تحليل بيانات الهجمات لمدة شهر وذلك بسبب صعوبة الحصول على البيانات وكونها من نوع البيانات الضخمة.

وتوصلت الدراسة إلى عدد من النتائج أهمها: تعرض المملكة لنوعين من الهجمات السيبرانية صنفت إلى: هجمات داخلية، وهجمات خارجية، كما ثبت ارتفاع نسبة استهداف قطاع الاتصالات السلكية واللاسلكية، وقطاع الاتصالات عبر الأقمار الصناعية، واتضح ارتفاع الهجمات من نوع Multiple attacks & Total Traffic، وكانت غالبية الهجمات موجهة للمنطقة الوسطى، يليها المنطقة الشرقية، واتضح ارتفاع نسبة الهجمات السيبرانية على المملكة من قبل دول الاتحاد الأوروبي والولايات المتحدة الأمريكية والأمارات العربية المتحدة وكانت غالبية الهجمات بدافع سياسي اقتصادي.

كما خرجت الدراسة بعدد من التوصيات أهمها: إنشاء منصة وطنية تفاعلية لمتابعة الهجمات على فضاء المملكة السيبراني للعمل على سد الثغرات الأمنية الموجودة في أجهزة القطاعين العام والخاص وإتاحة بياناتها للباحثين. ضرورة إجراء دراسة مماثلة عن المملكة العربية السعودية تتضمن بيانات عن الهجمات السيبرانية لفترات زمنية تتجاوز الشهر.

الكلمات المفتاحية: الأمن السيبراني- الهجمات السيبرانية- المنصات التفاعلية - جغرافية الجريمة.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

The effectiveness of using interactive platforms in spatial analysis to detect cyber-attacks on the Kingdom of Saudi Arabia

Dr: Fatmah Mousa Yahya Motaen

Associate Professor, Department of Physical Sciences-Geographic information systems program, College of Science, University of Jeddah.

Abstract:
The study investigated the effectiveness of using interactive platform data to detect cyber-attacks targeting Saudi Arabia, focusing on identifying the countries most frequently targeting Saudi cyberspace and the most affected sectors. A descriptive-analytical method was employed, with data collected from reports by Netscout Cyber Threat Horizon* and *SonicWall Security Center*. The analysis used *SPSS* and *ArcGIS* software, centering on one month's attack data due to the difficulty of accessing and processing large-scale information.

Key findings showed two types of cyber-attacks on Saudi Arabia: internal and external. The telecommunications and satellite communication sectors emerged as the most targeted, with *Total Traffic* and *Multiple Attacks* being the most common. Attacks were primarily concentrated in the central region, followed by the eastern region. Additionally, a substantial portion of these attacks originated from countries in the European Union, the United States, and the United Arab Emirates, often with .political and economic motivations.

The study recommended establishing a national interactive platform to monitor cyber-attacks on Saudi cyberspace, aimed at addressing security vulnerabilities across public and private sectors and making relevant data accessible to researchers. Additionally, it suggested conducting a similar study with cyber-attack data spanning longer time periods to provide more comprehensive insights.

Keywords: cybersecurity - cyberattacks - interactive platforms - geography of crime

المقدمة:

أدى ظهور التقنيات الحديثة في نظم المعلومات والتكنولوجيا الرقمية مثل انترنت الأشياء Internet of Things والحواجز المتسلسلة Block Chain وخدمات الحوسبة السحابية Cloud Services إلى ترابط غير مسبوق بين بلدان العالم والشركات والأفراد مما زاد من مخاطر الهجمات الالكترونية الخبيثة (بانقا، ٢٠١٩م، ص٧).

كما أدى دمج تكنولوجيا المعلومات والاتصالات في الحياة اليومية إلى تزايد التهديدات السيبرانية Cyber threats، ما دفع للبحث عن حلول وتقنيات أفضل لمكافحة التهديدات، وأدى بالمتخصصين

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

إلى دمج البيانات الجغرافية Geographical indications في التقنيات الحالية لتعزيز أنظمة البرمجيات والكشف عن مصادر ومواقع الهجمات السيبرانية Cyber attacks من خلال تدفق البيانات ومتابعة التحديات المستمرة التي تؤدي إلى تحسين عملية صنع القرار وتحديد الأولويات بشكل كبير.

كما تساهم نظم المعلومات الجغرافية GIS في دراسة تهديدات الأمن السيبراني Cyber threats لخلق الوعي بالمخاطر وايصال المعلومات المحورية حول تكرار التهديدات السيبرانية واكتشاف المنظمات والخدمات الأكثر استهدافا بهذه الهجمات. إضافة إلى اكتشاف التفاعلات المكانية Spatial interactions بين الدول المستهدَفة والدول المستهدِفة على حد سواء.

ويعد استخدام المنصات التفاعلية Interactive platforms التي تتعقب بيانات الهجمات السيبرانية، إحدى الوسائل المعينة للكشف عن الثغرات الأمنية التي تعتري مختلف الأنظمة على مستوى المنظمات والأفراد. كما تساعد على إنتاج الخرائط التفاعلية Interactive Maps التي توضح الهجوم الآني Instantaneous attack على مختلف أجهزة الدولة ومنظماتها، من خلال استخدام تقنيتي Real Time & Internet of Things.

وتعد المملكة العربية السعودية إحدى الدول التي عنيت بحماية فضائها السيبراني Cyber space، فأنشأت الهيئة الوطنية للأمن السيبراني في عام ١٤٣٩هـ، حيث قامت لاحقاً بإعداد ضوابط الأمن السيبراني للبيانات (DCC-1:2022) لوضع الحد الأدنى من متطلبات الأمن السيبراني لتمكين الجهات من حماية بياناتها خلال جميع مراحل دورة حياة البيانات (الهيئة الوطنية للأمن السيبراني،٢٠٢٢م).

وبالرغم من كافة الجهود لحماية الفضاء السيبراني من الهجمات السيبرانية إلا أن التقدم الكبير في مجال الذكاء الصناعي Artificial Intelligence واستخدام مختلف البرمجيات الحديثة Modern software، جعل جميع الدول في مختلف أرجاء العالم عرضة للاختراقات الأمنية، والهجمات الالكترونية بمختلف أشكالها، وهو ما يمثل حرب على اقتصاديات الدول وأمنها.

لذا جاءت هذه الدراسة للبحث في مشكلة فاعلية استخدام بيانات المنصات التفاعلية في التحليل المكاني للكشف عن الهجمات السيبرانية التي تستهدف الفضاء السيبراني للمملكة العربية السعودية.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

مشكلة الدراسة:

أدى الأقبال المتزايد على استخدام تقنيات الذكاء الصناعي Artificial Intelligence واستقبال وتحليل البيانات الضخمة Big Data مع الاستعانة بتقنيتي Real Time & Internet of Things إلى أن يصبح العالم أكثر ارتباطاً من خلال استخدام أنظمة الاتصالات والنظم الخبيرة Expert Systems، ما ساعد على استهداف الفضاء السيبراني Cyber space للدول واختراق مختلف أجهزتها والمساس بأمنها واقتصادها بل واختراق خصوصيات الأفراد، وهو ما أدى إلى نشوء مشكلات متعددة على مستوى الأمن الوطني والاجتماعي.

ما دفع المتخصصين لإنشاء المنصات السحابية التفاعلية ودمجها بتقنية نظم المعلومات الجغرافية السحابية Clouds GIS وذلك لتتبع مواقع الهجمات السيبرانية Cyber attacks وتحديد الأهداف على مستوى مختلف الدول وأجهزتها. وقد ساهمت الخرائط التفاعلية Interactive Maps في توضيح عمليات الهجوم في الوقت الآني Instant time، ورصدت كافة التفاعلات المكانية Spatial interactions لتلك العمليات بالاستعانة ببروتوكولات عناوين الأنترنت Internet address protocols.

وتعد المملكة العربية السعودية إحدى الدول التي تعاني من الهجمات السيبرانية على فضائها السيبراني من مختلف دول العالم والتي تستهدف مختلف خدمات المنشآت والقطاعات، كما تستهدف خدمات الأفراد. لذا جاءت هذه الدراسة للبحث في هذه المشكلة.

تساؤلات الدراسة:

جاءت هذه الدراسة للإجابة عن التساؤلات البحثية التالية:

١-ماهي أنواع الهجمات الالكترونية Cyber attacks على الفضاء السيبراني للمملكة العربية السعودية؟

٢-ماهي الدول الأكثر استهدافاً للمملكة العربية السعودية بالهجمات السيبرانية Cyber attacks؟

٣-ما هي القطاعات Sectors الأكثر استهدافاً بالهجمات السيبرانية في المملكة العربية السعودية؟

٤-ما مدى فاعلية استخدام بيانات المنصات التفاعلية لإجراء التحليلات المكانية Spatial analysis للهجمات السيبرانية على الفضاء السيبراني للمملكة العربية السعودية؟

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

أهداف الدراسة:

١-التعرف على أنواع الهجمات الالكترونية على الفضاء السيبراني للمملكة العربية السعودية.

٢-الكشف عن الدول الأكثر استهدافاً للمملكة العربية السعودية بالهجمات السيبرانية.

