اليات مركز دبى للأمن الإلكتروني للتوعية بالاستراتيجية الوطنية للأمن السيبرانى للحكومات الذكية عبر منصات التواصل الاجتماعي " أنستجرام نموذجا "

د. ولاء محمد الطاهر*

Dr.walaa Mohamed al tahir**

ملخص الدراسة

في ظل التطورات التكنولوجية الرقمية واعتماد الكثير من الدول على الخدمات الالكترونية فقد ظهرت الحكومات الالكترونية الذكية احد اهم أنماط الإدارة المعاصرة والمعتمدة بشكل كامل على التقنيات الرقمية الأكثر عرضة للهجمات السيبرانية ، ونظرا لصعوبة تحديد حجم تلك الهجمات فقد عملت الحكومات على تدشين العديد من المراكز الأمنية للعمل في المجال السيبرانى ، وتعد دولة الامارات العربية المتحدة من أوائل الدول التي قامت بإطلاق الحكومات الذكية عام 2013 ، ونظرا للمكانة الاستراتيجية التي تشغلها امارة دبى فقد أصبحت هدفا رئيسيا للهجمات الإلكترونية ، ولذلك فقد تم انشاء مركز دبى للأمن الإلكتروني 2014 ، متخذا شعار دبى الأكثر امان في العالم لاستراتيجيته

وقد تمثلت **مشكلة الدراسة** في التعرف على اليات تنفيذ الاستراتيجية الوطنية للأمن السيبرانى في التوعية بأخطار الهجمات السيبرانية والجرائم الإلكترونية ، وذلك من خلال تحليل المواد الإعلامية عبر منصات التواصل الاجتماعي لمركز الامن الإلكتروني بحكومة دبى الذكية ، وقد اتخذت الباحثة من أداة تحليل المضمون وسيلة للتحليل الكمي والكيفي بالاعتماد على منهج المسح الإعلامي ، حيث تم تحليل 133 مادة إعلامية متاحة على منصة انستجرام ، وبالاعتماد على نظرية ثراء وسائل الاعلام للتأكيد على أدوات التفاعلية التي تتيحها مثل هذه المنصات ودورها في احداث التوعية السيبرانية ، وقد وفرت المنصة العديد

* أستاذ الاعلام المساعد بكلية التربية النوعية جامعة الزقازيق

**Assistant Professor of Media - Faculty of Specific Education, Zagazig University

من أدوات التفاعل الشبكي مع الجمهور حيث وصلت نسبة التفاعلية على المنصة 90.9 % ، وقد كانت القضايا الثقافية هو الأكثر ظهورا على المنصة حيث وصلت الى 18.9 % من إجمالي قضايا التوعية السيبرانية ، كما تصدرت موضوعات الوعى التكنولوجي بنسبة 32.7 % حيث اكدت الدراسة أهمية مواجهة التكنولوجيا بوعى كامل ومهارة عالية ، وكانت استراتيجية اطلاق البوابات الالكترونية لتدعيم الوعى بأخطار التقنية الرقمية من اهم استراتيجيات الوعى السيبرانى 20.7 %

كما اوصت الدراسة بعدد من التوصيات على كافة الأصعدة الدولية والإقليمية والمحلية والمؤسساتية والتي من شانها تفعيل اليات الوعى السيبرانى لدى الجمهور ، والعمل على وجود مجتمع امن معلوماتيا بحماية الهياكل الأساسية للمعلومات من تلك الهجمات السيبرانية التي تضر بالأمن القومي والعالمي .

Mechanisms of the Dubai Cyber Security Center to raise awareness of the National Cybersecurity Strategy for smart governments through social media platforms "Instagram as a model""

.

مقدمة

أضحى علم المعلومات احد اهم العلوم في هذا العصر ، حيث انطلقت الثورة الصناعية الرابعة او ما يسمى بالثورة الرقمية الثانية من القدرات الهائلة على تخزين المعلومات ، والإمكانات غير المحدودة ، للوصول الى المعرفة ، فهذه الإنجازات تفتح الأبواب اليوم أمام ابتكارات وانجازات لا محدودة ، من خلال التكنولوجيات الناشئة في مجال الذكاء الاصطناعي ، والروبوتات والمركبات ذاتية القيادة والطباعة ثلاثية الأبعاد ، وتكنولوجيا النانو ، والتكنولوجيا الحيوية ، وعلم المواد والحوسبة الكمومية ، وسلسلة الكتل ، حيث عملت الثورة الرقمية الثانية على دمج التقنيات المادية والرقمية والبيولوجية ، وطمس الخطوط الفاصلة بينها .

وبالرغم من أن الطابع المفتوح لشبكة الانترنت هو مصدر قوتها ، لكنه أيضا موضع ضعفها الذى يعرضها لخطر الهجمات الالكترونية ، ولكى تحافظ الشبكة على طباعها المفتوح وقابليتها للتشغيل مع الأنظمة الالكترونية الأخرى interoperability لابد من أطر راعية تعزز أمن أنظمة المعلومات والبيانات ، وتضمن سلامتها، لذا فإن إقامة حيز موثوق وآمن في الفضاء الإلكتروني يعد أمرا جوهريا لمواجهة التحديات السيبرانية ، والحفاظ على البنية التحتية لتكنولوجيا المعلومات والاتصالات من التهديدات السيبرانية السريعة التطور [1].

وتعتبر الحكومة الإلكترونية احد أنماط الإدارة المعاصرة والمستحدثة فيما تقدمه من خدمات للمواطنين والهيئات المختلفة ، كمثال للاعتمادية العالمية على تقنية المعلومات في تقديم هذه الخدمات [2] حيث يعد مفهوم الحكومة الإلكترونية من ابرز المفاهيم التي ادخلتها الثورة المعلوماتية وشبكات الأنترنت الى الحياة اليومية للمواطنين ، والتي ظهرت نتيجة لتطورات تقنية تفاعلية تبنتها الحكومات في ربط مؤسساتها ببعضها البعض ، ووضع المعلومة في متناول الافراد ، وذلك لخلق علاقة شفافة تتصف بالسرعة والدقة وتهدف الى الارتقاء بجودة الأداء [3].

وتحتاج الحكومة الإلكترونية الى مراكز بيانات data centers الكبيرة المتكاملة، وربط بالشبكات المحلية WAN والواسعة LAN ، وكذلك يحتاج المستفيدون الى أجهزة الدخول الى مواقع الخدمة ، ويحتاجون الى وسائل للارتباط بالإنترنت للحصول على تلك الخدمات ، ولذلك يعد أمن المعلومات ضرورة ملحة ، فهو العلم الذى يعنى بحماية المعلومات من المخاطر، فلقد افسح هذا الفضاء السيبرانى الواسع والمتعدد والمتشعب المجالات عن محاور جديدة للصراع المعلوماتي ، كما بات يشكل منظومة اجتماعية تقنية واقتصادية ذات تأثير على الامن بأبعاده مهارات خبراء دوليين لردع قراصنة الانترنت (4) ، فلقد تعرضت حكومات وشركات وافراد للأذى البالغ التأثير بفعل مجموعة من الهجمات السيبرانية ففي عام 2017 استهدف احد برامج الفدية wannacry بعض الثغرات في أنظمة تشغيل مايكروسوفت ويندوز ، وأصاب الملايين من الحواسيب في 150 دولة في مختلف قطاعات الاعمال وأدى الى توقف عمليات التصنيع وأنظمة النقل وأنظمة الاتصالات (5) ، كما تم اطلاق NotPetya في يونيو 2017 ، وهو برنامج خبيث مدمر تم اطلاقه بواسطة الية تحديث البرامج لأحد برامج المحاسبة شائعة الاستخدام doc.me ، وفى غضون دقائق أصاب البرنامج الاف الأنظمة المتصلة بالأنترنت في اكثر من 65 دولة ، مما أدى الى تعطل الاعمال وتدمير الممتلكات في جميع انحاء العالم (6) .

ومع استمرار العديد من الدول في تركيز اهتماماتها على الخدمات الرقمية تتزايد فرص وتهديدات الإنترنت على حد سواء ، ومع زيادة اعتماد الاقتصاد والمجتمع والبنية التحتية المعلوماتية الحيوية اليوم على الإنترنت ، أصبح الحفاظ على استمرار الاتصال بشبكة الإنترنت أمراً ضرورياً لا غنى عنه ، وبالتالي أصبح لزاما على مختلف الدول أن تولى اهتماما ليس فقط للأمن السيبرانى ، ولكن أيضا للسياسات والتقنيات وأفضل الممارسات التي تعزز أمن البنية التحتية لشبكة الانترنت ، فالدولة التي لا تملك التكنولوجيا السيبرانية المحصنة أمنياً ، سيصبح فضاؤها السيبرانى المتضمن للأصول ، والموارد والمعلومات والخدمات ، والبنية التحتية لجميع القطاعات الحيوية عرضة للهجمات والتهديدات السيبرانية ، وبالتالي سيؤدي ذلك الى نتائج كارثية على أمنها القومي .

مشكلة الدراسة

في ظل الثورة الصناعية الرابعة والتقارب التكنولوجي الذى أدى الى تبديد الفواصل بين العالم الرقمي والبيولوجي بطرق أثرت بعمق على المجتمعات ، مما زاد من مخاطر الهجمات الإلكترونية الخبيثة ، فلقد تزايدت في السنوات الأخيرة عدد الهجمات والتهديدات السيبرانية بشكل حاد لتشمل الحروب والإرهاب والتجسس الرقمي ، ورغم اختلاف أغراض كل من تلك الهجمات ، الا ان القاسم المشترك بينهما هو استغلال ثغرات ونقاط ضعف المجال السيبرانى ، بهدف اختراق أجهزة الكمبيوتر وشبكات الحاسوب (7) ، حيث أن جرائم الكمبيوتر والإنترنت او ما يسمى cyber crimes ، هي ظواهر إجرامية تقرع أجراس الخطر لتنبه المجتمعات عن حجم المخاطر والخسائر ، التي يمكن ان تنجم عنها ، خاصة انها جرائم ذكية تنشا في بيئة الكترونية ، أو بمعنى أدق رقمية يقترفها أشخاص مرتفعي الذكاء ، ويمتلكون أدوات المعرفة التقنية ، مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية والثقافية والأمنية (8) .

ونظرا لصعوبة تحديد الحجم الحقيقي لتلك الهجمات ، ولطبيعة بيئة المخاطر الإلكترونية الغير محددة ، والتي لم يعد بمقدور أي كيان او مؤسسة معينة مواجهتها بمفردها ، وذلك بسبب عدم توفر السلطات والإمكانات والطاقات الكافية التي تمكنها من مجابهة نطاق او سرعة تطور الخطر الإلكتروني (9) ، فقد عملت الكثير من الدول على تدشين العديد من المراكز والمؤسسات للعمل في المجال السيبرانى ومواجهة المخاطر ، ففي دراسة أجرتها الأمم المتحدة تبين ان 90 % من الدول قد أنشات او تعمل على انشاء وحدات متخصصة في تحقيقات الجرائم السيبرانية والأدلة المعلوماتية (10).

وتعد دولة الإمارات العربية المتحدة من أوائل الدول العربية التي قامت بتطبيق نظام الحكومة الإلكترونية الذكية ، والقائمة بشكل شبه كامل على تقنيات العالم الرقمي (11) ، وهو ما دعاها الى اطلاق الاستراتيجية الوطنية للأمن السيبرانى ، والتي تهدف الى انشاء بنية تحتية الكترونية امنة وقوية للمواطنين ، من خلال تشجيع الابتكار

الرقمي ، وريادة الأعمال في مجال الامن السيبرانى ، وتمكين المؤسسات العامة والخاصة من حماية نفسها من الهجمات الإلكترونية ، وكذلك حماية أصول البنية التحتية المهمة ، وتكوين قوة عاملة ذات مستوى عالمي للأمن السيبرانى في الإمارات العربية المتحدة [12] ، وقد صدر القانون رقم 11 لسنة 2014 بشأن إنشاء مركز دبي للأمن الإلكتروني ، الذى يعد مركزا دوليا رائدا ذو ريادة تكنولوجية ، وتقوم استراتيجيته على التوعية الأمنية الإلكترونية التي ترمي إلى بناءً مجتمع معلوماتي آمن ، وأكثر إدراكا لمخاطر الأمن الإلكتروني [13] .

وقد تمثلت **مشكلة الدراسة الحالية** في التعرف على اليات مركز دبى للأمن الإلكتروني للتوعية بالاستراتيجية الوطنية للأمن السيبرانى لحكومة الامارات الذكية ، والدور الفاعل له في التوعية السيبرانية بمخاطر الثورة الرقمية الثانية، من خلال تحليل أدواته الاتصالية ورسائله الإعلامية الهادفة الى التوعية السيبرانية عبر صفحاته على موقع التواصل الاجتماعي .

أهداف الدراسة :

تستهدف الدراسةُ ما يلى :

- ✓ إلقاء الضَّوءِ على مفهومِ الجريمة الإلكترونية وأنواعها، وأساليب مواجهتها .
- ✓ توضيح أسس ومعالم الاستراتيجية الوطنية للأمن السيبرانى وبيان بنودها الأساسية .
- ✓ الإلمام بالأسس التي تقوم عليها مراكز الأمن السيبرانى والياتها لتنفيذ رؤيتها ورسالتها .
- ✓ التأكيد على أهميةِ استراتيجياتِ الوسائطِ المتعددة بمنصات التواصل الاجتماعي لتحقيق التأثير الفعال على الجمهور المتلقي .
- ✓ إبراز دور منصات التواصل الاجتماعي لمراكز الأمن السيبرانى في تنشيطِ الجمهور وإحداثِ التفاعلية مع موضوعات التوعية السيبرانية .

- ✓ التأكيد على أهمية ثَرَاءِ محتوى منصات التواصل الاجتماعي لمراكز الأمن السيبرانى بالأدوات، والاليات الاتصالية التي تمكن الجمهورَ من التَّفاعل مع محتوى الرسالة.
- ✓ التأكيد على ثراء منصات التواصل الاجتماعي بكافة أساليب واستمالات الإقناع للتأثير. على الجمهور المتلقي واقناعه لإحداث الأثر المطلوب .
- ✓ التعرف على متطلبات ومقومات ومعوقات إرساء معالم الحكومات الإلكترونية الذكية
- ✓ ادراك الافاق المستقبلية والحلول الممكنة لمواجهة مخاطر الفضاء السيبرانى.

الدراسات السابقة

أدت الثورة التكنولوجية الى اظهار مزايا نسبية عديدة لتطبيقاتها العملية في مختلف مجالات الحياة الإنسانية ، كما ساعدت على ترابط المجتمعات الإنسانية في ظل توجهات العولمة ، حيث ساهمت التوجهات العالمية المتزايدة نحو الانفتاح والترابط والتكامل بين المجتمعات الإنسانية المختلفة في نشوء ما يعرف اليوم بظاهرة العولمة ، وهى فلسفة جديدة لعلاقات الكونية ، والتي لها ابعاد سياسية واقتصادية واجتماعية وإدارية وقانونية وبيئية متكاملة، ويعد الاستجابة لمتطلبات البيئة المحيطة مطلب أساسي في ظل هذا العصر، حيث انتشار وتطبيق مفهوم وأساليب الإدارة الإلكترونية في كثير من المنظمات والمجتمعات، تجنبا لاحتمالات العزلة والتخلف عن مواكبة عصر ثورة الاتصالات والمعلومات (14) ، حيث أضحت الفضاءات العمومية ترسم حدودها باسلاك الكترونية ، واضحت المقاهي والنوادي أيضا بصيغة رقمية تحدد داخل فضاءات اثيرية لا مجالية أساسها روابط توجهها كائنات افتراضية تختزل الزمن وتذيب المسافات ، وتجعل الكل يتحرك في عالم افتراضي لا يخضع لمقاييس المكان لكنه يمضى بعيدا بالزمن (15) .

وقد ازدادت ابتكارات التكنولوجيا الرقمية الحديثة في الآونة الأخيرة ، مثل انترنت الأشياء internet of things والحواجز المتسلسلة block chain ، وخدمات الحوسبة السحابية cloud services ، والتي زادت من ترابط دول

العالم والافراد والشركات ، كما تضاعفت اعداد أجهزة الحاسوب المرتبطة مع بعضها البعض الى اكثر من ثلاثة اضعاف خلال الفترة 2015 الى 2020 [16]، ولكى يقوم الفضاء الإلكتروني او العالم الافتراضي بوظائفه ويحقق النظام والاستمرارية ولا يتوقف ، فلا بد من توفر الامن والأمان في الواقع الافتراضي [17].

وتهدف قوانين حماية المعطيات الشخصية إلى فرض الرقابة على استخدام ونقل المعطيات التي تخص الحياة الخاصة للأشخاص، من خلال منحهم الحق في التحكم ببياناتهم الشخصية، وفرض قواعد لاستخدام هذه البيانات من طرف المؤسسات والحكومات، وإنشاء هيئات تنظيمية لمراقبة تطبيق القوانين، وتختلف التشريعات التي تخص حماية المعطيات الشخصية من دولة إلى أخرى، حيث أن العديد من الدول لا تزال بدون قوانين في هذا المجال [18] ، ولأهمية المخاطر والهجمات الالكترونية والاثار الاقتصادية الكبيرة الناجمة عنها في دول مجلس التعاون الخليجي ، وضرورة مواجهة تهديدات الاقتصاد الشبكي ومراجعة الخطط الاستراتيجية للأمن الإلكتروني وسد الثغرات القائمة فيها ، تحددت مشكلة الدراسة لدى دراسة علم الدين بانقا (2019) [19] في ازدياد كثافة الهجمات والتهديدات الالكترونية في دول مجلس التعاون الخليجي ، وارتفاع تكاليفها المالية والاقتصادية في المنطقة مقارنة مع المناطق العالمية الأخرى ، وحاولت الدراسة التعرف على أداء دول مجلس التعاون الخليجي في مجال مواجهة الهجمات الالكترونية ، وتوصلت الى انه لا بد من تحسين الوعى والحوكمة والعمليات او المعالجات ، وسرعة تبنى واعتماد التكنولوجيا الحديثة ، كما اكدت على الدور المهم لحكومات دول مجلس التعاون الخليجي في بذل جهود كبيرة لتعزيز الامن السيبرانى ، وفى نفس الاطار البحثي هدفت دراسة نوال على البلوشية و نبهان حارث الحراصى (2020) [20] ، الى استكشاف واقع التحول الرقمي في عمان من خلال تقييم مستواها في التحول ، وذلك بتحليل محتوى الوثائق في هذا الجانب ، وتوصلت الى تفاوت مستوى التحول بالمؤسسات عينة الدراسة ، مع بذل الجهود لرفع المستوى في مشاريع البينة الأساسية للتحول الرقمي ومشاريع السلامة المعلوماتية والبوابات الالكترونية .

