# استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني

## دراسة تحليلية مقارنة

**د. أسماء أحمد أبو زيد علام***

**المستخلص**

يمثل الأمن السيبرانى أحد أهم أركان استراتيجية بناء الدولة الرقمية، وركيزة من الركائز الأساسية فى اقتصاد قائم على المعرفة التكنولوجية الذكية، لذا فان تحقيق الأمن السيبراني يعد مسئولية مشتركة بين جميع قطاعات الدولة.

فالهجمات السيبرانية لم تعد نتاج عمل أشخاص بمفردها أو مجموعات من القراصنة فقط ولكنها أصبحت تضم متخصصين في الجرائم السيبرانية يتعاونون معا ويستثمرون أموالا ضخمة فيها، فضلا عن المعرفة والخبرة والمثابرة، وأصبحت قدرات هؤلاء المتخصصين تعادل إن لم تكن أفضل من قدرات الجهات الفاعلة في الدولة.

وتسعى الدول العربية لتحسين قدراتها في تعزيز الأمن السيبراني، والسعي إلى تكثيف الحوار والتعاون الدولي في هذا المجال، والعمل الدؤوب على تعزيز قدراتها في مواجهة هجمات القراصنة .

وفي هذا الإطار تتحدد المشكلة البحثية في رصد وتحليل وتفسير استراتيجيات خطاب صحافة التكنولوجيا العربية في كل من مصر والسعودية تجاه الأمن السيبراني، من خلال تحليل آليات خطابات أبواب التكنولوجيا في الموقع الالكتروني لصحيفتي "اليوم السابع" المصرية و"عكاظ" السعودية، ومحددات تشكيل تلك الآليات، وكذلك العوامل والمتغيرات المؤثرة في إنتاج هذا الخطاب الصحفي سواء عوامل ومتغيرات مجتمعية، أو عوامل ومتغيرات لها علاقة بالمناخ الصحفي والإعلامي المنتج له، من خلال دراسة تحليلية لخطابات صفحات التكنولوجيا بصحيفة "اليوم السابع" المصرية، وصحيفة "عكاظ" السعودية خلال فترة الدراسة (من يناير 2018م إلى يناير2019م ).

**الكلمات الرئيسية** صحافة التكنولوجيا العربية؛ الأمن السيبرانى؛ تحليل الخطاب

* مدرس بقسم الصحافة بكلية الإعلام- جامعة القاهرة

# Arab Technology Journalism Speech Strategies Towards cyber security

Comparative Analytical Study

**Dr. Asmaa Ahmed Abu Zaid Allam***

## Abstract

Cybersecurity is one of the most important pillars of the strategy of building a digital state, and one of the basic pillars in an economy based on smart technological knowledge. Therefore, achieving cybersecurity is a shared responsibility among all sectors of the state.

Cyber-attacks are no longer the product of the work of single people or groups of hackers only, but they have become specialists in cybercrime cooperating together and investing huge funds in them, as well as knowledge, experience and perseverance, and the capabilities of these specialists have become equal, if not better, than the capabilities of state actors.

Arab countries seek to improve their capabilities to enhance cyber security, seek to intensify international dialogue and cooperation in this field, and work tirelessly to enhance their capabilities in the face of hacker attacks.

In this context, the research problem is determined in monitoring, analyzing and interpreting the discourse strategies of the Arab technology press in both Egypt and Saudi Arabia towards cyber security, through the analysis of the mechanisms of the discourses of technology doors on the website of the Egyptian newspaper "Youm Al-Sabea" and "Okaz" Saudi Arabia, and the determinants of the formation of these mechanisms. As well as the factors and variables affecting the production of this journalistic discourse, whether societal factors and variables, or factors and variables related to the journalistic and media climate that produces it, through an analytical study of the speeches of the technology pages in the Egyptian newspaper "Youm Al-Sabea" and the Saudi newspaper "Okaz" during the study period (from January 2018 to January 2019).

**Keywords** Arab technology journalism; cyber security; Discourse analysis

*Lecturer in Journalism Department, Faculty of Mass Communication - Cairo University

**مقدمة:**

انتشر مصطلح "الأمن السيبرانى" عقب الهجمات الإلكترونية التى حملت اسم "الفدية"*، والتى هاجمت مائة دولة منها مصر، وتسببت فى تعطل مرافق حيوية ببعض الدول، لذا يعد الأمن السيبراني أحد الشواغل الرئيسة للدول والمؤسسات، خاصة مع زيادة وتطور التهديدات والهجمات السيبرانية. فمع تزايد اعتماد الحياة على التكنولوجيا، أصبحت الحاجة إلى الوعي بالأمن السيبراني نشاطًا مهما يجب ممارسته للحد من التهديدات السيبرانية المتزايدة.

ويعرف الأمن السيبرانى بأنه أمن المعلومات على أجهزة وشبكات الحاسب الآلى، بما فى ذلك العمليات والآليات التى يتم من خلالها حماية معدات الحاسب الآلى والمعلومات والخدمات من أى تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث. ويركز الأمن السيبراني على مراعاة التدابير السياسية والقانونية والاقتصادية والتعليمية والتقنية مع الجهود المبذولة للحد من المخاطر المرتبطة بالفضاء الإلكتروني.[1]

ويعد الأمن السيبراني أحد أهم ركائز الاقتصاد الرقمي -فقد أصبح الإنترنت، والخدمات والأجهزة الرقمية، والتكنولوجيات الناشئة جزءاً أساسياً من الاقتصادات في جميع أنحاء العالم- مما يشير إلى أهمية الوعي بخطورة التهديدات السيبرانية وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية لتفعيل منظومة الأمن السيبراني في مختلف قطاعات الدولة، وزيادة الإنفاق على حماية البنى التحتية للاتصالات وتكنولوجيا المعلومات للمؤسسات المختلفة من المخاطر السيبرانية.

وتنقسم التهديدات السيبرانية إلى ثلاث فئات؛ وهي الهجمات على السرية، النزاهة، والتوافر. وتشمل الهجمات على السرية(Confidentiality) سرقة معلومات التعريف الشخصية، والحسابات المصرفية، أو معلومات بطاقة الائتمان. أما الهجمات على النزاهة(Integrity) ، فتعتمد على التخريب الشخصي أو المؤسساتي، وغالبًا ما تسمى بالتسريبات، بغرض كشف البيانات، والتأثير على الجمهور لإفقاد الثقة في تلك المؤسسة أو الشخصية. والهدف من الهجمات على التوافر (Availability)هو منع المستخدمين من الوصول إلى بياناتهم الخاصة إلى أن يدفعوا فدية ما.[2]

مما سبق تتضح خطورة التهديدات السيبرانية مقارنة بمثيلتها التقليدية، ففي حين تنصب التهديدات العسكرية التقليدية على استهداف الدول وجيوشها العسكرية وإقليمها الجغرافي بالأساس، تستهدف الهجمات السيبرانية أنظمة المعلومات والشبكات الإلكترونية التي تعتمد عليها الدول بشكل رئيسي مخلفةً نتائج تتراوح بين الأضرار

المادية الطفيفة، وتدمير البنية التحتية، وتسريب معلومات سرية، وسرقة البيانات، والمساس بالأمن القومي للدول.

كما يتضح أيضا تعدد أنماط تلك الهجمات من حالةٍ إلى أخرى، واختلاف أهداف كل منها، لتشمل: التجسس، واستعراض القوة، والانتقام، وإلحاق أضرارٍ مادية بالخصم، وغيرها، مما يعني تباين الآثر التدميري لتلك الهجمات من حالةٍ إلى أخرى، وإن كان أخطرها هو الهجمات المدمرة الصريحة ضد البنية التحتية الحيوية. أضف إلى ذلك طول أمد الفترة الزمنية بين وقوع الهجمة السيبرانية من جانب، واكتشاف وقوعها من جانبٍ آخر، والرد عليها من جانب ثالث. وقد لا يُكتشف عدد منها ابتداءً، وحتى وإن تم اكتشافها فإن كافة الدول التي توجه إليها أصابع الإتهام تُنكر قيامها بشنها.

فالتهديدات السيبرانية واحدة من أعقد وأخطر التهديدات التي تستهدف الدول والأفراد على حد سواء، وذلك بفعل طبيعتها المعقدة والمتطورة، وتضاؤل تكلفتها. وتجدر الإشارة إلى أن كافة دول العالم تشهد اهتماماً بارزاً بشأن الآمن السيبراني نظراً لتصاعد حدة الاختراقات الأمنية للبنية الالكترونية؛ لذا جعلت الحكومات فى جميع أنحاء العالم الأمن السيبرانى أولوية فى السنوات الأخيرة لدرء المتسللين، والجواسيس، والبرمجيات الخبيثة وغيرها من التهديدات لنظم الكمبيوتر الضعيفة.

وبالنسبة للدول العربية تتناول الدراسة الحالة المصرية والسعودية، فقد كشف المؤشر العالمي للأمن السيبراني "GCI" الذى يصدر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة لعام 2018، عن تراجع مصر 9 مراكز لتهبط من المركز الرابع عشر في العام السابق له لتحتل المركز الثالث والعشرين، وعلى المستوي العربي فقدت المركز الثاني لتصبح فى الترتيب الرابع.

واستطاعت السعودية أن تحتل المرتبة 13 عالمياً والأول عربيًا في المؤشر العالمي للأمن السيبراني، وقد أعلن الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز، عن إنشاء أكاديمية طويق المتخصصة في التقنيات المتقدمة، ومقرها جامعة الأميرة نورة بنت عبد الرحمن.

واتخذت الدراسة من تجربة الصحافة المصرية، والسعودية نطاقاً تطبيقياً فيما يتعلق بخطابها تجاه الآمن السيبراني؛ لمعرفة العوامل المؤثرة في تشكيل توجهات هذا الخطاب، ووظائفه، وحدود دوره، وآلياته، ومحددات تشكيل تلك الآليات، وكذلك العوامل والمتغيرات المؤثرة في إنتاج هذا الخطاب الصحفي؛ للوقوف على الواقع الراهن للآمن السيبراني في كل من مصر والسعودية.

**الدراسات السابقة:**

فى ضوء مسح الدراسات السابقة تم تقسيم الدراسات إلى محورين رئيسين: **المحور الأول**، تضمن الدراسات التي اهتمت بواقع الأمن السيبراني والتحديات التي تواجهه. وركز **المحور الثاني** على كيفية مواجهة تهديدت الأمن السيبراني، وذلك على النحو التالي:

**المحور الأول: الدراسات التي اهتمت بواقع الأمن السيبراني والتحديات التي تواجهه:**

أوضحت دراسة **Kolenko, M. M. (2019)**[3] أن توصيف الجوانب الثقافية والسلوكية للهجوم السيبراني، يعزز من الأمن السيبراني، ففهم العلاقة بين الثقافة والسلوك والضحية يوفر المزيد من المعرفة والفرص البحثية التي تساعد على تعزيز الوعي بتكتيكات الدفاع السيبراني، من خلال النظر في الاتجاهات السلوكية للمدافع، والتي تعكس القيم الثقافية، حيث توجد علاقة إحصائية دالة بين الضحية والقيم الثقافية.

وخلصت دراسة **Alotaibi, F. F. G. (2019)**[4] ودراسة [5] **Alabdulatif, A. (2018)** إلى أنه بالرغم من كون المملكة العربية السعودية واحدة من أسرع الدول النامية التي شهدت زيادة هائلة في استخدام الإنترنت وخدمات التكنولوجيا وكذلك الأجهزة النقالة للوصول إلى مختلف الخدمات، إلا أن هناك ضعف اهتمام بأدوات الأمن السيبراني، خاصة: أمن كلمة المرور وحماية البرامج الضارة وتدابير السلامة التي يجب اتخاذها مثل النسخ الاحتياطي، وتركيب برامج مكافحة البرامج الضارة.

وألقت دراسة **Lee, A. (2018)**[6] ودراسة **Sobré-Denton, M. (2016)**[7] الضوء على توظيف الشباب لنقاط الضعف في نظام الأمن السيبراني لتمرير آرائهم عير مواقع التواصل الاجتماعي، للاحتجاج ضد النظم السياسية التي يرونها مستبدة وفاسدة، وبناء مجتمع افتراضي تتم من خلاله المشاركة في التواصل لبناء المواطنة العالمية.

بينما كشفت دراسة **Chukwu, C. U. (2018)**[8] أن الفضاء الإلكتروني يعد بيئة آمنة للإرهاب الرقمي خاصة في أفريقيا، حيث يسهل من عمليات الاختطاف والقتل والاضطرابات الاجتماعية، لذا أوصت الدراسة بضرورة تعزيز الوعي بالأمن السيبراني، واعتماد سياسات واستراتيجيات أكثر صرامة فيما بين البلدان الأفريقية.

وأبرزت دراسة **Churchwell, C. (2018)**[9] أن عدم وضع تعريف محدد لمصطلحات مثل الجريمة السيبرانية والدفاع والانتقام السيبراني يحد من استراتيجيات الدفاع والهجوم السيبراني الأخلاقية التي تحافظ على العلاقات الدولية السلمية.

وأوضحت دراسة **Schneider, F. (2016)**[10] أن تطبيق الصين لنظم صارمة للأمن السيبراني، خاصة المحتوى السياسي الرقمي، بالتحديد فيما يتعلق بالقضايا التي تؤثر على شرعية الحزب الحاكم، يؤدي فعليًا إلى جعل الوسائط الرقمية في الصين تقع فعليا ضمن نظام وسائل الإعلام "التقليدية"، حيث تتعامل مع مواقع الويب ليس كمساحات للتفاعل الاجتماعي المتصل بالشبكة، ولكن كمصادر معلومات في اتجاه واحد تبث المحتوى المتعمد للجمهور.

وأكدت دراسة **Hammad, E. (2018)**[11] أن الأمن السيبراني نهجا استراتيجيا للتخطيط والتصميم والتشغيل؛ نتيجة لزيادة الاعتماد على الأدوات والشبكات السيبرانية، بالاقتران مع تزايد التهديدات الخطيرة القائمة على الإنترنت.

وأشارت نتائج دراسة **Ghazi-Tehrani, A. (2016)**[12] إلى أن عدم التعاون بين الجهات المختلفة، وعدم وجود معايير أمنية مقننة في الولايات المتحدة الإمريكية، بالإضافة إلى منظومة التشريعات الأمريكية يسهم في الحد من الأمن السيبراني.

وأشارت دراسة **Caldwell, Z. B. (2016)**[13] إلى افتقار العديد من المنظمات القدرة على تنفيذ برنامج لإدارة الأمن السيبراني بفعالية بسبب عدم القدرة على تقييم وقياس فعالية الجهود الأمنية التي تبذلها المنظمة.

**<u>المحور الثاني: الدراسات التي ركزت على كيفية مواجهة تهديدت الأمن السيبراني:</u>**

خلصت دراسة **Osmak, K. A. (2019)**[14] ودراسة **De Los Santos, S.** [15] **(2016)** إلى أهمية وضع نهج جديد لأمن الفضاء الإلكتروني لتلبية الاحتياجات الإلكترونية؛ فعند استعراض أطر وثائق الأمن السيبراني الصادرة عن حكومة الولايات المتحدة، نجد أن التهديدات مازالت قائمة، فالأمن السيبراني يفتقر إلى إطار فعال وسياسات لتلبية متطلباته.

وكشفت دراسة **Oloidi, A. (2019)**[16] أن نقاط الضعف التي قد توجد في إطار الأمن السيبراني للمؤسسات قد تؤدي إلى استغلال البنية التحتية للأمن السيبراني من قبل مجرمي الإنترنت، عبر أنشطة تحويل الأموال، والخسارة النقدية، وفقدان البيانات، والخرق الأمني، وسرقة المعلومات الشخصية للعميل، والتعدي على الملكية الفكرية، مما يؤدي إلى خسارة في أسهم العلامة التجارية المالية وخسارة ثقة المستثمر/العملاء في هذه المؤسسات. وحددت الدراسة عدة نقاط الضعف في منصة الأمن السيبراني، ومنها: برامج مكافحة الفيروسات وبرامج التجسس غير الفعالة، وعدم وجود خطط أمنية، وسياسات أمنية غير شاملة، وخطط التعافي من الكوارث غير الفعالة التي تضعف البنية التحتية لأمن الفضاء الإلكتروني

وقدمت دراسة **YIN, X. C. et a (2019)**[17] طريقة مبتكرة لحل الأمن السيبراني القائم على نظام كشف التسلل لاكتشاف النشاط الضار الذي يستهدف

طبقات بروتوكول الشبكة الموزعة (DNP3) في أنظمة التحكم الإشرافي والحصول على البيانات (SCADA). نظرًا لأن تقنية المعلومات والاتصالات متصلة بالشبكة ، فإنها تتعرض لهجمات جسدية وهجمات إلكترونية بسبب التفاعل بين أنظمة التحكم الصناعية وبيئة الإنترنت الخارجية باستخدام تقنية إنترنت الأشياء.