٣-التعرف على القطاعات الأكثر استهدافاً بالهجمات السيبرانية في المملكة العربية السعودية.

٤-الكشف عن مدى فاعلية استخدام بيانات المنصات التفاعلية لإجراء التحليلات المكانية Spatial analysis للهجمات السيبرانية على الفضاء السيبراني للمملكة العربية السعودية.

أهمية الدراسة:

١-تعد الدراسة إضافة علمية في مجال العلوم المكانية Spatial Sciences لسعيها لدراسة العلاقة التفاعلية بين نظم المعلومات الجغرافية السحابية Cloud GIS من خلال المنصات التفاعلية وتحليل البيانات السيبرانية في الوقت الآني Real Time.

٢-اتباع الاتجاهات الحديثة ضمن دراسة جغرافية الجريمة Geography of crime وربطها بالعلوم البينية كالأمن السيبراني Cyber Security، وذلك للكشف عن التفاعلات المكانية Spatial interactions.

٣-بناء خلفية علمية عن أهمية استخدام المنصات السحابية التفاعلية Interactive cloud platforms وأثرها في الكشف عن الهجمات السيبرانية Cyber attacks على مستوى المملكة العربية السعودية.

منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي التحليلي: الذي يركز على دراسة الظاهرة ووصفها وصفا دقيقا يعبر عنها كيفياً وكمياً، فالتعبير الكيفي يصف الظاهرة ويوضح خصائصها، اما التعبير الكمي فيعطيها وصفاً رقمياً يوضح مقدار هذه الظاهرة او حجمها او درجة ارتباطها مع الظواهر الأخرى (الحفظي، د.ت، ص٢).

بيانات الدراسة: تم جمع البيانات من المصادر التالية:

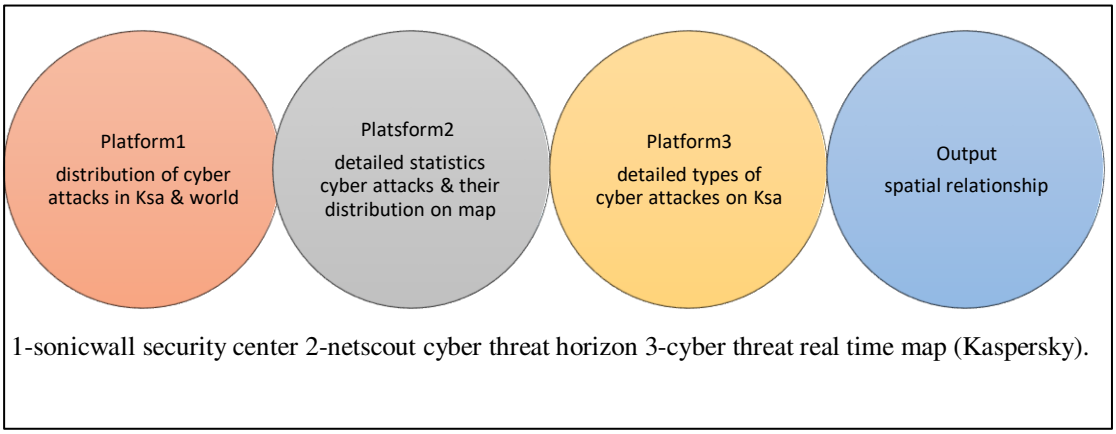
-بيانات المنصات التفاعلية: تم الاعتماد على البيانات الإحصائية من المنصات التالية:

Sonic wall security center- Digital Attack map- NetScout. Cyber threat horizon- Cyber threat Real-time map (Kaspersky).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

وقد تم استخلاص البيانات التالية: الإحصاءات الخاصة بنوعية الهجمات، الإحصاءات الخاصة بمواقع انطلاق الهجمات، الإحصاءات الخاصة بالمواقع المستهدفة بالهجمات، الإحصاءات الخاصة بالقطاعات المستهدفة. (شكل:١).

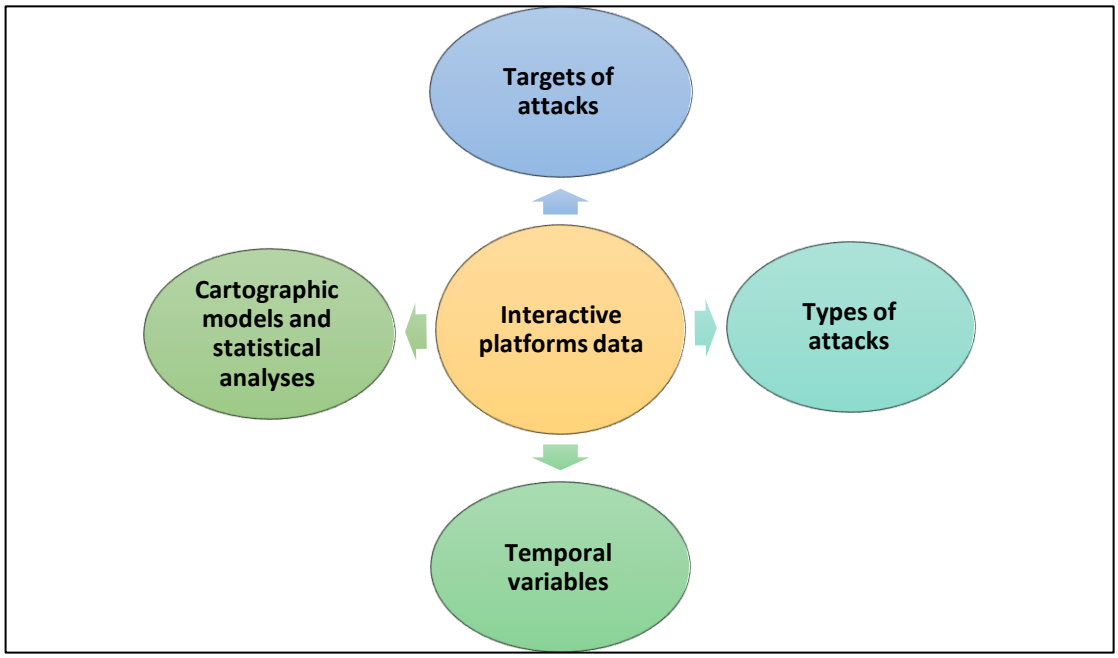
شكل (١) نموذج البيانات المكانية وفق المنصات التفاعلية



1-sonicwall security center 2-netscout cyber threat horizon 3-cyber threat real time map (Kaspersky).

ومن خلال هذه البيانات أمكن استخلاص النموذج التالي (شكل:٢).

شكل (٢) نموذج الدراسة



كما تم الاعتماد على البرامج التالية لتنفيذ عمليات تحليل البيانات واستخلاص النتائج:

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

-برنامج ARC GIS 10.8: تم الاعتماد على برنامج ARC GIS 10.8 لتحليل بيانات الدراسة لإيضاح الهجمات السيبرانية على الفضاء السيبراني للمملكة، مع تحديد مواقع الهجوم من مختلف دول العالم.

إجراءات الدراسة:

-تمت مراجعة كافة المنصات التفاعلية المذكورة في الشكل (١) وتحميل البيانات الخاصة بمعلومات الهجمات السيبرانية Cyber attacks لكافة دول العالم لعام ٢٠٢٣، تضمنت (أنواع الهجمات، أعدادها، القطاعات المستهدفة بالهجمات).

-تم الحصول على البيانات المكانية للهجمات السيبرانية على المملكة العربية السعودية من خلال منصة NetScout cyber threat horizon حيث إنها المنصة الوحيدة التي وفرت للباحثة بيانات دقيقة عن مواقع الهجمات على مختلف أجزاء المملكة ومناطقها، واحتوت المنصة على البيانات التالية (أنواع الهجمات، المدة الزمنية التي استغرقتها الهجمات بالدقائق والساعات، تاريخ وقوع الهجمات).

جدير بالذكر أن منصة NetScout cyber threat horizon تعُني بالكشف عن هجمات-(DDOS) Distributed Dential of Service-هجمات الحرمان من الخدمات، التي تصيب الشبكات أو السيرفرات المستضيفة لخدمات الانترنت الخاصة أو العامة، وهو ما من شأنه التأثير على الوضع الأمني أو الاقتصادي لخدمات الدولة أو الأفراد اللذين يتعرضون لهذا النوع من الهجمات، حيث تم رصد الهجمات التالية (DNS - TCP SYN- IPV4- Total Traffic-UDP -TCP IP Fragmentation- TCP ACK- L2TP Amplification- TCP RST-Amplification).

وقد تم الحصول على بيانات الهجمات السيبرانية التي تعرضت لها المملكة العربية السعودية لمدة شهر بداية من تاريخ ١-١٠ وحتى تاريخ ٣١-١٠-٢٠٢٣م وذلك من خلال منصة NetScout cyber threat horizon والتي وضحت المواقع الدقيقة للهجمات السيبرانية وهو ما تم الاعتماد عليه في عمليات التحليل المكاني.