ويعد مفهوم الحكومة الالكترونية أوسع من كونها برمجيات وحواسيب انترنت وغيرها من التقنيات ، فهي إدارة شاملة ينطوي عليها اجراء تغيير نوعى يهدف الى إعادة النظر بمفاهيم الإدارة العامة والمضامين التي تقدمها ، فهي صياغة لواقع جديد في ضوء العلاقات التبادلية بين الأجهزة الحكومية وجمهور المستفيدين من خدماتها من جهة أخرى في أي زمان ومكان [21] ، وفى هذا الاطار فقد تم وضع عددا من الأهداف تسعى الحكومات الالكترونية إلى تحقيقها، كإدارة البيانات من خلال اتباع استراتيجية واضحة وإرشادات مدروسة، تتوافق مع أفضل الممارسات الدولية ، والاعتماد على الشفافية وتعزيز الثقة بالأداء الحكومي ، وكذلك تحفيز المواطنين للمشاركة في تحسين الخدمات المقدمة لهم [22]، وقد تحددت مجالات البيانات الحكومية المفتوحة والتي من أهمها البيانات الدستورية، والقوانين، واللوائح التنظيمية والبيانات الديموغرافية ، والمعلومات المالية وما يتعلق بها كالميزانية، والإيرادات، والنفقات ، وكذلك بيانات التعليم وما يرتبط بها ، و بيانات النقل التي تتمثل في إحصاءات الحوادث، والمرافق، والحركات ، وبيانات الرعاية الصحية ، وبيانات تكنولوجيا المعلومات والاتصال.[23] ، وقد أظهرت دراسة onwubiko,c(2015) [24] الكثير من التحديات نتيجة لتزايد التواجد الرقمي عبر الأنترنت ، واحد هذه التحديات هي عرضة الافراد والمنظمات لجرائم الانترنت والجرائم الإلكترونية ، كما اكدت دراسة alotabi (2017) [25] ان الجرائم المتعلقة بإساءة استخدام هذه المعلومات على الانترنت في تزايد وتؤدى الى خسائر متنوعة ، اما دراسة [26] Anastacio,et.al (2013) فقد اكدت ان بعض المواقع الالكترونية لا يتم تحديثها باستمرار ، لذلك فان جودتها غير مضمونة الفائدة ، وقد يؤدى ذلك الى الفشل التام للبرامج المستخدمة في الحكومة الالكترونية ، وبذلك يتعين على كل حكومة الاخذ في الحسبان التدابير الأمنية المناسبة لضمان استمرار العمل وجودته ، مع وضع استراتيجية للحالات الطارئة والمفاجئة التي تتطلب حلولا سريعة للتعامل معها ، ففي عام 2016 هاجم القراصنة احدى الوكالات الحكومية السعودية بالإضافة الى منظمات في قطاعات الطاقة والصناعة والنقل والهيئة العامة للطيران المدني التي تنظم الطيران السعودي والحق خسائر ضخمة جراء هذا الهجوم [27] ، وقد حاولت دراسة الأمم المتحدة (2013)[28] التعرف على

ماهية الجرائم الالكترونية وأهدافها وتصنيف أنواع الجرائم الإلكترونية ووسائلها وطرق الوقاية منها ، وتوصلت الدراسة الى ان الجرائم التي تقع على العمليات الالكترونية باستخدام الوسائل الالكترونية تتأثر بطبيعة الجرائم وبالوسائل العلمية التي قد ترتكب بها ، مما قد يؤدى الى عدم اكتشاف العديد من الجرائم في زمن ارتكابها ، او عدم الوصول الى الجناة الذين يرتكبون هذه الجرائم او تعذر إقامة الدليل لإثباتها مما يترتب عليه الحاق الضرر بالأفراد وبالمجتمع ، كما توصلت الى اكثر الجرائم شيوعا وطرق الوقاية منها ،واوصت بأهمية دراسة علوم الازمات والكوارث التكنولوجية لأعداد خطط وقائية وامنية وعلاجية لهذه الازمات ، اما دراسة مجمع البحوث (2016)[29] فتكمن مشكلتها في تفاقم الجريمة الالكترونية وتعدد أنواعها وازدياد حجم خسائرها واضرارها، بحيث أصبحت مهددا حقيقا لأمن المعلومات في كافة المجالات العامة والحيوية بالقطاع الخاص والعام والافراد بل تعد مصدر خطورة على الامن القومي وعلى السلم والامن الدوليين ، مما يحتم إيجاد المعالجات والحلول العلمية والعملية للحماية من الجريمة الالكترونية والحد من ارتفاع معدلاتها ، واثارها المدمرة للأنظمة كما ا اكدتها العديد من الدراسات المتخصصة التي دقت ناقوس الخطر، من خلال دراسة الظاهرة حول العالم، ودور التعاون الدولي والإقليمي في مكافحتها وكشفها وضبط مرتكبيها ، أيضا حاولت الدراسة ابراز الواقع الحالي للجريمة الإلكترونية وحجمها واساليها واسبابها واثارها وتطورها وخسائرها على نطاق العالم بشكل عام وفى منطقة الخليج العربي بشكل خاص ، وقد توصلت الدراسة الى ان الجريمة الالكترونية ظاهرة إجرامية حديثة وليدة التطورات الهائلة والمتلاحقة في نظم تقنية المعلومات والاتصالات، وهى جريمة عابرة الحدود ويمكن ارتكابها من أي مكان في العالم عبر شبكة الانترنت ، وتتميز بسهولة إخفاء ادلتها إضافة الى تعقيدات التحقيق فيها وصعوبة ضبط مرتكبيها الى ان أصبحت مشكلة عالمية تهدد امن المجتمع الدولي ، وقد ارتفعت معدلات الجريمة الالكترونية بشكل ملحوظ من عقد التسعينات [29] ، كما تعرفت دراسة رمضان إبراهيم (2015)[30] على ادلة اثبات الجرائم الالكترونية في الشريعة الإسلامية والأنظمة الدولية بالاعتماد على المنهج الوصفي والتحليلي والمنهج التاريخي ، حيث قامت ببيان مفهوم الجريمة الإلكترونية وخصائصها ومظاهرها

والتحديات التي تقف امام القضاة عليها ، وتوضيح الحكم الشرعي فيها مع تحليل المادة العلمية والتعقيب عليها مع تتبع المراحل التاريخية لمواجهتها من خلال الأنظمة الدولية ، وقد توصلت الدراسة الى هشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الاجرامية الجديدة سواء على صعيد الملاحقة الجنائية في اطار القوانين الوطنية ، ام على صعيد الملاحقة الجنائية الدولية ، كما اثبتت ان الشريعة الإسلامية تميزت بمنهجها الفريد في مكافحة الجريمة واستئصالها من جذورها من خلال خطين متلازمين ومتوازيين وهما الجانب الوقائي والجانب العلاجي.

وجاءت دراسة الأمم المتحدة (2015)[31] لتمثل استعراضا سريعا في الوقت المناسب لجهود العدالة الجنائية والوقاية من الجريمة لمكافحة الجريمة السيبرانية ومنعها ، حيث رسمت صورة عالمية من خلال تسليط الضوء على الدروس المستفادة من الجهود المبذولة الحالية والسابقة ، وقد تناولت الدراسة مشكلة الجريمة السيبرانية من خلال منظور الحكومات والقطاع الخاص والاوساط الاكاديمية والمنظمات الدولية ، وتوصلت الدراسة الى ان الاعتماد على الوسائل التقليدية للتعاون الرسمي الدولي في مسائل الجريمة السيبرانية لا يكفى حاليا للاستجابة في الوقت المناسب لمقتضيات الحصول على ادلة الكترونية سريعة الزوال والتغير ، كما اكدت ان أنشطة منع الجريمة السيبرانية في جميع البلدان تتطلب تعزيز الشراكات بين القطاعين العام والخاص وادماج الاستراتيجيات الخاصة بالجريمة السيبرانية ضمن منظور أوسع للأمن السيبرانى ، وذلك من خلال نهج كلى يشتمل على زيادة الوعى ، كما تركزت مشكلة دراسة مالك عبد الهادي (2020)[32] في تحديد الدور الفاعل للأمن للحد من السيبرانى تهديدات الامن الفكري ، حيث استخدمت الدراسة المنهج الوصفي واعتمدت على الاستبانة في جمع المعلومات من عينة الدراسة ، وتوصلت الى وجود علاقة طردية بين استجابات عينة الدراسة لأهمية الامن لمواجهة السيبرانى تهديدات الامن الفكري لدى المجتمع السعودي ومتغيراتهم الديموغرافية و، كذلك تأكيدهم على الوسائل والأدوات التي يمكن من خلالها تعزيز دور الامن في الحد م السيبرانى ن تهديدات الامن الفكري لدى المجتمع السعودي ، كما أوضحت دراسة stavrou ,e, (2018)[33]ان رفع مستوى الوعى والأمان في الاستخدامات السيبرانية

الشائعة كالتسويق والخدمات المصرفية المختلفة واستخدام كلمات مرور قوية لحماية الحسابات يقضى على الجرائم الإلكترونية ، حيث اكدت هذه الدراسة ان استخدام كلمات مرور ضعيفة احد النقاط التي يتم استغلالها في الهجمات الإلكترونية، كما استهدفت دراسة yasin et al , (2018) [34] تحسين الوعى الأمني من خلال تصميم لعبة جادة لتعلم متطلبات الامن ، حيث اكدت الدراسة على أهمية تعزيز مفاهيم الامن في بيئات التعلم وانه من الضروري تعزيز هذه المفاهيم عن طريق استخدام الأساليب الشيقة والممتعة ومنها الألعاب الالكترونية ، اما دراسة بيان الشهراني (2020)[35] فقد هدفت الى التعرف على اثر تصميم الألعاب التعليمية الالكترونية لتعزيز مفاهيم الامن السيبرانى في حماية البريد الإلكتروني ، وحماية البيانات والمعلومات ، وكذلك تامين الأجهزة المحمولة، وسياسات السيبرانى التشفير، باستخدام برنامج game maker كأداة سهلة للتطبيق ولا تتطلب مهارات برمجية كبيرة ، وقد اعتمد البحث على المنهج التجريبي ، حيث تمثلت أدوات البحث في اختبار معرفي لقياس مفاهيم الامن السيبرانى ، وبطاقة تقييم منتج لتقييم تصاميم الألعاب الالكترونية ، وتوصلت الدراسة الى وجود فروق ذات دلالة إحصائية بين متوسطي درجات الطلاب وتحقيق المجموعات لمعياري بطاقة تقييم المنتج وهما المعايير الفنية والمحتوى العلمي في تصميم العابهن ، وفى ضوء نتائج البحث اوصت الدراسة بأهمية تعزيز تصميم العاب تعليمية في تعزز مفاهيم الامن السيبرانى ، ومشاركتها عبر وسائل التواصل الاجتماعي ، وتقديم برامج تدريبية حول تصميم وإنتاج الألعاب لما لها من اثر فعال على الطلاب، وهو ما اكدت عليه دراسة kasurinen,et,al (2018) [36] من ضرورة تعزيز مفاهيم الامن السيبرانى والممارسات السيبرانية من خلال تضمينها في التقنيات ، حيث اوصت بضرورة تعلم وممارسة الامن السيبرانى عن طريق تصميم واقتراح بيئة تعلم تجمع بين الألعاب والمختبرات الافتراضية ، وتوصلت النتائج الى نجاح هذه الأداة بالرغم من وجود بعض القضايا التي واجهت الطلاب خاصة مع الأجهزة المحمولة ، كما اوصت الدراسة بضرورة استخدام أدوات تعليمية جذابة وشيقة على الصعيد قبل الجامعي.

وعلى الصعيد الجامعي جاءت دراسة جبريل العريشى ، سلمى الدوسري ، (2018) [37] لتؤكد أهمية الجامعات باعتبارها من اهم المؤسسات التربوية التي تقع على قمة راس الهرم التعليمي ، وتقع بها العديد من الالتزامات التي تتعلق بمواجهة المشكلات التي تطرا على المجتمع وتلبيه احتياجاته ، والعمل على توعية افراده ، حيث ترتبط بالمجتمع ارتباطا وثيقا وتتفاعل معه وتؤثر فيه ، كما انها مسؤولة عن حماية الشباب من المخاطر والتهديدات ، خاصة تلك المتعلقة بالجانب الثقافي والمعلوماتي وما ينتج عنها من جرائم وانحرافات أخلاقية خصوصا مع التزايد في استخدام الأجهزة الإلكترونية الحديثة ،وقد هدفت الدراسة الى معرفة الدور الذى تقوم به مؤسسات التعليم العالي في تعزيز ثقافة امن المعلومات في المجتمع ، وتوصلت نتائج الدراسة الى ضورة تفعيل الأنشطة والمبادرات التي تدعم زيادة الثقافة لأمن المعلومات ، وعقد الندوات والدورات للتعريف بكبفبة الاستخدام الامن للتقنية ، وكذلك اوصت بضرورة ادراج محتوى الامن المعلوماتي وشموله في المواد الدراسية الجامعية ، كما اكدت دراسة مها الجثمى (2017)[38] على أهمية رفع مستوى التوعية بقضايا امن المعلومات لعموم المجتمع ، حيث ان الوعى بمفاهيم الامن السيبرانى يمكن المستخدمين من تحسين استخدامات الامن السيبرانى الخاصة بهم ، فهي تعتبر من الطرق والوسائل الجيدة في مكافحة المخاطر السيبرانية ، وعلى المجال الاسرى اكدت دراسة . ahmad ,et al (2019) [39] ان مستوى وعى الوالدين بأمن الأنترنت يزيد من فرصة حماية أبنائهم من مخاطر الجريمة السيبرانية ، حيث طبقت هذه الدراسة باستخدام تقارير المسح ل 872 من أولياء أمور الذين يبلغون من العمر 17 فاقل متوسط الفئة الأكثر عرضة لمثل هذه المخاطر السيبرانية .

وحول الدور الفاعل لمنصات الاعلام الجديد للتوعية بأخطار الجريمة الالكترونية والتوعية السيبرانية جاءت دراسة عبد الاله المطيري (2018) [40] حيث تمحورت مشكلة الدراسة في السؤال الرئيسي ما دور الاعلام الجديد في التوعية من اخطار الجريمة الإلكترونية من وجهة نظر عينة الدراسة ، وتوصلت نتائج الدراسة الى ان الأغلبية يستقون معلوماتهم ومعارفهم من خلال الوصول عبر المواقع الالكترونية ومواقع التواصل الاجتماعي لزيادة المعرفة

والاطلاع على كل ما هو محل اهتمامهم ،واكدت الدراسة على زيادة الحاجة الى توعية الجماهير عبر منصات الاعلام الجديد والمفضلة لديهم في كيفية محاربة الجرائم بشتى أنواعها ، كما قدمت دراسة ويليام مارسيلينو ، واخرون (2017)[41] مجموعة من التوصيات لبناء قدرة وسائل التواصل الاجتماعي دعما لعمليات المعلومات التي تعزز مهارة التواجد الافتراضي بأمان وبشكل ملائم للأمن القومي ، وارتكزت في توصياتها على نتائج دراسات استقصائية بحثية للدراسات السابقة القائمة حول تكنولوجيات تحليل وسائل التواصل الاجتماعي والممارسات الفضلى والقيود القانونية والأخلاقية المفروضة على تحليل وسائل التواصل الاجتماعي وتقاطع عمليات المعلومات مع تحليلات بيانات وسائل التواصل الاجتماعي ، اما دراسة احمد الخطيب (2019) [42] فقد اكدت على أهمية الجرائم المعلوماتية التي تدق ناقوس الخطر لكافة الدول حيث تهدف الجرائم المعلوماتية الى الاعتداء على كافة البرامج المخزنة داخل الحاسب الألى او الموجودة على شبكة الانترنت وتكمن خطورتها في انها تتطور سرا ، ويقوم عليها مجموعة من المجرمين يتمتعون بدرجة عالية من الذكاء ويمتلكون مهارات تقنية عالية باستخدام وسائل التكنولوجيا ، وهو ما ركزت عليه مشكلة الدراسة حول البحث عن كيفية استخدام مجرمي الانترنت لمواقع التواصل الاجتماعي لتنفيذ عملياتهم الاجرامية موضحا دور التشريعات القانونية من هذه العمليات ، وعلى جانب اخر تناولت دراسة عبد المجيد (2020) [43] ، الجرائم المترتبة على إساءة استخدام مواقع التواصل الاجتماعي ودورها في احداث الضرر للأخرين ، مما يتوجب معه بيان النصوص القانونية التي تعالج هذه الظاهرة ، وقد تجلت إيجابيات التشريع الإماراتي في معالجة إساءة استخدام هذه الوسائل وبشكل مفصل اكثر من غيرها من التشريعات الأخرى ، وهو ما عالجه القانون الاتحادي رقم 2 لسنة 2018 بشان مكافحة جرائم تقنية المعلومات ، بما يتفق مع محاور الدراسة الحالية من تأكيدها على الدور المهم للمشرع الإماراتي بمواكبته للعصر وإصدار القانون الاتحادي بغرض معالجة بعض المشكلات التي تنتج عن استخدام وسائل تقنية المعلومات ومن بينها وسائل التواصل الاجتماعي بشكل خاطئ وضار للأخرين .

الاطار النظري للدراسة

ترتكز الدراسة في إطارها النظري على **نظريةِ ثراء وسائل الإعلام "** Media Richness Theory"، والتي يشار إليها أحياناً بنظرية ثراء المعلومات، وهي إطار لوصف وسائل الاتصال على حسب قدرتِها على إنتاج المعلومات التي تنقلُ من خلالها ، وقد قام بوضع هذه النظرية كلًا من ريتشارد دافت Richard L. Daft، وروبرت لينجل Robert H. Len gel عام 1984، وقد كان الهدف منها في بداية الأمر، وصف وتقييم وسائلِ الاتصال داخل المنظمات (44) ، حيث أكد الباحثان ان الأهداف الرئيسية لأى ِ منظمة هي تقليل غموضِ الرسالة عن طريق اختيار الرسائل التي تحقق درجة من التفاعل مع الجمهور ، وتعمل نظريةُ ثراء وسائل الإعلام على دراسة معايير الاختيار بين الوسائل الإعلامية التكنولوجية وفقا لدرجة ثرائها المعلوماتي، وتوضح أن فاعلية الاتصال تعتمد على القدر الذي تستخدم به الوسيلة الأشكال التفاعلية للاتصال ، وطبقا للنظرية، فإن الوسائل الإعلامية التي توفر رجعَ صدى فوري تكون أكثرَ ثراء (45) .

وترتكز النظرية على أربعة معايير أساسية ؛ لترتيب ثراء الوسيلة ، من حيث درجة الثراء ، وهي سرعة رد الفعل، وقدرتِها على نقل الإشارات المختلفة باستخدام تقنيات تكنولوجية حديثة مثل الوسائط المتعددة والتركيز الشخصي على الوسيلة ، واستخدام اللغة الطبيعية ، وتعد منصات التواصل الاجتماعي من الوسائل الاعلامية المتميزة ، بفضل ما تمتلكه من أوجه للثراء الإعلامي ، مما جعل منها وسائل متزايدة الاستخدام من قبل أعداد كبيرة من الجمهور، وقد استمدت أوجه الثراء الإعلامي من استعمالها لشبكةِ الإنترنت ، وما وفره هذا الوسيط من خصائص ، جعل منها وسائل إعلامية متميزة ، من حيث الآنيةِ والتفاعليةِ واستخدامِ الوسائط المتعددة ، كما ان إتاحة فورية رجع الصدى ساعدتها على مواكبة للتطورات التكنولوجية المتسارعة، التي يشهدها الإعلام ف ي الوقت الحالي.

وترتكز الدراسة الحالية على هذه النظرية لتأكيد اهمية منصات التواصل الاجتماعي في احداث التوعية السيبرانية للجمهور المستهدف بفضل ثراءها

المعلوماتي والرقمي بالعديد من الأدوات التفاعلية التي تساعد على تحقيق اهداف القائم بالاتصال

تساؤلات الدراسة

- ✓ ما رؤية ورسالة مركز دبى للأمن الإلكتروني في مواجهة الجرائم السيبرانية ؟
- ✓ ما هي اهم الموضوعات والقضايا المتعلقة بالأمن السيبرانى على منصة انستجرام ؟
- ✓ ما هي اهم الأهداف الاتصالية والإعلامية لموضوعات التوعية السيبرانية؟
- ✓ ما هي أكثر القوالب الإعلامية ظهورا على منصة انستجرام ؟
- ✓ ما أكثر أساليب الإقناع المستخدمة برسائل المركز الإعلامية لتنفيذ استراتيجية مركز دبى للأمن الإلكتروني بحكومة دبى الذكية ؟
- ✓ ما أشكال وانماط المصادر المعلوماتية لموضوعات التوعية السيبرانية على المنصة ؟
- ✓ ما استراتيجيات الامن الإلكتروني الأكثر ظهورا على منصات التواصل الاجتماعي ؟
- ✓ ما اليات تنفيذ مركز الامن الإلكتروني للاستراتيجية الوطنية للأمن السيبرانى ؟
- ✓ كيف كانت اليات التفاعل مع الجمهور على منصة انستجرام ؟
- ✓ ما هو حجم التفاعلية على منصة انستجرام حول موضوعات التوعية السيبرانية ؟
- ✓ هل حرصت المنصة على ثراء المضمون الاتصالي بالوسائط الرقمية ؟
- ✓ ما هي أهم أنماط الوعى السيبرانى التي اشتملت عليها الرسائل الإعلامية على المنصة؟

الإجراءات المنهجية للدراسة:

نوع الدراسة والمنهج المستخدم:

تندرج هذه الدراسة ضمن الدراسات الوصفية التي تستهدف الكشفَ عن المعلومات، والبياناتِ عن الظاهرة المراد دراستها من خلال إجراء القياسات الضرورية لمتغيرات الدراسة كميًّا (46) ومعالجتِها احصائيا للوصول إلى تفسيراتٍ علمية بشأنها ، ولذا تعتمد هذه الدراسة على **منهجِ المسح الإعلامي** بمستوياته الوصفي والتحليلي من أجل الإجابة على تساؤلات الدراسة والوصولِ إلى نتائج علمية مؤكدة بشأن الظاهرة ، وقد تمثلت متغيرات الدراسة في الدور الفعال لمركز دبى للأمن الإلكتروني للتوعية السيبرانية لمواطني دولة الامارات العربية المتحدة كمتغير تابع ، اما المتغيرات المستقلة فتمثلت في ثراء منصات التواصل الاجتماعي لمركز الأمن الإلكتروني بالوسائط الرقمية ودورها في التأثير على المتلقي واقناعه بالتأثيرات السلبية لجرائم الفضاء السيبرانى ، ونجاحها في بناء مجتمع واع بمخاطرها .