وأوصت دراسة **Vanover, J. K. (2018)**[18] بضرورة توفير آليات حماية وأمن أكثر قوة لمستخدمي الإنترنت، وتوسيع الخيارات الأمنية التي يمكن أن تحمي بشكل أفضل المستخدمين.

وسلطت دراسة **Smith, C. (2018)**[19] الضوء على "النظافة السيبرانية"، وهو المصطلح المستخدم للجمع بين الأمن السيبراني والسلامة السيبرانية والأخلاقيات الإلكترونية، والذي يتضمن: على سبيل المثال لا الحصر، سلامة الإنترنت، وصيانة الحساب عبر الإنترنت، ومعرفة الكمبيوتر، ومسؤولية الفرد. حتى يتمكن الأشخاص من حماية أنفسهم والآخرين عبر الإنترنت، من خلال تخزين المعلومات الشخصية على تطبيقات ومواقع مختلفة بآمان.

وأشارت نتائج دراسة **Cook, K. D. (2017)**[20] إلى أن استراتيجيات الأمن السيبراني الناجحة، والاعتماد على الموردين الخارجيين لخدمات البنية التحتية، والتوعية بالأمن السيبراني قد تكون بمثابة دليل تأسيسي للآخرين لتقييم نقاط الضعف في التهديدات السيبرانية والتخفيف من حدتها.

وأبرزت دراسة **Dawson, M. (2017)**[21] الضوء على أهمية خلق بيئة تعليمية في كل مكان (U-Learning) لتعليم مفاهيم الأمن السيبراني، وصياغة السياسات التي تؤثر على الحوسبة الآمنة، ودراسة الآثار على الأمن الوطني والدولي، مما يؤدي إلى تحسين دور الأمن السيبراني في التعليم والتكنولوجيا ومختلف السياسات.

وأكدت دراسة **Imranuddin, M. (2017)**[22] على أهمية تعاون الدول العربية مع مختلف الوكالات الدولية لتحسين أمنها السيبراني، حتى لا تتعرض الدولة برمتها للخطر.

وأوضحت دراسة **Streifel, T. E. (2017)**[23] أن الردع السيبراني يمثل الهيمنة داخل المجال الإلكتروني، والذي يعد بمثابة رادع عن صراع في المستقبل مع خصم محتمل؛ فإذا شنت الدول المتنافسة صراعا مسلحا، فإن الهجمات السيبرانية ستستخدم لخلق نفس الذعر والآثار النفسية على المدنيين والعسكريين وحكومة بلد ما. وعلى الرغم من أنه لا يمكن القضاء تماما على الهجمات السيبرانية، فإن هناك حاجة إلى إيجاد حل وقائي حتى تتمكن الدولة من حماية المدنيين على نحو أفضل مما يقلل من المخاوف ويخلق الثقة الإلكترونية بين الجمهور.

وشددت دراسة **Layne, C. (2017)**[24] على أن أفضل رادع للجريمة السيبرانية هو فهم أنواع الهجمات حتى يمكن اتخاذ خطوات دفاعية للحد من أثر الهجمات المماثلة في المستقبل.

واتفقت معها دراسة **Abraham, S. (2016)**[25] التي أكدت أهمية وضع استراتيجية فعالة لتحليلات أمن الفضاء الإلكتروني من أجل التقليل إلى أدنى حد من المخاطر وحماية الهياكل الأساسية الحيوية من التهديدات الخارجية قبل أن تبدأ حتى. فما زلنا نفتقر إلى التقنيات الفعالة لقياس المخاطر الأمنية التنبؤية لمؤسسة بدقة مع الأخذ بعين الاعتبار السمات الديناميكية المرتبطة بنقاط الضعف الأمنية التي يمكن أن تتغير بمرور الوقت.

وأرجعت دراسة **McGee, T. M. (2016)**[26] الحاجة إلى تدابير واستراتيجيات الأمن السيبراني المتقدمة إلى التطور الحديث للهجمات السيبرانية والاهتمام الشديد لوسائط الإعلام عند وقوع الهجمات والخروقات.

وألقت داسة **Betz, D. J., & Stevens, T. (2013)**[27] الضوء على أهمية مشاركة المجتمع الدولي في وضع سياسة عامة للأمن السيبراني وتقييم وضعه الحالي، في محاولة للتكيف مع الحقائق الأمنية الجديدة لعصر المعلومات.

حيث كشفت دراسة **Burton, J. (2013)**[28] أن التعاون المؤسسي في قضايا الأمن السيبراني وظهور معايير الأمن السيبراني يعوقهما التنافس الاستراتيجي بين الولايات المتحدة وروسيا والصين وأن التحالفات العسكرية تكافح للتكيف مع الدفاع الجماعي ضد التهديدات السيبرانية. في حين أن بيئة الأمن السيبراني المعولمة تؤدي إلى تآكل العزلة الجغرافية للدول الصغيرة؛ مثل حكومة نيوزيلندا التي تكافح من أجل صياغة توازن مستدام بين الأمن والخصوصية في الاستجابة لقضايا الأمن السيبراني.

**التعليق على الدراسات السابقة:**

استخدمت معظم الدراسات السابقة المنهج المسحي، كما وظفت الاستبيان كأداة لجمع المعلومات وتحقيق أهداف الدراسة. في حين أضافت الباحثة المنهج المقارن لرصد وتحليل وتفسير استراتيجيات خطاب صحافة التكنولوجيا العربية في كل من مصر والسعودية تجاه الأمن السيبراني، من خلال توظيف تحليل الخطاب لصفحات التكنولوجيا بصحيفة "اليوم السابع" المصرية، وصحيفة "عكاظ" السعودية خلال فترة الدراسة.

وتشير الدراسات السابقة إلى تزايد معدلات الهجمات السيبرانية على اختلاف طبيعتها، وطبيعة الفاعل الذي تستهدفه، والهدف من ورائها.

وتأخذ الهجمات السيبرانية شكل المنحنى الآخذ في الصعود، وهي الهجمات التي لا يمكن للدول أو الشركات الكبرى أن تنأى بنفسها عنها. والأكثر خطورة من ذلك،

قدرتها على استهداف العمليات الانتخابية لأعرق الديمقراطيات. وكما يتضح، تتعدد أسباب تلك الهجمات لتشمل ثغرات الأمن السيبراني، مثل: البرامج غير المرخصة، وشهادات الأمان منتهية الصلاحية، وتدابير الأمن السيبراني غير الكافية، وغيرها .

كما تكشف الهجمات عن اتجاهات ودوافع جديدة من التشفير إلى الفدية، إلى استغلال نقاط ضعف الأجهزة المحمولة للهجمات من أجل المصالح الوطنية. وشملت الهجمات كذلك البنية التحتية لتكنولوجيا المعلومات، والمستشفيات، والموانئ، والمطارات، والصحف، وغيرها. وأصبحت البرمجيات الخبيثة أيضًا متعددة الوظائف في منهجيتها وأغراضها، مما أدى إلى حدوث هجمات هجينة تجمع بين برامج التشفير والتشفير الخبيث .

وفي ظل تعدد التهديدات السيبرانية، التي تشمل: "الحرب الرقمية Digital Warfare "، و"الإرهاب الرقميDigital Terrorism "، و"التجسس الرقمي Digital Espionage "، بجانب التزايد المضطرد في أعداد الهجمات السيبرانية في السنوات القليلة الماضية؛ تتزايد أهمية "الردع السيبراني" لتأمين أجهزة الحاسب الآلي، وأنظمة المعلومات، والبنى التحتية من ناحية، والحيلولة دون تكرار تلك الهجمات من خلال تحديد الخصم على نحوٍ دقيق وتوعده بالانتقام ردًّا على هجومه، من ناحيةٍ ثانية، وحماية الأمن القومي للدول الذي بات رهنًا بالفضاء السيبراني، من ناحيةٍ ثالثة.

**مشكلة الدراسة:**

لم تعد الهجمات السيبرانية نتاج عمل أشخاص بمفردها أو مجموعات من القراصنة فقط ولكنها أصبحت تضم متخصصين في الجرائم السيبرانية يتعاونون معا ويستثمرون أموالا ضخمة فيها، فضلا عن المعرفة والخبرة والمثابرة، وأصبحت قدرات هؤلاء المتخصصين تعادل إن لم تكن أفضل من قدرات الجهات الفاعلة في الدول؛ لذا تسعى الدول العربية لتحسين قدراتها في تعزيز الأمن السيبراني، والسعي إلى تكثيف الحوار والتعاون الدولي في هذا المجال،

وفي هذا الإطار تتحدد المشكلة البحثية في رصد وتحليل وتفسير استراتيجيات خطاب صحافة التكنولوجيا العربية في كل من مصر والسعودية تجاه الأمن السيبراني، من خلال تحليل آليات خطابات أبواب التكنولوجيا في الموقع الالكتروني لصحيفتي "اليوم السابع" المصرية و"عكاظ" السعودية خلال فترة الدراسة (من يناير 2018م إلى يناير2019م )، ومحددات تشكيل تلك الآليات، وكذلك العوامل والمتغيرات المؤثرة في إنتاج هذا الخطاب الصحفي سواء عوامل ومتغيرات مجتمعية، أو عوامل ومتغيرات لها علاقة بالمناخ الصحفي والإعلامي المنتج له.

**وترجع أهمية الدراسة إلى:**

1- **الأهمية المعرفية:** ندرة الدراسات التي تطرقت لمفهوم الآمن السيبراني في الحقل الإعلامي، بالرغم من أهمية دعم جهود الدولة للأمن القومى وتنمية المجتمع ، خاصة فى ظل تزايد التهديدات والتحديات المستقبلية فى المجال السيبرانى والمجتمع الرقمى ولرصد ومجابهة المخاطر والتهديدات المتزايدة.

بالإضافة إلى تنوع أشكال إصدارات صحافة التكنولوجيا في الدول العربية، ومن الأهمية بمكان الرصد الإعلامي لكل ما تقدمه هذه الصحف من جديد.

لذا تسعى الباحثة لاكتشاف طبيعة خطاب صحافة التكنولوجيا العربية، عبر تحليل إسترتيجيات ومرتكزات هذا الخطاب، وتحديد مدى مراعاة الصحف محل الدراسة لأبعاد الآمن السيبراني لتحقيق مزيد من التأثير.

2-**الإضافة التطبيقية:** أهمية الآمن السيبراني، حيث تتزايد أهمية القدرة على التعامل مع المعلومات فى البيئة الإلكترونية بطرق آمنة، من خلال الحصول على المعارف التوعوية الضرورية ذات العلاقة بالتهديدات الأمنية، بالإضافة إلى طرق التعامل معها عبر استخدام أساليب الدفاع المناسبة وتطبيقها بكفاءة وفاعلية.

**أهداف الدراسة وتساؤلاتها:**

تسعى الباحثة لتحقيق هدف رئيس، هو: تفسير إستراتيجيات الأمن السيبراني في خطاب صحافة التكنولوجيا في كل من مصر والسعودية، خلال فترة الدراسة (من يناير 2018م إلى يناير2019م)؛ بغية استكشاف الآليات التي استخدمتها صحف الدراسة، والعوامل والمتغيرات المؤثرة في إنتاج هذا الخطاب، وذلك من خلال الإجابة على التساؤلات التالية:

1. ما الأطروحات التي ارتكزت عليها خطابات صحف الدراسة فيما يتعلق بالأمن السيبراني في كل من مصر والسعودية؟
2. كيف دللت خطابات صحف الدراسة على أطروحاتها إزاء الأمن السيبراني في كل من مصر والسعودية؟
3. ما الأساليب الإقناعية والاستمالات التأثيرية التي استند إليها الخطاب الصحفي محل الدراسة؟ وما دلالات توظيفها في سياق الأمن السيبراني في كل من مصر والسعودية؟
4. ما المرجعيات التي استندت إليها الخطابات الصحفية محل الدراسة في سياق الأمن السيبراني في كل من مصر والسعودية؟
5. ما القوى الفاعلة البارزة في الخطابات الصحفية محل الدراسة بشأن الأمن السيبراني في كل من مصر والسعودية؟ وما طبيعة التصورات والأدوار المنسوبة إليها؟

6. لماذا نسبت الصحف محل الدراسة سمات وأدوار بعينها للقوى الفاعلة بخطابها تجاه الأمن السيبراني في كل من مصر والسعودية؟
7. ما الآليات التي استخدمتها الخطابات الصحفية محل الدراسة بشأن الأمن السيبراني في كل من مصر والسعودية؟
8. كيف وظفت الخطابات الصحفية محل الدراسة هذه الآليات؟ وما هي محددات تشكيلها في ضوء استراتيجيات الخطاب، والتكنيكات التي تم توظيفها في سياق كل آلية؟
9. ما العوامل والمتغيرات المؤثرة في إنتاج الخطاب الصحفي محل الدراسة بشأن الأمن السيبراني في كل من مصر والسعودية؟ وكيف أثرت هذه العوامل في إنتاج الخطاب الصحفي محل الدراسة؟

**<u>الإطار النظرى للدراسة:</u> اعتمدت الدراسة في بنائها النظري على نظرية المسئولية الاجتماعية لوسائل الإعلام:[29]**

تعد نظرية المسئولية الاجتماعية إحدى النظريات التي صنفها "ماكويل" لتفسير الممارسات الإعلامية داخل المجتمع، والتي أكد فيها على حرية وسائل الإعلام في مقابل التزامها بمسئوليتها تجاه المجتمع، وهو ما يسمى بالحرية الإيجابية.

ووفقا لمبادئ نظرية المسئولية الاجتماعية فإنه على صحافة التكنولوجيا في كل من مصر والسعودية مراعاة آمن وسلامة المجتمع المصري والسعودي القومي، من خلال الحفاظ على آمن المجتمع وصيانة مقدراته خاصة الامين السيبراني. والذي يمثل أحد أهم أركان استراتيجية بناء الدولة الرقمية، وركيزة من الركائز الأساسية فى اقتصاد قائم على المعرفة التكنولوجية الذكية، لذا فان تحقيق الأمن السيبراني يعد مسئولية مشتركة بين جميع قطاعات الدولة، خاصة المؤسسات الصحفية.

ومن هنا فان نظرية المسئولية الاجتماعية تشير إلى أهم العناصر التي يجب الالتزام بها حتى تحقق وسائل الإعلام دورها المسئول في المجتمع، ومن ثم تفيد النظرية في مناقشة نتائج الدراسة فيما يتصل بخطاب صحافة التكنولوجيا في كل من مصر والسعودية تجاه الآمن السيبراني الذي صار أولوية لدرء التهديدات الالكترونية بكافة أشكالها، وذلك في إطار تعزيز الجهود العالمية لمكافحة الهجمات السيبرانية، خاصة أنها باتت تطال الدول الكبيرة والصغيرة على حد سواء في ضوء تسارع التطورات التكنولوجية والتقنيات المستخدمة في هذا المجال.

**<u>الإطار المنهجى: نوع الدراسة ومناهجها:</u>**

نظراً لأن هذه الدراسة تنتمي إلى الدراسات الوصفية التحليلية التفسيرية المقارنة فإنها اعتمدت على المناهج التالية:

1- **منهج المسح:** توظفه الباحثة في مسح كافة المواد الصحفية المتعلقة بالأمن السيبراني في كل من مصر والسعودية بكل من: موقع "اليوم السابع" باب "علوم وتكنولوجيا"، وموقع "عكاظ " باب.

2- **المقارنة المنهجية:** تستخدمه الباحثة لرصد أوجه التشابه والاختلاف بين الخطابات الصحفية محل الدراسة، بما يحقق أهداف الدراسة في الوقوف على حدود الاتساقات والاختلافات في خطابات صحف الدراسة.

**أساليب التحليل:** تعتمد الدراسة على أسلوب تحليل الخطاب.

## الإطار الإجرائي

### مجتمع الدراسة:

المجتمع الأصلي للدراسة الدول العربية، ولتحديد أي من هذه الدول سيتم دراسة صحافة التكنولوجيا بها قامت الباحثة بالاستعانة بالعديد من المراجع التي تنوعت بين الدراسات الأكاديمية المتخصصة، والتواصل مع عدد من الأكاديميين المهتمين بالآمن السيبراني[30] واختارت الباحثة **مصر والسعودية**.