-تم تصفية البيانات Data Filtering والاستبقاء على ما يخدم أهداف الدراسة ويجيب عن تساؤلاتها مثل: أسم المنصة التفاعلية، نوع الهجمات السيبرانية، تاريخ الهجمات السيبرانية، الدول المصدرة للهجمات السيبرانية، القطاعات المستهدفة بالهجمات، أوقات الهجمات السيبرانية، وتحليلها إحصائيا بواسطة برنامج SPSS.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

-الدراسات السابقة:

اهتمت قلة من الدراسات بدراسة العلاقة بين الجرائم الالكترونية أو جرائم الأمن السيبراني بالتركيز على الأبعاد المكانية منها:

دراسة (Du & Yang, 2013) التي تناولت التحليلات الزمانية والمكانية للهجمات السيبرانية واسعة النطاق، وقد سعت الدراسة إلى وصف الهجمات السيبرانية والتنبؤ بها، ومناقشة التحليلات الزمنية والمكانية المتكاملة لتحليل الهجمات واسعة النطاق، وقد استخدمت الدراسة تطبيق فكرة مركزية الدرجة والتجمع الهرمي التكتلي.

وقد توصلت إلى العديد من النتائج كان أهمها: اكتشاف أنواع مختلفة من الهجوم ما سمح بظهور عدد من الأنماط المكانية التي ساهمت في وضع مخطط لتصنيف مصادر الهجوم في مختلف الفترات الزمنية. كما تم إثبات فاعلية تطوير نماذج ماركوف لتمييز واستنتاج الهجوم السيبراني.

أما (Amin, Sevil, Kocak & Francia, Hoover, 2020) فقد تناولوا التحليل المكاني للموارد الموحدة الضارة بالاعتماد على محددات الموقع لعناوين URL دراسة حالة مجموعة البيانات لعام ٢٠١٦م. وقد جاءت الدراسة بهدف تحديد التجمعات المكانية للبلدان التي لديها معدلات عالية من الهجمات عبر الانترنت، حيث تم الحصول على مجموعة بيانات الهجوم السيبراني من المعهد الكندي للأمن السيبراني، وقد تم استخدام برنامج Sat scan TM لإجراء التحليلات المكانية لبلد الهجوم.

كما جاءت الدراسة بغرض الإجابة عن بعض التساؤلات منها: ماهي الدول التي تتصدر قائمة منشأ الهجمات السيبرانية، من حيث عددها؟ وما هي الدول التي تأتي في مقدمة مصادر الهجمات السيبرانية من حيث المخاطر النسبية؟ وهل تختلف النقاط المكانية الساخنة لأصل الهجوم السيبراني عن المخاطر المكانية للنقاط الساخنة للهجوم السيبراني؟

وقد خرجت الدراسة بعدد من النتائج كان أبرزها: أثبات جدوى التحليلات المستخدمة في الدراسة كأداة للأمن السيبراني، كما ثبت أنه بالإمكان التعامل مع تحليل بيانات الأمن السيبراني باستخدام مختلف الأدوات والأساليب. كما أوصت الدراسة بإمكانية إجراء دراسة على نفس البيانات بهدف الكشف عن الاتجاهات الموضوعية للمخاطر وخطط الدفاع والهجمات السيبرانية.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

كما تناول (Molla & Dawood, Veerasamy, 2023) تطبيق البيانات الجغرافية المكانية في الأمن السيبراني، وقد جاءت الدراسة بهدف استكشاف فائدة البيانات الجغرافية المكانية للأمن السيبراني، إضافة إلى السعي للبحث في مجالات التطبيق الرئيسية التي يمكن أن تقدمها البيانات الجغرافية المكانية في مجال الأمن السيبراني، والسعي لتوليد أفكار حول التقنيات الجديدة التي يمكن استخدامها لتمثيل الأمن السيبراني. وسعت الدراسة للإجابة عن تساؤلات عدة كان أهمها: ماهي مواقع مصادر الهجمات؟ وماهي مواقع البنية التحتية الوسيطة في الهجمات السيبرانية؟ وماهي الأساليب الرئيسة المستخدمة؟

وقد توصلت الدراسة لعدد من النتائج كان أهمها: إثبات فاعلية استخدام البيانات الجغرافية المكانية للأمن السيبراني، وتحديد بيانات التهديد السيبراني مثل مواقع الهجمات وعددها ونسبتها وتاريخ الهجوم.

أما دراسة (Chen, Hao, Ding & Jiang, Dong, Zhang & Guo,Gao,2023) فقد سعت إلى استكشاف النظام الجغرافي العالمي للجرائم السيبرانية والقوى الدافعة لها، حيث استخدمت الدراسة النماذج الخطية المعممة (GLMS) وهو امتداد لنموذج الانحدار المنتظم الذي يتضمن توزيع الاستجابة غير العادية ووظائف النمذجة.

وقد خرجت الدراسة بعدد من النتائج كان أهمها: أدى البحث عن التوزيع المكاني لعناوين IP الخاصة بالجرائم الالكترونية إلى الكشف عن التباين المكاني الكبير على المستوى العالمي. كما ثبت عند إجراء تقييم الملاءمة الشاملة علاقة جيدة أدت إلى تأكيد الفرضيات في النموذج المفاهيمي، حيث جاءت جميع العلاقات ذات دلالة إحصائية، كما ثبت ارتفاع الانحراف المعياري للعوامل السياسية والأمن السيبراني، إضافة إلى إثبات ارتفاع الآثار المباشرة للعوامل الاجتماعية والاقتصادية على الجرائم السيبرانية.

التحليل والمناقشة:

تعد مناقشة الهجمات السيبرانية إحدى القضايا ذات الأبعاد الهامة والمؤثرة على أمن واقتصاديات الدول والأفراد، لذا يأتي هذا الجزء من الدراسة لمناقشة المشكلة على مستوى العالم مع التركيز على المملكة العربية السعودية وفق المحاور التالية:

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

المحور الأول: تحليل الهجمات السيبرانية على مستوى العالم:

أولا: تحليل الهجمات السيبرانية حسب شهور السنة:

أثبتت نتائج تحليل جدول (١) الخاص باستعراض عدد الهجمات السيبرانية على مستوى العالم خلال عام ٢٠٢٣م، والنصف الأول من عام ٢٠٢٤م، تقارب عدد الهجمات السيبرانية خلال كافة شهور السنة، حيث أثبتت النتائج أنه بالرغم من تعرض مختلف دول العالم إلى ملايين الهجمات، إلا أنه لم يكن هناك فارق كبير في عدد الهجمات بين مختلف شهور السنة، مما يعني إنه لا يوجد تركيز على شهر معين دون غيره لزيادة عدد الهجمات السيبرانية.

جدول (١) عدد الهجمات السيبرانية على مستوى العالم خلال عام ٢٠٢٣م ومنتصف ٢٠٢٤م

Month	2023 Million	2024 Million
JAN	445.56	579.87
FEB	373.63	468.18
MAR	459.53	558.69
APR	414.23	716.19
MAY	494.28	-
JUN	575.52	-
JUL	695.48	-
AUG	532.76	-
SEP	474.48	-
OCT	750.48	-
NOV	625.66	-
DEC	625.28	-

المصدر: من عمل الباحثة بناء على التقرير الأمني الصادر من Sonic wall security center للعام ٢٠٢٣م. النشرة الأمنية الصادرة من Sonic wall security center للنصف الأول من العام ٢٠٢٤م.

ثانيا: التحليل الجغرافي للهجمات السيبرانية حسب نوع الهجوم:

أثبتت نتائج تحليل جدول (٢) أن الولايات المتحدة الامريكية قد تصدرت كافة دول العالم في إرسال الهجمات السيبرانية، وخاصة هجمات البريد العشوائي (Spam volume)، وهجمات التصيد الاحتيالي (Phishing volume) وبرامج الفدية (Ransomware) بنسبة بلغت (٨٠%) و (٧٩%) و (٧٥%) من إجمالي الهجمات السيبرانية على مستوى العالم على التوالي.

كما جاءت دولة الهند ثانياً في تصدر الهجمات السيبرانية وخصوصاً من نوع Crypto jacking، وهو نوع من الجرائم الالكترونية التي تنطوي على الاستخدام غير المصرح به لأجهزة الكمبيوتر، والهواتف الذكية أو الأجهزة اللوحية أو حتى الخوادم من قبل مجرمي الانترنت لاستخراج العملات المشفرة بدافع الربح، حيث بلغت هذه الجرائم (٢٧%)، فيما جاءت جرائم التصيد الاحتيالي

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

(Phishing volume) ثانياً بنسبة (٢٣%)، مما يدلل على أن غالبية الهجمات ربما كانت بدافع القرصنة الاقتصادية أو لأغراض سياسية.