مجتمع الدراسة وعينتها

حددت الباحثة مجتمع الدراسة في مراكز الأمن السيبرانى والإلكتروني بالحكومات الذكية ، وقد اقتصر إطار البحث على اختيار مركز الأمن الإلكتروني بحكومة دبى بدولة الإمارات العربية المتحدة كعينة عمدية ، وهى أول حكومة عربية ذكية معتمدة في كافة تعاملاتها على الأنظمة الرقمية بشكل كامل في التعامل مع مستخدميها ، كما حددت الباحثة اطار التحليل في منصات التواصل الاجتماعي ، المتاحة على الموقع الإلكتروني للمركز لكافة المستخدمين، وذلك من اجل التعرف على أدواته الاتصالية لتحقيق ورؤية ورسالة المركز في الوصول الى مجتمع واع بمخاطر التكنولوجيا وتحقيق الامن الإلكتروني وتنفيذ استراتيجية حكومة دبى الذكية للتوعية السيبرانية ، وقد تم الاختيار العمدى لموقع انستجرام كموقع للتواصل الاجتماعي ، من ضمن منصات المركز للتواصل المجتمعي ، وذلك بعد عمل دراسة استطلاعية لجميع

المنصات التابعة للمركز ، حيث توصلت الباحثة الى ان منصة انستجرام من أكثر منصات المركز تفاعلا من قبل الجمهور ، حيث وصل عدد مشتركي الحساب الى 1927 مشترك ، وهو أكبر منصة من حيث عدد المشتركين ، وقد تم تحليل عينة عمدية من المواد الإعلامية على منصة المركز" انستجرام " بواقع 133 مادة إعلامية posts من 205 مادة إعلامية posts متاحة على منصة انستجرام متعلقة بموضوعات وقضايا الأمن السيبرانى والتوعية السيبرانية ، حيث اعتمدت الباحثة على المادة الإعلامية كوحدة للتحليل .

أداة جمع البيانات:

في إطار منهج المسح تم استخدام أداة تحليلِ المضمون content analysis لتحليل مضمون منصة التواصل الاجتماعي " انستجرام " شكلاً ومضموناً، والحصول على نتائج كمية تساهم في إعطاء تفسيرات كيفية ، توضح اليات مركز دبى للأمن الإلكتروني في التوعية السيبرانية حول مخاطر الامن المعلوماتي لدى المواطنين الأمارتين واستراتيجياته في بث رسائله الاتصالية لمواجهة الجريمة الإلكترونية وادارتها ومدى تفاعل الجمهور معها

الصدق والثبات:

قامت الباحثةُ من أَجل الوصولِ إلى صدق استمارة التحليلِ بعرضِها على مجموعة من المحكمين (*) ، من أَجل اختبار مدى صلاحيتها للتحليل وتم التعديل وفقا لرؤيتِهم العلمية ، ولاختبار ثبات الاستمارة فقد اعتمدت الباحثة في ذلك على معادلة هولستي ، وبتطبيق المعادلةِ ظهرت نسبة الثبات والتي وصلت الى 91% تقريبًا ، وهى نسبة عالية ، تدل على وضوح المقياس بين المحللين وصلاحيتِه للتطبيق.

ادبيات الدراسة

نظرا للتحولات الاقتصادية والاجتماعية والثقافية الرقمية الحديثة ، فقد ظهر نمط جديد من الجرائم ، تجسد في الجرائم المعلوماتية التي أصبحت تمثل خطرا كبيرا على الأفراد والمؤسسات ، فلقد أدى ظهور التقنيات الجديدة في نظم

المعلومات ، والتكنولوجيا الرقمية مثل أنترنت الأشياء Things of Internet ، والحواجز المتسلسلة Chain Block وخدمات الحوسبة السحابية services Cloud الى زيادة مخاطر الهجمات الإلكترونية ، وجعل بعض المنظمات الدولية مثل صندوق النقد الدوليIMF والمنتدى الاقتصادي العالمي WFE تضع المخاطر الإلكترونية في صدارة المخاطر النظامية risk Systemic التي تواجه النظام الاقتصادي العالمي (47) ، الأمر الذى دفع الدول الى العمل الجدى للحد من هذه الجرائم التي تلحق الضرر بالأفراد من خلال التوعية والوسائل الوثائقية الأمنية وغيرها من الطرق (48) ، وتعد الحكومة الإلكترونية احد الطرق الحديثة والمتطورة ، والتي تتكامل بها المؤسسات لاستخدام التقنية الرقمية لتزويد المواطنين باليات أفضل وأسرع وأيسر للوصول الى المعلومات الحكومية ، مما يعطى المواطنين فرصة افضل للمشاركة بآرائهم ومقترحاتهم لدى المؤسسات الحكومية (49) ، كما تساعد على الاستفادة من تراكم المعرفة والتقدم التقني المرافق لها في توسيع قاعدة المستفيدين من الخدمات العامة ، من حيث وفرة تلك الخدمات ، وأساليب تقديمها بوسائل الكترونية تمكن من الاطلاع عليها في أي زمان ومكان على أساس المساواة والعدالة بين المعنيين (50) ، كما تتيح الحكومة الالكترونية لمستفيديها التمتع بمعايير الخصوصية والسرية المناسبة ، والأمن والمصداقية ، الأمر الذى يؤدى الى النمو والتطوير في مجال خدمات الجمهور (51) .

وقد صنف المنتدى الاقتصادي العالمي كل من الامارات العربية المتحدة والمملكة العربية السعودية وقطر في الآونة الأخيرة ضمن أفضل عشرة دول في أهمية الاتصالات وتقنية المعلومات لرؤية الحكومة للمستقبل (52) ، وهو ما أكدته **دراسة ايمان عيسى (2019)** (53) حيث قامت برصد وتحليل واقع بوابات الحكومة الإلكترونية لعينة من دول مجلس التعاون الخليجي ، وتوصلت الدراسة الى حصول بوابة الإمارات العربية المتحدة على المركز الأول من حيث درجة الاكتمال بين بوابات دول المجلس المختارة ، وللحكومة الإلكترونية عدة ابعاد ، **فالبعد السياسي** يعتبر عاملا مهما لنجاح الحكومة الإلكترونية وهو أن تتوفر

الرغبة السياسية التي تسهم في تكوين الرأي السياسي ، وذلك من منطلق القناعة الاهلية والايمان بالأهداف والغايات والفوائد التي ستعود على الدول منها .

كما يعد **البعد التشريعي او القانوني** او بما يسمى بالبناء القانوني لإرساء معالم الحكومة الإلكترونية ، والذى لا يمكن اغفاله او الاستهانة به بأي حال من الأحوال ، لما له من أهمية قصوى في ضمان حقوق جميع الأطراف ، حيث أن نشأة الحاجة الى انشاء حكومة الكترونية تستدعى توفير بالضرورة تشريعات قانونية جديدة ، فهناك تشريعات خاصة بتجريم اقتحام المواقع الالكترونية او اتلافها، وتجريم انتهاك حق الخصوصية ، وتجريم انتهاك سر التوقيع الإلكتروني، وتشريعات تواجه أوجه فك التشابك بين الإدارات الحكومية بما يكفل مرونة توفير الخدمات ، وكذلك تشريعات تنظم نشر المعلومات وامنها ، وشرعية تداول البيانات ، وسرية البيانات وخصوصيتها ، والمحافظة على خصوصية المعلومات والمعاملات الشخصية [54] ، حيث أكدت العديد من الدراسات ان الجانبان القانوني والتشريعي يلعبا دورا مهما في اطار التحول الرقمي ، اذ لابد من توافر تشريعات تنظم عمليات الإتاحة والاستخدام للخدمات الإلكترونية [55] كما توصلت **دراسة ندى جراح (2012)** [56] الى أن من أسباب فشل الحكومة الإلكترونية بدولتي سوريا والعراق عدم وجود تشريعات تنظم عملية الاستخدام، بينما أظهرت **دراسة محمد سالم المحمدي (2010)** [57] عدم وجود تعارض بين التشريعات بوزارة التجارة والصناعة بسلطنة عمان ومتطلبات الحكومة الإلكترونية .

اما البعد الإداري للحكومة الالكترونية الذى يضمن عملية الإبداع والابتكار الإداري ، وهو بلا شك سوف يحدث تغييرا في الهيكل الإداري لأجهزة الحكومة للنهوض بمستوى الخدمات الحكومية التي توفرها ، الأمر الذى ينعكس بشكل مباشر على تعزيز العمليات والإجراءات الإدارية ، وللحكومة الإلكترونية **بعدا توعويا** لا يقل أهمية عن غيره من الابعاد ، حيث ان التجارب العالمية والإقليمية التي فشلت في تنفيذ الحكومة الإلكترونية ترجع بالأساس الى أنها لم تأخذ بعد التوعية كعامل رئيسي في برامج التطبيق واتجاهاتها ، وبالتالي خلقت ما يمكن ان تسميته بأعداء الحكومة الالكترونية ، وهو ما يؤكد أهمية التوعية المجتمعية

لتوضيح أهمية الحكومية الالكترونية في تطوير الأداء الحكومي ، كما ان نشر الثقافة الإلكترونية سيؤدى الى كسر الحاجز النفسي من التحول الى الحكومة الإلكترونية ، وفى ذلك تشير **دراسة محمود إبراهيم ، بسمة الحداد (2018)**[58] أن أمن المعلومات أحد العوامل المهمة للتنبؤ بتقبل استخدام الخدمات لإلكترونية من قبل الافراد والمؤسسات .

أما **البعد الاقتصادي** للحكومة الإلكترونية فيلعب دورا فاعلا في بناء رؤيتها ورسالتها ، حيث أن تحفيز التجارة الإلكترونية وخلق صناعات تقنية متطورة تعتمد على البنية التحتية للحكومة الإلكترونية ، ويتمثل **البعد الفني** للحكومة الإلكترونية في استخدام الإمكانات الهائلة لتكنولوجيا المعلومات في زيادة القدرة الحكومية على توفير المعلومات لكافة الأطراف بسهولة ويسر [59] ، ولقد هدفت **دراسة Ubaldi, B. (2013)**[60] ، إلى تسليط الضوء على المبادئ، والمفاهيم والمعايير الرئيسية التي تقوم عليها مبادرات البيانات الحكومية المفتوحة ، حيث تناولت أهمية البيانات الحكومية المفتوحة والفوائد التي تعود على المجتمعات نتيجة تبني استراتيجية البيانات المفتوحة ، ويعد التحول الى حكومة ذكية هي المرحلة التالية بعد الحكومة الإلكترونية ، ويمكن تعريف الحكومة الذكية بانها حكومة تقدم الخدمات للمستفيدين بالتعاون مع جهات الكترونية أخرى للحصول على البيانات اللازمة لتقديم الخدمة بشكل آلي الى المستفيد [61].

وترتبط الحكومات الإلكترونية الذكية بوجود المدن الذكية ، حيث توفر بيئة ذكية معتمدة على تطوير منظومة العمل الحكومي باستخدام الوسائل الالكترونية في تقديم الخدمات الحكومية [62] وتعرف المدن الذكية بانها المدن المعتمدة على التقنيات الإلكترونية التي انتجها عصر تكنولوجيا المعلومات بداية من المدينة الرقمية الى المدينة الإلكترونية ثم الافتراضية ، وتعتمد المدن الذكية على التقنيات الرقمية والفراغات الافتراضية عبر شبكات المعلومات والتطبيقات المختلفة [63] .

كما تتكون المدن الذكية من **الشبكات** ، وهى المكون الأساسي لنقل وتبادل البيانات والمعلومات بين الافراد والمؤسسات من خلال التطبيقات الرقمية ،

وتتنوع شبكات المدن الذكية فهناك شبكات الالياف الضوئية Optical Fiber ، وشبكات الخط المشترك الرقمي Digital Subscriber Line DSL ،وشبكة WI-FI ، وهى شبكات واسعة النطاق وفائقة السرعة والدقة (64) ، أيضا من مكونات المدينة الذكية **قاعدة البيانات والتحليلات** حيث تمثل البيانات اهم العناصر التي تدعم نجاح تحول المدينة الى مدينة ذكية ، لذا يتم تجميع البيانات من الأنظمة الحكومية القائمة وتطبيقات الأنترنت والأجهزة المتنقلة ، ثم تحليل كافة البيانات لتحويلها الى رؤى وانشطة ذات قيمة (65) ، هناك أيضا **التطبيقات** من ضمن المكونات ومنها تطبيقات مخصصة لقطاعات بعينها وتطبيقات لمختلف قطاعات المستخدمين ، مثل خدمات الانترنت والأجهزة المتنقلة (الهواتف الذكية والأجهزة اللوحية وأجهزة الاستشعار).

ويعد **المستخدمين النهائيين** احد اهم مكونات المدينة الذكية ، فاعتماد الأفراد والهيئات على تطبيقات الأنترنت و الهواتف الذكية او الأجهزة اللوحية و أجهزة الاستشعار عن بعد GPS امر أساسي للاعتراف بالمدينة كمدينة ذكية على نحو حقيقي (66) ، وتصنف التجارب العالمية المدن الذكية الى صنفين الأول هو انشاء مدن ذكية جديدة ، والثاني هو تحول مدن قائمة الى مدن ذكية ، وتحتل امارة دبى صدارة المدن في الشرق الأوسط وافريقيا ، وفقا لمسح ميرسر لجودة الحياة 2015 ، فيما تحتل أبو ظبى المرتبة الثانية ، ويعتبر تحول مدينة دبى الى مدينة ذكية هو النموذج التقني لرؤية الحكومة الإلكترونية في مجال الاتصالات وتكنولوجيا المعلومات (67).

وترتكز حكومة دبى الذكية على **ركائز ست** وهى البنية التحتية والنقل والاتصالات والخدمات المالية والتخطيط العمراني والكهرباء، ويعتمد نجاح حكومة دبى الذكية على تقنيات الاتصال والبيانات ، ويمثل إنترنت الأشياء واقعا ملموسا الى حد كبير في دبى الذكية ، ويمثل الان عنصرا أساسيا ضمن طموح دبى المدينة الأكثر ذكاء في العالم ، حيث تعتمد على العديد من منصات المدن الذكية ، كما تعتمد المدينة على منهج EMC للمدن الذكية وهو منهج يهدف الى توفير منصات المدن الذكية المفتوحة والمرنة ، والتي توفر البنى التحتية التقنية

كخدمات افتراضية على الانترنت والقائمة على تحليل البيانات مع ضمان امنها[68] .

وتستند EMC للمدن الذكية الى **ثلاث ركائز** مفتوحة وقابلة للتوسعة ، وتتوافق بشكل وثيق مع اطار IDC من خلال ثلاث طبقات ، وهى **طبقة البنية التحتية** وهى الخدمات الافتراضية على الانترنت **وطبقة بحيرات البيانات** لتوفير بيانات مفتوحة وحمايتها واداراتها وتحليلها ومشاركتها ، **وطبقة التطبيقات** التي توفر عائدات البيانات ، وتوفر الطبقات الثلاث الرئيسية الأساس لمنصة المدن الذكية إمكانية التشغيل الإلكتروني للبنية التحتية والبيانات والتطبيقات باطار امنى قوى، ويوفر الاطار الأمني الرئيسي إمكانية التحقق من هوية المستخدمين ، والاستجابة للحالات الحرجة، ومراقبة العمليات الأمنية ، وإدارة التهديدات المتطورة المستمرة ، والتحليلات الأمنية على مستوى المنصة للمدن الذكية في البيئات السحابية للبرمجيات المشغلة داخليا وخارجيا ، ويحاط هذا الاطار بطبقة للحوكمة، وإدارة المخاطر ، بما يسمح للمدن بإدارة المخاطر الأمنية الخاص بها واتخاذ الإجراءات الضرورية للمعالجة [69] .

ويؤدى الاعتماد المتزايد على تكنولوجيات المعلومات والاتصالات بالحكومات الذكية الى ظهور إمكانات وفرص جديدة للتنمية الثقافية والاجتماعية والاقتصادية والسياسية والقانونية ، الا أنه يترافق معه زيادة المخاطر الالكترونية نتيجة الاستخدام السيء وغير المسؤول لهذه التكنولوجيات ، كما يؤدى التزايد المستمر في اعداد مستخدمي الانترنت الى تزايد عدد المستخدمين الذين قد يصبحون ضحايا للمخاطر الإلكترونية ، اما نتيجة الاستخدام الخاطئ او غير المسؤول للأنترنت وتطبيقاتها ، واما نتيجة الهجمات الموجهة لأجهزتهم الإلكترونية غير المحمية بالشكل الملائم

ومما يزيد من تعقيد المخاطر الإلكترونية اليات إخفاء المعلومات التي يعتمدها مخترقو الشبكات hackers ، وهى ما تعرف بالغفلية anonymity ، وكذلك الابتكارات التي يعتمدونها عند توجيه هجماتهم السيبرانية ، بالإضافة الى الطبيعة الدولية للجريمة السيبرانية [70] ، وفى هذا الإطار من المهم مكافحة المخاطر

المرتبطة بتبادل المعلومات والخدمات والمنتجات الرقمية والبنية التحتية الحرجة، كما انه من المهم أيضا وضع الية تنظيمية واستراتيجية شاملة للأمن السيبرانى، وذلك بالتعاون مع الصناعة الرقمية المتخصصة في هذا المجال للحماية من الجرائم الالكترونية ، والإرهاب الرقمي ، ومن إساءة استخدام الشبكة المعلوماتية، و توفير اليات واضحة لوضع سياسات الامن السيبرانى وتنظيم الإجراءات الوقائية والتصحيحية ، ووضع استراتيجية للتعاون المحلى والتوعية المجتمعية ، وكذلك التعاون الدولي في وضع وتنفيذ سياسات متعددة الأطراف لمكافحة الجرائم الإلكترونية العابرة الحدود [71] .

وتعد حروب الفضاء السيبرانى اختراق للشبكة العنكبوتية او للحاسوب اختراقا غير مصرح به للتأثير على الأنظمة الحاسوبية ، بغرض إضافة او تغيير او تزييف بيانات ، او التسبب في تعطيل جهاز حاسوب ، او اتلافه، او إتلاف أي جهاز متصل بشبكة التحكم [72] ، وتتضح السمات العسكرية والسياسية والاقتصادية للفضاء السيبرانى في خلق أدوات تهديد مختلفة وخطيرة تقوم بأحداث اضرار ملموسة كبيرة ومدمرة ، فذلك التدمير والضرر يتعدى النظام الحاسوبي بمراحل متقدمة ، حيث اثبتت دراسة **Solomon (jonathan2011)** [73] أنه يمكن للهجمات السيبرانية ان تتسبب في دمار هائل يطول الأمن القومي للدول ، ويمكنها أيضا أن تستهدف القيادة السياسية والأنظمة العسكرية والمواطنين العزل .