مبررات اختيار هذه الدول:

وقع الاختيار على **مصر**، والتي تشهد حراكاً قوياً في مجال الآمن السيبراني، الذى تجسد في إنضمام مصر للاتفاقية العربية لمكافحة جرائم الانترنت والإرهاب الالكترونى وإنشاء المجلس الأعلى للأمن السيبرانى، وقد جاءت المادة (31) من دستور 2014 لتؤكد على أن " أمن الفضاء المعلوماتى جزء أساسى من منظومة الاقتصاد والأمن القومى، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذى ينظمه القانون". وتحتل مصر المرتبة 23 عالميا والرابعة عربيا في المؤشر العالمي للأمن السيبراني (GCI (Global Cybersecurity Index لعام 2019م الذي يصدره الاتحاد الدولي للاتصالات التابع للأمم المتحدة.

أما **السعودية** فتحتل المرتبة 13 عالمياً والأول عربيًا في هذا المؤشر، مما يشير إلى اهتمام وطني كبير في تطوير الأمن السيبراني في المملكة للوصول إلى فضاء سيبراني سعودي آمن وموثوق يمكن النمو والازدهار لدعم تحقيق رؤية المملكة 2030.

### عينة الدراسة التحليلية:

تختص الدراسة بصحافة التكنولوجيا العربية المصرية والسعودية التي تهتم بالآمن السيبراني، وتشمل عينة صحف الدراسة.

**(1)** صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع: اليوم السابع" صحيفة إلكترونية يومية، تصدر عن الشركة "المصرية للصحافة والنشر والإعلان"، وهى الشركة الناشرة لصحيفة "اليوم السابع" المطبوعة التى

تصدر يومياً، وتتسم صفحة "علوم وتكنولوجيا" بأنها أكثر الصفحات والأبواب في الصحافة المصرية اهتماما بالتكنولوجيا والأمن السيبراني، وذلك وفق مؤشرات دراسة استطلاعية أجرتها الباحثة.

**(2)** صفحة التكنولوجيا بجريدة عكاظ: تصدر الصحيفة عن مؤسسة الطباعة والصحافة والنشر، وقد صدر العدد الأول من الصحيفة في 28 مايو 1960م، وقد أطلقت الموقع الالكتروني الخاص بها، وتتسم صفحة "تكنولوجيا" بموقع الجريدة بأنها أكثر الصفحات والأبواب في الصحافة السعودية اهتماما بالتكنولوجيا والأمن السيبراني، وذلك وفق مؤشرات دراسة استطلاعية أجرتها الباحثة.

**العينة الزمنية:** تشمل فترة الدراسة تحليل خطابات صفحات التكنولوجيا في الموقع الالكتروني لصحيفتي "اليوم السابع" المصرية و"عكاظ" السعودية خلال الفترة من يناير 2018م إلى يناير2019م، وتستخدم الباحثة أسلوب الحصر الشامل لصحف الدراسة بديلاً لأسلوب العينة.

**عينة المواد الخاضعة للدراسة:** تتمثل فى جميع الأشكال الصحفية التي تتناول الأمن السيبراني في كل من مصر والسعودية في صحف الدراسة.

**وحدة التحليل:** لما كانت الدراسة تستهدف – بشكل رئيس– رصد وتحليل وتفسير الأطروحات الرئيسة المتضمنة في خطاب الصحف محل الدراسة بشأن الأمن السيبراني في كل من مصر والسعودية، فتم الاعتماد على الموضوع كوحدة للتحليل والعد.

**أدوات جمع البيانات: استمارة تحليل الخطاب:** لتحديد القوى الفاعلة ومسارات البرهنة والأطر المرجعية بغية استكشاف الآليات التي استخدمتها صحف الدراسة في خطابها إزاء الأمن السيبراني في كل من مصر والسعودية، والعوامل، والمتغيرات المؤثرة في إنتاج هذا الخطاب بالصحف محل الدراسة.

**اختبارات الصدق والثبات:**

**أ- الصدق الظاهرى Face Validity:**

استعانت الباحثة بالأساتذة المتخصصين فى مجال الإعلام والسياسة،* لتحكيم استمارة الدراسة التحليلية، مما أسفر عن عدة ملاحظات أفادت الباحثة.

**ب- اختبارات الثبات Reliability:**

تم اختبار ثبات على 25 وحدة موضوع من كل صحيفة من الصحف عينة الدراسة التحليلية، وذلك بعد مرور فترة شهرين على الانتهاء من عملية جمع البيانات، وأسفر التطبيق عن نسبة ثبات بلغت 97%، مما يؤكد الثقة فى ثبات عملية التحليل وتعبير استمارة التحليل واستيعابها للخطاب.

**مفاهيم الدراسة:**

**الأمن السيبراني:** يشمل الأمن السيبراني أمن المعلومات على أجهزة وشبكات الحاسب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث[31].

واستخدمت الباحثة هذا المفهوم باعتبار الأمن السيبراني ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، التي تهدف عادةً إلى الوصول إلى المعلومات أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية، وصولا إلى تهديد آمن الدولة.

**امن المعلومات:** يهتم امن المعلومات بحماية كل ما يتعلق بالمعلومات ضمن الحاسب أو خارجه وليس حماية الحاسب كله، بالتالي تتلخص مهمة هذا النوع من الأمن في حماية المعلومات أينما وجدت.[32]

وعليه فإن الامن السيبراني يهتم بحماية المعلومات من التعرض للسرقة من قبل مصادر خارجية على شبكة الإنترنت، بينما أمن المعلومات يهتم بالمعلومات أينما وجدت.

**صحافة التكنولوجيا:** يشير المفهوم العلمي لصحافة التكنولوجيا إلى الصحف التي توظف الفنون الصحفية لتقديم الموضوعات وتوصيل المعلومات الخاصة بالتكنولوجيا. ويضم مفهوم صحافة التكنولوجيا المجلات والجرائد سواء مطبوعة أو الكترونية التي تعرض محتوى التكنولوجيا، وكذلك الصفحات المتخصصة في التكنولوجيا بالصحف العامة.[33]

واستخدمت الباحثة هذا المفهوم بالتطبيق على أبواب التكنولوجيا بالمواقع الالكترونية للصحف العامة وتكتب باللغة العربية.

**نتائج الدراسة:**

شمل تحليل خطاب صحافة التكنولوجيا العربية محل الدراسة جميع الموضوعات المتعلقة بالأمن السيبراني والتي بلغت 702 موضوعًا صحفيًا، حيث جاء 243 موضوعًا بموقع صحيفة اليوم السابع أما موقع جريدة عكاظ فطرحت 459 موضوعًا صحفيًا حول الأمن السيبراني خلال فترة الدراسة.

وأوضحت نتائج التحليل أن موقع جريدة اليوم السابع محل الدراسة في خطابها إزاء الأمن السيبراني وظف الفنون الإخبارية بنسبة 90%، وفي المرتبة الثانية جاءت الفنون الاستقصائية (التحقيقات) بنسبة 10%. أما موقع جريدة عكاظ فوظف الفنون

الإخبارية بنسبة 65%، وفي المرتبة الثانية جاءت مواد الرأي بنسبة 20%، ثم الفنون الاستقصائية (التحقيقات) بنسبة 15%.

وهوما يؤخذ على الصحف محل الدراسة خاصة موقع جريدة اليوم السابع التي لم تنوع في توظيف الفنون الصحفية المتعددة لطرح موضوعات الأمن السيبراني، لنشر الوعي بها بين القراء، بما يتناسب مع أهمية وخطورة التهديدات السيبرانية.

وكشفت نتائج تحليل خطاب صحافة التكنولوجيا العربية محل الدراسة إزاء الأمن السيبراني عن عدة نتائج تناقشها الباحثة عبر المحاور التالية:

**أولاً: أطروحات خطاب صحافة التكنولوجيا العربية محل الدراسة والحجج الداعمة لها إزاء الأمن السيبراني:**

**جدول رقم (1)**

أطروحات خطاب صحافة التكنولوجيا العربية محل الدراسة إزاء الأمن السيبراني

| أطروحات خطاب صحافة التكنولوجيا محل الدراسة إزاء الأمن السيبراني | موقع جريدة اليوم السابع (مصر) | | موقع جريدة عكاظ (السعودية) | |
|---|---|---|---|---|
| | ك | % | ك | % |
| أطروحات عرضت تعاظم أهمية الأمن السيبرانى بالنسبة لمصر والسعودية | 36.4 | %5 | 114.75 | %25 |
| أطروحات ناقشت واقع التهديدات السيبرانية التي تواجهها مصر والسعودية | 109.35 | %45 | 68.85 | %15 |
| أطروحات ركزت على الاجراءات الدفاعية التي تتخذها مصر والسعودية دفاعا عن الأمن السيبراني | 97.2 | %40 | 275.4 | %60 |
| **الإجمالي** | 243 | %100 | 459 | %100 |

تمحورت أطروحات خطاب صفحة **"**علوم وتكنولوجيا**"** بموقع جريدة اليوم السابع إزاء الأمن السيبراني حول التأكيد على تعاظم أهمية الأمن السيبرانى بالنسبة لجمهورية مصر العربية، حيث يمثل الأمن السيبرانى أحد أهم أركان استراتيجية بناء مصر الرقمية كما أنه **"ركيزة من الركائز الأساسية فى اقتصاد مصر القادم القائم على المعرفة التكنولوجية الذكية"**[34]، لذا فالأمن السيبرانى بالنسبة لمصر مسئولية مشتركة بين جميع قطاعات الدولة.

واتخذت صفحة "تكنولوجيا" بموقع جريدة عكاظ خطوات استباقية من خلال تقديم أطروحات حول المواطنة الرقمية كإحدى ركائز رؤية المملكة ٢٠٣٠ التي يعمل صناع القرار لهيكلتها وتدعيمها بالشكل المناسب، فـــ**"هناك تهديدات حقيقية لعل أصعبها ما يتعرض له الناس من سرقات واختلاسات وأسوأها ما يحدث من فضائح ومشكلات أخلاقية"**.[35]

واتفقت الصحيفتان على أن الحاجة للأمن السيبراني هي حاجة دفاعية عن الذات والمنجزات الوطنية، فلم تعد الهجمات السيبرانية نتاج عمل أشخاص بمفردها أو مجموعات من القراصنة فقط ولكنها أصبحت تضم متخصصين في الجرائم السيبرانية يتعاونون معا ويستثمرون أموالا ضخمة فيها، فضلا عن المعرفة والخبرة والمثابرة، وأصبحت قدرات هؤلاء المتخصصين تعادل إن لم تكن أفضل من قدرات الجهات الفاعلة في الدولة.[36]

وركزت صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع على مناقشة واقع التهديدات السيبرانية التي تواجهها مصر، حيث استغل القراصنة أزمة فيروس "كورونا" كوسيلة لنشر البرامج الخبيثة، فيظهر قراصنة الإنترنت على أنهم مسئولون صحيون، ويثيرون فزع الهدف عبر رسائل مخصصة لإجبارهم على فتح مستند "مايكروسوفت وورد" المرفق، الذى يزعم أنه يحتوى على تحديثات ومعلومات صحية حول "تفشى فيروس كورونا" فى المنطقة.

ويصيب Emotet جهاز الكمبيوتر، مع تحديد جميع شبكات "واى فاي" المجاورة، التى تُستهدف لاحقا بهجمات قوية، باستخدام قاعدة بيانات مخزنة تحتوى على كلمات مرور قائمة على "التخمين الدقيق"، لمحاولة خرقها.

وبمجرد الاتصال بشبكة "واى فاي" وتحديد جميع المستخدمين والأجهزة المستهدفة المحتملة، "يغفو" البرنامج لمدة 14 ثانية لتجنب إثارة أى شك قبل الهجوم، وترك إدارة النظام حتى آخر رمق، لتجنب إطلاق الإنذار فى وقت مبكر. كما يجمع كل مجموعات اسم المستخدم وكلمة المرور الناجحة، ويضيفها إلى قاعدة البيانات للنشر فى المستقبل، فى هجمات لاحقة.[37]

ورصدت صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع تعرض الموقع الرسمى لوزارة الصحة والسكان، للاختراق من قبل هاكرز، مما تسبب فى تعطله عن العمل، إلا أنه لم يكن يحمل بيانات حساسة، ولكن مجرد بيانات استرشادية.[38]

كما طرح موقع اليوم السابع قضية إتاحة موقع فيس بوك بيانات الملايين من المستخدمين للسرقة، حيث اكتشف باحثون أمنيون بشركة Up Guard للأمن السيبرانى أن بيانات مئات الملايين من مستخدمى فيس بوك يتم تخزينها على خوادم أمازون السحابية دون حماية، إذ تم العثور على بيانات شديدة الحساسية، وتتضمن كلمات المرور وعناوين البريد الإلكترونى وأسماء الحسابات وأرقام التعريف والتعليقات وردود الفعل، قابلة للقراءة والتحميل من قبل أى شخص.[39]

وحذرت صفحة "تكنولوجيا" بموقع جريدة عكاظ من ثغرة أمنية في تطبيق WhatsApp تسمح بزرع برنامج تجسسي عن طريق إجراء مكالمة عبر التطبيق ومن خلالها يتم اختراق الجهاز.[40]

وسلطت صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع الضوء على أخطاء الموظفين أو الإجراءات غير المقصودة والتي تؤدى إلى أكثر من نصف حوادث الأمن السيبرانى فى الشبكات الصناعية، مثل: إصابات البرامج الضارة، وكذلك الهجمات المستهدفة الأكثر خطورة، حيث تعانى المنظمات من نقص فى المحترفين للتعامل مع التهديدات الجديدة.[41]

وأرجع موقع اليوم السابع خطورة الهجمات السيبرانية إلى ثلاث عناصر، وهى: استنادها إلى تقنيات متقدمة ومتطورة، وغالباً ما تكون تلك التقنيات حكراً على دول معدودة وشركات كبرى، كما أن كثيرا من تلك التقنيات سرية وغير متاحة للتصدير، وقد تحتوى النسخ المتاحة منها للتصدير على أبواب خلفية أو ثغرات تجعلها مصدراً لتهديدات إضافية.

وكذلك سرعة وسهولة انتشارها، فنشر الفيروسات الخبيثة أو شن هجمات إعاقة الخدمات وغيرها من الأخطار السيبرانية يمكن أن يحدث بسرعة فائقة وسهولة فى ظل انتشار واتساع نطاق استخدام شبكات الاتصالات وتكنولوجيا المعلومات، ونظراً لسهولة شن الهجمات وبث الفيروسات عبر الحدود من أى مكان وبأرخص التكاليف، كما يصعب وقد يستحيل تعقب مصدر تلك التهديدات والأخطار فى الوقت المناسب لتداركها والتغلب عليها.

بالإضافة إلى اتساع نطاق تأثيرها، سواء من حيث التأثير المباشر أو غير المباشر على البنى التحتية وما قد يتعبه من أضرار أو خسائر فادحة، وكذلك من حيث إمكانية الأضرار بمصالح الجهات العامة والخاصة، والتأثير على جموع كبيرة من المواطنين بصورة مفاجئة وفى وقت قصير وعن بعد.

وقد ظهرت أنماطا جديدة "**خطيرة للغاية**" من الهجمات السيبرانية تستهدف إعاقة الخدمات الحيوية، وكذلك نشر برمجيات خبيثة وفيروسات لتخريب أو تعطيل البنى التحتية للاتصالات وتكنولوجيا المعلومات ونظم التحكم الصناعية الحيوية وخاصة فى المرافق الهامة" وذلك عبر عدة قنوات تشمل الشبكات اللاسلكية والذاكرة النقالة بالإضافة إلى القنوات الأخرى الشائعة". البريد الإلكترونى ومواقع الإنترنت والشبكات الاجتماعية وشبكات الاتصالات السلكية، مما يؤثر تأثيرا ملموسا على البنية التحتية لتلك المنشآت والمرافق وعلى الخدمات والأعمال المرتبطة بها، وقد ثبت عمليا أنها ليست بمنأى عن التعرض للهجمات السيبرانية الشرسة، حتى لو كانت غير متصلة بالانترنت.