جدول (٢) التوزيع المكاني للهجمات السيبرانية على مستوى العالم

الدولة	النسبة المئوية (%) للهجمات السيبرانية حسب نوعها								
	Malware	Intrusion	Ransomware	Https1	Spam2	Phishing3	Crypto4	Malware5	IOT6
USA	59	43	75	27	80	79	43	35	0
China	5	0	0	0	0	0	0	0	0
United Kingdom	5	0	0	24	0	0	0	6	0
India	4	0	23	0	0	0	27	0	0
Unknown	0	0	0	22	0	0	0	0	0
The Netherland	0	21	0	0	0	0	0	0	17
Romania	0	8	0	0	0	0	0	0	0
Poland	0	4	0	0	0	0	0	0	47
Germany	0	0	0	0	8	0	0	0	0
Canda	0	0	0	5	3	4	3	0	0
Brazil	0	0	0	0	3	3	0	0	0
Chile	0	0	0	0	0	3	23	0	0
Liechtenstein	0	0	0	0	0	0	0	29	0
Argentina	0	0	0	0	0	0	0	5	0
Switzerland	0	0	0	0	0	0	0	0	9
Bulgaria	0	0	0	0	0	0	0	0	8
Others	27	24	2	22	7	11	4	25	19
SUM	100	100	100	100	100	100	100	100	100

المحور الثاني: تحليل الهجمات السيبرانية على مستوى المملكة العربية السعودية:

يعد البحث عن تحليل الهجمات السيبرانية على مستوى الدولة الواحدة من العوامل التي تعين الباحثين على استكشاف مواضع الخلل والضعف في البنية الرقمية الحيوية، مما يساعد في توجيه الخطط العلاجية للتقليل من مخاطر الهجمات بل ومعالجة مواضع الضعف في مختلف الأنظمة والقطاعات، لذا يأتي هذا الجزء من الدراسة لتحليل الهجمات السيبرانية التي تعرضت لها المملكة العربية السعودية للفترة من تاريخ ١-١٠ وحتى تاريخ ٣١-١٠-٢٠٢٣م. ويأتي التركيز على هذه الفترة تحديداً لأنها البيانات التي تمت إتاحتها للباحثة من منصة NetScout cyber threat horizon، حيث عُنيت هذه المنصة بتحديد التوزيع الجغرافي للهجمات السيبرانية حسب عناوين بروتوكولات الانترنت IP التي تعرضت للهجوم، مما يجعل تحديد مواقع الهجمات دقيقاً ويمكن الاعتماد عليه لتحليل نتائج هذه الدراسة.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

أولا: القطاعات الأكثر استهدافاً بالهجمات السيبرانية في المملكة العربية السعودية خلال النصف الثاني من عام ٢٠٢٣م:

اتضح من تحليل جدول (٣) الخاص باستعراض القطاعات الأكثر استهدافاً بالهجمات السيبرانية على مستوى المملكة العربية السعودية للنصف الثاني من العام ٢٠٢٣م. استهداف قطاع الاتصالات السلكية واللاسلكية وقطاع الاتصالات عبر الأقمار الصناعية، وبالنظر لمتوسط مدة الهجوم نجد أنه تراوح بين ٨-١٧ دقيقة، مما يدل على وجود بعض الثغرات الأمنية التي يستغلها المهاجمين للقيام بسرقة البيانات وعمليات القرصنة. وربما يأتي التركيز على هذه القطاعات بسبب عمليات الحوكمة الالكترونية لكافة الأنظمة في المملكة العربية السعودية، مما يجعل استهداف هذه القطاعات أمراً غير مستغرب خاصة في ظل تحول المملكة وفق رؤية ٢٠٣٠م ومحاولة المهاجمين تعطيل قطاع الاتصالات بشكل عام للتأثير على الوضع الاقتصادي والأمني للمملكة العربية السعودية. فيما انخفضت الهجمات السيبرانية الموجهة إلى أجهزة تخزين الكمبيوتر ورحلات الطيران المجدولة بالرغم من ارتفاع متوسط مدة الهجوم على كلا القطاعين بما يتراوح بين ٥٦-٧٩ دقيقة.

جدول (٣) القطاعات الأكثر استهدافا بالهجمات السيبرانية في المملكة العربية السعودية خلال النصف الثاني من عام ٢٠٢٣م

القطاع المستهدف	التكرار	اعلى هجوم للبيانات	اعلى تأثير للبيانات	متوسط مدة الهجوم
الاتصالات السلكية واللاسلكية	136.220	416.6 Gbps	60.36 Mpps	17 Minutes
الاتصالات عبر الأقمار الصناعية	99.809	123.27 Gbps	11.25 Mpps	8 Minutes
ناقلات الاتصالات اللاسلكية	708	28.64 Gbps	2.89 Mpps	21 Minutes
شركات تجميع وتصنيع الكمبيوترات	274	9.45 Gbps	1.5 Mpps	10 Minutes
معالجة البيانات والاستضافة والخدمات ذات الصلة	168	4.45 Gbps	8.52 Mpps	21 Minutes
أجهزة تخرين الكمبيوتر	88	6.08 Gbps	1.14 Mpps	79 Minutes
رحلات الطيران المجدولة	32	0.1 Gbps	0.2 Mpps	56 Minutes
خدمات الكمبيوتر	25	14.91 Gbps	1.81 Mpps	4 Minutes
النشر والبث عبر الانترنت وبوابات البحث على الويب	16	2.03 Gbps	0.2 Mpps	7 Minutes

المصدر: من عمل الباحثة بناء على النشرة الأمنية الصادرة من Nets count DDOS Threat Intelligence, (2023).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

ثانيا: تحليل الهجمات السيبرانية على المملكة العربية السعودية للفترة من ١|٣١-١٠-٢٠٢٣م.

١-أنواع الهجمات السيبرانية:

بتحليل جدول (٤) يتضح تساوي نسبة هجمات Total Traffic التي تستهدف تعطيل حركة مرور الانترنت بجعله غير متاح للمستخدمين، مع الهجمات السيبرانية المتعددة Multiple attacks التي تعرض لها الفضاء السيبراني للمملكة لتبلغ (٣٢,٧%)، مما يدل أنه ربما استهدفت تلك الهجمات الخدمات الحكومية وخدمات القطاع الخاص أو خدمات الأفراد لغرض سرقة البيانات أو عمليات التجسس الإلكترونية او لأغراض سياسية. وجاءت هجمات DNS Amplification ثانياً بنسبة بلغت (١٣%) ومن المعروف أن هذا النوع من الهجمات يستهدف منع المستخدمين من الوصول إلى نظام أو خدمة أو موقع ويب عن طريق تعطيله تماماً، مما يقود لاستنتاج أن هذا النوع من الهجوم ربما يستهدف البنية الرقمية الحيوية لكل من خدمات القطاعين الخاص والعام، التي تعد ركيزة رؤية المملكة ٢٠٣٠م.

فيما سجلت هجمات L2TP Amplification، TCP ACK، IP Fragmentation، نسباً منخفضة جدا بين باقي الهجمات، لذا ينبغي التركيز على دراسة وتحليل البيانات لفترات زمنية تتجاوز الشهر للمساهمة في الحكم على دقة النتائج.

جدول (٤) أنواع الهجمات السيبرانية المهاجمة للفضاء السيبراني للمملكة العربية السعودية للفترة من ١|٣١-١٠-٢٠٢٣م.

أنواع الهجمات السيبرانية	العدد	%
TCP	99	4.8
L2TP Amplification	3	0.1
TCP ACK	6	0.3
IP Fragmentation	2	0.1
Total Traffic	669	32.7
IPV4	87	4.3
UDP	208	10.2
TCP SYN	24	1.2
DNS Amplification	265	13
Multiple attacks	668	32.7
TCP RST	12	0.6
Total	2043	100

المصدر: من عمل الباحثة بناء على التقرير الأمني الصادر من (Nets count DDOS Threat Intelligence, 2023).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

٢-المدة المستغرقة للهجمات السيبرانية.

بتحليل جدول (٥) يتضح أن غالبية الهجمات السيبرانية (٦٢,٨%) قد استغرقت بين (١-١٠ دقائق)، حيث كانت غالبية الهجمات من نوع Total Traffic بنسبة بلغت (٢٩,٢%) بين باقي الهجمات، (جدول: ٦). فيما جاءت ثانياً الهجمات التي استغرقت بين (١١-٢٠ دقيقة) لتبلغ (١٩,٦%) من إجمالي الهجمات، سجلت الهجمات المتعددة Multiple attacks وهجمات DNS Amplification الصدارة بين باقي الهجمات التي استغرقت هذا الزمن.

وتجدر الإشارة إلى أن الهجمات التي تعرضت لها المملكة خلال فترة الدراسة من نوع الهجمات القصيرة، إلا أن هذا لا ينفي تعرض فضاء المملكة السيبراني إلى خطر سياسي وأمني بل واقتصادي جراء هذه الهجمات، خاصة إذا ما اقترنت بالخطر الجيوسياسي الذي تتعرض له حدود المملكة الشمالية والجنوبية على حداً سواء، مما يبرر تزايد الهجمات السيبرانية من نوع Total Traffic وMultiple attacks وذلك للإضرار بمصالح المملكة.

وبتتبع نتائج تحليل العلاقة بين الزمن المستغرق للهجمات السيبرانية وبين أنواع الهجمات السيبرانية أثبت التحليل الاحصائي لقيمة كاي تربيع النسبية الاحتمالية (٨٢٣,٧٨١) وجود فروق جوهرية بين المتغيرين عند مستوى دلالة (٠,٠٠٠)، بدرجة بلغت (٠,٣٠٦) لمعامل كريمر عند مستوى دلالة (٠,٠٠٠) وهي علاقة تعد متوسطة بين المتغيرين.