ولعلنا نستدل بالهجوم الإلكتروني الروسي على تالين العاصمة الاستونية عضو الناتو عام 2007 اثر خلافات سياسية ، وكان هذا يعد اول هجوم دولي بمفهومه السيبرانى ، والذى قام بشل البنى التحتية الحرجة في استونيا لمدة ثلاثة أسابيع، وتسبب بإيقاف البنوك والمصالح الحكومية والبث التليفزيوني والخدمات الالكترونية والصحف الرقمية [74] ، وكذلك تكرر الهجوم السيبرانى وأثره المكلف على جورجيا من قبل روسيا في عام 2008 ، وعلى أجهزة التصنت الإيرانية في عام 2010 من قبل الولايات المتحدة الامريكية والكيان الصهيوني، والهجوم على شبكة الكهرباء الإلكترونية عام 2015 ، والتدخل الروسي في الانتخابات الأمريكية [75] ، وهو ما اكدت عليه **دراسة Stevens tim**

(2015)[76]والتي أثبتت ان الهجمات السيبرانية تملك مجموعة كاملة من الأساليب والأدوات التي يمكنها التأثير المدمر في الفضاء السيبرانى وللهجمات السيبرانية عدة ابعاد استراتيجية ، ففي **البعد السياسي** تقع على مسؤولية الدولة الحفاظ على الأمن الرقمي ، وتامين كافة المؤسسات والمنظمات العاملة في حدودها السيادية من أي اعتداءات او هجمات سيبرانية ، من خلال سن القوانين والتشريعات ، اذ أكدت **دراسة خالد دخليز (2017)** [78] أهمية وجود قوانين وتشريعات خاصة بالتعاملات الإلكترونية في البيئة الرقيمة ، كما تؤكد **دراسة طوربيا ندير (2019)** [78] ان من أهم الأمور الواجب القيام بها عند تطبيق الحكومة الإلكترونية هي تحديث القوانين والتشريعات .

كما يعد **البعد الاقتصادي** من الأبعاد التي ترتبط بشكل أساسي بسيادة الدولة ، وتقع من ضمن مسؤولياتها في تعزيز الأمن الرقمي للمؤسسات والشركات الاقتصادية ، اما **البعد الاجتماعي** فمن التحديات والمصاعب التي تواجه الحكومات والدول هو جعل المستخدمين والعاملين على الشبكة الدولية للمعلومات امنين بعيدين عن الأخطار السيبرانية التي تهدد السلم والأمن المجتمعي ، والأهم والأصعب هو وضع استراتيجيات تثقيفية وتوعوية للحد من الأخطار السيبرانية[79] .

كما تمثل البروتوكولات والخدمات عناصر أساسية لضمان امن البنية التحتية لشبكة الانترنت ، حيث يعد فرق التصدي لحوادث أمن الحاسبات المعرف باسم فرق الاستجابة للطوارئ الحاسوبية ، بمثابة منظمة معنية بتلقي الحوادث الأمنية الحاسوبية ودراستها والاستجابة لها ، وتؤدى فرق التصدي لحوادث أمن الحاسبات وظيفة حيوية لتبادل المعرفة لضمان الامن المعلوماتي .

وهناك العديد من الدول تخصص فرقا للتصدي لحوادث الحاسبات ، وهناك بعض الدول تخصص مراكز تنسيق أوسع نطاقا للأمن السيبرانى ، والتي تشمل مهامها التواصل والتدريب المستمر واعتماد خبراء للأمن السيبرانى [80] ، ويهدف فريق الاستجابة الوطني لطوارئ الحاسب الآلي في دولة الإمارات العربية الى حماية البنية التحتية لتكنولوجيا المعلومات ، ونشر المعلومات

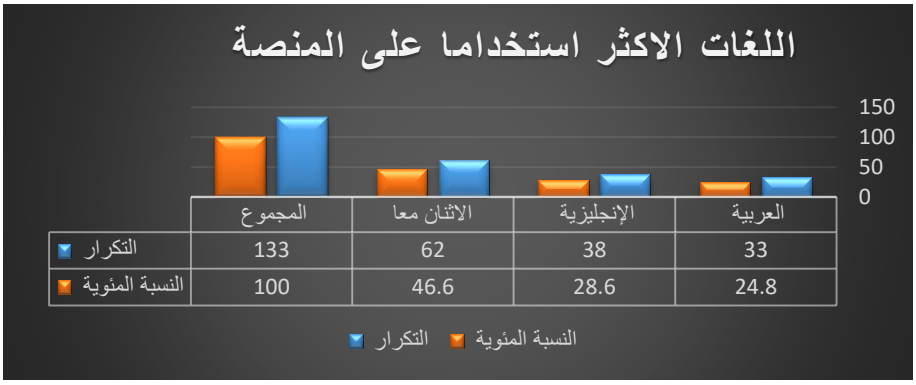
المتعلقة بالتهديدات والثغرات وحوادث الامن السيبرانى ، ويقدم أيضا مجموعة من الخدمات للجهات الحكومية مثل الاستجابة للحوادث والطب الشرعي الرقمي، وتقييم عمليات الاحتيال الإلكتروني [81] .

ويعد مركز الأمن الإلكتروني بإمارة دبى مركزا دوليا رائدا ووجهة إقليمية جاذبة لأنشطة المؤسسات المحلية والإقليمية والدولية ، تجذبها ريادة تكنولوجية ، حيث تقوم استراتيجية المركز على التوعية الأمنية الإلكترونية ، وبناءً مجتمع معلوماتي آمن ، وأكثر إدراكا لمخاطر الأمن الإلكتروني ، ومن الأهداف الرئيسية الأخرى لهذه الاستراتيجية الحد من مخاطر الشبكة ومكافحة أي اختراقات لها ، وتمكين المستخدمين أفرادا ومؤسسات من الوصول إلى تقنيات المعلومات المختلفة بما يدعم نجاح الاستراتيجية ، فنظرا للمكانة العالمية التي تشغلها إمارة دبي فقد أصبحت هدفاً رئيسياً للهجمات الإلكترونية التي تؤثر على أعمال القطاع العام والخاص ، وكذلك على مستوى الأفراد، ولذا فقد صدر القانون رقم 11 لسنة ٢٠١٤ بشأن إنشاء مركز دبي للأمن الإلكتروني ، بهدف تطوير استخدام الوسائل اللازمة في مجال أمن المعلومات ، ووضع المعايير الكفيلة بتوفير الأمن الإلكتروني ، والإشراف على تنفيذها ، وإعداد خطة استراتيجية لمواجهة أي مخاطر أو اعتداءات على المعلومات ، وتوضح هذه الاستراتيجيةّ الإجراءات اللازمة لبناء مجتمع واع بمخاطر الأمن الإلكتروني [82] وتشكل دولة الإمارات العربية المتّحدة هدفا أساسيا لأعمال القرصنة الأخلاقية في مجال الأمن المعلوماتي ، حيث شهد عام 2016 خسارة بقيمة 14.5 مليار درهم ، بسبب الجرائم الإلكترونية، وتشير الإحصائيات الصادرة عن شرطة دبي الى أن واحد من أصل خمسة من سكان الإمارة وقع ضحية للجرائم الإلكترونية خلال عام 2015 ، وقد ارتفعت اعداد تقارير الجرائم الإلكترونية بنسبة 23 % خلال عام 2016 ، ومن المتوقع أن تزداد هذه المعدلات بشكل أسرع حتى عام 2020، ويهدف مركز دبي للأمن الإلكتروني وفقا لقانون إنشائه الى مكافحة الجرائم الإلكترونية ، وأعمال القرصنة وتطوير الحلول التقنية اللازمة للحد منها [83] .

مناقشة نتائج الدراسة التحليلية

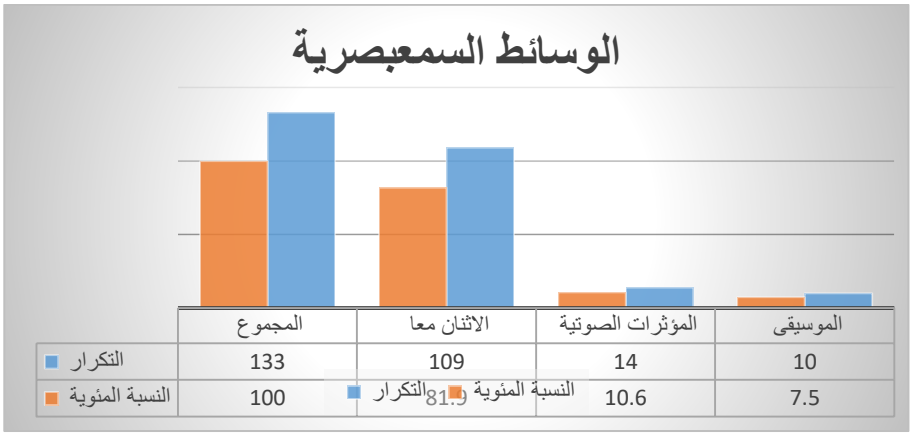
أولا : فئات الشكل

شكل رقم (1)



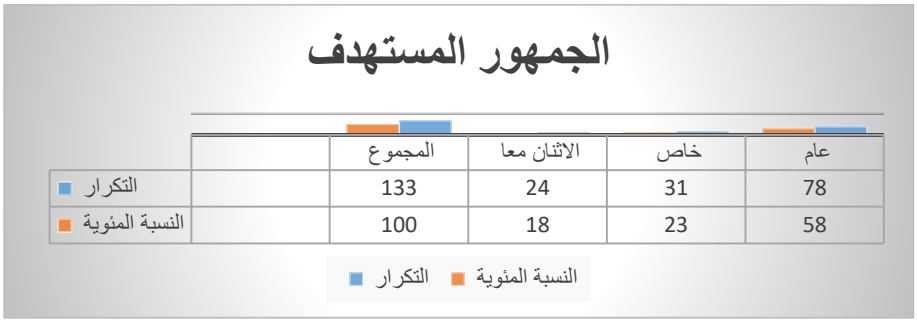
تسفر بيانات الرسم البياني رقم (1) على غلبة اللغتان العربية والانجليزية على المواد الإعلامية المذاعة والمنشورة على منصة التواصل الاجتماعي **انستجرام** لمركز الأمن الإلكتروني بحكومة دبى الذكية ، حيث وصـــل ذلك الى نســـبة 46.6 وهى اللغات الأكثر اســـتخداما في العالم ، تلاها اللغة الإنجليزية بنســـبة 28.6 % كلغة عالمية ، ثم اللغة العربية بنسبة 24.8 % .

شكل رقم (2)



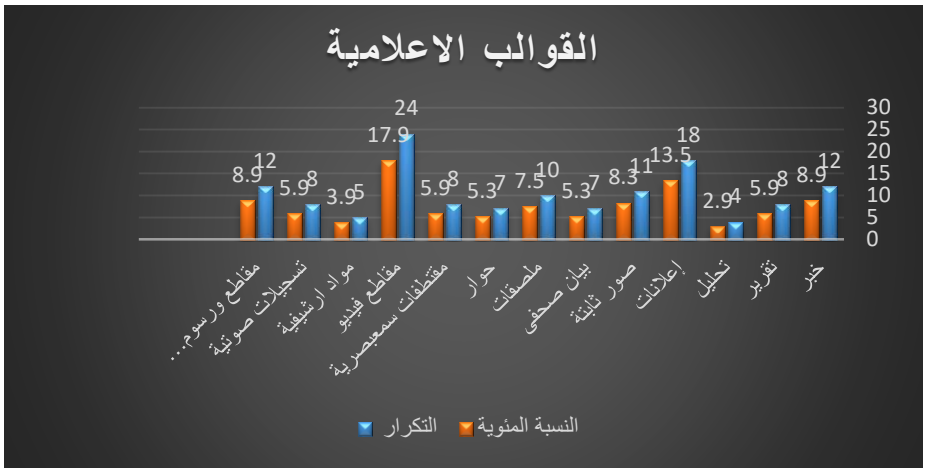
تسفر بيانات الشكل رقم (2) تحرص منصات وسائل التواصل الاجتماعي على اتاحة الوسائط متعددة ، ودمجها بفاعلية برسائلها الإعلامية بما يحقق استراتيجيةً اتصالية متميزة للمنصات ، فالدمج بين الوسائط السمعية والبصرية يحقق إرضاء لكافة الجماهير على اختلاف انماطهم وأذواقهم ، و تدل البيانات الواردة على حرص منتجى المواد الإعلامية على صفحة الانستجرام بمركز الأمن الالكترونى بدبى الذكية ، على الدمج بين المؤثرات الصوتية والموسيقى حيث جاء ذلك بنسبة 81.9 % ، وتلعب المؤثرات الصوتية دورا أساسيا في التأكيد على واقعية الحدث واتمام فهم المتفرج للصورة التي يراها وفى شد انتباهه، أما الموسيقى فتعطى ايقاعا ماديا محسوسا للصورة [84] .

شكل رقم (3)



جاء التركيز على الجمهور بشكل عام بسنبة كبيرة وصلت الى 58 % نظرا لأهمية الموضوع لكافة شرائح المجتمع دون تخصيص حيث أثبتت **دراسة احمد القاضي (2014)** [85] ان تطور البنية الأساسية لتقنيات المعلومات والاتصالات بالمدينة الذكية يتم من خلال جمع البيانات وتصنيفها وتحديد حقوق مختلف الجهات في الوصول للبيانات دون تخصيص لأى من الفئات او الجهات، فالهدف العام هو بناء القدرات والمهارات لدى الجمهور لدعم تعامله مع تطبيقات المدنية الذكية ورفع قدراته الابتكارية حيث انه الركيزة الأساسية للمنظومة الذكية ، لكن هناك بعض الرسائل الموجهة الى فئات مستهدفة وقد جاء ذلك بنسبة 23 % ، أما الرسائل الموجهة للطرفين الجمهور العام والخاص بنفس الوقت جاءت بنسبة 18 % .

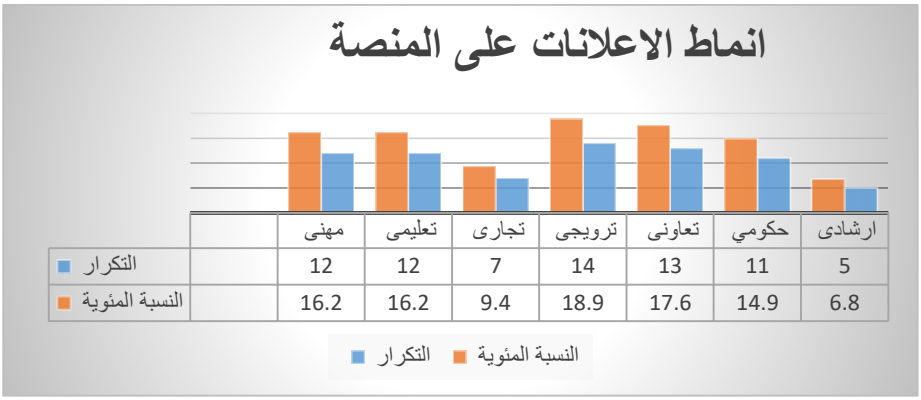
شكل رقم (4)



اتضح من بيانات الشكل السابق ان مقاطع الفيديو تصدرت القوالب الإعلامية على منصة الانستجرام بنسبة 17.9 % ، ثم الإعلانات بنسبة 13.5 % ، أما الرسوم الجرافيكية الثابتة والمتحركة وقالب الاخبار فقد جاءوا بالترتيب الثالث بنسبة 8.9 % ، جاءت بعدها الصور الثابتة و بنسبة 8.3 % ، والملصقات بنسبة 7.5 % ، كملصقات بعنوان ، **ممارسات تقنية صحية ، نصائح لتسديد المدفوعات بأمان ، وحقائق واراء ، والوعى = امان** ، كما تساوى كلا من المقتطفات السمعبصرية والتسجيلات الصوتية والتقارير الصحفية بنسبة 5.9 % ، حيث كانت هناك العديد من التغطيات التليفزيونية الحية للفاعليات المقامة بالمركز ، مثل تغطية الدورة الثالثة بعنوان **الذكاء الاصطناعي ومستقبل الامن** السيبرانى ، والمخيم الصيفي بعنوان **معسكر قادة الفضاء الإلكتروني** ، أما البيان الصحفي وقالب الحوار فقد جاءوا بنفس الترتيب بنسبة 5.3 % ، وتعد البيانات الصحفية والإذاعية news releases من أكثر الأدوات استخدامًا اثناء الاحداث الطارئة ، حيث تستخدم البيانات الصحفية المذاعة والمطبوعة لتوضيح الحقائق واحداث التوعية اللازمة [86] وقد كانت هناك مجموعة من البيانات الصحفية المنطلقة عبر المتحدث الرسمي للمركز والمتجاوبة مع الاحداث الجارية مثل البيانات الخاصة **بجائحة كوفيد 19** واهمية التأكد من صحة الإصابة وعدم

الانجراف وراء الشائعات والمواقع المضللة ، والتعرف على اليات حماية المعدات الطبية من الاختراقات الأمنية ، بالإضافة الى التوجيهات بشان حماية مكتسبات الثورة الرقمية ومواكبة التحولات التكنولوجية ، أيضا كانت هناك حوارات واحاديث صحفية لصحف وقنوات تليفزيونية من القائمين على المركز فيما يخص الامن السيبرانى وتحدياته ، وفى الترتيب قبل الأخير جاءت المواد الارشيفية بنسبة 3.9 % ، وجاءت التحليلات الإخبارية بنسبة 2.9 % .

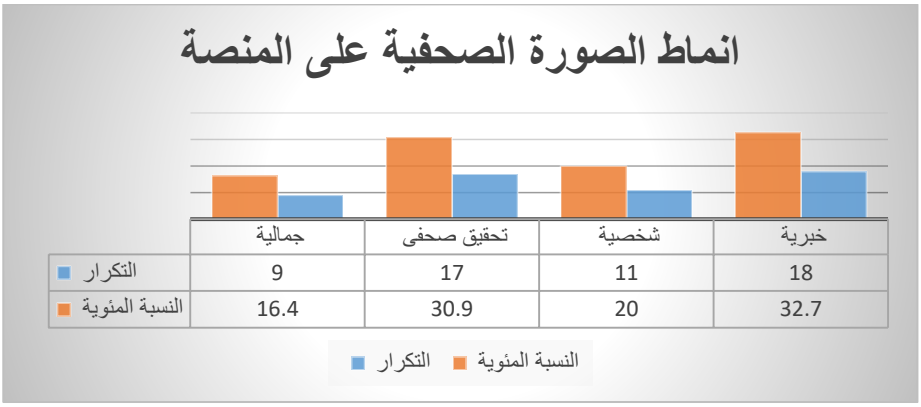
شكل رقم (5)



اصبح الإعلان واحدا من اكثر نشاطات الاتصال تأثيرا على المجتمعات المعاصرة ، فكما يؤثر في ترويج السلع والخدمات فانه يسهم عمليا في نشر القيم والاتجاهات الجديدة ويعمل على تغيير العادات والأذواق لدى الناس، ووفقا لبيانات الرسم البياني السابق جاء الإعلانات الترويجية في التربيب الأول بنسبة 18.9 % ، تلاها الإعلانات التعاونية بنسبة 17.6 % ، تأتى بعد ذلك الإعلانات التعليمية والمهنية بنسبة 16.2 % ، اما الاعلانات الحكومية جاءت بنسبة 14.9 % ، وفى الترتيب قبل الأخير جاءت الاعلانات التجارية بنسبة 9.4 % ، وأخيرا الإعلانات الارشادية بنسبة 6.8 % ، ومن أمثلة الإعلانات الدعائية على منصة انستجرام " **الوقاية الإلكترونية من فيروس كورونا** ، وكذلك إعلانات لترويج رؤية ورسالة المركز ، وإعلانات دعائية شعارها " **احمى نفسك** ، أيضا إعلانات للترويج لحضور الفاعليات والقمم والمسابقات التي يعقدها ، كالإعلان

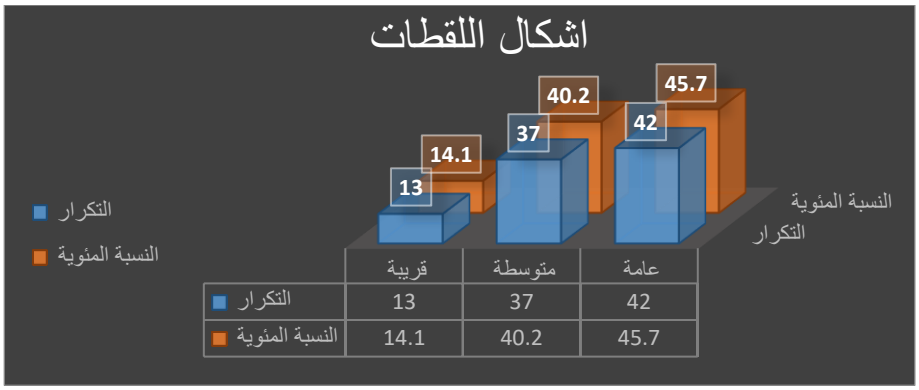
عن مسابقة سحب لتامين الحسابات ، والاعلان عن **اليوم العالمي للبيئة** ، والاعلان عن فاعلية **تسوق بأمان عبر الانترنت** ، والاعلانات عن الدعوة للالتحاق بمعرض الوظائف 2019 ، والمشاركة في **جائزة الابتكار البحثي** التي يعقدها المركز ، كما يشارك المركز بالإعلان عن خدمات الامن السيبرانى بدولة الامارات ، حيث تم الإعلان عن **مختبر الامن الإلكتروني** وهو احدث مختبر علمي وبحثى في مجال انترنت الأشياء والذكاء الاصطناعي وتقنيات البلوك ، وهو الأول بالشرق الأوسط بجامعة دبى المخصص لخلق ابتكارات بحثية غير مسبوقة لمواجهة تحديات الامن الإلكتروني ، كما أن هناك حملات دعاية كالدعاية عن **سحاب الكترونى اقوى** ، واطلاق حملات مجتمعية للطفل والاسرة كحملات **حافظي على امن طفلك ، وأطفالنا اليوم**.