وقد انتشرت مؤخرا نوعية خطيرة من الهجمات والجرائم السيبرانية تعتمد على تقنيات متقدمة "كالحوسبة السحابية والذكاء الاصطناعى وانترنت الاشياء وأجهزة تنصت على شبكات الاتصال السلكية واللاسلكية وبرمجيات لفك شفرة واختراق الأنظمة الشبكات والحاسبات وقواعد البيانات،

وبرمجيات لتشفير العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات لتسخيرها فى القيام بعمليات اجرامية وتعاملات مشبوهة دون علم أصحابها فيما يسمى بالشبكات الألية، حيث يمكن أن تضم شبكة آلية واحدة عشرات أو مئات الآلاف أو ملايين من الحواسب أو الأجهزة المتصلة بالانترنت "انترنت الأشياء"التى يمكن استخدامها لشن هجمات متنوعة، مثل الهجمات الموزعة لإعاقة الخدمات على شبكات ومواقع مستهدفة لأغراض اجرامية كالتخريب والإرهاب والتهديد والترهيب والإبتزاز.

وفى حين أنه من المرجح أن تطوير الفيروسات المعقدة والشرسة يتم على مستوى متقدم ويستلزم منظومة خبرات مركبة لا تتوافر إلا فى الدول المتقدمة تقنيا، وذلك لأغراض استراتيجية وحربية يمكن لتلك الدول استخدامها بدلا من أو (الى جانب) الهجمة العسكرية التقليدية فيما يسمى بالـ **"الحروب السيبرانية"**، الا أنه قد بدأ بالفعل نقل هذه الأنماط واستنساخها من قبل التنظيمات الإرهابية والتشكيلات العصابية الدولية للاستخدام فى العمليات الإرهابية وفى الجرائم المنظمة وفى تهديد وتعطيل البنى التحتية للاتصالات والمعلومات، وبالتالى يتوقع العديد من الخبراء فى مجال الأمن السيبرانى تنامى انتشار الهجمات السيبرانية الشرسة فى الفترة القادمة.

وتعد سرقة الهوية الرقمية من أخطر الجرائم التى تهدد مستخدمى الإنترنت ومستقبل الخدمات الإكترونية، حيث قد تتعرض البيانات الشخصية للمستخدم إلى السرقة بهدف انتحال شخصيته والاستيلاء على ممتلكاته وأمواله أو للزج باسمه فى تعاملات مشبوهة أو غير قانونية، وعادة ما يستعين سارق الهوية بمعلومات موجودة بالفعل على الانترنت، وبخاصة على مواقع شبكات التواصل الاجتماعية والمهنية المفتوحة أو قواعد البيانات والمعلومات القومية والشبكات الخاصة بالخدمات الحكومية وخدمات الضمان الاجتماعى وشبكات الرعاية الصحية ومواقع التجارة الإلكترونية والأسواق الافتراضية وشبكات المدفوعات الإلكترونية والصرافات الآلية وبورصة الأوراق المالية، فضلا على أنه قد تتعرض الأدوات والأنظمة المستخدمة فى إجراء المعاملات الإلكترونية للسرقة أو التخريب مما يشكل خطرا كبيرا على مصالح المستخدمين ومستقبل الخدمات الإلكترونية وقد تؤثر الهجمات الموسعة على القطاع المالى الوطنى بوجه عام.

كما قد تتعرض البيانات الخاصة بالمؤسسات العامة والشركات للسرقة مما يكبدها خسائر فادحة مادية وأدبية، فضلا عن الأضرار بسمعتها خسارتها لعمالئها وأصولها الأدبية، مما قد يضر بالاقتصاد الوطنى بوجه عام.[42]

وعلى الجانب الآخر حددت صفحة "تكنولوجيا" بموقع جريدة عكاظ دافعين رئيسيين لاستمرار الهجمات السيبرانية على السعودية، ويتبلور العامل الأول بزيادة التحولات الرقمية التي تشهدها البلاد على مستوى الخدمات التي تقدمها القطاعات الحكومية بمختلف مستوياتها وتصنيفاتها، فيما يتعلق العامل الثاني بالأحداث الجيوسياسية التي تشهدها المنطقة، والتي تلعب فيها الرياض دوراً محورياً؛ ما يجعلها عرضةً للكثير من الهجمات السيبرانية في أي وقت. [43]

وأرجع موقع جريدة عكاظ تصدر السعودية عام 2018 قائمة الدول العربية في عدد الهجمات السيبرانية الموجهة ضدها واحتلالها المرتبة الـ17 عالمياً في هذا الإطار، بسبب اقتصادها القوي الذي يعد واحداً من أقوى اقتصادات الشرق الأوسط وتصنيفها ضمن أقوى 20 اقتصادا عالميا، مما جعل الشركات والمؤسسات السعودية هدفاً مباشراً وغير مباشر للهجمات السيبرانية، بهدف تعطيل أعمالها، والاستيلاء على بياناتها. [44]

أما عن الاجراءات الدفاعية التي تتخذها مصر دفاعا عن الأمن السيبراني فأكدت صفحة **"**علوم وتكنولوجيا**"** بموقع جريدة اليوم السابع على سعي مصر لإيقاف أي محاولات واختراقات سيبرانية مهما تعاظم اسلوبها وتقنياتها؛ لذا تنفق وزارة الاتصالات 6 مليار جنيه، لتعزيز شبكات الإنترنت وحتى يتم القضاء على مقولة **"السيستم واقع"**، فالهدف هو الاستمرارية، وضمان جودة الخدمات، وسرعتها، وتمكين الجهات والتعاون معها للقيام بعملها. [45]

بينما اتخذت الإجراءات الدفاعية عن الأمن السيبراني في السعودية طابع رعاية خادم الحرمين الشريفين الملك سلمان بن عبدالعزيز آل سعود، بصفة خاصة؛ حيث سلطت صفحة "تكنولوجيا" بموقع جريدة عكاظ الضوء على رعاية خادم الحرمين الشريفين لأعمال المنتدى الدولي للأمن السيبراني في نسخته الأولى بالرياض، وبتوجيه ولي العهد نائب رئيس مجلس الوزراء وزير الدفاع الأمير محمد بن سلمان بن عبدالعزيز، بتبني مبادرتين كريمتين من سموه لخدمة الأمن السيبراني العالمي وهما «حماية الأطفال في العالم السيبراني» و«تمكين المرأة في الأمن السيبراني».

وذلك في إطار ما تشهده المملكة من مسيرة التحديث والتطوير وفق رؤية 2030، التي رسمت التوجهات والأهداف للوصول إلى فضاء سيبراني سعودي يحقق أعلى معايير الأمن والموثوقية الدولية، وإدراك حجم التحديات المتجددة في دول العالم مع التوسع في استخدامات التقنية في جميع مسارات الحياة، وتعزيز التعاون الدولي في هذا المجال.

وتتمحور مبادرة ولي العهد لحماية الأطفال في الفضاء السيبراني حول تطوير أفضل الممارسات والسياسات والبرامج لحماية الأطفال في العالم السيبراني، لمواجهة التهديدات السيبرانية المتزايدة التي تستهدف الأطفال أثناء استخدامهم شبكة الإنترنت

وتعريضهم لجرائم سيبرانية متنوعة بعيداً عن أعين أسرهم، بما في ذلك استغلالهم وجعلهم ضحايا للانقياد وارتكاب الجرائم بحقهم، والتأثير الفكري على توجهاتهم ودفعهم لتبني أيديولوجيات متطرفة وإرهابية تشكل خطراً على الدول والمجتمعات، كما تشمل تلك الجرائم بحق الأطفال، التنمر السيبراني، وسرقة البيانات الشخصية، والاحتيال. وسيكون أحد أبرز أهداف المبادرة هو وضع البرامج وتكوين الشراكات الدولية لتعزيز تحقيق الأهداف المبتغاة على المستوى الدولي والعمل على تبني أفضل الممكنات من قبل المعلمين، والأسر، وصناع القرار لحماية الأطفال في الفضاء السيبراني الدولي.

أما المبادرة الثانية فتتحدد في تمكين المرأة في الأمن السيبراني، والتي تدعو لتكثيف الجهود لتشجيع المرأة ودعمها في مجال الأمن السيبراني وتمكينها من الحصول على التعليم والتأهيل المطلوب لتمكينها من المشاركة الفاعلة في بناء قطاع الأمن السيبراني ولتتبوأ المناصب القيادية فيه، وهو ما يمثل إضافة نوعية لجودة وتنوع المهارات في الأمن السيبراني، علاوةً على الإسهام في تقليص نقص المهارات والمواهب في الأمن السيبراني على المستوى الدولي.[46]

وطرح موقع اليوم السابع أهم التدابير اللازمة لمواجهة الأخطار السيبرانية، وبرامج عمل الاستراتيجية الوطنية للأمن السيبرانى في مصر(2017- 2021)، والتي تشمل: برنامج لتطوير الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية، وبرنامج لتطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبراني وتأمين البنى التحتية الحيوية، وبرنامج لحماية الهوية الرقمية (برنامج المواطنة الرقمية)، وتفعيل البنى التحتية اللازمة لدعم الثقة في التعاملات الالكترونية بوجه عام وفي الخدمات الحكومية الالكترونية بوجه خاص، وبرنامج لإعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في قطاعات الدولة الحيوية، وبرنامج لدعم البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني، وبرنامج للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية للأفراد والمؤسسات والجهات الحكومية، وبأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها.[47]

وشددت جريدة عكاظ على وعي المملكة العربية السعودية لحجم المخاطر الأمنية الكبيرة التي ينطوي عليها الفضاء الافتراضي، وهو ما دعاها إلى تأسيس هيئة وطنية للأمن السيبراني عام 2017، كما تم انشاء كلية الأمير محمد بن سلمان للأمن السيبراني، إضافة للاتحاد السعودي للأمن السيبراني والبرمجة والدرونز، لتوفير كوادر وطنية مؤهلة، وتعمل الهيئات الحكومية بمجملها في المملكة على تحسين وتقوية أمنها السيبراني؛ وذلك في خطوة احتياطية لمرحلة تهدف إلى تقليص الآثار

السلبية لأي هجوم إلكتروني محتمل، وتخطط المملكة لنشر شبكة الجيل الخامس التي ستلعب دوراً مهماً في تحقيق الاستفادة المثلى من التقنيات الحديثة.

بالإضافة إلى إقبال المنتجين المتزايد على إعادة تصميم تطبيقاتهم ورفعها إلى السحابة، مما يتيح للعملاء إمكانيات أوسع للاستفادة بفعالية أكبر من أحدث التقنيات الصاعدة؛ مثل الذكاء الاصطناعي وإنترنت الأشياء وسلسلة الكتل (البلوك تشين)، والروبوتات.[48]

مما دعا شركات الأمن السيبراني لتعزيز استثماراتها في المملكة، حيث قامت بعض الشركات ومنها شركة «تريند مايكرو» وهي من إحدى الشركات العالمية الرائدة في حلول الأمن الرقمي بتحويل قيادتها الاستراتجية في منطقة الشرق الأوسط من دبي إلى الرياض.[49]

وأبرزت صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع تحسن مؤشرات جاهزية مصر فى مواجهة التهديدات الإلكترونية واستعدادها لإدارة الحوادث السيبرانية والجرائم المرتبطة بشبكة الإنترنت، من خلال مجموعة من التدابير اللازمة لحماية البيانات والمعلومات والنظم والشبكات من الانتهاك أو التخريب أو الضياع؛ ومنها: قيام وزارة الاتصالات وتكنولوجيا المعلومات بإنشاء المركز المصرى للاستجابة للطوارئ المعلوماتية CERT لتعزيز أمن البنية المعلوماتية وبنية الاتصالات فى مصر، وتشكيل المجلس الأعلى للأمن السيبرانى، بالإضافة إلى جهود إعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبرانى بمختلف القطاعات بالتعاون والشراكة مع القطاع الخاص والجامعات ومؤسسات المجتمع المدنى؛ وقيام وزارة الاتصالات وتكنولوجيا المعلومات بتنفيذ أجندة تشريعية بدأت مع إصدار قانون مكافحة جرائم تقنية المعلومات الذى غطى مجموعة من الجرائم التى تستهدف المواطنين والاستثمار والجهات الحكومية والخاصة، ويضع حجية فى الإثبات للأدلة الرقمية مما يضمن الوصول لمرتكبى الجرائم الإلكترونية المختلفة لحماية المواطنين وتشجيع الاستثمار، ويضع حجر الأساس فى مكافحة الجرائم السيبرانية، وقامت أيضا بإعداد مشروع قانون حماية البيانات الشخصية الذى حصل على موافقة مجلس الوزراء حيث يهدف القانون إلى حماية بيانات المواطنين فى البنية الرقمية، وتشجيع الاستثمار فى مراكز استضافة البيانات، وتشجيع تكنولوجيات الذكاء الاصطناعى والحوسبة السحابية، كما يجرى الإعداد لمشروع قانون المعاملات الإلكترونية لوضع ضمانات للتجارة الإلكترونية، بالإضافة إلى وضع معايير والتزامات لمقدمى خدمات المعاملات الإلكترونية المختلفة بما يشجع على عمليات الشمول الرقمى والشمول المالى.[50]

وأشار موقع اليوم السابع إلى أن تقنيات "البلوك تشين" من أكثر البرمجيات التى ستضاعف حجم أعمال قطاع الأمن الرقمى. و"البلوك تشين" هو السجل الذى يحفظ

أى تغيرات فى المعلومات المخزنة فى مركز البيانات، وبالتالى حماية هذه البيانات من مختلف التغييرات التى من الممكن أن تحدث فى قواعد البيانات والمعلومات فى كل قطاع يريد حفظ البيانات بشكل آمن. كما ان برامج البلوك تشين تقوم بإعادة حفظ البيانات الأصلية على شبكات المعلومات، حال تغيرها وإعادتها إلى أصلها، حيث لا يُمكن مع هذه التكنولوجيا التلاعب فى البيانات لدى أى جهة، ويحظى البلوك تشين بخصائص توفر الحماية الرقمية فى حالة عمليات نقل البيانات والمعلومات من منظومة رقمية إلى أخرى، باستخدام تطيقات عديدة للتخزين، ونقل البيانات وتأمينها.[51]

وسلط موقع اليوم السابع الضوء على توقيع اتفاقية تعاون بين المعهد القومى للاتصالات التابع لوزارة الاتصالات وتكنولوجيا المعلومات وشركة سيسكو العالمية بهدف إطلاق أول أكاديمية للأمن السيبرانى لشركة سيسكو فى مصر. وتأتى أهمية هذه الاتفاقية نظرا لتطور الهجمات السيبرانية على المستوى العالمى الأمر الذى يتطلب معه ضرورة توافر كوادر مؤهلة ومدربة فى مجال الأمن السيبرانى فى مصر.[52]

وفي هذا الاطار تم توقيع اتفاقيات ومذكرات تفاهم بين الجانبين المصرى والصينى وتبادل للخبرات فى العديد فيما يتعلق بالتحول الرقمى والأمن السيبرانى.[53]

بينما اهتمت صفحة "تكنولوجيا" بموقع جريدة عكاظ بعمل المجلس التنسيقي السعودي الإماراتي (أنشئ مايو 2016) على توفير الوقاية لشبكات المعلومات والبيانات في الدولتين، وتأمينها من الهجمات السيبرانية التي تستهدفها، وذلك من خلال التعاون في مجال التقنيات الحديثة لأمن المعلومات، وهو ما يدعم جهود تعزيز الأمن السيبراني، ويوفر فضاء سيبرانياً موثوقاً للبلدين، يؤمّن تبادل المعلومات والخبرات.[54]

وركزت صفحة "تكنولوجيا" بموقع جريدة عكاظ على الجانب التوعوي أكثر، فقد اصدرت الهيئة الوطنية للأمن السيبراني السعودي، وثيقتي إرشادات الأمن السيبراني لموفري خدمة التجارة الإلكترونية وإرشادات الأمن السيبراني للمستهلكين عبر التجارة الإلكترونية، وذلك بالتعاون مع مجلس التجارة الإلكترونية، لتحقيق تجربة تسوق إلكترونية آمنة تُسهم في حماية أجهزتهم وحساباتهم ومعلوماتهم الشخصية أثناء عمليات التسوق الإلكترونية.