جدول (٥) الزمن المستغرق للهجمات السيبرانية

الزمن المستغرق	العدد	%
10-1	1283	62.8
20-11	401	19.6
30-21	120	5.9
40-31	44	2.2
50-41	33	1.6
59-51	29	1.4
more than an hour	133	6.5
Total	2043	100

المصدر: من عمل الباحثة بناء على التقرير الأمني الصادر من Nets count DDOS Threat Intelligence, (2023).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

جدول (٦) العلاقة بين نوع الهجمات السيبرانية والزمن المستغرق للهجمة

نوع الهجمة		الزمن المستغرق للهجمة بالدقائق (M) والساعات (H)						
		10-1 M	20-11 M	M30-21	M40-31	M50-41	M59-51	More 1 H
TCP	العدد	11	17	13	4	4	0	50
	%	0.5	0.8	0.6	0.2	0.2	0	2.4
L2TP Amplification	العدد	3	0	0	0	0	0	0
	%	0.1	0	0	0	0	0	0
TCP ACK	العدد	1	5	0	0	0	0	0
	%	0.0	0.2	0	0	0	0	0
IP Fragmentation	العدد	2	0	0	0	0	0	0
	%	0.1	0	0	0	0	0	0
Total Traffic	العدد	596	43	14	3	0	5	8
	%	29.2	2.1	0.7	0.1	0	0.2	0.4
IPV4	العدد	10	14	10	25	9	0	19
	%	0.5	0.7	0.5	1.2	0.4	0	0.9
UDP	العدد	122	50	19	6	0	10	1
	%	6	2.4	0.9	0.3	0	0.5	0
TCP SYN	العدد	23	1	0	0	0	0	0
	%	1.1	0	0	0	0	0	0
DNS Amplification	العدد	127	58	31	0	10	9	30
	%	6.2	2.8	1.5	0	0.5	0.4	1.5
Multiple attacks	العدد	379	210	33	6	10	5	25
	%	18.6	10.3	1.6	0.3	0.5	0.2	1.2
TCP RST	العدد	9	3	0	0	0	0	0
	%	0.4	0.1	0	0	0	0	0
Total	العدد	1283	401	120	44	33	29	133
	%	62.8	19.6	5.9	2.2	1.6	1.4	6.5
Likelihood Ratio	Value				Significance			
	823.781				0.000			
Cramer's V	.306				0.000			

المصدر: من عمل الباحثة بناء على التقرير الأمني الصادر من (Nets count DDOS Threat Intelligence, 2023).

٣-التحليل الجغرافي للهجمات السيبرانية المستهدفة للفضاء السيبراني للملكة العربية السعودية.

وضحت نتائج تحليل جدول (٧) أن المملكة العربية السعودية قد تعرضت لنوعين من الهجمات السيبرانية تم تصنيفها إلى (هجمات داخلية، هجمات خارجية) بناء على مصادر الهجمات. وقد تفوقت الهجمات ذات المصادر الخارجية في نسبتها فبلغت (٨٤,٩%)، فيما بلغت نسبة الهجمات ذات المصدر الداخلي التي يديرها مهاجمين من داخل المملكة (١٥,١%).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

جدول (٧) توزيع الهجمات السيبرانية على المملكة العربية السعودية حسب مصادر الهجمات

مصدر الهجمات	العدد	%
داخلي من داخل المملكة	308	15.1
خارجي من خارج المملكة	1735	84.9
المجموع	2043	100

المصدر: من عمل الباحثة بناء على التقرير الأمني الصادر من (Nets count DDOS Threat Intelligence, 2023).

جدير بالذكر أن المملكة العربية السعودية قد تعرضت لهجمات سيبرانية من ٧٠ دولة من مختلف أنحاء العالم، منها ٧ دول تزايدت هجماتها عن (٥١ هجمة)، بنسبة بلغت (٥٧,٧%)، تصدرت بعض دول الاتحاد الأوروبي والولايات المتحدة الامريكية والامارات العربية المتحدة قائمة الدول المهاجمة. وتعد هذه نتيجة طبيعية نظراً للتقدم التكنولوجي لتلك الدول، خاصة الولايات المتحدة الامريكية التي بلغت نسبة هجماتها منفردة (٢٠%)، وهو أمر غير مستغرب في ظل رغبة الولايات المتحدة في السيطرة على كافة دول العالم، من خلال الاستحواذ على المعلومات السرية أو تعطيل حركة الملاحة أو الخدمات أو القيام بعمليات القرصنة للبيانات الحيوية، خاصة إذا ما تعلق الأمر بالمملكة العربية السعودية التي تعد في طليعة الدول المؤثرة على مستوى العالم لمكانتها الدينية ولامتلاكها للثروة النفطية، كما تحظى المملكة بتأثير كبير على الصعيدين العربي والإسلامي، مما يجعل استهداف فضائها السيبراني لأغراض أمنية وسياسية واقتصادية أمر وارد، (جدول: ٨).

جدول (٨) الدول المهاجمة للمملكة العربية السعودية

منشئ الهجمات	تكرار الهجمات	عدد الهجمات	%
بلجيكا- تايلاند- سوريا- كولومبيا- استونيا- فنلندا- بورندي- المجر- اسبانيا- بلغاريا- رومانيا- ماليزيا- المغرب- بولندا- فلسطين- سيشل- النرويج- المكسيك- سويسرا- كوريا الجنوبية- قبرص- كندا- الجزائر- الارجنتين- الكويت- تايوان- البرتغال- صربيا- سلوفاكيا- كينيا- سلوفانيا- الاكوادور- سلطنة عمان- إيران- لتوانيا- كرواتيا- بنما- بنجلاديش- نيجيريا- لاتفيا- إيطاليا- الدنمارك- جنوب افريقيا- اليابان.	10-1	142	8.2
باكستان- كوريا الشمالية- السويد- الفلبين- الأردن	20-11	68	3.9
استراليا- أوكرانيا- تركيا- البرازيل- النمسا- الهند	30-21	160	9.2
مصر- روسيا- فيتنام	40-31	113	6.5
الصين- سنغافورة- البحرين- قطر- إيطاليا	50-41	251	14.5
المانيا- فرنسا- اندونيسيا- الولايات المتحدة الامريكية- الامارات العربية المتحدة- هولندا- المملكة المتحدة	51 MORE	1001	57.7
المجموع		1735	100

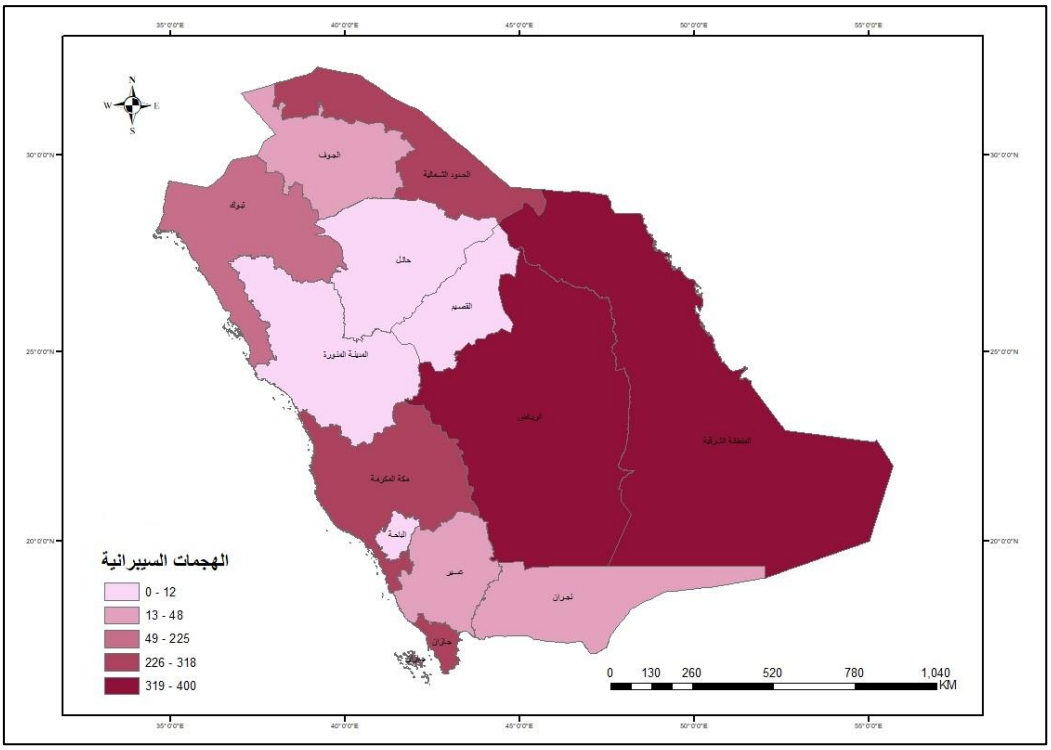
المصدر: من عمل الباحثة بناء على التقرير الأمني الصادر من (Nets count DDOS Threat Intelligence, 2023).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

٤- التحليل الجغرافي للهجمات السيبرانية على مستوى المملكة العربية السعودية.