شكل رقم (6)



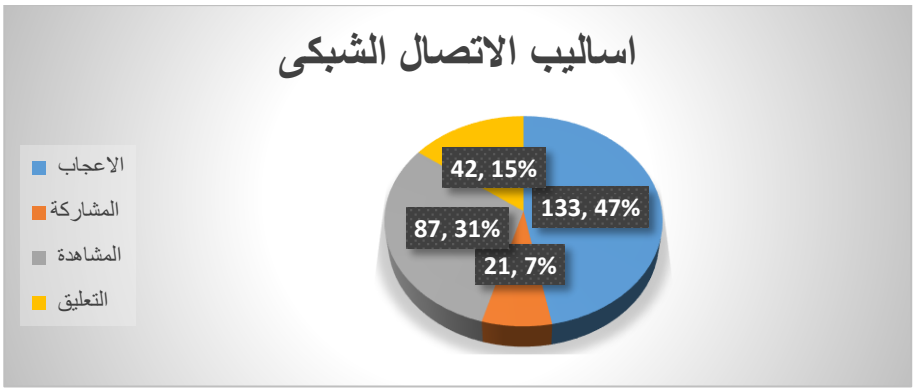
افصحت نتائج الشكل السابق على حصول الصورة الخبرية على الترتيب الأول بنسبة 32.7 % ، تلاها صورة التحقيق الصحفي بنسبة 30.9 % ، وقد كانت أغلب الصور تحمل عبارات استفهامية او تعجبية لجذب الانتباه وتحقيق التأثير ، ومن أمثلة تلك العبارات التالية ، **هل سبق وان تعرضت حساباتك للاختراق ؟، كيف اتخذت التدابير لتامين حسابك ؟ ، هل تعمل بإحدى هذه النصائح؟ ، متى قمت بإجراء نسخة احتياطية لأجهزتك ؟**، ثم جاءت الصور الشخصية بنسبة 20% ، كصور حاكم دبى والقائمين على المركز وبعض الصور لشخصيات عامة .

شكل رقم (7)



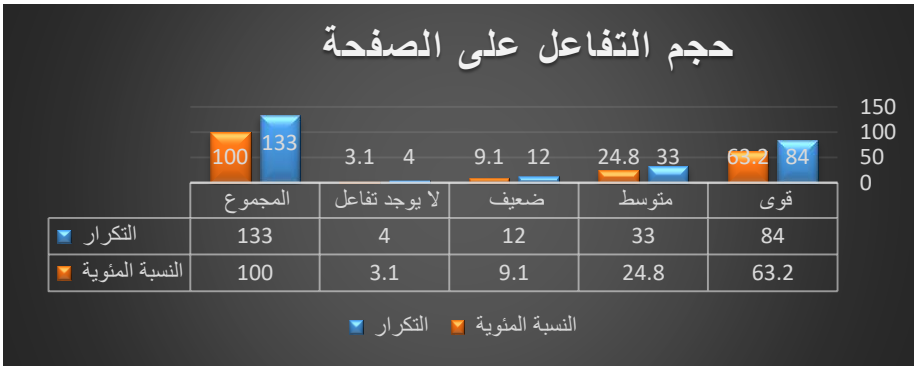
ووفقا لنتائج جدول رقم (7) كانت اللقطات العامة البعيدة هي الأكثر استخداما اثناء التغطية التليفزيونية ، حيث جاءت بالترتيب الأول بنسبة 45.7 % ، جاءت بعدها اللقطات المتوسطة بنسبة 40.2% ، وأخيرا اللقطات القريبة بنسبة 14.1%، وان استعمال أنواع محددة من هذه اللقطات المكونة لمختلف الصور له دور في ترسيخ المعلومات لتحقيق تأثير معين لدى المشاهد وتوجيه استجاباته باعتبار ان كل نوع له دلالته الخاصة ، فاللقطة العامة تستعمل في صرف انتباه المشاهد عن شيء معين، بينما تستخدم اللقطة القريبة للتأكيد على الشيء المصور اوعلى موقف او رأى معين من خلال التركيز على ردود الأفعال والملامح، اما اللقطة المتوسطة فتقع بين اللقطة العامة والقريبة ، وتستخدم بغرض اشعار المتفرج بالحميمية والتعاطف مع الشيء المصور [87] ، وقد كانت اغلب اللقطات مأخوذة من الفاعليات المقامة بالمركز والتغطيات الحية للقاءات والفاعليات، والتي تنوعت لقطاتها من عامة بعيدة لإظهار الفاعلية بكامل ابعادها، واللقطات القريبة جدا على ملصقات او شخصيات لإبراز اهميتهم داخل الحدث ولقطات توسطت ذلك .

شكل رقم (8)



نظرا لأهمية التفاعل مع جماهير المركز على صفحة المركز على انستجرام ، فقد وفرت المنصة العديد من أساليب وأدوات الاتصال الشبكي والرقمي، وذلك لتوفير مزيد من التفاعلية مع الجماهير ، وقد كان أسلوب الاعجاب من اكثر أساليب الاتصال الآلي والشبكي ظهورا في العينة حيث وصل الى 47 % ، تلاه المشاهدة بنسبة 31% ، ثم التعليق بنسبة 15 % ، وأخيرا المشاركة بنسبة 7 % .

شكل رقم (9)

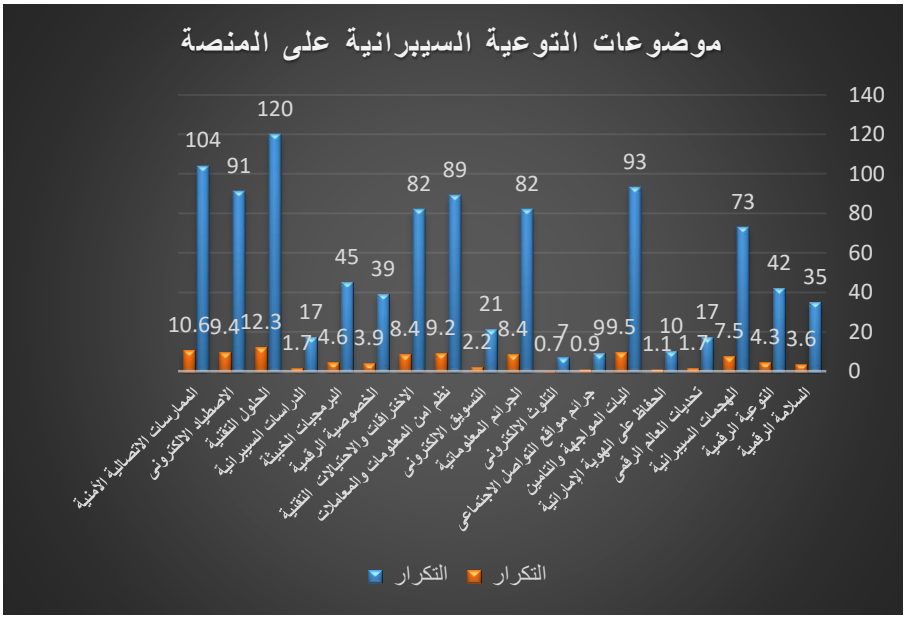


كنتيجة لتوفر العديد من أساليب الاتصال الشبكي على الصفحة من مشاركة ومشاهدة واعجاب وتعليق ، جاءت نسبة التفاعلية عالية حيث وصل نسبة التفاعلية بشدة 63.2 %

، ثم جاء التفاعلية بدرجة متوسطة بنسبة 24.8 % ، ثم جاءت نسبة التفاعلية الضعيفة بنسبة 9.1 % ، وأخير كان عدم التفاعل بنسبة 3.1 % .

ثانيا / فئات المضمون

شكل رقم (10)

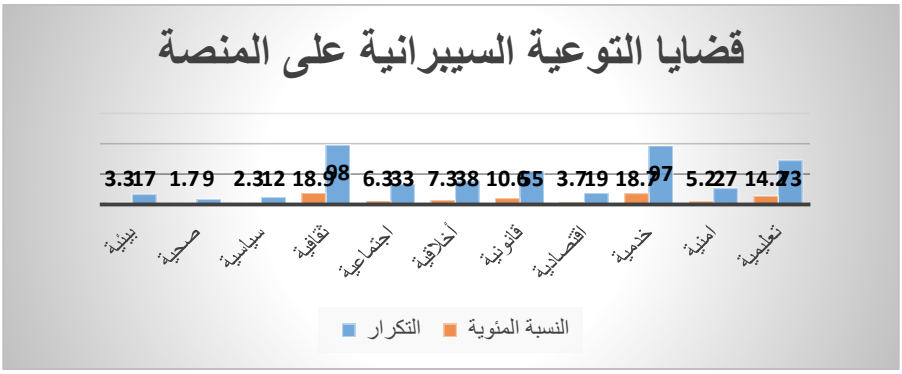


وفقا لرسالة مركز دبى للأمن الالكترنى في إيجاد مجتمع واعى بمخاطر التكنولوجيا وعلى دراية باليات الامن المعلوماتى فقد تناولت المنصة العديد من الموضوعات الخاصة بالأمن الالكترونى ورسالته ، حيث حرص المركز على تقديم الحلول الامنة لمشكلات التقنية والأمن السيبراني بالترتيب الأول ، وهو ما جاء بنتائج الشكل السابق حيث جاء ذلك بنسبة 12.3 % ، تلاها الممارسات الاتصالية الامنة بنسبة 10.6 % ، ثم اليات المواجهة والتامين بنسبة 9.5 % ، ثم موضوعات الاصطياد الالكترونى بنسبة 9.4 % ، ثم نظم المعلومات والمعاملات بنسبة 9.2 % يليها الاختراقات والاحتيالات التقنية بنسبة 8.4 % ، تساوى معها بالنسبة الجرائم المعلوماتية ، وقد سردت **دراسة اسراء إبراهيم**

(2018) [88] طرق الجرائم الالكترونية من تخريب المعلومات وإساءة استخدامها وتزويرها وتزيفها ، وكذلك انتهاك الخصوصية والتصنت والتجسس والتشهير والدخول غير القانوني للشبكات ، أيضا قرصنة البرمجيات والبيانات والمعلومات والمطاردة والملاحقة والابتزاز والإرهاب الإلكتروني ، اما الهجمات السيبرانية فجاءت بنسبة متقاربة الى حد ما حيث وصلت الى 7.5 %.

وفى الترتيبات الاخيرة توالت موضوعات التوعية الرقمية والخصوصية والسلامة الرقمية بنسب 4.6 ، 4.3، 3.9 ، 3.6 % على التوالي ، وهو ما يتوافق مع **دراسة بارنى دارن (2015)** [89] على أهمية التركيز على الاستثمار الرقمي في الرأسمال البشرى ، والعمل على سد الفجوة الرقمية من خلال الاستثمار في برامج التعليم ، ثم تساوت بعد ذلك موضوعات تحديات العالم الرقمى مع موضوعات الأبحاث والدراسات السيبرانية بنسبة 1.7 % ، ثم جاءت موضوعات التوعية حول جرائم مواقع التواصل الاجتماعى بنسبة 0.9 % ، وأخيرا جاء التلوث الاكترونى بنسبة 0.7 % بالترتيب الأخير.

شكل رقم (11)

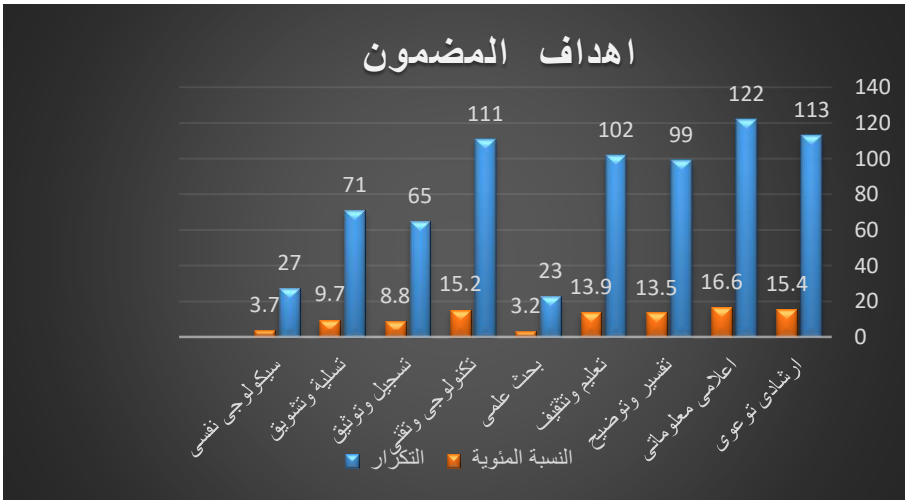


وفقا لنتائج تحليل الشكل السابق جاءت القضايا الثقافية بالترتيب الاول بسبنة 18.9 % فلقد اثبتت **دراسة على حداده (2019)** [90] ان باستطاعة الحكومة الإلكترونية الذكية القيام بدور مهم في الكشف عن سياسات الامن المعلوماتي وتثقيف المواطنين بها واعلامهم بمخططاتها ومشروعاتها ، حيث ان اطمئنان

المواطن للخدمات الإلكترونية يعطيه الثقة والأمان ، جاء بعد ذلك بنسب متقاربة القضايا الخدمية بنسبة 18.7 % ، ثم جاءت القضايا التعليمية بالترتيب الثالث بنسبة 14.2 % ، وفى التريب الرابع القضايا القانونية بنسبة 10.6 % ، والقضايا الأخلاقية بنسبة 7.5 % ، تلتها القضايا الاجتماعية بنسبة 6.3 % ، اما قضايا الامن جاءت بنسبة 5.2 % ، ثم القضايا الاقتصادية بنسبة 3.7 % ، وعن تأثير الهجمات السيبرانية على الوضع الاقتصادي للدول توصلت **دراسة علم الدين بانقا (2019)** [91] ان الهجمات السيبرانية الخبيثة في مقدرتها التدمير والحاق الضرر بالمؤسسات الاقتصادية .

وتتمثل المشكلة الاقتصادية للهجمات الالكترونية الخبيثة في عدم قصورها على المؤسسة المستهدفة وحدها وانتشار اثارها الخارجية السلبية negative externalities الى القطاعات الأخرى خصوصا في المؤسسات التي تعمل في مجال البنية التحتية الحيوية والتي قد تنتشر عبرها الاثار السلبية للهجمات الى الأنشطة الاقتصادية الأخرى فتتعطل تلك الأنشطة مما يفاقم الخسارة الناجمة عن هذه الهجمات وأخيرا تتوالى القضايا البيئية والقضايا السياسية والقضايا الصحية في الترتيبات الاحيرة بنسب 3.3 ، 2.

شكل رقم (12) .

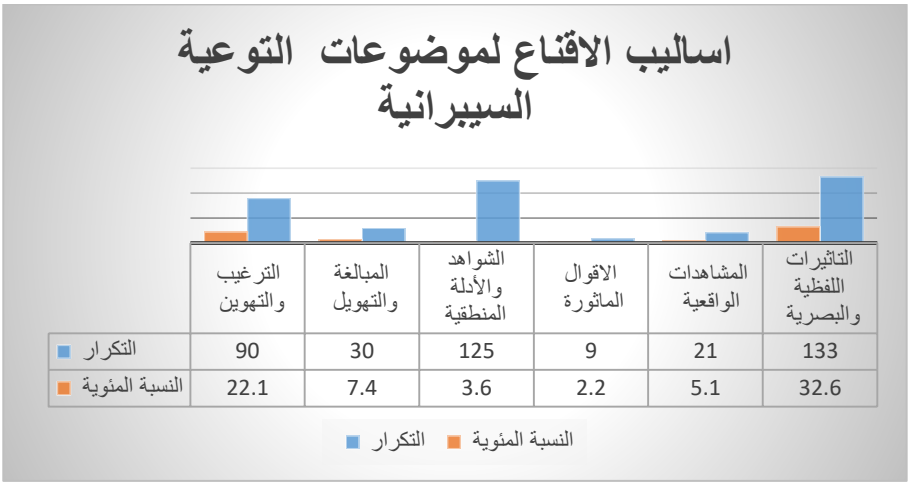


يتحليل نتائج الجدول السابق اتضح ارتفاع نسبة الهدف الإعلامي والمعلوماتى للرسائل الاعلامية على منصة الانستجرام لمركز الامن الالكترونى ، وذلك حيث حصلت على نسبة 16.6 % تلاها الهدف الارشادي والتوعوي بنسبة 15.4 % وتقدم منظمة الايسكو مجموعة إرشادات للحماية السيبرانية في هذا الاطار حيث تضمنت مجموعة إرشادات خاصة بالاتصالات الإلكترونية ، وتضمنت أيضا ارشاد الملكية الفكرية في المجال السيبرانى وارشادات التجارة الالكترونية وحماية حقوق المستهلك ، وكذلك إرشادات معالجة البيانات ذات الطابع الشخصي ، وارشادات الحفاظ على امن الدولة والدفاع الوطني وارشادات الجرائم الالكترونية او السيبرانية [92] اما الهدف الخاص بابراز المعالم التكنولوجية والتطبيقات التقنية جاءت في الترتيب الثالث بنسبة 15.2 % ، جاء بعد ذلك هدف التعليم والتثقيف بنسبة 13.9 % حيث يعد تعلم المهارات الرقيمة امر ضروري خلال القرن الحادي والعشرين ، ولذلك فالدول تطبق استراتيجيات شاملة للمهارات الرقمية وتحرص ان تتمتع شعوبها بالمهارات التي تحتاجها لتكون اكثر قابلية للإنتاجية والابداع والنجاح ، الى جانب بقائها امنة وسالمة في التواصل عبر الانترنت [93]

جاء بعد ذلك هدف التوضيح والتفسير بنسبة 13.5 % ، اما هدف التسلية والتشويق كهدف هام من أهداف الاتصال جاء بنسبة 9.7 % ، يليه هدف التسجيل والتوثيق بنسبة 8.8 % ، ثم جاء هدف التأكيد على الحالة النفسية والسيكولوجية للمتلقى بنسبة 3.7 % ، حيث يمكن لذوى المهارات الرقمية النفاذ الامن الى الاخبار والمعلومات والوصول الى الخدمات الهامة المتعلقة بالصحة الإلكترونية والحكومة الإلكترونية ، والتمويل الرقمي والنقل الذكي ، حيث أنه لم تعد المهارات الرقمية المطلوبة تقتصر على العمليات الأساسية للمعدات والبرمجيات والبريد الإلكتروني بل تم تحديثها الى المهارات الرقمية المطلوبة للتعامل مع الذكاء الاصطناعي ، والبيانات الضخمة وسلسلة كتل البيانات والحوسبة السحابية ، وانترنت الأشياء والتعلم الألي والتطبيقات المتنقلة وإدارة الشبكات [94] ، وأخيراجاء التأكيد على أهمية الأبحاث والدراسات السيبرانية والأمن الالكترونى والمعلوماتى بنسبة 3.2 % ، فلقد طورت العديد من المنظمات الدولية اطر

المهارات الرقمية ، حيث قامت المفوضية الأوروبية بتدشين اطار للكفاءة الرقمية للمواطنين (DigComp) ، وهو أداة لتحسين الكفاءة الرقمية لدى المواطنين ومساعدة أصحاب الشأن على صياغة السياسات التي تدعم الكفاءة الرقمية وتخطيط مبادرات التعليم والتدريب لتحسين الكفاءة الرقمية لدى فئات مستهدفة محددة [95].