ويواكب صدور هاتين الوثيقتين انتشار التجارة الإلكترونية واعتمادها على وسائل تقنيات المعلومات والاتصالات من جهة، ويواكب من جهة أخرى ظهور جيل جديد من التهديدات السيبرانية التي تستهدف المستهلكين وموفري الخدمة من خلال الاختراقات الأمنية لأنظمة التجارة الإلكترونية وبياناتها، وعبر هجمات تعطيل الخدمات، وغيرها من التهديدات التي تستهدف تسريب البيانات وسرقه الأموال

وتعطيل الخدمات والتأثير على توافر الأنظمة.مما يساهم في رفع الوعي الأمني لدى جميع المتعاملين مع هذا النمط الجديد من التجارة، ولترسيخ أفضل الممارسات؛ لمواجهة تلك التهديدات والحد من آثارها.[55]

كما أبرزت صفحة "تكنولوجيا" بموقع جريدة عكاظ توقيع شركة أرامكو السعودية وشركة الإلكترونيات المتقدمة، اتفاقية تطوير وتصنيع مشترك لجهاز الأمن السيبراني «صمام البيانات»، الأول من نوعه في المملكة، والذي يعد من أهم أدوات الأمن السيبراني، ويستخدم لحماية شبكات اتصالات المنشآت الحيوية من الهجمات السيبرانية، ومنع أي اختراق خارجي وبالتالي حماية المعلومات القيمة والأنظمة الصناعية الحساسة، ويتميّز الجهاز بسهولة تركيبه وتهيئته وصيانته، وبسرعة معالجة للمعلومات تصل إلى 10 جيجابت/ثانية. ويضمن جهاز «صمام البيانات» نقل البيانات بشكلٍ آمن لتوفير أقصى درجات الأمن لشبكات المُنشآت، وتم تطويره وتصنيعه من قبل كفاءات وطنية.[56]

**ثانياً: أساليب الإقناع واستمالات التأثير في خطاب صحافة التكنولوجيا محل الدراسة:**

**1- أساليب الإقناع في خطاب صحافة التكنولوجيا العربية محل الدراسة:**

تنوعت أساليب الإقناع المقدمة داخل خطاب صحافة التكنولوجيا العربية محل الدراسة إزاء الأمن السيبراني، ما بين: أسلوب تقديم الأدلة والشواهد، ووضوح الأهداف، حيث وظفت صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع أسلوب تقديم الأدلة والشواهد بنسبة 60 %، بينما وظفته صفحة "تكنولوجيا" بموقع جريدة عكاظ بنسبة 30%.أما وضوح الأهداف فوظفته صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع بنسبة 40 %، بينما وظفته صفحة "تكنولوجيا" بموقع جريدة عكاظ بنسبة 70%، وذلك على النحو التالي:

وظفت صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع أسلوب تقديم الأدلة والشواهد للتأكيد على تحسن مؤشرات أداء وكفاءة مصر في مواجهة التهديدات الإلكترونية وإدارة الأزمات والتصدي للجرائم الإلكترونية، حيث شغلت مصر المركز 23 دوليا والرابع اقليميا فى مؤشر قياس الاستعداد للأمن السيبرانى الذى صدر من قبل الاتحاد الدولي للاتصالات فى أغسطس 2018.

كما استخدم موقع اليوم السابع أسلوب تقديم الأدلة والشواهد لإبراز استعداد الدولة المصرية لمواجهة الأخطار السيبرانية من خلال: الدعم السياسى والمؤسسى الاستراتيجى والتنفيذى، ويشمل ذلك الوعى بخطورة التهديدات السيبرانية وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية، مع الاهتمام بالاستعداد المسبق بما

يشمل الخطط الاستراتيجية والتنفيذية وخطط الطوارئ وآليات التنسيق العرضى وإعداد الكوادر والتجهيزات التقنية واللوجستية.

وأبرزت صفحة "تكنولوجيا" بموقع جريدة عكاظ -من خلال توظيف أسلوب تقديم الأدلة والشواهد- ضرورة مواءمة سياسات الأمن السيبراني والتعاون في تطوير التقنية وتبادل المعلومات والخبرات بين شركات القطاع الخاص والقطاع العام سواء الجهات الحكومية أو واضعي السياسات أو الجهات التشريعية. فالتهديدات السيبرانية أصبحت أكثر أهمية من أي وقت مضى، لاسيما أن طبيعة المخاطر السيبرانية ليس بمقدور جهة واحدة منفردة التعامل معها، بل تتطلب شراكات كبيرة وتعاون متبادل بين جميع الأطراف ذات العلاقة، كما أنه من الأهمية التسريع في تطوير إطار عالمي واضح يشكّل مرجعية قانونية دولية في الحوكمة السيبرانية، ويعزّز إجراءات الردع والعقاب للجهات التي تتورط في أعمال جرائم الإرهاب السيبراني.

ووظفت صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة أسلوب وضوح الأهداف للتأكيد على سعي مصر لإيقاف أي محاولات واختراقات سيبرانية مهما تعاظم اسلوبها وتقنياتها، وتأمين البنى التحتية للاتصالات وتكنولوجيا المعلومات في مختلف القطاعات وخاصة القطاعات الحيوية؛ بالإضافة إلى أهمية الاستعداد اللازم لمواجهة الأخطار السيبرانية المختلفة خاصة هجمات إعاقة الخدمات الحيوية وتخريب البني التحتية، ونشر الفيروسات الخبيثة والهجمات المركزة، وسرقة البيانات الخاصة والهوية الرقمية.

أما صفحة "تكنولوجيا" بموقع جريدة عكاظ فوظفت أسلوب وضوح الأهداف لإبراز مسيرة التحديث والتطوير التي تشهدها السعودية وفق رؤية 2030، والتي رسمت التوجهات والأهداف للوصول لمجتمع حيوي واقتصاد مزدهر، وإلى فضاء سيبراني سعودي يحقق أعلى معايير الأمن والموثوقية الدولية، وإدراك حجم التحديات المتجددة في دول العالم مع التوسع في استخدامات التقنية في جميع مسارات الحياة، وتعزيز التعاون الدولي في هذا المجال.

**2- استمالات التأثير في خطاب صحافة التكنولوجيا العربية محل الدراسة:**

تنوعت استمالات التأثير التي برزت في خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة ما بين استمالات عقلانية بنسبة 90% واستمالات عاطفية بنسبة 10%. أما خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ فوظف الاستمالات العقلانية بنسبة 80%، والاستمالات العاطفية بنسبة 20%.

وبرزت الاستمالات العقلانية في توظيف خطاب صحافة التكنولوجيا العربية محل الدراسة بشكل رئيس لاستمالات تقديم الأرقام والإحصائيات، والاستشهاد بالمعلومات والأحداث الواقعية، وبناء النتائج على مقدمات، وذلك على النحو التالي:

وظف خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة استمالة تقديم الأرقام والإحصائيات لابراز تحسن مؤشرات أداء وكفاءة مصر في مواجهة التهديدات الإلكترونية وإدارة الأزمات والتصدي للجرائم الإلكترونية، حيث شغلت مصر المركز 23 دوليا والرابع اقليميا فى مؤشر قياس الاستعداد للأمن السيبرانى الذى صدر من قبل الاتحاد الدولي للاتصالات فى أغسطس 2018.

فقد تحسنت مؤشرات جاهزية مصر فى مواجهة التهديدات الإلكترونية واستعدادها لإدارة الحوادث السيبرانية والجرائم المرتبطة بشبكة الإنترنت، حيث شغلت مصر الترتيب الرابع عشر دوليا بين الدول الـ194 دولة فى مؤشر قياس الاستعداد للأمن السيبرانى الذى أصدره الاتحاد الدولى للاتصالات فى يونيو 2017، كما شهدت مصر انخفاضًا ملحوظاً فى معدل قرصنة البرمجيات بنسبة نقطتين مئويتين لتصل إلى 59%؛ وفقاً لما أفاد به الاتحاد العالمى لمنتجى البرمجيات التجارية "BSA".

وتشير التوقعات العالمية إلى زيادة قيمة الخسائر من الهجمات والجرائم السيبرانية علي مستوي العالم عن 2 ترليون دولار أمريكي عام 2019، كما يتوقع زيادة الانفاق علي أنظمة وخدمات أمن المعلومات في العام القادم إلى 124 مليار دولار حيث تجاوز الإنفاق في العام الحالي 100 مليار دولار.

ووفق تقرير صادر عن شركة "ترينـد مايكرو"، العالمية المتخصصة فى مجال حلول الأمن الرقمى هناك مخاوف من تنامى وتيرة الهجمات السيبرانية على مصر، حيث أشارت الشركة إلى أن إجمالى عدد البرمجيات الخبيثة التى اكتشفتها الشركة فى البلاد قد وصل إلى 242.411 برمجية خبيثة خلال الربع الأخير من عام 2017 وحدة، ما يمثل زيادة بنسبة 25% عن الربع الثالث من نفس العام والذى شهد اكتشاف 194.719 برمجية خبيثة.
ووفقاً لهذه النتائج، فإن مصر تأتى فى المرتبة الثالثة من حيث أكثر الدول تعرضاً لتهديدات البرمجيات الخبيثة على مستوى القارة الأفريقية، حيث سجلت جنوب أفريقيا أكبر عدد من البرمجيات الخبيثة والذى بلغ 2.289.997 برمجية خبيثة، وتلتها المغرب بـ341.279 برمجية خبيثة. وكشف التقرير، عن أن قطاع التصنيع فى مصر كان الأكثر تضرراً من هجمات البرمجيات الخبيثة، وتلاه قطاع التعليم، ثم القطاعات الحكومية، والقطاعين العقارى والتكنولوجى.

ومن خلال استمالة تقديم الأرقام والإحصائيات استنكر خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع كون مصر أخر دولة من الدول العربية اصدرت قانون مكافحة جرائم تقنية المعلومات، فهناك 145 دولة فى العالم لديها هذا القانون، والدول العربية غالبيتها لديها هذا القانون حتى السودان.

أما خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ فوظف استمالة تقديم الأرقام والإحصائيات للتحذير من تربع السعودية العام الماضي (2018) على قائمة الدول العربية في عدد الهجمات السيبرانية الموجهة ضدها واحتلت المرتبة الـ17 عالمياً في هذا الإطار.

فقد تعرضت المملكة لتهديدات بالبرمجيات الخبيثة بلغت أوجها في الشهر الأول من عام 2019م حيث بلغت 921,512 ملفاً مصاباً. وانخفض هذا الرقم في فبراير إلى 898,093، وشهد ارتفاعاً طفيفاً في مارس ليصل إلى 904,983. وقد حققت المملكة نتائجاً طيبة في تجنب هجمات الفدية، وحلت في المركز الثالث في الشرق الأوسط، إضافة لمنع من استضافة أحد عناوين URL الخبيثة في المملكة 726 مرة، فيما تخطى عدد تهديدات البريد الإلكتروني الخبيثة التي تم حظرها عبر بروتوكول IP للمرسِل في المملكة 50.6 مليوناً.

ولمواجهة مخاطر التهديدات السيبرانية خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ فوظف استمالة تقديم الأرقام والإحصائيات لابراز تحقيق المملكة المرتبة الأولى عالمياً في إصلاحات بيئة الأعمال في تقرير البنك الدولي. كما ان المملكة الأولى على مستوى دول مجموعة الـ20 من حيث نسبة الحركة التي تخدم الامتداد الآمن لنظام أسماء النطاقا (DNSSEC)، بنسبة بلغت 96% من إجمالي الحركة في المملكة. وذلك بعد أن مكَّنت الهيئة الامتداد الآمن لنظام أسماء النطاقات في جميع شبكات المشغلين؛ بهدف الرفع من مستوى أمان ومتانة البنية التحتية للمجتمع الرقمي.

وقد كشف تقرير بعنوان «توقعات سوق الأمن السيبراني في الشرق الأوسط وأفريقيا حتى العام 2023م» الصادر حديثًا، عن نمو سوق الأمن السيبراني في المملكة العربية السعودية إلى 5.5 مليار دولار بحلول عام 2023. وشهد عام 2019م ارتفاع قيمة سوق الأمن السيبراني إلى 3 مليارات دولار (ما يعادل 11 مليار و25 مليون ريال)، مع زيادة الاستثمارات في القطاع.

وبحسب الاتحاد الدولي للإتصالات التابع للأمم المتحدة (ITU)، احتلت المملكة العربية السعودية المرتبة الأولى على المستوى الإقليمي والثالث عشر على المستوى العالمي من بين 175 دولة، في المؤشر العالمي للأمن السيبراني (GCI) لعام 2018، متقدمةً 33 مرتبة عن ترتيبها السابق.

وشهدت النسخة الثالثة من تقرير التنافسية الرقمية العالمية، الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية (IMD)، تقدماً في ترتيب المملكة العربية السعودية، حيث حلّت المملكة في المركز السابع عالمياً في مؤشر الأمن السيبراني، الذي يندرج ضمن مؤشر تكامل تكنولوجيا المعلومات. الأمر الذي ينعكس على الجاهزية المستقبلية للمملكة، وطبيعة الأعمال ومفاهيم الابتكار فيها، ويرتقي بمستوى الخدمات ويسرّع وتيرتها. علاوة على ما سبق، شهد الأداء السعودي

أيضاً قفزةً نوعيةً وتقدماً غير مسبوق في مؤشري البيئة التنظيمية الرقمية، وتوافر رأس المال للقطاع الرقمي، الأمر الذي يعكس تركيز الحكومة السعودية على تبني التحول الرقمي وكل ما تمثله الرقمنة من فرص وفوائد اقتصادية واجتماعية. ويعدّ ذلك نتيجة مباشرة للإستراتيجية الرقمية، وبرنامج التحوّل الوطني، والرؤية السعودية 2030.

ووظف خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة استمالة الاستشهاد بالمعلومات والأحداث الواقعية للتأكيد على أهمية استعداد مصر لمواجهة الأخطار السيبرانية المختلفة خاصة هجمات إعاقة الخدمات الحيوية وتخريب البني التحتية، ونشر الفيروسات الخبيثة والهجمات المركزة، وسرقة البيانات الخاصة والهوية الرقمية.

ومن خلال استمالة الاستشهاد بالمعلومات والأحداث الواقعية أبرز خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ اتباع المملكة إجراءات مشددة لتعزيز أمنها السيبراني، تتمثل في: تطبيق أنظمة المراقبة والتحكم باستخدام الذكاء الاصطناعي، والشراكات مع الجهات الرائدة في مجال الأمن السيبراني، والاستثمار في تطوير الكفاءات البشرية القادرة على التعامل مع هذا النوع من التهديدات الخطيرة.

أما استمالة بناء النتائج على مقدمات فوظفها خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة للتأكيد على أهمية التوعية المجتمعية بالفرص والمزايا التى تقدمها الخدمات الإلكترونية المؤمنة للأفراد والمؤسسات، وبأهمية الأمن السيبرانى لحماية تلك الخدمات من المخاطر والتحديات التى قد تواجهها، فضلا عن حماية الخصوصية وإطلاق برامج حماية الأطفال والنشء على الإنترنت، فالمشكلة تكمن فى سهولة الوصل للإنترنت وصعوبة السيطرة على الأجيال الجديدة للوصل للإنترنت.

فيما برزت الاستمالات العاطفية في توظيف الخطاب محل الدراسة لاستمالات التخويف، بالإضافة إلى الاستشهاد بشخصيات مشهورة، وكذلك آراء مواطنين عاديين.

حيث وظف خطاب موقع جريدة اليوم السابع محل الدراسة استمالة التخويف، حيث تعرض الموقع الرسمى لوزارة الصحة والسكان، للاختراق من قبل هاكرز، مما تسبب فى تعطله عن العمل، وقال المخترقون إنهم "**هاكرز إيرانيون**"، **ووضعوا رسالة قالوا فيها: "دائما قريبين لك، نعرف هويتك، ومعلوماتك خاصة بنا.. احذر**".[57]

واستخدم خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ استمالة أفعل التفضيل للتأكيد على أن التهديدات السيبرانية في المنطقة تتزايد، **والمملكة هي الأكثر استهدافاً**، مما يتطلب عملا مضاعفا لمكافحة التهديدات.[58]

ومن خلال استمالة الاستشهاد بشخصيات مشهورة أكد خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ على أن **"الأمن السيبراني ليس مجرد تقنيات بل هو نمط حياة"**، هكذا قال مات قرانيارد مدير عام المنظمة العالمية للاتصالات البريطانية خلال المنتدى الدولي للأمن السيبراني في مدينة الرياض.[59]

**ثالثاً: بالنسبة للأطر المرجعية التى استند إليها خطاب صحافة التكنولوجيا العربية محل الدراسة:**

تنوعت الإحالات المرجعية التي اعتمد عليها خطاب صحافة التكنولوجيا العربية محل الدراسة ما بين: سياسية، وأحداث واقعية، وقانونية، والخسائر والنتائج، ومرجعية الأهمية، وذلك على النحو التالي:

المرجعية السياسية (التصريحات): اتخذ خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة تصريحات عمرو طلعت وزير الاتصالات، **"إن مصر دولة مستهدفة وكلما زادت التكنولوجيا أصبحنا أكثر عرضة لتهديدات أمننا السيبراني"**، مضيفا: **"نسعى لإيقاف أي محاولات واختراقات سيبرانية مهما تعاظم اسلوبها وتقنياتها"**.[60] كمرجعية للتأكيد على أهمية الوعى بخطورة التهديدات السيبرانية وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية لتفعيل منظومة الأمن السيبرانى فى مختلف قطاعات الدولة، وزيادة الإنفاق على حماية البنى التحتية للاتصالات وتكنولوجيا المعلومات للمؤسسات المختلفة من المخاطر السيبرانية فى ظل تزايد الهجمات السيبرانية المتعددة.