أظهرت نتائج تحليل جدول (٩) عند مناقشة التحليل الجغرافي للهجمات السيبرانية على مستوى المملكة العربية السعودية، ارتفاع نسبة الهجمات السيبرانية التي استهدفت البنية الرقمية الحيوية في وسط المملكة حيث بلغت (٢٠,٢%)، ولعل في هذه النتيجة تحديداً ما يؤيد أن الهجمات السيبرانية على وسط المملكة جاءت لأغراض جيوسياسية، خاصة إن المنطقة الوسطى تتضمن العاصمة السياسية للدولة (الرياض)، مما يجعل التركيز على فضائها السيبراني أمر في غاية الأهمية في عمليات الهجوم وقرصنة البيانات التي من شأنها التأثير على الأمن الوطني والاقتصادي-الاجتماعي، (شكل: ٣).

شكل (٣) توزيع الهجمات السيبرانية على المملكة العربية السعودية



المصدر: من عمل الباحثة بناء على بيانات الدراسة ٢٠٢٣م.

فيما جاء استهداف الأجزاء الشرقية ثانياً، بنسبة بلغت (١٨,١%) من إجمالي الهجمات. وهو أمر غير مستغرب خاصة أن المنطقة الشرقية تعد مركزً للطاقة الرئيسية للمملكة العربية السعودية وتتضمن أكبر حقول النفط البرية والبحرية (الغوار، والسفانية)، كما أنها تتمتع ببنية تحتية عالية

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

المستوى للنقل والخدمات اللوجستية، مما يقود لاستنتاج أن تلك الهجمات السيبرانية ربما جاءت بغرض الحاق الاضرار بالبنية التحتية للمنطقة، إضافة لإلحاق الاضرار باقتصاد المملكة.

على حين سجلت الأجزاء الجنوبية الغربية أدنى الهجمات السيبرانية بنسبة (٢,٢%)، ولا يعد انخفاض الهجمات على هذه الأجزاء مؤشراً ذا دلالة، ربما بسبب تركيز الدراسة على فترة زمنية محددة، مما يستوجب دراسة المشكلة بصورة مستفيضة بالتركيز على فترات زمنية تتجاوز الشهر للحكم على دقة النتائج.

جدول (٩) توزيع الهجمات السيبرانية على مستوى المملكة العربية السعودية

المنطقة	العدد	%
الشمال	325	15.9
الجنوب	348	17
شرق	370	18.1
غرب	318	15.6
وسط	412	20.2
شمال غرب	225	11
جنوب غرب	45	2.2
المجموع	2043	100

-تحليل العلاقة بين نوع الهجمات وموقعها الجغرافي:

يتضح من تحليل جدول (١٠) أن الأجزاء الشمالية والجنوبية من المملكة العربية السعودية قد سجلت نسبة متساوية (٤,٧%) للهجمات من نوع Total Traffic. فيما تزايدت هجمات Total Traffic على المنطقة الوسطى فبلغت (٧,٦%). ولعل في هذه النتيجة ما يؤيد أن الهجمات السيبرانية جاءت لاستهداف البنية الرقمية الحيوية لغرض تعطيل الخدمات العامة والخاصة، وتكبيد المملكة خسائر فادحة، (شكل: ٤، ٥، ٦، ٧، ٨، ٩).

فيما تعرضت المملكة للهجمات المتعددة Multiple attacks على كافة أجزاءها المشمولة بالدراسة وبنسب متقاربة تراوحت بين (٤,٥%) في المنطقة الشمالية، (٥,٦%) في المنطقة الجنوبية، (٥,٧%) في المنطقة الشرقية، (٦%) على المنطقة الوسطى، ولعل في هذه النتائج ما يدل أن فضاء المملكة السيبراني قد تم استهدافه لأغراض جيوسياسية واقتصادية.

في حين انخفضت هجمات TCP ACK، IP Fragmentation، TCP SYN، TCP RST على كافة أجزاء المملكة، ويعزى الانخفاض إلى محدودية بيانات الدراسة واقتصارها في التحليل على مدة

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

محددة لم تتجاوز الشهر، مما يدفعنا إلى ضرورة التنويه على أهمية إجراء دراسات أخرى مشابهة تتضمن تحليل الهجمات السيبرانية على مدار العام.

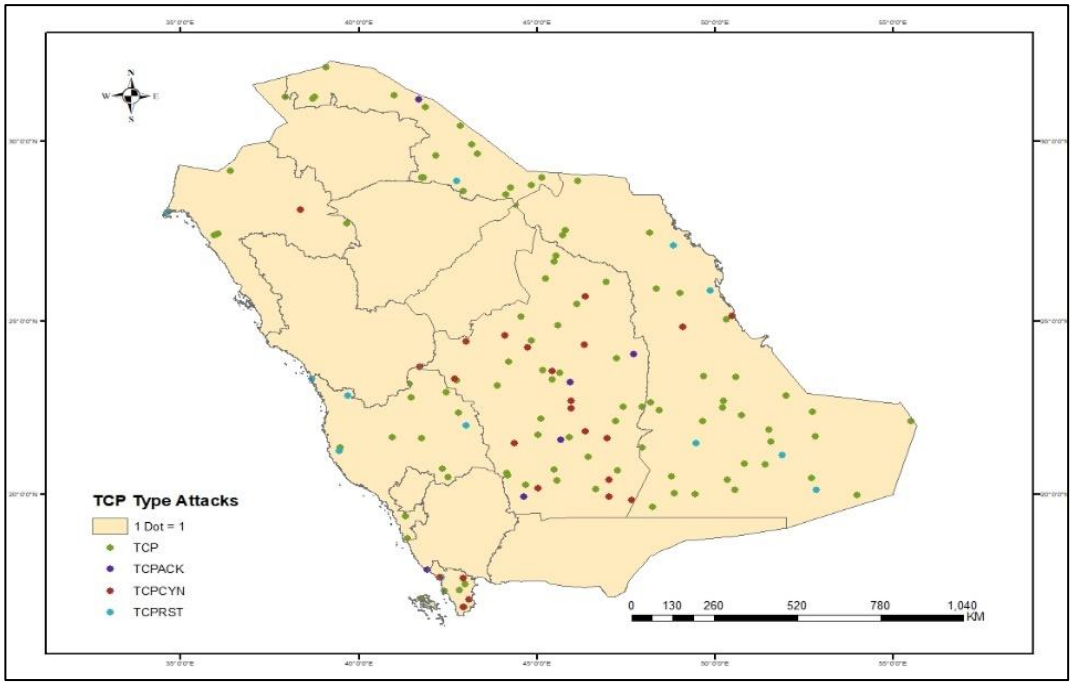
جدول (١٠) توزيع الهجمات السيبرانية على المملكة العربية السعودية

نوع الهجمات		توزيع الهجمات السيبرانية على مستوى المملكة						
		شمال	جنوب	شرق	غرب	وسط	شمال غرب	جنوب غرب
TCP	العدد	17	5	33	11	29	4	0
	%	0.8	0.2	1.6	0.5	1.4	0.2	0
L2TP Amplification	العدد	0	1	0	0	0	2	0
	%	0.0	0.0	0	0	0	0.1	0
TCP ACK	العدد	1	1	0	0	4	0	0
	%	0.0	0.0	0	0	0.2	0	0
IP Fragmentation	العدد	0	0	0	1	0	1	0
	%	0.0	0	0	0.0	0	0	0
Total Traffic	العدد	96	95	128	83	156	87	24
	%	4.7	4.7	6.2	4.1	7.6	4.3	1.2
IPV4	العدد	19	34	2	15	16	1	0
	%	0.9	1.7	0.1	0.7	0.8	1.1	0
UDP	العدد	44	36	26	49	40	12	1
	%	2.2	1.8	1.2	2.4	2	0.6	0
TCP SYN	العدد	0	4	2	0	17	1	0
	%	0.0	0.2	0.1	0	0.8	0	0
DNS Amplification	العدد	55	57	57	32	43	16	5
	%	2.7	2.8	2.7	1.6	2.1	0.8	0.2
Multiple attacks	العدد	92	114	117	123	107	100	15
	%	4.5	5.6	5.7	6	5.2	4.9	0.7
TCP RST	العدد	1	1	5	4	0	1	0
	%	0.0	0.0	0.2	0.2	0	0	0
الإجمالي	العدد	325	348	370	318	412	225	45
	%	15.9	17	18.1	15.6	20.2	11	2.2