شكل رقم (13)

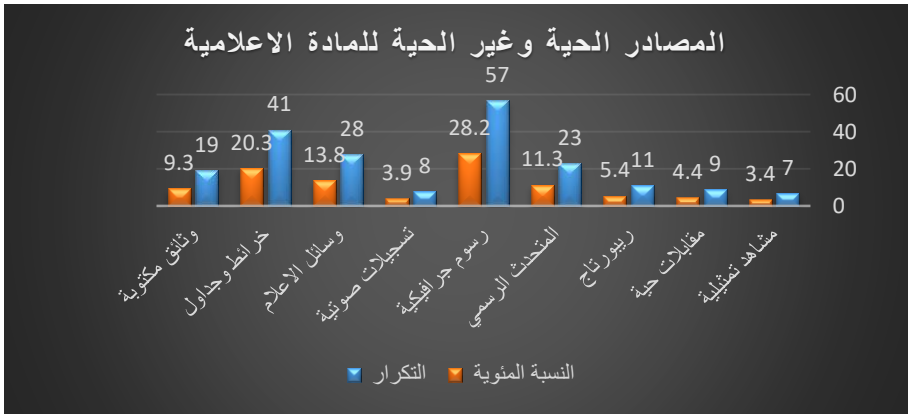


اتضح من نتائج الجدول السابق اعتماد منصة انستجرام على استمالة الاقناع بوصفه عملية فكرية يحاول احد الطرفين التأثير على الاخر واخضاعه لفكرة ما ، وبتحليل بيانات الرسم البياني السابق اتضح اعتماد المواد الإعلامية على المنصة على الدمج بين الإستمالات العقلية والإستمالات العاطفية لإقناع الجمهور والتأثير فيهم وتوعيتهم التوعية المطلوبة لمواجهة مثل هذه التحديات السيبرانية ، حيث ان فاعلية الإستمالات العاطفية تتوقف الى حد كبير على اقناع الافراد بالتفكير المنطقي [96] ، وقد جاءت التأثيرات اللفظية والبصرية بنسبة 32.6 % ، ثم جاء بعد ذلك أسلوب الترغيب والتهوين بنسبة 22.1 % ، يليها أسلوب المبالغة والتهويل والتخويف بنسبة 7.4 % ، وتعد استمالات التخويف من الإستمالات العاطفية التي تحمل رسائل اقناعية توضح الاضرار الاجتماعية

التي تترتب على عدم الاستجابة لمحاذير الرسائل الإقناعية ، وليس الهدف منها فقط هو اثارة الرعب بين المتلقين ، ولكن الشرح والتوضيح وتقديم الحقائق وصولا الى الاتجاه الإيجابي بالضغط على وتر الخوف كاستجابة انفعالية لما قد يهدد الانسان وامنه وصحته ، كما يشير مصطلح التخويف الى النتائج غير المرغوبة التي تترتب على عدم اقتناع المتلقي او قبوله لتوصيات القائم بالاتصال(97)

وهناك الكثير من الرسائل التحذيرية على منصة انستجرام والتي تحمل في طياتها الخوف من عواقب عدم الاستجابة لها من جانب المتلقي مثل **تمهل وفكر** ، قبل ادخال بيانات البطاقة الائتمانية والانتباه لأدوات التطبيقات **واحذر قبل ان تنقر** ، **احذر من التصيد الإلكتروني ، احذر من مشاركة بياناتك** ، اما المشاهدات الواقعية جاءت بنسبة 5.1 % ، ثم الشواهد والأدلة المنطقية بنسبة 3.6 % ، حث ان تقديم الأدلة يكون وقعه اكبر على الجماهير الذكية أي أولئك الذين يتوقعون اثباتا للأفكار المعروضة عليهم (98) ، وأخيرا الأقوال المأثورة جاءت بنسبة 2.2 % ، وتقديم الأقوال المأثورة لنماذج لقادة الرأي يساعد الفرد على تقبل السلوك المرغوب لميل الفرد الطبيعي الى الاقتداء بنماذج معنية ، ومن الأقوال المأثورة المنشورة على المنصة "**الجميع مسؤول عن الجميع** " هاشتاق بعنوان "**لاشى مستحيل** # ، **الهوية الإعلامية الإماراتية#** .

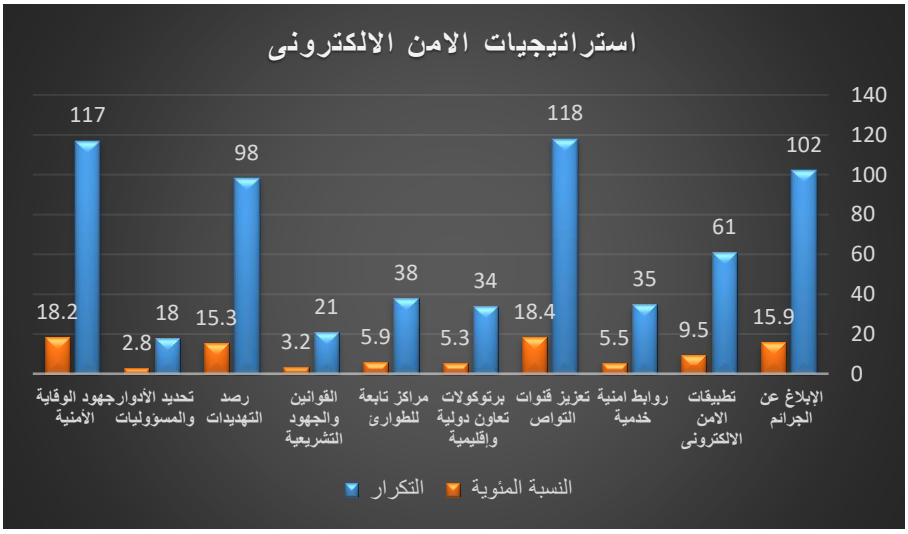
شكل رقم (14)



حول طبيعة المصادر التي اعتمدت عليها المواد الاتصالية على منصة الانستجرام ، افصح الرسم البياني السابق عن عدة نتائج من أهمها حصول الرسوم الجرافيكية الثابتة والمتحركة على الترتيب الأول بنسبة 28.2 % ، وهو ما يتوافق مع تقنيات الإنتاج الإذاعي الرقمي، ثم جاءت الخرائط والجداول بالترتيب الثاني بنسبة 20.3 % ، وفى الترتيب الثالث جاءت المواد الإعلامية المأخوذة من وسائل الإعلام الأخرى بنسبة 13.8%، اما المتحدث الرسمي عن مركز الامن الإلكتروني بحكومة دبى الذكية كمصدر هام للمعلومات جاء في الترتيب الرابع بنسبة 11.3%، وجاءت الوثائق المكتوبة في ترتيب متأخر بنسبة 9.3 %، تلاها الريبورتاج بنسبة 5.4 % .

ويعد التحقيق الصحفي احدى صور التغطية الشاملة للأحداث والمناسبات، كتهنئة مدير المركز للفائزين بالمسابقات التي ينظمها المركز ايضا التغطية الحية لفاعليات مجتمعية، كفاعلية **لنستمر في حماية كوكبنا** وإعادة التدوير الامن للأجهزة الإلكترونية، **وساعة الأرض** والوقاية من التلوث الإلكتروني، وقد جاءت المقابلات الحية بنسبة 4.4 % ، لتغطية تلك الفاعليات ، وفى الترتيب قبل الأخير جاءت التسجيلات الصوتية كمصدر غير حي بنسبة 3.9 % ، وأخيرا جاءت المشاهد التمثيلية كنوع من أنواع الدراما حيث تمثل مصدر حي من مصادر المعلومات ولقت قبولاً جماهيرياً واسعا تمثل في نسبة المشاهدة العالية والإعجاب بالمحتوى ، وتمثل ذلك بنسبة 3.4 %

شكل رقم (15)

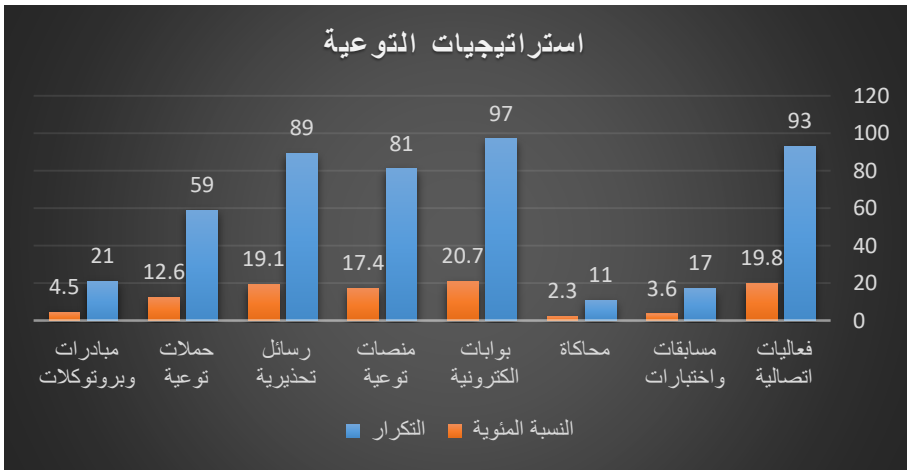


اتضح من البيانات السابق ذكرها ان استراتيجيات تعزيز التواصل بين الجمهور والمركز الإلكتروني عبر قنواته الاتصالية كانت من اهم استراتيجيات الأمن الإلكتروني المتخذة لمواجهة تحديات الأمن السيبرانى ، جاء ذلك بنسبة 18.4 % ، وهذا ما دعا حلف الناتو للتدخل وتأسيس مركز متخصص بأمن الفضاء السيبرانى لفهم المخاطر ووضع الاستراتيجيات لمواجهتها وتعزيز التواصل المجتمعي [99] ، تلاها بالمركز الثاني الجهود والتدابير الأمنية كاستراتيجيات هامة من قبل مركز الأمن الإلكتروني ، وذلك بنسبة 18.2 % ، ثم جاء استراتيجية الإبلاغ عن جرائم الانترنت وجرائم الأمن المعلوماتي بالترتيب الثالث بنسبة 15.9 % ، اما رصد التهديديات الأمنية كاستراتيجية هامة لتحديد حجم المخاطر السيبرانية جاءت بنسبة 15.3 % بالترتيب الرابع .

وفى هذا الإطار حددت **دراسة ذنيب القحطاني (2015)** [100] الإجراءات الأمنية التالية للوقاية من الهجمات السيبرانية ، كاستخدام جدار الحماية fire well لفحص المعلومات الداخلية والخارجة والسماح لها بالمرور في حالة مطابقتها للمواصفات ، وكذلك التوقيع الرقمي وهى تقنية تفيد في إمكانية عدم تزوير الرسائل الإلكترونية ، كما اكدت على وضع سياسة امنية للشبكة وحشد كل الإمكانيات البشرية والمادية لتطبيقها ، كما اوصت برسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرام الأنترنت ، وتوعية الأفراد ونصحهم لماهية الجرائم الالكترونية وكل ما يترتب عليها من مخاطر ، وكذلك الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف عن هوية مرتكب الجريمة والاستدلال عليه باقل وقت ممكن ، وكذلك الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية كالحسابات البنكية والباقات الائتمانية وغيرها ، وفى الترتيب الخامس جاءت استراتيجية الإعلان عن تطبيقات الامن الإلكتروني بنسبة 9.5 % ، ثم الإعلان عن المراكز المرتبطة بمركز الأمن الإلكتروني بنسبة 5.9 % ، ثم جاء بعد ذلك أيضا الإعلان عن بروتكولات تعاون دولية وإقليمية في مجال الامن الإلكتروني وحماية المعلومات بنسبة 5.9 % ، **كالتعاون المبرم مع جامعة الشارقة** في مجال الامن المعلوماتي **ومذكرة التفاهم المنعقدة مع المعهد البريطاني** من اجل تضافر الجهود والمساهمة لجعل دبى مدينة اكثر أمانا بالعالم وكذلك عقد **الندوات كندوة الإمارات** IEEE بالتعاون مع sumit 2019 لتسليط الضوء على تأثير الذكاء الصناعي لمواجهة تحديات الفضاء الرقمي ، تلا ذلك الإعلان عن روابط وتطبيقات امنية وخدمية لحماية المواطنين من الاحتيالات والاختراقات بنسبة 5.5% ، كالإعلان عن **مبادرة**

اطلاق منصة المعلومات للتهديدات الإلكترونية ، واطلاق سياسة امن المواقع الالكترونية بالتعاون مع الجهات الحكومية، وكذلك اطلاق منصة دعم امتثال الجهات الحكومية لمؤشرات الامن الإلكتروني، ثم تقارب بعد ذلك في الظهور استراتيجيان " الترويج للقوانين والجهود التشريعية المأخوذة والمحددة ضد جرائم الأمن المعلوماتي ، فمع تقدم تكنولوجيا المعلومات والاتصالات وانتشارها ودخولها بكافة القطاعات الاقتصادية والاجتماعية عملت معظم الدول على تحديث الإطار التنظيمي والقانوني الخاص بها ليتواءم مع المتطلبات العصرية الخاصة بالفضاء السيبرانى ، ومن هنا تبرز أهمية إيجاد اطار لتنسيق التشريعات السيبرانية إقليمياً ودولياً ، ويساهم وجود التشريعات السيبرانية في تحسين التجارة الإلكترونية البينية ، كما يساعد في تحفيز الاستثمارات المحلية ، وجلب الاستثمارات الخارجية لتطوير استخدام تكنولوجيا المعلومات والاتصالات وتطبيقاتها المختلفة والاتصالات عبر وضع اطر تشريعية وقانونية ملائمة (101)، ثم جاءت استراتيجية تحديد الأدوار والمسؤوليات الملقاة على عاتقي المسؤولين عن الأمن الإلكتروني وكذلك الملقاة على عاتق المواطنين لحماية انفسهم لتوعيتهم التوعية اللازمة بنسبة 3.2 % ، 2.8% .

شكل رقم (16)



من ركائز الاستعدادي للأخطار السيبرانية الدعم السياسي والمؤسسي الاستراتيجي والتنفيذي ويشمل ذلك الوعى بخطورة التهديدات السيبرانية ، وضرورة التعامل معها كأولوية بأعلى قدر من الجدية ، مع الاهتمام بالاستعداد

المسبق بما يشمل الخطط الاستراتيجية والتنفيذية ، واعداد الكوادر والتجهيزات التقنية واللوجستية ، ووضع الإطار التشريعي الملائم لأمن الفضاء السيبرانى ، ومكافحة الجرائم السيبرانية ، وحماية الخصوصية والهوية الرقمية وأمن المعلومات [102] ، وفى هذا الإطار تدل بيانات شكل رقم (16) على تركيز المواد الإعلامية بمنصة المركز على انستجرام على الإعلان عن البوابات الإلكترونية لتدعيم الوعى الاستراتيجي بأهمية إجراءات الأمن والحماية الإلكترونية ضد الهجمات الإلكترونية والسيبرانية ، جاء ذلك بنسبة 20.7 % ، فالهجمات السيبرانية بطبيعتها تتعدى الحدود الجغرافية للدول ، وعادة ما تعتمد على شبكات الجريمة المنظمة بشقيها التقليدي والتقني ، لذلك فالمواجهة الفاعلة للهجمات والجرائم السيبرانية تستلزم التعاون والتنسيق على المستوى الوطني ، وتشغيل البنى التحتية في القطاعات الحيوية بالإضافة الى التعاون والتنسيق على المستويين الدولي والإقليمي مع المنظمات الدولية والتجمعات الإقليمية والمنتديات العالمية المهنية والتخصصية [103] ، تلاها بالترتيب الثاني استراتيجية التوعية عبر كافة الفعاليات الاتصالية التي يجريها مركز الأمن الإلكتروني بحكومة دبى الذكية من مؤتمرات وندوات وورش عمل ودورات تدريبية واجتماعات بشكل مستمر ودوري ، لتدشين إجراءات وتطبيقات التوعية السيبرانية و قد رصدت الباحثة العديد من الفاعليات التي قام بها المركز لتنفيذ رؤيته ورسالته الاتصالية ، فهناك العديد من الندوات واللقاءات حول موضوعات الامن السيبرانى والذكاء الاصطناعي ، كما عقدت العديد من الاجتماعات وجلسات الحوار لمنصة دبى للأبحاث والدراسات السيبرانية لمناقشة تحديات الأمن الإلكتروني ووضع الحول المبتكرة لها وتقديم ورق عمل لاستشراق مستقبل الاعلام الإلكتروني ، أيضا تم افتتاح **قمة الذكاء السيبرانى** ، والاجتماع الرابع عشر للجنة العربية للإعلام الإلكتروني حول **مخاطر الألعاب الالكترونية** وتأثيرها على الأمن المجتمعي العربي ، انعقد أيضا مؤتمر **ومعرض الخليج للأمن الرقمي** الذى ضم 12000 رائد ونحبة من الخبراء الدوليين وابرز الشركات الرائدة في مجال امن وحماية المعلومات ، كما تم رصد تغطية المركز لافتتاح معرض **ومؤتمر الأمن الإلكتروني بدبى** ، وتغطية الشراكات المختلفة لتحقيق الأمن الإلكتروني ، كانت هناك أيضا جلسات حوارية لمناقشة رؤية

استراتيجية دبى للأمن الإلكتروني ، أيضا حرص المركز على عقد العديد من الدورات التد ربيبة لأفضل خبراء للأمن الإلكتروني ، حاء ذلك بنسبة 19.8 % ، فقد أكدت **دراسة نيال ادلبى (2017)** [104] أهمية الحاجة الى وجود جهاز تحقيق رسمي متخصص يضطلع بدور مهم من ناحية اجراء التحقيقات في الجرائم السيبرانية ، بخبرات فنية تمكنها من جمع الأدلة الرقيمة من مسرح الجريمة وحفظ الأدلة وضمان موثوقيتها وصدقيتها وتحليلها واستخراج الاستنتاجات القانونية منها وتقديمها للقضاء ضمن تقرير متكامل .

ثم بالترتيب الثالث جاءت استراتيجية الرسائل التحذيرية للمواطنين كاستراتيجية مهمة للتوعية ضد جرائم الأمن المعلوماتي وذلك بنسبة 19.1% ، اما منصات التوعية السيبرانية جاءت بالترتيب الرابع بنسبة 17.4 % ، ثم استراتيجية حملات التوعية السيبرانبة بنسبة 12.6 % ، حيث تعمل على التوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الإلكترونية المؤمنة للأفراد والمؤسسات ، وبأهمية الأمن السيبرانى لحماية تلك الخدمات من المخاطر ، والتحديات التي قد تواجهها [105] فتوعية المستخدمين وتدريبهم على المبادئ الأساسية للأمن السيبرانى يجب ان يكون جزءا أساسيا من أي استراتيجية او مبادرة وطنية او إقليمية لمكافحة الجرائم السيبرانية [106] .