أما خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ فوظف المرجعية السياسية من خلال تصريحات وزير التجارة والاستثمار الدكتور ماجد القصبي، بأن **"التهديدات السيبرانية في المنطقة تتزايد، والمملكة اليوم هي الأكثر استهدافاً، مما يتطلب عملا مضاعفا لمكافحة التهديدات"**.[61] لإلقاء الضوء على المواطنة الرقمية كإحدى ركائز رؤية السعودية ٢٠٣٠ التي يعمل صناع القرار لهيكلتها وتدعيمها بالشكل المناسب والمأمول

مرجعية الخسائر والنتائج: وظف خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة هذه المرجعية للتحذير من خطورة الهجمات السيبرانية، من حيث إمكانية الأضرار بمصالح الجهات العامة والخاصة، والتأثير على جموع كبيرة من المواطنين بصورة مفاجئة وفى وقت قصير وعن بعد.

مرجعية الأهمية: استخدم خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة مرجعية الأهمية لإبراز خطورة الهجمات السيبرانية، والتي أصبحت تضم متخصصين في الجرائم السيبرانية تعادل قدراتهم، إن لم تكن أفضل من قدرات الجهات الفاعلة في الدولة.

ووظف خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ مرجعية الأهمية لتسليط الضوء على أهمية التسريع في تطوير إطار عالمي واضح يشكّل مرجعية قانونية دولية في الحوكمة السيبرانية، ويعزّز إجراءات الردع والعقاب للجهات التي تتورط في أعمال جرائم الإرهاب السيبراني.

المرجعية القانونية**:** برز هذا النمط من الاستشهادات في سياق تأكيد خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة على أهمية مشروعات القوانين المنظمة لقطاع الاتصالات وتكنولوجيا المعلومات، مثل قانون تنظيم الاتصالات، قانون الملكية الفكرية، قانون التوقيع الإلكتروني، قوانين خصوصية البيانات، والجرائم الالكترنية، وقانون مكافحة جرائم تقنية المعلومات في مصر، والأمن السيبراني. مما يسهم في تفهم المجتمع المصري لتقنية المعلومات وشكلها الاحترافي بما يتناسب مع التوجهات الاقتصادية لحلول تكنولوجيا المعلومات ووسائل الاتصالات.

مرجعية الأحداث الواقعية: وظف خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة هذه المرجعية للتأكيد على ان الأمن السيبرانى على رأس أولويات وزارة الاتصالات وتكنولوجيا المعلومات منخلال المشاركةفي العديد من الفاعليات الاقليمية والدولية.

ومن خلال مرجعية الأحداث الواقعية أكد خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ على أن الأمن السيبراني أولوية في السياسات الدفاعية الوطنية. فقد أعلنت أكثر من 130 دولة حول العالم عن تخصيص أقسام وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني، تضع خطة إستراتيجية وطنية للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة وتعزز التعاون الوطني بين الحكومة ومنظومة صناعة الاتصالات والمعلومات ومقاومة وردع الجريمة السيبرانية وتجهيز قدرات وطنية لإدارة الحوادث المتعلقة بالفضاء السيبراني وتشكيل ثقافة وطنية للأمن السيبراني.

**رابعًا: بالنسبة للقوى الفاعلة البارزة في خطاب صحافة التكنولوجيا العربية محل الدراسة:**

برز في خطاب صحافة التكنولوجيا العربية محل دراسة مجموعة من الفاعلين الرئيسيين، أبرزهم: جمهورية مصر العربية، والمملكة العربية السعودية، والأمن السيبراني، والهجمات السيبرانية، المجلس الأعلى للأمن السيبراني بمصر، والهيئة الوطنية للأمن السيبراني السعودي، وذلك على النحو التالي:

جاءت مصر كإحدى القوى الفاعلة الرئيسة في خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة، حيث أنها تحرص على تأمين البني التحتية للاتصالات وتكنولوجيا المعلومات ورفع مستوى الاستعداد لمواجهة الأخطار

السيبرانية بما يساهم في تعزيز دور صناعة تكنولوجيا الاتصالات والمعلومات في تنمية القدرة التنافسية لمصر وخلق فرص عمل وجذب الاستثمارات. كما أنها تتقدم بخطىً ثابتة في مجال تنمية وتطوير قطاع الاتصالات وتكنولوجيا المعلومات باعتباره أحد القطاعات الهامة للاقتصاد القومي.

ووصف خطاب صحيفة اليوم السابع محل الدراسة مصر بأنها: "**على أول الطريق في سلسة من تشريعات، والقوانين المنظمة لتقنيات المعلومات**"[62]، كما أنها "**دولة مستهدفة، وأكثر عرضة لتهديدات أمنها السيبراني**".[63]

أما السعودية فجاءت كقوى فاعلة رئيسة في خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ، والتي تعمل على إزالة البيروقراطية وتسريع وتعزيز بيئة العمل والاستثمار، لمواجهة التهديدات السيبرانية، وقد ركزت رؤية المملكة 2030 على النمو الموجه بالتكنولوجيا والتأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال وتبوء مكانة رائدة في الاقتصاد الرقمي.

وأسند خطاب جريدة عكاظ العديد من السمات الإيجابية للمملكة، حيث وصفها بأنها: "**تعي حجم المخاطر الأمنية الكبيرة التي ينطوي عليها الفضاء الافتراضي، ولديها اهتمام وطني كبير في تطوير الأمن السيبراني**".[64]

وبرز الأمن السيبراني كقوى فاعلة في خطاب صحافة التكنولوجيا محل الدراسة، فقد اعتبر خطاب موقع اليوم السابع الأمن السيبرانى أمن المعلومات على أجهزة وشبكات الحاسب الآلى، بما فى ذلك العمليات والآليات التى يتم من خلالها حماية معدات الحاسب الآلى والمعلومات والخدمات من أى تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث، ويشمل الحماية من اختراق شبكات المعلومات فى البلاد والمعلومات السرية والهجمات الإليكترونية وفيروسات الـ"سوفت وير" وغيرها.[65]

ويشكل الأمن السيبرانى في خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ "مجموع الأطر القانونية والتنظيمية، والهياكل التنظيمية، وإجراءات سير العمل إضافة إلى الوسائل التقنية والتكنولوجية التي تمثل الجهود المشتركة للقطاعين الخاص والعام، المحلية والدولية والتي تهدف إلى حماية الفضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية وحماية سرية المعلومات الشخصية واتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني".[66]

وأسند خطاب صحافة التكنولوجيا محل الدراسة للأمن السيبرانى العديد من السمات الإيجابية، حيث وصفه خطاب موقع اليوم السابع بأنه: "**أحد أهم أركان استراتيجية بناء مصر الرقمية، ركيزة من الركائز الأساسية فى اقتصاد قائم على المعرفة التكنولوجية الذكية**".[67]

ويرى خطاب موقع عكاظ الأمن السيبراني باعتباره: **"أسلوب حياة، وتعلّمه أصبح ضرورة لا بد منها.. نظراً لأن حياتنا اليومية أصبحت أكثر اعتماداً على الإنترنت.."** [68]

وجاءت الهجمات السيبرانية كإحدى القوى الفاعلة الرئيسة في خطاب صحافة التكنولوجيا محل الدراسة، فوفق خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ الهجوم السيبراني على دولة ما في العالم بمثابة الهجوم العسكري، وتخدم الهجمات السيبرانية أهداف معينة وفي مقدمتها الأهداف السياسية، ليس بمقدور جهة واحدة منفردة التعامل معها، بل تتطلب شراكات كبيرة وتعاون متبادل بين جميع الأطراف ذات العلاقة.

ووصفها خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع بأنها**: "خطيرة، وتستند إلى تقنيات متقدمة ومتطورة، كما أنها تتعدى الحدود الجغرافية للدول، وتعتمد على شبكات الجريمة المنظمة بشقيها التقليدى والتقني".**[69] واعتبر خطاب موقع جريدة عكاظ التهديدات السيبرانية **"إرهاب متنامٍ يتخطى حدود المؤسسات والدول".**[70]

وجاء المجلس الأعلى للأمن السيبراني كإحدى القوى الفاعلة الرئيسة في خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع، حيث تم تكليف الجهات الحكومية بكافة مستوياتها بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السبرانى، فيما يتعلق بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات الخاصة بها، واتخاذ كافة الإجراءات الفنية والإدارية لمواجهة الأخطار والهجمات السبرانية، لتعزيز أمن البنية المعلوماتية وبنية الاتصالات فى مصر، بالإضافة إلى جهود إعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبرانى بمختلف القطاعات.

وبرزت الهيئة الوطنية للأمن السيبراني كإحدى القوى الفاعلة الرئيسة في خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ، حيث تسعى للوصول إلى فضاء سيبراني سعودي آمن وموثوق، من خلال تأهيل وتطوير كوادر وطنية متخصصة لسد الفجوة في مجال الأمن السيبراني، لرفع مستوى الوعي ونشر التحذيرات وتعزيز المعرفة بأخطار الأمن السيبراني.

**خامساً: بالنسبة لآليات خطاب صحافة التكنولوجيا العربية محل الدراسة إزاء الأمن السيبرانى:**

اعتمد خطاب صحافة التكنولوجيا العربية محل الدراسة على آليتين رئيسيتين عند تناوله الأمن السيبراني، وهي: آلية المسئولية، وآلية الكشف والتنوير، وضمت كل آلية مجموعة من الاستراتيجيات والتكنيكات، وذلك على النحو التالي:

آلية المسئولية: اعتمد خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع ضمن هذه الآلية على استراتيجيات التأكيد على اهتمام الحكومة المصرية بملف الأمن السيبراني، فمصر لديها حلول وكوادر قادرة على وقف الهجمات السيبرانية ووضع تصورات مستقبلية لتطور الجريمة الإلكترونية، ووقف مخاطرها على المجتمع المصري.

واعتمد الخطاب على عدة تكنيكات منها ابراز دور الحكومة المصرية من خلال تسليط الضوء على الأسس التي وضعتها وزارة الاتصالات وتكنولوجيا المعلومات لمواجهة التحديات التي تفرضها التهديدات السيبرانية، حيث تم تشكيل المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات EG Cert التابع للجهاز القومي لتنظيم الاتصالات فى أبريل 2009، كما تم تشكيل المجلس الأعلى للأمن السيبرانى في 2017 ؛ للارتقاء بمستوى الاستعداد لمواجهة المخاطر السيبرانية في شتى قطاعات الدولة .

ووظف الخطاب استراتيجية الوصف أوالتشخيص، للإجرات التي تتخذها مصر لاعمال الأمن السيبراني، خاصة مشروعات القوانين المنظمة لقطاع الاتصالات وتكنولوجيا المعلومات، مثل قانون تنظيم الاتصالات، وقانون الملكية الفكرية، وقانون التوقيع الإلكتروني، وقوانين خصوصية البيانات، والجرائم الالكترنية، والأمن السيبراني.

كما اعتمد الخطاب محل الدراسة على استراتيجية بث الأمل، فالجهود الحكومية فى طريق التحول إلى الوطن الرقمى، والذى يشتمل على منصة الخدمات والهوية الموحدة للمواطن والاستراتيجيات الوطنية للأمن السيبراني والذكاء الاصطناعي.

بالإضافة إلى استراتيجية استشراف المستقبل، حيث تسعى مصر لتطوير استراتيجية شاملة متكاملة لصناعة أمن المعلومات وحماية البيانات، من أجل ضمان ثقافة إلكترونية آمنة ومجتمع معلوماتي آمن وتحديد أدوار ومسؤوليات الجهات الحكومية والموظفين العاملين لديها والمتعاملين معها.

أما خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ فاعتمد ضمن آلية المسئولية على التأكيد على وعي المملكة العربية السعودية بحجم المخاطر الأمنية الكبيرة التي ينطوي عليها الفضاء الافتراضي، وهو ما دعاها إلى تأسيس هيئة وطنية للأمن السيبراني عام 2017، كما أن الهيئات الحكومية بمجملها في المملكة تعمل على تحسين وتقوية أمنها السيبراني من أجل حماية بياناتها، وعملياتها، وخدماتها وأماكن تخزين معلوماتها؛ وذلك في خطوة احتياطية لمرحلة تهدف إلى تقليص الآثار السلبية لأي هجوم إلكتروني محتمل.

وفي هذا السياق وظف خطاب موقع عكاظ استراتيجية التساؤل، **كيف يمكن أن يكون لكل شخص منا تأثير واعٍ في معالجة المعلومات؟** كما وظف الخطاب محل

الدراسة استراتيجية الخطاب المباشر، لا تتعاطى مع كل ما يصلك على أنه مسلمات، ولا تتداول المعلومة إلا من مصدرها المباشر، لا تترك حساباتك رهن حسن النية أو الأجهزة سهلة الوصول. [71]

يالإضافة إلى استراتيجية الاستشراف، تهدف المملكة إلى أن تكون ضمن أكبر 20 دولة رقمية رائدة عالمياً بحلول عام 2030. كما اعتمد الخطاب على استراتيجية الخلاص، فالاستهدافات السيبرانية على السعودية تستدعي الانتباه واليقظة، فوفقاً لرؤية 2030، تعمل الحكومة السعودية على دعم قطاع تقنية المعلومات، وتعزيز الفكر الإبداعي والابتكاري للشركات وحماية بياناتها وأنظمتها الإلكترونية. مع الأخذ في الاعتبار أهمية التركيز على رأس المال البشري بدلا من التزكيز الكامل على الأدوات والتقنيات التي تحتاجها الشركات والأجهزة الحكومية لمواكبة العصر الرقمي.

آلية الكشف والتنوير: اعتمد خطاب صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع ضمن هذه الآلية على استراتيجيات أن مصر دولة مستهدفة وكلما زادت التكنولوجيا أصبحت أكثر عرضة لتهديدات أمنها السيبراني؛ لذا تنفق وزارة الاتصالات 6 مليار جنيه، لتعزيز شبكات الإنترنت .

ووظف الخطاب محل الدراسة ضمن هذه الآلية استراتيجيات الخلاص من التهديدات السيبرانية، من خلال اتباع نهج شامل متعدد الطبقات - يجمع بين الحماية التقنية والتدريب المنتظم لمتخصصى أمن تكنولوجيا المعلومات ومشغلى الشبكات الصناعية – بما يضمن بقاء الشبكات محمية من التهديدات ومهارات البقاء محدثة. كما يجب وضع منهجية ومدونة سلوك وخطة عمل لتحويل الانترنت إلى أداة من أدوات التنمية المشتركة بين دول العالم وليس فقط استحواذ بعض دول العالم على مكون الانترنت وما يطرحه من معلومات وبيانات.

أما خطاب صفحة "تكنولوجيا" بموقع جريدة عكاظ فاعتمد ضمن آلية الكشف والتنوير على التأكيد على رؤية المملكة 2030 على النمو الموجه بالتكنولوجيا والتأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال وتبوء مكانة رائدة في الاقتصاد الرقمي وتحقيق نهضة تقنية تخدم مستقبل الاقتصاد الوطني للمملكة وأن تكون بيئة جاذبة للشركات العالمية المختصة في هذا المجال.