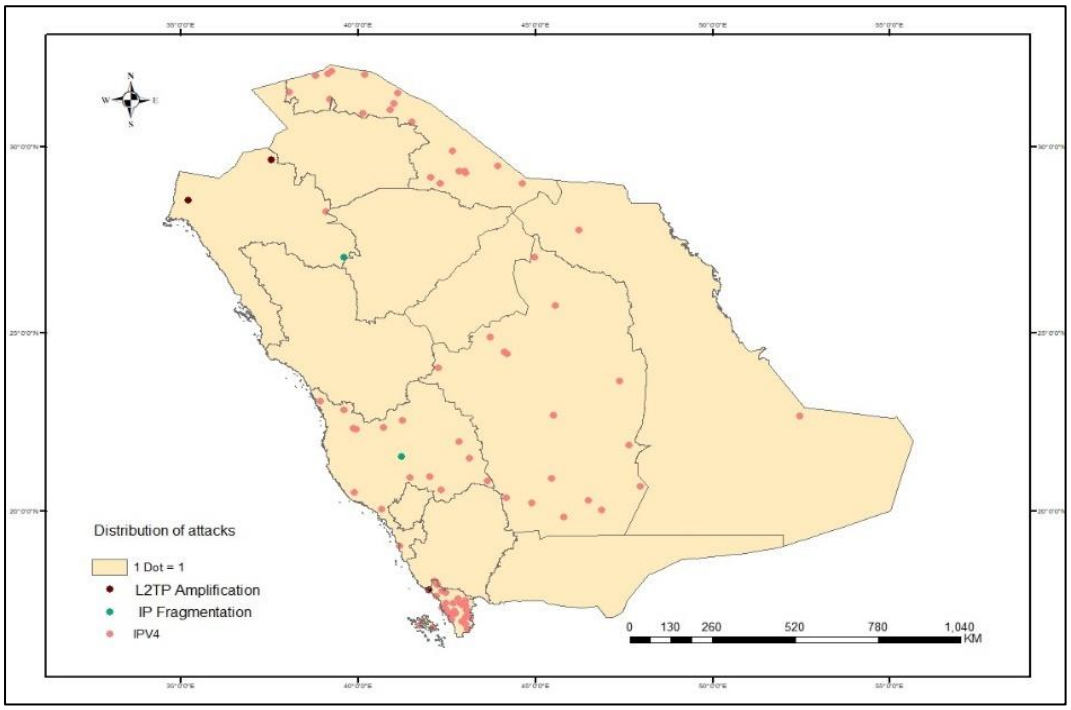
المصدر: من عمل الباحثة بناء على التقرير الأمني الصادر من (Nets count DDOS Threat Intelligence, 2023).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

شكل (٤) توزيع الهجمات السيبرانية من نوع TCP



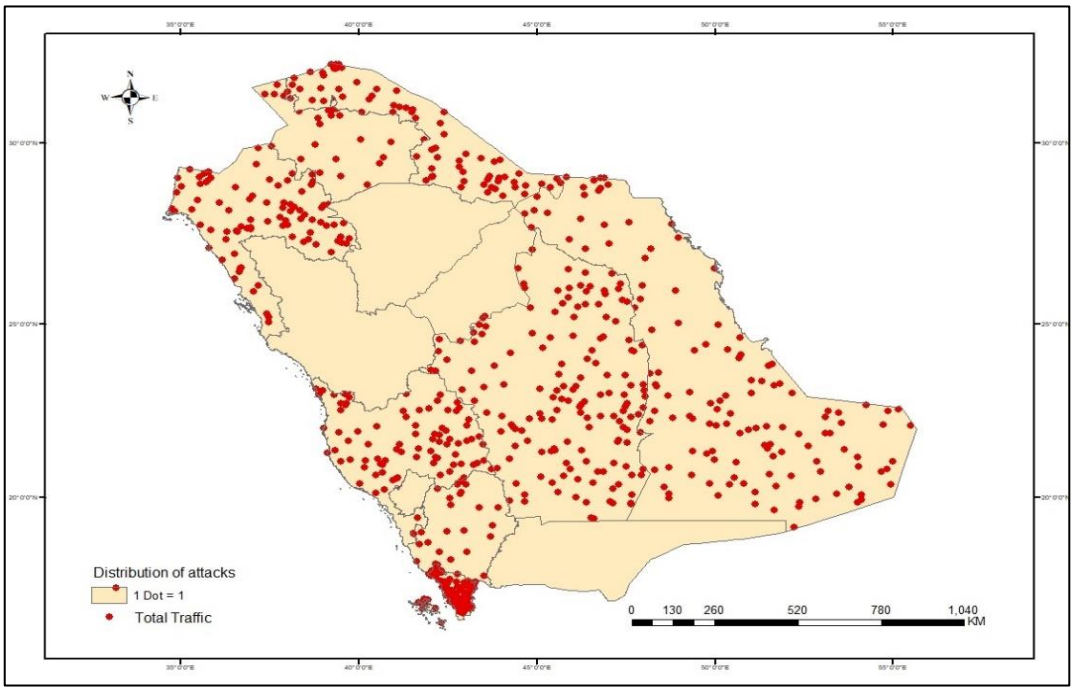
شكل (٥) توزيع الهجمات السيبرانية من نوع L2TP- IP Fragmentation-IPV4



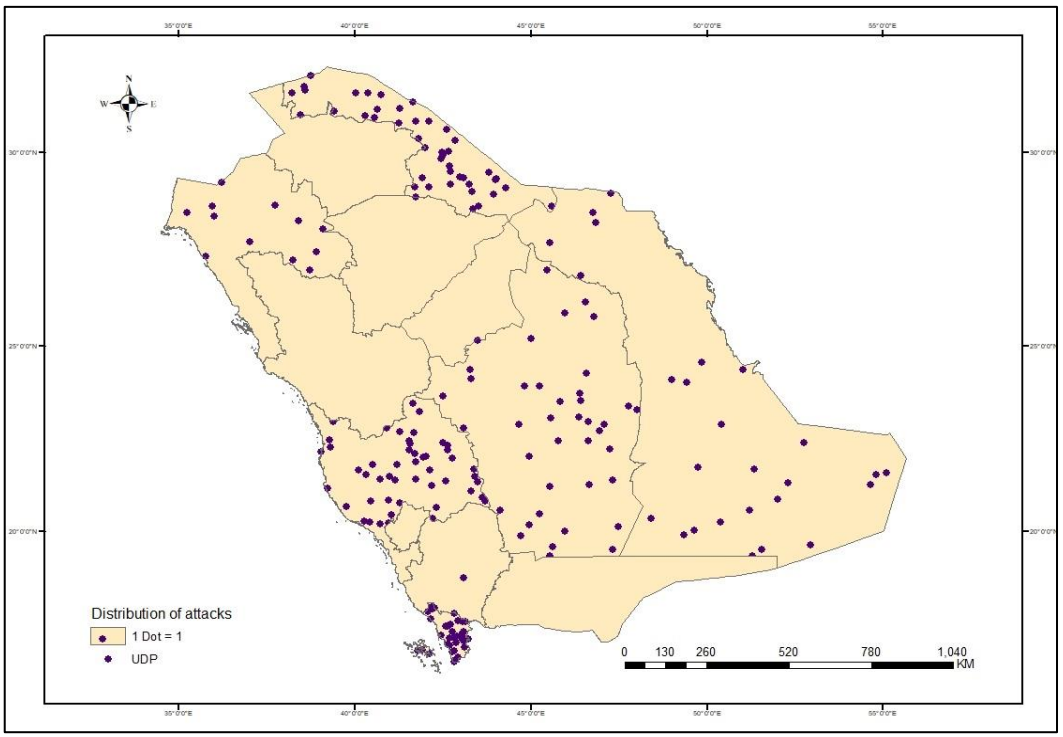
المصدر: من عمل الباحثة بناء على بيانات الدراسة ٢٠٢٣م.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

شكل (٦) توزيع الهجمات السيبرانية من نوع Total Traffic



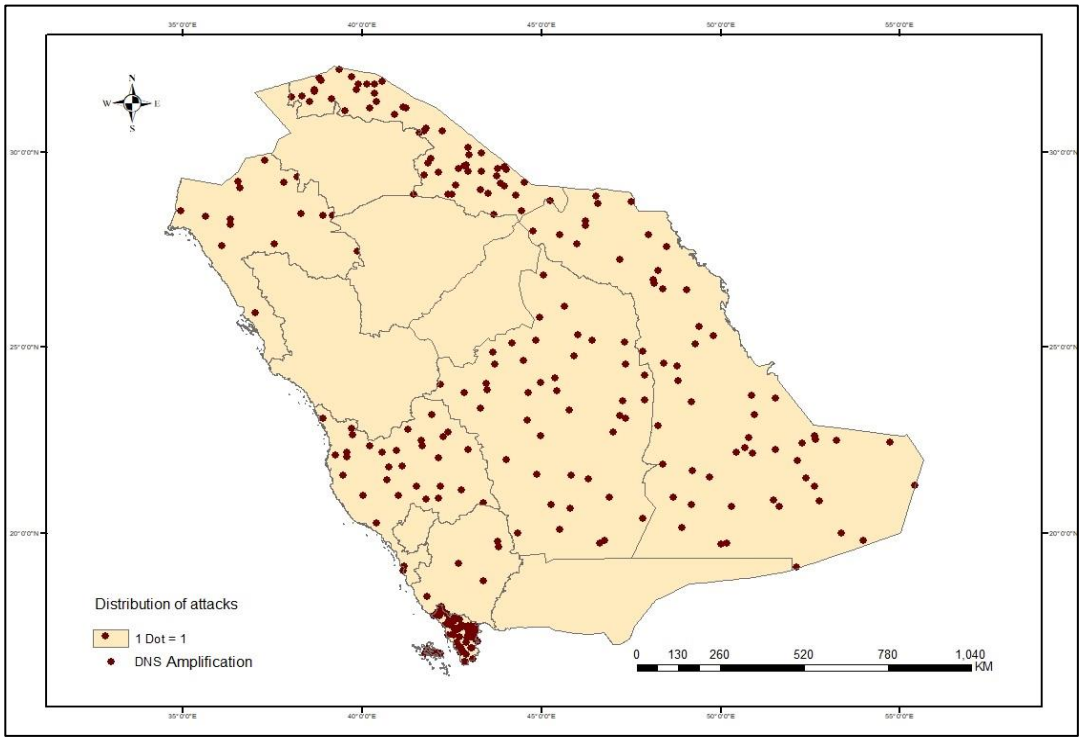
شكل (٧) توزيع الهجمات السيبرانية من نوع UDP