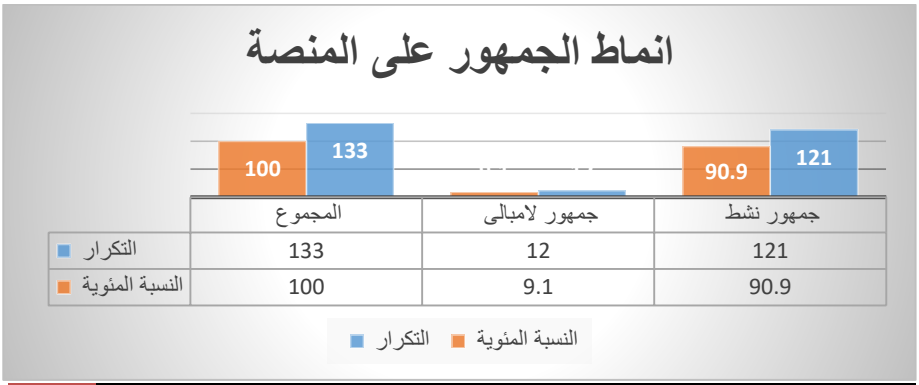
فالمركز يقدم حملاته التوعوية في جميع المجالات ، فاستجابة للأحداث الجارية بعد ازمة كورونا وتعليق جميع الاعمال والأنشطة بكافة المؤسسات ، قام المركز بحملات توعية بعنوان **العمل عن بعد بأمان معلوماتي** ، لاستهداف بناء فضاء رقمي امن ، هناك أيضا حملات توعية أخرى شملت عدة مجالات متعلقة بالأمن الإلكتروني، كحملة **خصوصيتك على الانترنت مهمة ، سافر بأمان ، ومركبات القيادة الامنة** .

وجاءت المبادرات والبروتكولات بنسبة 4.5 % كاستراتيجيات التعاون الدولي والاقليمي ضد الهجمات والجرائم السيبرانية ، حيث رصدت الباحثة التعاون الإقليمي للمركز مع هيئة الانظمة والخدمات الذكية بأبو ظبى لبناء **خبرات**

المستقبل الرقمي للإمارات ، وكذلك اتفاقية المركز مع مؤسسة الأبحاث لجعل **دبى اكثر فضاء امن** .

ولأهمية الاتفاقيات الدولية في مجال الأمن السيبرانى أصدرت الأمم المتحدة قرارات عدة بخصوص الجرائم السيبرانية او المعلوماتية ، وفى المنطقة العربية تم وضع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، كما اعدت الاسكوا في اطار تشريعي مشروعها الإقليمي إرشادات الاسكوا للتشريعات السيبرانية [107] ، وتوصى دراسة الأمم المتحدة بضرورة إيجاد اليات رسمية وغير رسمية للتعاون القضائي بين الدول ، ويهدف التعاون الدولي الى تبادل المعلومات والدروس المستفادة من التجارب والممارسات الفضلى [108] ، جاءت بعد ذلك المسابقات والاختبارات بنسبة 3.6 % وهى تعتبر من استراتيجيات التوعية من خلال التحفيز للمشاركة ببرامج من شانها تدعيم التوعية السيبرانية ، وأخيرا جاءت المحاكاة بنسبة 2.3 % ، وتعتبر المحاكاة استراتيجية مهمة للتوعية حيث يحاكى مركز الامن الإلكتروني المراكز ذات التوجه المشترك والرسالة والرؤية الواحدة ، من خلال تفعيل ما يعرف بالاستعداد والاستجابة لطوارئ الحاسبات والشبكات في القطاعات الحيوية على المستوى الوطني ، انطلاقا من التجربة الرائدة في قطاع تكنولوجيا الاتصالات والمعلومات للمتابعة الأمنية لشبكات الاتصالات والمعلومات الوطنية والحواسيب المتصلة بها ، والتعامل مع ايه اخطار سيبرانية او هجمات تهددها والتوعية والاعداد لمواجهتها [109] .

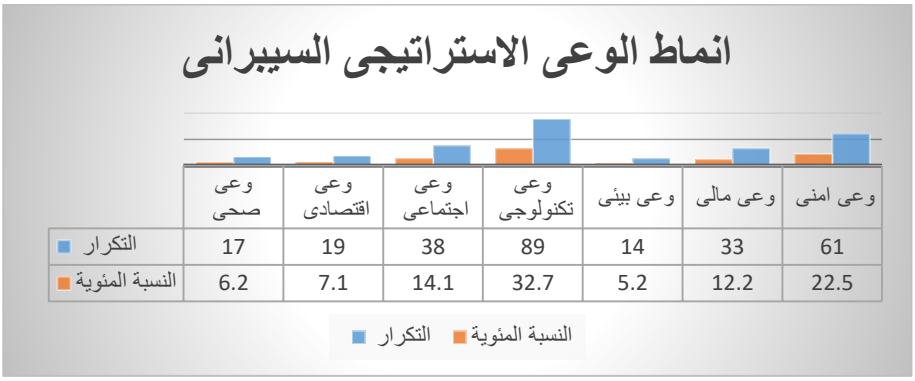
شكل رقم (17)



تحقيقا لمبدا التفاعلية والانية ، التي تنص عليها نظريةُ ثراء الوسائلِ الإعلامية ، تعد منصة انستجرام بمركز دبى للأمن الإلكتروني أكثرَ ثراءً ، حيث تتيح لزوار المنصة العديدَ من الآليات للمشاركة والتفاعلِ مع موضوعَاتِها الحيوية ورسائلها الإعلامية حول موضوعات الأمن المعلوماتي الإلكتروني ، والتي تهم قطاعًا كبيرًا جدًا من الجماهير.

حيث أفصحت نتائج الشكل السابق على ارتفاع نسبة التفاعلية، ووصلت نسبة الجمهور النشط الى 90.9 % ، بينما كان الجمهور اللامبالي نسبته 9.1%.

شكل رقم (18)



يشهد العالم اليوم ثورة علمية وتكنولوجية تجتاح شتى مجالات العلوم ومناشط الحياة البشرية ، ويجب على الانسان ان يساير تلك التكنولوجيا وليس هذا فحسب بل يجب عليه مواجهتها والتعامل معها بوعى كامل وبمهارة فائقة ، وتتطلب مواجهة التكنولوجيا وعيا كاملا بأبعادها الإيجابية وامتلاك مهارات التعامل معها، بالتالي فان وعي أفراد أي مجتمع علمياً وتكنولوجياً لم يعد دربا من الرفاهية والترف، بل أصبحت تلك الحاجة ضرورة حتمية فرضتها الظروف الراهنة [110]، ويعد الأمن البشرى بمفهومه الشامل هاجسا عالميا، وكفالة الأمن تأتى من خلال الوقاية المبكرة وهى اسهل من التدخل اللاحق والتصدي لهذه التهديدات قبل تأزمها [111] ، وتعد التوعية من مصادر الفهم والتوضيح والإرشاد ، وهى

مأخوذة من الحفظ والفهم والإدراك والعمل ، والأصل في الوعى ضم الشيء [112] ، وهى بمثابة افهام الغير وتحفيظه ما ينبغي عليه فعله وارشاده[113] .

وتتمثل اهم أساليب التوعية في الأسلوب المعرفي الذى يعنى بتزويد الفرد بكل المعارف والمعلومات ، والمام الجمهور بهذه المعارف يحقق وحدة الفكر والمفاهيم ، اما الأسلوب المهارى فيهدف الى تنمية قدرة الجمهور وصقل مهاراته في الاستعمال الأمثل والإلزام ، وأخيرا الأسلوب السلوكي ويعنى تهذيب سلوك الفرد من خلال التركيز على الجوانب النفسية والسعي الى إقناعه بتقبل القواعد واساسيات السلوك [114] .

وفى هذا الإطار تستند خطة دبي الاستراتيجية للأمن الإلكتروني على تنفيذ مجموعة من المحاور الرئيسية لخلق فضاء إلكتروني آمن ، ومجتمع واع بمخاطر الأمن الإلكتروني ، حيث يهدف مركز دبى للأمن الإلكتروني الى بناء الوعي والمهارات والقدرات اللازمة لإدارة مخاطر الأمن الإلكتروني في المؤسسات العامة والخاصة والأفراد ، كما يهدف الى تشجيع الابتكار والبحث العلمي في مجال الامن الإلكتروني، وإنشاء فضاء إلكتروني يتسم بالحرية والعدل والأمن من خلال التركيز على زيادة مهارات الخبراء في الأمن الإلكتروني ، والامتثال لمعايير المرونة في الفضاء الإلكتروني ، وتقديم الدعم لإدارة الجرائم المرتبطة بالأمن الإلكتروني واعتماد آليات متطورة لمواجهة التهديدات، وتوفير منصات الكترونية رقمية امنة لتبادل المعلومات ، والتعاون المحلي والدولي لمواجهة التهديدات العالمية السيبرانية ، من خلال الاعتماد على التشريعات والقوانين خاصة بالأمن الإلكتروني [115] .

وتدل بيانات الجدول السابق على ارتفاع نسبة الوعى التكنولوجي برسائل المركز على المنصة ، جاء ذلك بالترتيب الأول بنسبة 32.7 % وهو امر طبيعي ، وفقا لرسالة ورية المركز فالوعى التكنولوجي هو المعرفة والفهم والإدراك والشعور بتطبيقات التكنولوجيا الحديثة ، مما قد يؤثر على توجيه السلوك نحو الاستخدام والتوظيف الأمثل لهذه التطبيقات والعناية بها والوقاية من الاثار المحتملة عن استخدام تلك التكنولوجيا [116] ، ويعمل المركز على تنمية الوعى

التكنولوجي و النهوض بالفرد وقدرته على استخدام التكنولوجيا وزيادة وعيه وفهمه وادراكه لأخطارها ، فقد اكدت **دراسة وداد الجمل (2017)** [117] انه في ظل الثورات المعرفية الرقمية المتسارعة ، كان لا بد من الجمع بين الأسس العامة للوعى التكنولوجي سواء كان معرفياً او مهارياً او قيمياً ، فالأساس المهارى يشمل المهارات العقلية والعملية والاجتماعية اللازمة للتعامل مع التكنولوجيا وتطبيقاتها ، والأساس المعرفي الذى يشمل المعلومات اللازمة لفهم طبيعة التكنولوجيا وخصائصها ومبادئها وعلاقاتها ، أما الأساس القيمي وهو الذى يقيم حدود أخلاقية للتعامل مع التكنولوجيا وتطبيقاتها والالتزام بتلك الحدود، جاء بعد ذلك بالترتيب الوعى الأمني بنسبة 22.5 % ، فالتوعية الأمنية تعنى بث ونشر المعرفة بين افراد الشعب وتزويدهم بكل ما يتعلق بحياتهم اليومية من الناحية الأمنية من حيث الحقوق والواجبات [118] ،أما الوعى الاجتماعي جاء بالترتيب الثالث بنسبة 14.1 % ، وفى ذلك اكدت **دراسة عايد الحميدان (2004)** [119] ان تحقيق الامن الاجتماعي يشمل كافة النواحي الحياتية التي تهم الانسان المعاصر ، فهو يشمل الاكتفاء المعيشي والاقتصادي والاستقرار الحياتي في المجتمع ووجوده وكيانه وتعلقه بارضه ووطنه وتامين الخدمات الأساسية وسلامته وامنه وإرساء البيئة المجتمعية ، ومن حملات الوعى الاجتماعي حملة **رمضان بأمان** بعد حدوث الجائحة العالمية " ازمة كورونا " ، ثم جاء الوعى المالي بنسبة 12.2 % ، ثم الوعى الاقتصادي بنسبة 7.1 % ، وقد تم رصد ندوة بعنوان **العملات الافتراضية ودورها في جرائم الإرهاب وغسيل الأموال** لتحقيق التوعية الاقتصادية ، ثم تقارب بعد ذلك كلا الوعى الصحي والوعى البيئي في الظهور بنسبة 6.2 ، 5.2 % على التوالي بالعينة التحليلية ، ومن الفاعليات التوعوية الهادفة الى الوعى الصحي للمستخدمين رصدت الباحثة ندوة تم الإعلان عنها على منصة انستجرام عن الوعى الصحي البيئي.

خاتمة الدراسة

الدراسة في نقاط

- ✓ تعتبر شبكة الأنترنت من أكثر مظاهر التكنولوجيا الحديثة ، والتي قد نجحت إلى حد كبير في فتح فرص التعارف والتعاون والتواصل بين الأفراد بناء على علاقات افتراضية ، وتعد مواقع التواصل الاجتماعي من أشهرها على الإطلاق فهي تلقى الكثير من الإقبال من طرف جميع الشرائح الاجتماعية على حد سواء ، وقد اسفرت العديد من الدراسات عن سلبيات مواقع التواصل الاجتماعي ودورها في نشر الجرائم الالكترونية ، بينما تطرقت الدراسة الحالية الى الاستخدام الإيجابي لمنصات التواصل الاجتماعي لمكافحة الجريمة الالكترونية وتوعية الجمهور السيبرانية عبر استراتيجياتها الاتصالية المختلفة .
- ✓ هدفت الدراسة الى توفير نظرة تحليلية متعمقة حول مخاطر الفضاء السيبرانى ، ووسائل تعزيز وتنسيق الجهود الدولية والإقليمية لمكافحة الجرائم الإلكترونية ، والعمل على تقديم مقترحات واطار توجيهي من اجل تعزيز الأمان السيبرانى وبناء الثقة بتكنولوجيا المعلومات والاتصالات والفضاء السيبرانى ، من خلال التعرف على متطلبات ومقومات ومعوقات إرساء معالم الحكومات الإلكترونية الذكية ، بالتطبيق على مركز دبى للأمن الإلكتروني ، وهو احدى مراكز الأمن السيبرانى الرائدة في مجال مكافحة الجريمة السيبرانية بدولة الامارات العربية المتحدة ، موضحة اليات المركز لتنفيذ رؤيته ورسالته ، باستخدام منصات التواصل الاجتماعي التابعة للمركز و المعتمدة على العديد من الاستراتيجيات الاتصالية لإنتاج مواد إعلامية تحقق من خلالها التوعية السيبرانية بأخطار الفضاء الرقمي وجرائمه السيبرانية ، حيث حرصت منصة التواصل الاجتماعي انستجرام بمركز الامن الإلكتروني بدبى الذكية على اتاحة الوسائط المتعددة للجمهور للتعبير بفاعلية عن آرائهم بما يحقق استراتيجية اتصالية متميزة للمنصة ، كما هدفت المنصة الى بناء مهارات الجمهور العام التوعوية فيما يتعلق بأخطار الجرائم السيبرانية ، دون تخصيص لفئات معينة اثناء توجيه خطاب التوعية

السيبرانية ، وهو ما هدف اليه مركز الامن الإلكتروني بدبى الذكية من بناء قدرات ومهارات الجمهور السيبرانية ، وقد جاء ذبك بنسبة 58 % .

- ✓ نظرا لحاجة الجمهور الى التفاعل مع المضمون فقد اعتمدت المنصة على معالجة مضمون التوعية السيبرانية لأخطار الجريمة الالكترونية من خلال البيانات الصحفية المذاعة والمطبوعة لما لها من مصداقية وتأثير قوى على الجماهير وجعله اكثر تفاعلا مع المضمون المقدم ، كما استخدمت المنصة الإعلانات بكافة انماطها تجاوبا مع الاحداث الجارية ، حيث اشتملت العينة التحليلية على معالجات إعلامية للأيام العالمية ، وكذلك اشتملت العينة على الاستراتيجيات التوعوية الرقمية لرسائل الوقاية من فيروس كورونا ، من خلال التوعية بأنماط التطبيقات الامنة المناسبة للاستخدام في التسويق والترويج للحملات الإعلامية والوصول الى المعلومات .
- ✓ نظرا لأهمية التفاعل مع الجمهور على صفحة المركز على انستجرام ، فقد وفرت المنصة العديد من أساليب وأدوات الاتصال الشبكي والرقمي، وذلك لتوفير مزيد من التفاعلية مع الجماهير ، وقد كان أسلوب الاعجاب من اكثر أساليب الاتصال الآلي والشبكي ظهورا في العينة حيث وصل الى 47 % ، تلاها المشاهدة بنسبة 31 % ، ثم التعليق بنسبة 15 % ، وأخيرا المشاركة بنسبة 7 % .
- ✓ تناولت المنصة العديد من الموضوعات باستخدام العديد من الاستراتيجيات للوصول الى مجتمع امن وواعى ، وقد كان من اهم تلك الموضوعات التوعية بأبرز الحلول الامنة لمشكلات التقنية وتحقيق الامن السيبرانى ، أيضا حرصت المنصة على معالجة موضوعات الاصطياد الإلكتروني والاختراقات والاحتيالات ، وقد عالجت المنصة موضوعات السلامة الرقمية والتوعية الرقمية بما يتعلق بموضوعات التعليم عن بعد والمنصات الرقمية المستخدمة وكيفية تأمينها اثناء جائحة كورونا .
- ✓ اكدت الدراسة على تأثير الهجمات السيبرانية على الوضع الاقتصادي ، حيث حرصت المنصة على معالجة الموضوعات والقضايا الاقتصادية من ضمن استراتيجياتها للتوعية السيبرانية بأخطار الجرائم الإلكترونية على الامن الاقتصادي الإقليمي والعالمي ، كما جاءت القضايا الثقافية بنسبة عالية

وصلت وصلت 18.9 % من إجمالي قضايا التوعية السيبرانية ، والتي تؤكد استطاعة الحكومة الإلكترونية الذكية القيام بدور مهم في الكشف عن سياسات الامن المعلوماتي ، وتثقيف المواطنين بها واعلامهم بمخططاتها ومشروعاتها ، حيث ان اطمئنان المواطن للخدمات الإلكترونية يعطيه الثقة والأمان لحكومته .

- ✓ كان من اهم اهداف المنصة اعلام وتثقيف الجمهور وارشادهم وتوعيتهم لرسائله الإعلامية حول الجرائم السيبرانية ، حيث قدم مجموعة من الارشادات للحماية السيبرانية في هذا الاطار ، فيما يتعلق بالاتصالات الإلكترونية ، وارشاد الملكية الفكرية في المجال السيبراني ، وارشادات التجارة الالكترونية وحماية حقوق المستهلك ، وكذلك إرشادات معالجة البيانات ذات الطابع الشخصي ، وارشادات الحفاظ على امن الدولة والدفاع الوطني وارشادات الجرائم الالكترونية او السيبرانية .
- ✓ أوضحت نتائج الدراسة التحليلية ان استراتيجيات تعزيز التواصل بين الجمهور والمركز الإلكتروني عبر قنواته الاتصالية كانت من اهم استراتيجيات مركز الأمن الإلكتروني المتخذة لمواجهة تحديات الامن السيبراني. ، كما كانت هناك العديد من المبادرات ومذكرات التفاهم مع العديد من المؤسسات الدولية والإقليمية التي اطلقها المركز لتعزيز استراتيجياته الاتصالية، وقد جاءت هذه المبادرات والبروتكولات بنسبة 4.5% كاستراتيجيات التعاون الدولي والاقليمي ضد الهجمات والجرائم السيبرانية ، حيث رصدت الباحثة التعاون الإقليمي للمركز مع هيئة الانظمة والخدمات الذكية بأبو ظبى لبناء خبرات المستقبل الرقمي للإمارات ، وكذلك اتفاقية المركز مع مؤسسة الأبحاث لجعل دبى اكثر فضاء امن .
- ✓ استندت استراتيجة مركز الامن الإلكتروني لدبى الذكية من خلال استراتيجياته الاتصالية على منصة انستجرام على ركيزة مهمة وهى الاستعداد للأخطار السيبرانية بالدعم السياسي والمؤسسي الاستراتيجي والتنفيذي ويشمل ذلك الوعى بخطورة التهديدات السيبرانية ، وضرورة التعامل معها كأولوية بأعلى قدر من الجدية ، مع الاهتمام بالاستعداد المسبق بما يشمل الخطط الاستراتيجية والتنفيذية ، واعداد الكوادر والتجهيزات التقنية

واللوجستية ، ووضع الإطار التشريعي الملائم لأمن الفضاء ، السيبراني ومكافحة الجرائم السيبرانية ، وحماية الخصوصية والهوية الرقمية وأمن المعلومات

- ✓ اتخذ المركز من المحاكاة استراتيجية مهمة للتوعية السيبرانية ، حيث يحاكى مركز الامن الإلكتروني المراكز ذات التوجه المشترك والرسالة والرؤية الواحدة ، من خلال تفعيل ما يعرف بالاستعداد والاستجابة لطوارئ الحاسبات والشبكات في القطاعات الحيوية على المستوى الوطني ، انطلاقا من التجربة الرائدة في قطاع تكنولوجيا الاتصالات والمعلومات للمتابعة الأمنية لشبكات الاتصالات والمعلومات الوطنية والحواسيب المتصلة بها ، والتعامل مع ايه اخطار سيبرانية او هجمات تهددها والتوعية والاعداد لمواجهتها .
- ✓ واختتمت النظرة التحليلية لاستراتيجيات دبى الذكية للأمن السيبرانى خلال مركز الامن الإلكتروني واستراتيجيته للتوعية السيبرانية معتمدة على منصات التواصل الاجتماعي كوسيلة مهمة لإيصال رسالته الاتصالية للجمهور على تنفيذ مجموعة من المحاور الرئيسية لخلق فضاء إلكتروني آمن، ومجتمع واع بمخاطر الأمن الإلكتروني ، حيث يهدف مركز دبى للأمن الإلكتروني الى بناء الوعي والمهارات والقدرات اللازمة لإدارة مخاطر الأمن الإلكتروني في الفضاء الرقمي .