ووظف الخطاب محل الدراسة ضمن هذه الآلية استراتيجية الخلاص، فبيئة التهديدات السيبرانية تتطلب من الحكومات والأفراد إعطاء أولوية خاصة لاتخاذ الإجراءات والتدابير اللازمة لحماية أنفسهم من الهجمات، ويتطلب هذا الأمر تحديد الثغرات الأمنية التي يمكن للقراصنة استغلالها عبر كامل سلسلة التوريد. وفي الوقت عينه، ينبغي على الحكومات والمؤسسات أن تستثمر في إجراءات جدية للامن السيبراني أو للحماية من هجمات خطرة يمكن أن تعرض عملياتها كافة للمخاطر.

**مناقشة النتائج:**

سيتم مناقشة النتائج في ضوء ما توصلت إليه الدراسة من نتائج كاشفة، بالإضافة إلى مناقشتها في ضوء أهداف الدراسة وتساؤلاتها، وكذلك في ضوء الإطار النظري، والدراسات السابقة، وذلك على النحو التالي:

**أولا: مناقشة النتائج في ضوء النتائج العامة للدراسة:**

على مستوى أطروحات خطاب صحافة التكنولوجيا العربية محل الدراسة والحجج الداعمة لها إزاء الأمن السيبراني: اتفق خطاب صحافة التكنولوجيا العربية محل الدراسة على أن الحاجة للأمن السيبراني هي حاجة دفاعية عن الذات والمنجزات الوطنية، فلم تعد الهجمات السيبرانية نتاج عمل أشخاص بمفردها أو مجموعات من القراصنة فقط ولكنها أصبحت تضم متخصصين في الجرائم السيبرانية يتعاونون معا ويستثمرون أموالا ضخمة فيها، فضلا عن المعرفة والخبرة والمثابرة، وأصبحت قدرات هؤلاء المتخصصين تعادل إن لم تكن أفضل من قدرات الجهات الفاعلة في الدولة.

واتخذت صفحة "تكنولوجيا" بموقع جريدة عكاظ خطوات استباقية من خلال تقديم أطروحات حول المواطنة الرقمية كإحدى ركائز رؤية المملكة ٢٠٣٠ التي يعمل صناع القرار لهيكلتها وتدعيمها بالشكل المناسب.

على مستوى أساليب الإقناع في خطاب صحافة التكنولوجيا العربية محل الدراسة: وظف خطاب صحافة التكنولوجيا العربية محل الدراسة أسلوب تقديم الأدلة والشواهد، ووضوح الأهداف، لإبراز استعداد كل من مصر والسعودية لمواجهة الأخطار السيبرانية، لاسيما أن طبيعة المخاطر السيبرانية ليس بمقدور جهة واحدة منفردة التعامل معها، بل تتطلب شراكات كبيرة وتعاون متبادل بين جميع الأطراف ذات العلاقة، كما أنه من الأهمية التسريع في تطوير إطار عالمي واضح يشكّل مرجعية قانونية دولية في الحوكمة السيبرانية، ويعزّز إجراءات الردع والعقاب للجهات التي تتورط في أعمال جرائم الإرهاب السيبراني.

على مستوى استمالات التأثير في خطاب صحافة التكنولوجيا العربية محل الدراسة: وظف خطاب صحافة التكنولوجيا العربية محل الدراسة الاستمالات العقلانية بنسبة تفوق الاستمالات العاطفية بدرجة كبيرة .

وبرزت الاستمالات العقلانية في توظيف خطاب صحافة التكنولوجيا العربية محل الدراسة بشكل رئيس لاستمالات، حيث اتفق خطاب صحافة التكنولوجيا العربية محل الدراسة في توظيف استمالات تقديم الأرقام والإحصائيات، والاستشهاد بالمعلومات والأحداث الواقعية، وبناء النتائج على مقدمات، لابراز

تحسن مؤشرات أداء وكفاءة كل من مصر والسعودية في مواجهة التهديدات الإلكترونية وإدارة الأزمات والتصدي للجرائم الإلكترونية

على مستوى الأطر المرجعية التي استند إليها خطاب صحافة التكنولوجيا العربية محل الدراسة: تنوعت الإحالات المرجعية التي اعتمد عليها خطاب صحافة التكنولوجيا العربية محل الدراسة ما بين: سياسية، وأحداث واقعية، وقانونية، والخسائر والنتائج، ومرجعية الأهمية، للتأكيد على أهمية الوعى بخطورة التهديدات السيبرانية، وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية لتفعيل منظومة الأمن السيبرانى فى مختلف قطاعات الدولة، وزيادة الإنفاق على حماية البنى التحتية للاتصالات وتكنولوجيا المعلومات للمؤسسات المختلفة من المخاطر السيبرانية فى ظل تزايد الهجمات السيبرانية المتعددة.

على مستوى القوى الفاعلة البارزة في خطاب صحافة التكنولوجيا العربية محل الدراسة: برز في خطاب صحافة التكنولوجيا العربية محل دراسة مجموعة من الفاعلين الرئيسيين، أبرزهم: جمهورية مصر العربية، والمملكة العربية السعودية، والأمن السيبراني، والهجمات السيبرانية، والمجلس الأعلى للأمن السيبراني بمصر، والهيئة الوطنية للأمن السيبراني السعودي، لإبراز دور كل منهم في تأمين البني التحتية للاتصالات وتكنولوجيا المعلومات ورفع مستوى الاستعداد لمواجهة الأخطار السيبرانية.

على مستوى آليات خطاب صحافة التكنولوجيا العربية محل الدراسة إزاء الأمن السيبراني: اعتمد خطاب صحافة التكنولوجيا العربية محل الدراسة على آليتين رئيسيتين عند تناوله الأمن السيبراني، وهي: آلية المسئولية، وآلية الكشف والتنوير، للتأكيد على اهتمام الحكومة المصرية والسعودية بملف الآمن السيبراني، واستعدادهما لوقف الهجمات السيبرانية ووضع تصورات مستقبلية لتطور الجريمة الإلكترونية، ووقف مخاطرها على المجتمع.

**ثانيا: مناقشة النتائج في ضوء أهداف الدراسة وتساؤلاتها:**

استطاع البحث تحقيق الهدف الرئيسي الذي يتمثل في: تفسير إستراتيجيات الأمن السيبراني في خطاب صحافة التكنولوجيا في كل من مصر والسعودية ، خلال فترة الدراسة (من يناير 2018م إلى يناير2019م)؛ بغية استكشاف الآليات التي استخدمتها صحف الدراسة، والعوامل والمتغيرات المؤثرة في إنتاج هذا الخطاب.

وقد استطاعت الباحثة تحقيق هذا الهدف من خلال الإجابة على تساؤلات الدراسة، فقد قامت الدراسة التحليلية بالإجابة عن تساؤلات الدراسة المعنية بالأطروحات التي ارتكزت عليها خطاب صحف الدراسة في سياق استراتيجيات

. كما فسرت الدراسة التحليلية الأساليب الإقناعية والاستمالات التأثيرية التي استند إليها الخطاب الصحفي محل الدراسة ودلالات توظيفها، ورصدت الدراسة التحليلية القوى الفاعلة البارزة في الخطابات الصحفية محل الدراسة، كما حددت الدراسة التحليلية المرجعية التي استندت إليها الخطابات الصحفية محل الدراسة، وكذلك الآليات التي استخدمتها الخطابات الصحفية محل الدراسة ومحددات تشكيلها في ضوء استراتيجيات الخطاب والتكنيكات التي تم توظيفها في سياق كل آلية.

وأفاد تحليل الخطاب الباحثة في تفسير النتائج وصياغة رؤية متكاملة فيما يتعلق بخطاب صحافة التكنولوجيا محل الدراسة تجاه الأمن السيبراني، حيث مكن تحليل الخطاب الباحثة من الاقتراب من إستراتيجيات الخطاب محل الدراسة، وتحديد الأطروحات، والأساليب الإقناعية والاستمالات التأثيرية، والقوى الفاعلة البارزة في الخطابات الصحفية، والمرجعية التي استندت إليها، والآليات التي ارتكزت عليها خطابات صحف الدراسة.

**ثالثا: مناقشة النتائج في ضوء الإطار النظري:**

في ضوء نظرية المسئولية الاجتماعية قامت صحف الدراسة بالتعبير عن قضايا الأمن السيبراني الخاصة بكل من مصر والسعودية، فقد اتفق خطاب صحافة التكنولوجيا العربية محل الدراسة على أن الحاجة للأمن السيبراني هي حاجة دفاعية عن الذات والمنجزات الوطنية.

بالإضافة إلى أن صحف الدراسة طرحت حلول لمواجهة الهجمات السيبرانية واتخذت صفحة "تكنولوجيا" بموقع جريدة عكاظ خطوات استباقية من خلال تقديم أطروحات حول المواطنة الرقمية كإحدى ركائز رؤية المملكة ٢٠٣٠ التي يعمل صناع القرار لهيكلتها وتدعيمها بالشكل المناسب.

**رابعا مناقشة النتائج في ضوء الدراسات السابقة:**

اتفقت نتائج الدراسة مع معظم الدراسات السابقة، حيث اتفقت نتائج الدراسة مع: دراسة [72] **Kolenko, M. M. (2019)** ، ودراسة [73] **Cook, K. D. (2017)**، ودراسة [74] **Dawson, M. (2017)** حول أهمية الوعي المجتمعي بخطورة التهديدات السيبرانية وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية، مع الاهتمام بالاستعداد المسبق بما يشمل الخطط الاستراتيجية والتنفيذية وخطط الطوارئ وآليات التنسيق العرضى وإعداد الكوادر والتجهيزات التقنية واللوجستية.

وكذلك اتفقت مع نتائج دراسة [75] **Ghazi-Tehrani, A. (2016)** فيما يتعلق بأهمية التعاون بين الجهات المختلفة، ووجود معايير أمنية مقننة لتحقيق الأمن السيبراني.

كما اتفقت مع دراسة [76]**Hammad, E. (2018)** حول أن الأمن السيبراني نهجا استراتيجيا للتخطيط والتصميم والتشغيل؛ نتيجة لزيادة الاعتماد على الأدوات والشبكات السيبرانية.

واتفقت مع دراسة [77]**Osmak, K. A. (2019)** ودراسة [78] **De Los Santos, S. (2016)** حول أن الأمن السيبراني يفتقر إلى إطار فعال وسياسات لتلبية متطلباته.

واتفقت الباحثة مع دراسة **[79]Imranuddin, M. (2017)** التي أكدت على أهمية تعاون الدول العربية مع مختلف الوكالات الدولية لتحسين أمنها السيبراني، حتى لا تتعرض الدولة برمتها للخطر.

كما اتفقت الباحثة مع دراسة [80]**Layne, C. (2017)** [81] **Abraham, S. (2016)** على أن أفضل رادع للجريمة السيبرانية هو فهم أنواع الهجمات حتى يمكن اتخاذ خطوات دفاعية للحد من أثر الهجمات المماثلة في المستقبل.

واختلفت نتائج الدراسة مع: دراسة [82]**Churchwell, C. (2018)** حول عدم وضع تعريف محدد لمصطلحات مثل الجريمة السيبرانية والدفاع والانتقام السيبراني، لأن كل من مصر والسعودية لديهم تعريف واضح لهذه المصطلحات.

**مقترحات الدراسة:**

- ابراز الخطاب الصحفي لضرورة توفير آليات حماية وأمن أكثر قوة لمستخدمي الإنترنت، وتوسيع الخيارات الأمنية التي يمكن أن تحمي بشكل أفضل المستخدمين.
- توظيف الفنون الصحفية لنشر التوعية المجتميعة بالفرص والمزايا التى تقدمها الخدمات الإلكترونية المؤمنة للأفراد والمؤسسات، وبأهمية الأمن السيبرانى لحماية تلك الخدمات من المخاطر والتحديات التى قد تواجهها، فضلا عن حماية الخصوصية وإطلاق برامج حماية الأطفال والنشء على الإنترنت.
- الجاهزية بالنسبة لمجال الأمن السيبراني ليست مطلقة نظراً لأن المخترق عادة يبحث عن ثغرات، كما أن صناعة أمن المعلومات تستغرق وقت كبير في بنائها بقطاعات الدولة المختلفة، لذا فإنه من الأهمية تامين التعاملات الرقمية عبر ثلاث محاور رئيسية، هي: الإطار التشريعي، والتوعية المجتمعية، والحلول التكنولوجية التي تنتجها الشركات.
- لابد من التعاون المكثف بين مختلف الحكومات والدول والشعوب لتحقيق الأمن السيبراني، وهذا يتطلب وضع منهجية ومدونة سلوك وخطة عمل لتحويل الانترنت إلى أداة من أدوات التنمية المشتركة بين دول العالم وليس فقط استحواذ بعض دول العالم على مكون الانترنت وما يطرحه من معلومات وبيانات.

## هوامش الدراسة:

* تعتبر فيروسات الفدية أحد أشكال البرمجيات الخبيثة التي تطالب الضحايا بدفع فديةٍ مالية مقابل فك تشفير المعلومات والبيانات التي تحول دون الوصول إليها. وفي هذا السياق، يثير دفع الفدية جدلًا بين خبراء الأمن السيبراني؛ فعلى الرغم من تضاؤل قيمة الفدية مقارنةً بإعادة بناء الأنظمة والبنية التحتية المعلوماتية في كثيرٍ من الأحيان؛ إلا أن دفعها يشجع الأنشطة الإجرامية، ويُعَدُّ مكافأة للقراصنة والمتسللين

[1] تعريف وزارة الاتصالات وتكنولوجيا المعلومات بجمهورية مصر العربية، متاح من خلال:
http://www.mcit.gov.eg/Ar/TeleCommunications/Cyber_Security

[2] Oloidi, A. (2019). **Cyber-security challenges in financial institutions in nigeria: A multiple case study** (Order No. 13813041). Available from ProQuest Dissertations & Theses Global. (2207495699). Retrieved from https://search.proquest.com/docview/2207495699?accountid=178282

[3] Kolenko, M. M. (2019). **Cyber Defender Cultural Patterns and Operational Behavior** (Order No. 27547553). Available from ProQuest Dissertations & Theses Global. (2318150054). Retrieved from https://search.proquest.com/docview/2318150054?accountid=178282

[4] Alotaibi, F. F. G. (2019). **Evaluation and enhancement of public cyber security awareness** (Order No. 27679789). Available from ProQuest Dissertations & Theses Global. (2307364066). Retrieved from https://search.proquest.com/docview/2307364066?accountid=178282

[5] Alabdulatif, A. (2018). **Cybercrime and Analysis of laws in Kingdome of Saudi Arabia** (Order No. 13836663). Available from ProQuest Dissertations & Theses Global. (2186929778). Retrieved from https://search.proquest.com/docview/2186929778?accountid=178282

[6] Lee, A. (2018). **Invisible networked publics and hidden contention: Youth activism and social media tactics under repression.** New Media & Society, 20(11), 4095–4115. https://071139r7l-1104-y-https-doi-org.mplbci.ekb.eg/10.1177/1461444818768063

[7] Sobré-Denton, M. (2016). **Virtual intercultural bridgework: Social media, virtual cosmopolitanism, and activist community-building**. New Media & Society, 18(8), 1715–1731. https://071139r7l-1104-y-https-doi-org.mplbci.ekb.eg/10.1177/1461444814567988

[8] Chukwu, C. U. (2018). **Combating digital terrorism in Africa** (Order No. 10932298). Available from ProQuest Dissertations & Theses Global. (2108654463). Retrieved from https://search.proquest.com/docview/2108654463?accountid=178282

[9] Churchwell, C. (2018). **Denial of service attacks: Defensive VHE9DXNOHE9DXNO versus offensive countermeasures** (Order No. 10935090). Available from ProQuest Dissertations & Theses Global. (2114952416). Retrieved from https://search.proquest.com/docview/2114952416?accountid=178282

[10] Schneider, F. (2016). **China's 'info-web': How Beijing governs online political communication about Japan**. New Media & Society, 18(11), 2664–2684. https://071139r7l-1104-y-https-doi-org.mplbci.ekb.eg/10.1177/1461444815600379

[11] Hammad, E. (2018). **Cyber-physical modeling and analysis for smart grids: Resiliency & cyber security** (Order No. 10687680). Available from ProQuest Dissertations & Theses Global. (2086387370). Retrieved from https://search.proquest.com/docview/2086387370?accountid=178282

[12] Ghazi-Tehrani, A. (2016). **Regulating cyber space: An examination of U.S.-China Relation**s (Order No. 10125391). Available from ProQuest Dissertations & Theses Global. (1796355323). Retrieved from https://search.proquest.com/docview/1796355323?accountid=178282

[13] Caldwell, Z. B. (2016). **A security measure paradigm for assessing industrial control system cyber security management effectiveness** (Order No. 10142167). Available from ProQuest Dissertations & Theses Global. (1823238547). Retrieved from https://search.proquest.com/docview/1823238547?accountid=178282

[14] Osmak, K. A. (2019). **A new approach to cyber-security** (Order No. 13895158). Available from ProQuest Dissertations & Theses Global. (2240080463). Retrieved from https://search.proquest.com/docview/2240080463?accountid=178282

[15] De Los Santos, S. (2016). **The impact of an absent national cyber security attack reporting policy** (Order No. 10037473). Available from ProQuest Dissertations & Theses Global. (1775002268). Retrieved from https://search.proquest.com/docview/1775002268?accountid=178282

[16]Oloidi, A. (2019). **Cyber-security challenges in financial institutions in nigeria: A multiple case study** (Order No. 13813041). Available from ProQuest Dissertations & Theses Global. (2207495699). Retrieved from https://search.proquest.com/docview/2207495699?accountid=178282

[17] YIN, X. C. et a (2019). **Toward an Applied Cyber Security Solutionn in IoT-Based Smart Grids: An Intrusion Detection System Approach**. **Sensors (14248220)**, [s. l.], v. 19, n. 22, p. 4952, 2019. DOI 10.3390/s19224952. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=140380753&site=ehost-live. Acesso em: 20 fev. 2020.