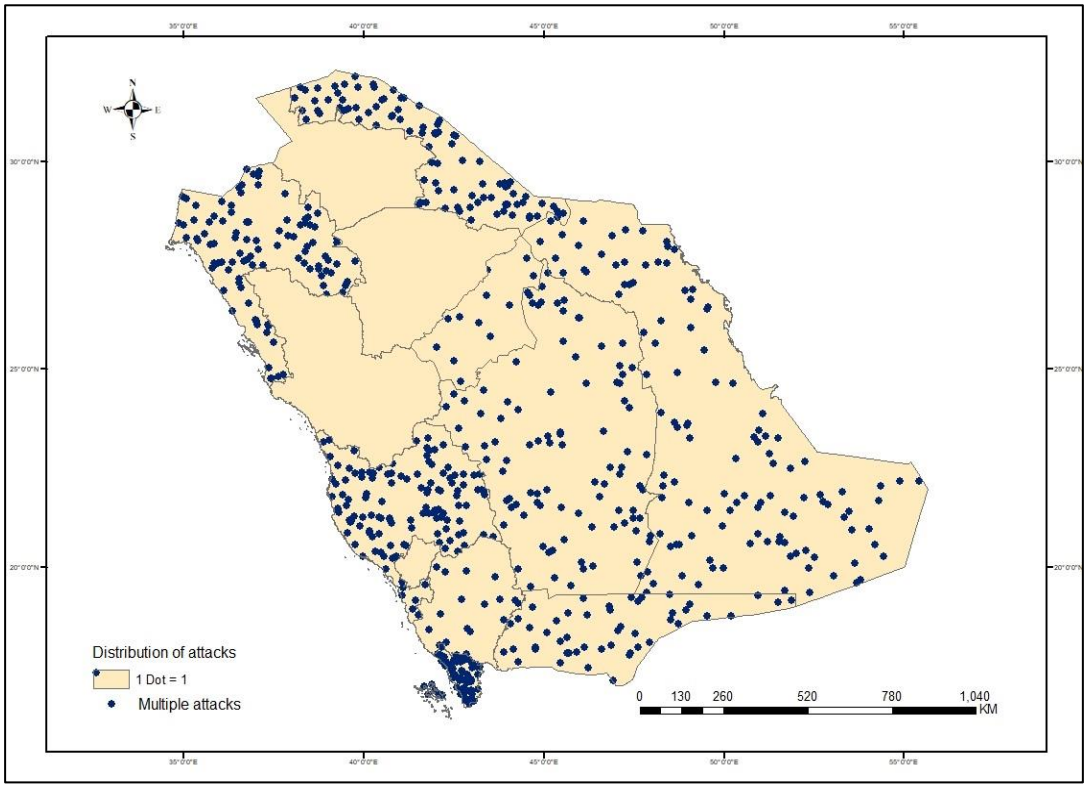
المصدر: من عمل الباحثة بناء على بيانات الدراسة ٢٠٢٣م.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

شكل (٨) توزيع الهجمات السيبرانية من نوع DNS Amplification



شكل (٩) توزيع الهجمات السيبرانية من نوع Multiple attacks



المصدر: من عمل الباحثة بناء على بيانات الدراسة ٢٠٢٣م.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

النتائج والتوصيات: اسفرت الدراسة عن عدد من النتائج نوجزها فيما يلي:

-أثبتت نتائج الدراسة فاعلية استخدام المنصات التفاعلية في إجراء التحليلات المكانية، خاصة منصة NetScout cyber threat horizon التي تضمنت الأبعاد المكانية للهجمات السيبرانية على المملكة العربية السعودية مقترنة بالأبعاد الزمنية وبأسماء الهجمات، إلا إنها لم توفر معلومات عن القطاعات المستهدفة بالهجمات وهو ما اقتضى اللجوء لبيانات عدد من المنصات الأخرى.

-ثبت ارتفاع نسبة استهداف قطاع الاتصالات السلكية واللاسلكية وقطاع الاتصالات عبر الأقمار الصناعية، كما ثبت أن هجمات Total Traffic والهجمات المتعددة Multiple attacks كانت من أكثر أنواع الهجمات استهدافاً للفضاء السيبراني للملكة.

-اتضح أن غالبية الهجمات السيبرانية التي استهدفت الفضاء السيبراني للمملكة كانت قصيرة المدى تراوحت بين (١-١٠ دقائق)، وغالبيتها كانت من نوع Total Traffic.

-تعرضت المملكة لنوعين من الهجمات حسب مصادر الهجوم، هجمات داخلية وخارجية، وقد كانت غالبية الهجمات الخارجية من بعض دول الاتحاد الأوروبي والولايات المتحدة الأمريكية والأمارات العربية المتحدة، إلا أن الهجمات بلغت أقصاها من الولايات المتحدة الأمريكية بدافع سياسي واقتصادي.

-ارتفاع نسبة الهجمات السيبرانية على وسط وشرق المملكة لأغراض جيوسياسية واقتصادية. على حين سجلت الأجزاء الجنوبية الغربية أدنى الهجمات السيبرانية، ولا يعد انخفاض الهجمات على هذه الأجزاء مؤشرا ذا دلالة، بسبب تركيز الدراسة على فترة زمنية محددة، مما يستوجب دراسة المشكلة بصورة مستفيضة بالتركيز على فترات زمنية تتجاوز الشهر للحكم على دقة النتائج.

توصيات الدراسة:

١-إنشاء منصة وطنية تفاعلية لمتابعة الهجمات على فضاء المملكة السيبراني للعمل على سد الثغرات الأمنية الموجودة في أجهزة القطاعين العام والخاص وإتاحة بياناتها للباحثين.

٢-إجراء دراسات مماثلة على مستوى الدول، حيث إن إجراء الدراسات على مستوى أكبر من الدولة هو أقرب ما يكون للتعميمات.

٣-ضرورة إجراء دراسة مماثلة عن المملكة العربية السعودية تتضمن بيانات عن الهجمات السيبرانية لفترات زمنية تتجاوز الشهر، لضمان مصداقية ودقة التحليل.

٤-تعاون الهيئة الوطنية للأمن السيبراني في تزويد الباحثين بالبيانات الخاصة بالاختراقات الأمنية، وإشراك الباحثين من مختلف التخصصات في إجراء الدراسات المتعلقة بهذا الشأن.

المراجع العربية:

الحفظي، هاني بن محمد. (د.ت). المنهج الوصفي التحليلي. الهيئة الملكية للجبيل وينبع، إدارة الخدمات التعليمية.

خليفة، إيهاب. (٢٠١٩م). الأمن السيبراني: الماهية والإشكاليات. رؤى مصرية، مركز الأهرام للدراسات السياسية والاستراتيجية.

بانقا، علم الدين. (٢٠١٩م). مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي. المعهد العربي للتخطيط، سلسلة دراسات تنموية: الكويت.

Amine, R., Sevil, Hakki. & Kocak, Salih., LII, G. (2020). The Spatial Analysis of the Malicious Uniform Resource (URLs). MDPI. DOI: 10.3390|info12010002.

Chen, Shuai., Hao, M., Ding, Fangyu. & Jiang, D., Dong, Jiping., Zhang, Shize., Guo, Qiquan & Geo, Chundong. (2023). Exploring the global geography of cyber crime and its driving forces. Humanities & Social Sciences Communication. DOI: 10.1057|s41599-023-01560-X.

Veerasamy, N., Moolla, Yaseen. & Dawood, Zubeida. (2023). Application of Geospatial Data in cyber security. Proceeding of the 21st European Conference on Cyber warfare and security.

Yang, H. (2013). Temporal and Spatial Analyses for larg-scale Cyber Attacks. Handbook of computational Approaches to Counterterrorism (PP.559-578). DOI: 10.1007|978-1-4614-5311-6-25.

Security report. (2023). Nets count DDOS Threat Intelligence.

Security report. (2023). Sonic wall security center.

https://www.geeksforgeeks.org/tcp-ip-hijacking

https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack

https://www.f5.com/labs/learning-center/what-is-a-dns-amplification-attack

https://stackoverflow.com/questions/251243/what-causes-a-tcp-ip-reset-rst-flag-to-be-sent

https://www.paloaltonetworks.com/cyberpedia/what-is-l2tp

https://www.baeldung.com/cs/tcp-protocol-syn-ack

https://www.imperva.com/learn/ddos/ip-fragmentation-attack-teardrop

https://nca.gov.sa/reports

February 28th DDoS Incident Report - The GitHub Blog