[18] Vanover, J. K. (2018). **Exploring the cyber security improvements needed by internet game users to reduce cyber security threats** (Order No. 13424956). Available from ProQuest Dissertations & Theses Global. (2188505483). Retrieved from https://search.proquest.com/docview/2188505483?accountid=178282

[19] Smith, C. (2018). **Cyber security, safety, & ethics education** (Order No. 10974125). Available from ProQuest Dissertations & Theses Global. (2126685981). Retrieved from https://search.proquest.com/docview/2126685981?accountid=178282

[20] Cook, K. D. (2017). **Effective cyber security strategies for small businesses** (Order No. 10602149). Available from ProQuest Dissertations & Theses Global. (1936383794). Retrieved from https://search.proquest.com/docview/1936383794?accountid=178282

[21] Dawson, M. (2017). **Hyper-connectivity: Intricacies of national and international cyber securities** (Order No. 10800987). Available from ProQuest

Dissertations & Theses Global. (2013953161). Retrieved from https://search.proquest.com/docview/2013953161?accountid=178282

[22] Imranuddin, M. (2017). **A study of cyber laws in the United Arab Emirates** (Order No. 10637498). Available from ProQuest Dissertations & Theses Global. (1989708727). Retrieved from https://search.proquest.com/docview/1989708727?accountid=178282

[23] Streifel, T. E. (2017). **The psychological effects of armed cyber attacks during conflict** (Order No. 10623225). Available from ProQuest Dissertations & Theses Global. (1957414904). Retrieved from https://search.proquest.com/docview/1957414904?accountid=178282

[24] Layne, C. (2017). **Cyber attacks against critical infrastructure** (Order No. 10622909). Available from ProQuest Dissertations & Theses Global. (1957428360). Retrieved from https://search.proquest.com/docview/1957428360?accountid=178282

[25] Abraham, S. (2016). **Cyber-security analytics: Stochastic models for security quantification** (Order No. 10111643). Available from ProQuest Dissertations & Theses Global. (1799589225). Retrieved from https://search.proquest.com/docview/1799589225?accountid=178282

[26] McGee, T. M. (2016). **Evaluating the cyber security in the internet of things: Smart home vulnerabilities** (Order No. 10163507). Available from ProQuest Dissertations & Theses Global. (1844998318). Retrieved from https://search.proquest.com/docview/1844998318?accountid=178282

[27]Betz, D. J., & Stevens, T. (2013). A**nalogical reasoning and cyber security. Security Dialogue**, 44(2), 147–164. https://071139r7l-1104-y-https-doi-org.mplbci.ekb.eg/10.1177/0967010613478323

[28]Burton, J. (2013). **Small states and cyber security: The case of New Zealand. Political Science**, 65(2), 216–238. https://071139r7l-1104-y-https-doi-org.mplbci.ekb.eg/10.1177/0032318713508491

[29] **الرجوع إلى:**

- Denis Mc Quail, **Mc Quail Mass Communication Theeory**. 6TH (ed), (London: Sage Publication, 2010),Pp185-186.
- John Vivian, **The Media of Mass Communication**, (USA: Pearson Education Inc,2006), Pp490.
- Melisande Middleton, **Social Responsibility in The Media**, (Oxford University: CIME, 2009).
- عادل عبد الغفار، **أبعاد المسئولية الاجتماعية للقنوات الفضائية المصرية الخاصة**، (جامعة القاهرة، كلية الإعلام،المؤتمر العلمي السنوي التاسع، مايو 2003).

[30] **بالرجوع إلى:**

- د. رغدة البهي: المدرس بكلية الاقتصاد والعلوم السياسية جامعة القاهرة، ورئيس وحدة الأمن السيبراني بالمركز المصري للفكر والدراسات الاستراتيجية.
- د. سماح عبد الصبور: المدرس بكلية الاقتصاد والعلوم السياسية، جامعة القاهرة.

* **قام بتحكيم إستمارة الدراسة:**

- أ.د نجوى كامل: أستاذ الصحافة، كلية الإعلام - جامعة القاهرة.
- أ.د محمد محمد حسين: أستاذ العلوم السياسية، كلية الإقتصاد والعلوم السياسية- جامعة القاهرة.

- أ.د محي الدين محمد قاسم: أستاذ العلوم السياسية، كلية الإقتصاد والعلوم السياسية- جامعة القاهرة.
- د. رغدة البهي: المدرس بكلية الاقتصاد والعلوم السياسية جامعة القاهرة، ورئيس وحدة الأمن السيبراني بالمركز المصري للفكر والدراسات الاستراتيجية.
- د. سماح عبد الصبور: المدرس بكلية الاقتصاد والعلوم السياسية، جامعة القاهرة.

[31] تعريف وزارة الاتصالات وتكنولوجيا المعلومات بجمهورية مصر العربية، **مرجع سابق**.

[32] Hammad, E. **Op. Cit,** Pp28.

[33] ماجدة عبد المرضي، **الصحافة المتخصصة: إشكاليات الواقع وآفاق المستقبل**، ط1، (القاهرة: دار العالم العربي، 2010)، ص 65.

[34] هبة السيد، تقرير، **وزير الاتصالات يفتتح المؤتمر الوطنى للأمن السيبرانى**، موقع جريدة اليوم السابع، 02 ديسمبر 2019 06:24 م، متاح عبر http://www.youm7.com/4528606

[35] أريج الجهني، مقال، **الأمن السيبراني أسلوب حياة**، موقع جريدة عكاظ، 6 فبراير 2020 02:29، متاح عبر https://www.okaz.com.sa/articles/authors/2009058

[36] **بالرجوع إلى:**

- مدحت عادل، تقرير **ندوة بالمركز المصرى للدراسات الاقتصادية تناقش الأمن السيبرانى ومخاطره**، موقع جريدة اليوم السابع، 17 ديسمبر 2019 12:38 م، متاح عبر http://www.youm7.com/4549587
- تقرير، **خبير تقني: الهجوم السيبراني على دولة ما في العالم بمثابة الهجوم العسكري**، موقع جريدة عكاظ، 15 أكتوبر 2018 13:44، متاح عبر https://www.okaz.com.sa/local/na/1678752

[37] تقرير، **خبراء يحذرون: هاكرز يستغلون فيروس كورونا لنشر البرمجيات الخبيثة**، موقع جريدة اليوم السابع، 13 فبراير 2020 10:00 م، متاح عبر http://www.youm7.com/4630349

[38] هبة السيد، تقرير: **مسؤول بـ"الأمن السيبرانى": موقع وزارة الصحة لم يكن يحمل بيانات حساسة**، موقع جريدة اليوم السابع، 01 فبراير 2020 03:27 م، متاح عبر http://www.youm7.com/4613163

[39] محمد السيد وزينب عبد المنعم، تحقيق، **فضيحة جديدة لفيس بوك.. الموقع أتاح بيانات الملايين من المستخدمين للسرقة**، موقع جريدة اليوم السابع، 05 أبريل 2019 06:37 ص، متاح عبر http://www.youm7.com/419571

[40] "تقرير، **الأمن السيبراني "يحذر من ثغرة أمنية في «واتساب»**، موقع جريدة عكاظ، 14 مايو 2019 20:27، متاح عبر https://www.okaz.com.sa/last-stop/na/1726893

[41] مؤنس حواس، تقرير، **أخطاء الموظفين تؤدى إلى نصف حوادث الأمن السيبراني**، موقع جريدة اليوم السابع، 31 أغسطس 2019 02:17 م، متاح عبر http://www.youm7.com/4397315

[42] هبة السيد، تقرير،**3 عناصر وراء خطورة التهديدات السيبرانية.. أبرزها سرعة انتشارها**، موقع جريدة اليوم السابع، 22 ديسمبر 2018 06:00 ص، متاح عبر http://www.youm7.com/4076498

[43] تحقيق، **نمو سوق «الأمن السيبراني» في السعودية 20 مليار ريال بحلول 2023**، موقع جريدة عكاظ، 12 يونيو 2019 15:53، متاح عبر https://www.okaz.com.sa/economy/na/1731709

[44] تحقيق، **الاقتصاد السعودي هدف لـ«الهجمات السيبرانية»**، موقع جريدة عكاظ، 25 أغسطس 2019 16:48، متاح عبر https://www.okaz.com.sa/economy/na/1743366

[45] هشام عبد الجليل، تقرير، **عمرو طلعت وزير الاتصالات: الحكومة تصرف 6 مليار جنيه لإنهاء مقولة "السيستم واقع"**، موقع جريدة اليوم السابع، 01 فبراير 2020 09:57 م، متاح عبر http://www.youm7.com/4613699

[46] تقرير، **مجلس الوزراء: إنشاء 11 هيئة ثقافية.. وتفويض وزير الثقافة بممارسة اختصاصات مجالسها**، موقع جريدة عكاظ، 4 فبراير 2020 15:53، متاح عبر https://www.okaz.com.sa/news/local/2008826

[47] هبة السيد، تقرير، **وزير الاتصالات: الدولة حريصة على تأمين البنية التحتية**، موقع جريدة اليوم السابع، 25 ديسمبر 2018 12:44 م، متاح عبر http://www.youm7.com/4080689

[48] تقرير، **تزامناً مع تنظيمها للمنتدى الدولي للأمن السيبراني.. ورناستها لـ«G20» المملكة الأولى عربيا والـ13 عالميا بالالتزام في الأمن السيبراني**، موقع جريدة عكاظ، 23 يناير 2020 19:12، متاح عبر https://www.okaz.com.sa/news/local/2006875

[49] تقرير، **شركات الأمن السيبراني تعزز استثماراتها في المملكة**، موقع جريدة عكاظ، 13 نوفمبر 2018 19:06، متاح عبر https://www.okaz.com.sa/last-stop/na/1685601

[50] هبة السيد، تقرير، **وزير الاتصالات يوجه بحماية البنية التحتية لمواجهة الهجمات السيبرانية**، موقع جريدة اليوم السابع، الأحد، 23 سبتمبر 2018 03:37 م، متاح عبر http://www.youm7.com/3961901

[51] هبة السيد، تقرير، **الاتصالات: 385 مليار دولار حجم أعمال الأمن السيبرانى ومصر تحتل المرتبة الـ14**، موقع جريدة اليوم السابع، 06 مارس 2018 05:28 م، متاح عبر http://www.youm7.com/3682156

[52] هبة السيد، تقرير، **تعاون بين قومى الاتصالات وسيسكو العالمية لإطلاق أكاديمية الأمن السيبرانى بمصر**، موقع جريدة اليوم السابع، 04 ديسمبر 2017 05:52 م، متاح عبر http://www.youm7.com/3539605

[53] هبة السيد، تقرير، **وزارة الاتصالات تبرم اتفاقيات متعددة مع شركات صينية بمجال التكنولوجيا**، موقع جريدة اليوم السابع، 29 أبريل 2019 09:00 م، متاح عبر http://www.youm7.com/4224458

[54] تقرير، **في الاجتماع الثاني للمجلس تكامل سعودي - إماراتي.. بـ7 مبادرات وإنجازات لمجلس التنسيق بين البلدين**، موقع جريدة عكاظ، 28 نوفمبر 2019 19:02، متاح عبر https://www.okaz.com.sa/local/saudi-arabia/1758239

[55] تقرير، **بالتعاون مع مجلس التجارة الإلكترونية «هيئة الأمن السيبراني» تصدر إرشادات مقدمي التجارة الإلكترونية والمستهلكين**، موقع جريدة عكاظ، 10 نوفمبر 2019 15:59، ، متاح عبر https://www.okaz.com.sa/local/na/1755525

[56] تقرير،"أرامكو" **توقع اتفاقية لتصنيع أول جهاز من نوعه للأمن السيبراني في المملكة**، موقع جريدة عكاظ، 25 فبراير 2020 12:32، متاح عبر https://www.okaz.com.sa/economy/na/2012183

[57] هبة السيد، تقرير: **مسؤول بـ"الأمن السيبرانى": موقع وزارة الصحة لم يكن يحمل بيانات حساسة، مرجع سابق**.

[58] تقرير، **وزير التجارة: التهديدات السيبرانية تتزايد.. والمملكة الأكثر استهدافاً**، موقع جريدة عكاظ، 4 فبراير 2020 21:58، متاح عبر https://www.okaz.com.sa/news/local/2008878

[59] أريج الجهني، **مقال، الأمن السيبراني أسلوب حياة**، موقع جريدة عكاظ، الخميس 6 فبراير 2020 02:29، متاح عبر https://www.okaz.com.sa/articles/authors/2009058

[60] هشام عبد الجليل، تقرير، **عمرو طلعت: الحكومة تصرف 6 مليار جنيه لإنهاء مقولة "السيستم واقع"، مرجع سابق**.

[61] تقرير، **وزير التجارة: التهديدات السيبرانية تتزايد.. والمملكة الأكثر استهدافاً، مرجع سابق**.

[62] هبة السيد، تقرير، **مسؤول بجهاز الاتصالات: مصر لديها كوادر قادرة على وقف الهجمات الإلكترونية، مرجع سابق.**

[63] هشام عبد الجليل، تقرير، **عمرو طلعت: الحكومة تصرف 6 مليار جنيه لإنهاء مقولة "السيستم واقع"، مرجع سابق**

[64] تقرير، **هيئة الأمن السيبراني» تستعرض تجارب المملكة في تعزيز الأمن المعلوماتي بسويسرا**، موقع جريدة عكاظ، 8 أبريل 2019 22:14، متاح عبر https://www.okaz.com.sa/local/na/1717853

[65] هبة السيد، تقرير، **وزير الاتصالات يوجه بحماية البنية التحتية لمواجهة الهجمات السيبرانية، مرجع سابق**.

[66] بندر السالم، مقال، **الأمن السيبراني، مرجع سابق**.

[67] هبة السيد، تقرير، **وزير الاتصالات يفتتح المؤتمر الوطنى للأمن السيبرانى، مرجع سابق**.

[68] أريج الجهني، مقال، **الأمن السيبراني أسلوب حياة، مرجع سابق**.

[69] هبة السيد، تقرير،**3 عناصر وراء خطورة التهديدات السيبرانية، مرجع سابق**.

[70] تقرير، **رئيس أرامكو: مواجهة التهديدات السيبرانية أولوية قصوى، مرجع سابق**.

[71] أريج الجهني، مقال، **الأمن السيبراني أسلوب حياة، مرجع سابق**.

[72] Kolenko, M. M. (2019). **C Op. Cit**.
[73] Cook, K. D. (2017). **Op. Cit**.
[74] Dawson, M. (2017). **Op. Cit**.
[75] Ghazi-Tehrani, A. (2016). **Op. Cit**.
[76] Hammad, E. (2018). **Op. Cit**.
[77] Osmak, K. A. (2019). **Op. Cit**.
[78] De Los Santos, S. (2016). **Op. Cit**.
[79] Imranuddin, M. (2017). **Op. Cit**.
[80] Layne, C. (2017). **Op. Cit**.
[81] Abraham, S. (2016). **Op. Cit**.
[82] Churchwell, C. (2018). **Op. Cit**.