توصيات الدراسة

اوصت الدراسة بمجموعة من التوصيات على النحو التالي

أولا : على الصعيد الدولي والإقليمي

- ✓ العمل على تحقيق الامن السيبراني.وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الالية والشبكات المعلوماتية الدولية .
- ✓ سن تشريعات دولية تغطى كافة الثغرات القانونية في مجال وجود فضاء سيبراني امن .

- ✓ تطوير القدرات التقنية على شبكة الإنترنت ، وإنشاء شرطة الإنترنت الدولية للقبض المباشر على مرتكبي الجرائم حال دخولهم على الشبكة من خلال التتبع الفني للجهاز أو الخط الهاتفي الذي ارتكبت منه الجريمة .
- ✓ تشجيع الاقتصاديات العالمية للاستثمار في مجال الامن السيبرانى .
- ✓ دعم بناء القدرات للدول النامية للنهوض بمستوى التعامل مع مخاطر الامن السيبرانى .
- ✓ استثارة الوعي على مستوى السياسات الدولية بقضايا حماية الأمن السيبراني.
- ✓ تطوير مرونة البنية التحتية لشبكة الأنترنت من خلال تحقيق ربط افضل بين الشبكات .
- ✓ تدشين منصات دولية من اجل مناقشة تهديدات الامن السيبرانى .
- ✓ الدعوة الى المنتديات الدولية للأمن السيبرانى لمناقشة التحديات والتهديدات السيبرانية ، وبحث الفرص التنموية والاستثمارية في مجال الامن السيبرانى.
- ✓ توفير الدعم للبحوث اللازمة لتعزيز مستقبل الجهود الدولية المبذولة في مجال حماية المعلومات الحيوية .
- ✓ تعديل قواعد الإجراءات الجنائية الدولية لتتلاءم مع تلك الجرائم السيبرانية وأيضا ضرورة التنسيق والتعاون الدولي امنيا واجرائيا وقضائيا في مجال مكافحتها .

نطاقات تفعيل التوصيات السابقة تقع على عاتق :

دوليًا : تلك المنظمات المعنية بالجرائم السيبرانية واستراتيجيات الوعى الرقمى كالاتحاد الدولي للاتصالات، الجمعية العالمية لتقييس الاتصالات، الايسكو، مكتب الأمم المتحدة المعنى بالجريمة والمخدرات ،و منظمة الأمم المتحدة للتربية والعلوم والثقافة (اليونسكو) ، وغيرها من المنظمات الدولية المهتمة بمجال الامن السيبرانى .

إقليميًا : تلك المنظمات التي اخذت على عاتقها مواجهة الجريمة الالكترونية وتحدياتها السيبرانية الراهنة مثل اللجنة الاقتصادية والاجتماعية لغربي اسيا

(الاسكوا) ، مجلس دول التعاون الخليجى ،والاتحاد الافريقى ، وغيرها من المنظمات المعنية بمواجهة الجرائم السيبرانية .

ثانيا : على الصعيد المحلى

- ✓ وضع استراتيجية وطنية لحماية الهياكل الأساسية الحيوية للمعلومات والفضاء السيبراني من الهجمات السيبرانية
- ✓ المشاركة في الجهود الدولية الرامية إلى تنسيق الأنشطة الوطنية ذات الصلة بالوقاية من الحوادث والاستعداد والتصدي لها، والتعافي منها.
- ✓ تحديد الموارد اللازمة للمشـــاركة في القيام بدراســـات شـــاملة مشـــتركة بين القطاعات الحكومية والخاصـــة ، عن طريق التدريبات والندوات والدورات التدريبية ممن اجل الحصول على فضاء سيبرانى امن .
- ✓ إقامة نظام وطني مذسق للاستجابة لأمن الفضاء السيبراني لتلافي الحوادث السيبرانية وتتبعها وردعها .
- ✓ انشاء منصة إقليمية لتبادل المعلومات المتعلقة بالتهديدات السيبرانية وإرساء معالم الوعى السيبرانى .
- ✓ تطوير البنية التشـــريعية الجنائية الوطنية من اجل ســـن تشـــريعات قانونية لحماية البنية التحتية من الجرائم الرقمية
- ✓ ضـــرورة تخصـــيص جهاز امنى متمكن علميا وعمليا وفنيا وتقنيا لمواجهة تحديات الامن السيبرانى .
- ✓ انشـــاء شـــراكات بين القطاعين العام والخاص لمكافحة الجرائم الســـيبرانية باعتبارها من الجرائم العابرة للحدود الوطنية ، لذلك تتطلب جهودا مشتركة على المستويات الوطنية والإقليمية والدولية بغرض تبادل الخبرات وتحسين طرق مكافحتها .
- ✓ صياغة مشروع قانون حماية خصوصية البيانات ، واطار لتامين المعلومات الوطنية.
- ✓ تمكين المنظمات والمؤســـســـات من خلق ثقافة تعاونية لأمن البنية التحتية للأنترنت من اجل تحقيق الرخاء الاقتصادي والاجتماعي .
- ✓ زيادة مرونة الشبكات لمواجهة الهجمات ، من خلال تيسير التنوع في الربط الشبكي محليا

- ✓ الاعتماد على استراتيجية اتصالية موحدة الأهداف عبر منصات التواصل الاجتماعي والمواقع الإلكترونية ووسائل الاعلام للترويج لثقافة وطنية للأمن السيبرانى .
- ✓ تعزيز سياسات البيانات المفتوحة التي يمكن أن تضمن استدامة منصات أو مبادرات تبادل البيانات لحماية المواطنين من سوء استخدام البيانات وجرائم الإنترنت .
- ✓ تشجيع وتعزيز البحث والتطوير في مجال تكنولوجيا المعلومات والاتصالات من خلال إنشاء بوابة وشبكات جامعية وبوابات التعلم الإلكتروني والمكتبات الإلكترونية الرقمية .

نطاقات تفعيل التوصيات السابقة تقع على عاتق :

الحكومات الوطنية الذكية والالكترونية ، الوزارات المعنية بتقنية المعلومات والاتصالات ، وكذلك الجامعات الالكترونية ، والمؤسسات المتخصصة كمراكز الامن الإلكتروني الوطنية ، والهيئات الوطنية للأمن السيبرانى وشركات الاتصالات الوطنية الحكومية والخاصة .

ثالثا : على الصعيد المؤسسي

- ✓ تشكيل شراكات مؤسساتية حكومية وغير حكومية تتضمن استراتيجيات المهارات الرقمية .
- ✓ تامين البيئة الالكترونية او الرقمية الكلية للمؤسسات .
- ✓ وضع وتصميم خطط واستراتيجيات لبناء المناعة ضد المخاطر الإلكترونية السيبرانية .
- ✓ تدشين وحدات واقسام بالمؤسسات تختص بإدارة المخاطر الالكترونية .
- ✓ وضع الخطط والإجراءات والبروتوكولات بشأن الاستجابة لحالات الطوارئ، واختبارها، والتمرين عليها .
- ✓ تيسير عملية تبادل المعلومات وبناء العلاقات بين جميع الوحدات المؤسسية بصورة امنة ومراقبة .

- ✓ وضع استراتيجية محددة للأمن السيبراني داخل المؤسسات بما يتناسب مع طبيعة كل مؤسسة ، من اجل النهوض بثقافة الوعى السيبراني.
- ✓ المشاركة في مبادرات الامن السيبراني الوطنية بالاتصالات والتنسيق وتعزيزها .
- ✓ مواجهة العقبات القانونية واللوائح الداخلية الروتينية لكافة المؤسسات ، والتي تحول دون مشاركة المعلومات واجراء الأبحاث المتعلقة بالثغرات الأمنية والحوادث والتهديدات للمؤسسات الوطنية .
- ✓ تنظيم المؤتمرات واللقاءات الدورية بين المؤسسات من اجل تدشين تعاون وبرتوكول مؤسسي يقوم على الاستفادة من الخبرات من اجل ردع الجريمة الالكترونية .
- ✓ تدشين المنصات الرقمية بالتعاون بين المؤسسات الحكومية وغير الحكومية لإنتاج مواد إعلامية للدعاية والترويج لسياسة البيانات المفتوحة وتوعية الجمهور المتعامل مع المنظمات باليات حماية هذه البيانات تفادى مخاطر الفضاء السيبراني .

نطاقات تفعيل التوصيات السابقة تقع على عاتق :

المؤسسات الحكومية وغير الحكومية على اختلاف سياساتها مع تخصيص إدارات ووحدات لتنفيذ استراتيجيات الامن السيبرانى ومكافحة الجريمة الالكترونية ورفع مهارات الوعى الرقمي لمنسوبي المؤسسات .

مراجع الدراسة

(1) Culture a Developing for Practices Best, **Networks Communication and Information Securing**. , 2017 (ITU Cybersecurity)

(2) الحكومة الالكترونية ، (1427) ، **سلسلة دراسات** ، معهد البحوث والاستشارات ، جامعة الملك عبد العزيز ، جدة ، الإصدار التاسع ، ص 66

(3) جمال محمد غيطاس ، (2002) الحكومة الإلكترونية ليست مشروع ولكن أفكار وأساليب عمل ، **مقال منشور** ، جريدة الأهرام المصرية ، السنة 126 ، العدد 9 ، 6 أكتوبر

(4) إبراهيم الباروك ، (2017) ، وزارة الدفاع ، التعاون مع الوزارات والقطاع الخاص في مجال الأمن السيبرانى ، ورقة عمل ، **مؤتمر الامن السيبرانى والدفاع السيبرانى** ، الجامعة اللبنانية والوكالة الجامعية للفرنكوفرنية AUF ، ص 48

(5)https://**www.nao.org**.uk/report/investigation-wannacry-cyber-attak-and-the-nhs/2017

(6) https://**www.theregister.co.uk**/2018/01/24after notpetya replaced everything/.2018

(7) Deadening Dorothy , (2015) , **rethinking the cyber domain and deterrenc** JFQ, 2nd quarter pp8-15

(8) اسراء جبريل رشاد مرعى ، (2018) ، الجرائم الإلكترونية ، الأهداف والأسباب طرق الجريمة ومعالجتها ، **مجلة الدراسات الإعلامية** ، المركز الوطني الديمقراطي ، العدد الأول ، 2018 ، يناير يص 428

(9) ديالا جميل محمد الرازي ، (2012) ، الحكومة الإلكترونية ومعوقات تطبيقها : دراسة تطبيقية على المؤسسات الحكومية في قطاع غزة ، مقال منشور ، **مجلة الجامعة الإسلامية للدراسات الاقتصادية والإدارية** ، المجلد العشرين ، العدد الأول ، ، ص ص 195-196

10) United nation office on drugs and crime ,(2013) **UNODC** , comprehensive study on cybercrime , draft , febuary,pp152-154

(11) محمد عثمان أبو مهارة (2012) ، مقومات ومعوقات تطبيق الحكومة الالكترونية ، **بحث منشور** ، كلية الاقتصاد والعلوم السياسية ، ليبا ، جامعة مصراتة ، ص 7

(12) https://**www.tra.gov.ae/userfiles/**assets/lw3seruamd.pdf

(13) حكومة دبى ، (2017) ، مركز دبى للأمن الإلكتروني ، **استراتيجية دبى للأمن الإلكتروني** ، النسخة 1

(14)عاشور عبد الكريم ، دور الإدارة الالكترونية في ترشيد الخدمة العمومية في الولايات المتحدة الامريكية والجزائر ، **رسالة ماجستير غير منشورة** ، كلية الحقوق ، جامعة منتسوري قسطنطينية ، العلوم السياسية والعلاقات الدولية ، 2009-2010 ، ص 13

(15)حجيبة قاوقو ، الفضاء العمومي الإلكتروني والتعبئة السياسية الذكية ، **مجلة الدراسات الإعلامية** ، المركز الديمقراطي العربي ، العدد الأول ، 2018 ، ص 170

(16)جورج اسحق حنين ، دراسة عن الجرائم المعلوماتية والإلكترونية عبر شبكة الانترنت وسبل مواجهتها ، **الإدارة المركزية لمركز المعلومات والتوثيق** ، 2018

(17) اسراء جبريل رشاد مرعى ، الجرائم الالكترونية ، الأهداف والأسباب طرق الجريمة ومعالجتها ، **مجلة الدراسات** الإعلامية ، المركز الوطني الديمقراطي ، العدد الأول ، 2018 ، يناير ص 435

(18) اللجنة الاقتصادية والاجتماعية لغربي اسيا (الاسكوا) ، الجوانب القانونية للحكومة المفتوحة والبيانات المفتوحة ، **مكتب الأمم المتحدة** ، 2020 ، ث 29

(19)علم الدين بانقا ، مخاطر الهجمات الالكترونية (السيبرانية) واثارها الاقتصادية : دراسة حالة دول مجلس التعاون الخليجي ، 2019 ، **المعهد العربي للتخطيط** ، العدد 63

(20) نوال على البلوشية ، نبهان حارث الحراصى ، على سيف العوفي ، واقع التحول الرقمي في المؤسسات العمانية ، **دار دراسات المعلومات والتكنولوجيا** ، جمعية المكتبات المتخصصة ، فرع الخليج العربي ، 2020

(21) محمد عبد الهادي ، توجهات امن وشفافية لمعلومات في ظل الحكومة الإلكترونية ، ، **المؤتمر العربي الثالث في تكنولوجيا المعلومات والتنمية الإدارية** ، شفافية امن المعلومات في ظل الحكومة الالكترونية ، شرم الشيخ ، 2-6 أكتوبر 2004 ، ص 124

(22)Ivanov, M., Varga, M., & Bach, M. P. (2014). Government open data portal: How government strategies should be more open. **Paper presented,** at the 674686-. Available from: https://search. proquest.com/docview/1566187264?accountid=142 90

(23) ايمان محمد عيسى ، منى داخل السريحى ، **منصة البيانات المفتوحة وتفعليها عبر بوابات الحكومة الإلكترونية لدول مجلس التعاون الخليجي ، دراسة مقارنة** ، جامعة الملك عبد العزيز ، قسم علم المعلومات ، دار جامعة حمد بن خليفة للنشر ، كيوشاينس ، 2019 ص 5

(24) Onwubiko, C. (2015). Cyber Security Operations Centre Security Monitoring for protecting Business and supporting, Cyber Defense Strategy**. international Conference on Cyber Situational Awareness**, Data Analytics and Assessment, Cyber SA, pp. 1-10.

(25)Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2017). A Survey of Cyber-Security Awareness in Saudi Arabia. **International Conference for Internet Technology and Secured Transactions.**

(26) Anastacio,blanco,villaba&al-dahoud,2013 , e government : benefits , risks and a proposal to assessment including could computing and critical infrestruture . in the 6 th, **international conference on information technology .**retrieved from http://ezproxysrv.squ.edu.com,2048/login?url=://search.ebscohost.com/login.aspx?direct=true&db=edb&an=93420988site=edsscope=site

(27)رغدة البهى ، (2018)الردع السينرانى : المفهوم والاشكاليات والمتطلبات ، **مجلة الدراسات الإعلامية** ، المركز الديمقراطي العربي ، العدد الأول ، يناير ، ص ص 210-211

(28)دراسة شاملة عن الجريمة السيبرانية ، 2013 ، **مكتب الأمم المتحدة المعنى بالمخدرات والجريمة** ، فيينا ، الأمم المتحدة ، نيويورك ،

(29) مجمع البحوث والدراسات ، 2016 ، **الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها** ، أكاديمية الأمير نايف بن عبد العزيز للبحوث الامنية ، ، مجلس التعاون لدول الخليج العربية ، الأمانة العامة ، اكاديمية السلطان قابوس لعلوم الشرطة ، نزوى ، سلطنة عمان .

(30) إبراهيم رمضان إبراهيم عطايا ، (2015) الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية ، دراسة تحليلية تطبيقية ، العدد الثلاثون ، الجزء الثاني ، **مجلة البحوث القانونية** ، كلية الشريعة ، طنطا

(31) الأمم المتحدة ، اللجنة الاقتصادية والاجتماعية لغربي اسيا ، (2015) **الأمان في الفضاء السيبرانى ومكافحة الجرائم السيبرانية في المنطقة العربية** ، توصيات سياسية ، نيويورك

(32) مالك فهد عبد الهادي ، (2020) الامن السيبرانى ودوره في الحد من تهديدات الامن الفكري ، **رسالة ماجستير** ، جامعة نايف العربية للعلوم الأمنية ، كلية العلوم الاستراتيجية

(33) tavrou, E. (2018). Enhancing Cyber Situational Awareness : A New Perspective of Password Auditing Tools. 2018 ,**International Conference On Cyber Situational Awareness**, Data Analytics And Assessment (Cyber SA), pp. 1-4

(34) Yasina, A., Liu, L., Li, T., Wang, J., & Zowghi, D. (2018). Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG**). Information and Software Technology**, pp. 179-200

(35) بيان ناصر محمد الشهراني ، (2020) اثر برنامج تدريبي قائم على تصميم العاب تعليمية الكترونية باستخدام برنامج game maker لإكساب مفاهيم الامن السيبرانى لدى طالبات المرحلة المتوسطة ، **مجلة البحث العلمي في التربية** ، العدد 21 ، سيتمبر 2020

(36) Kasurinen , J., & Kettunen , M. (2018, MAY). LEARNING CYBER SECURITY: TEACHING TECHNICALLY CHALLENGING TOPICS WITH GAMES AND VIRTUAL LABORATORIES. **International Journal on Information Technologies** & Security, pp. 103-114.

(37) جبريل حسن العريشى ، سلمى عبد الرحمن محمد الدوسري ، 2018 ، دور مؤسسات التعليم العالي في تعزيز ثقافة امن المعلومات في المجتمع ، **مجلة مكتبة الملك فهد** ، ص ص 302 -273

(38)مها دخيل الله الجثمى ، 2017 ، مستوى الوعى بقضايا امن المعلومات لدى طالبات المرحلة الثانوية بالمدارس الحكومية بمدينة الرياض ، **مجلة العلوم الإنسانية والاجتماعية** ، ص ص 355 – **400**

(39) Ahmad, N., Mokhtar, U., Fariza Paizi Fauzi, W., Othman, Z., Hakim Yeop, Y., & Huda Sheikh Abdullah, S. (2019). Cyber Security Situational Awareness among Parents. Proceedings of the 2018 **Cyber Resilience Conference,** CRC 2018.

(40) عبد الاله عوض مطلق الشلاحى المطيري ، (2018)، دور الاعلام الجديد في التوعية من الجرائم الالكترونية ـ **رسالة ماجستير** ، جامعة نايف العربية للعلوم الأمنية ، كلية العلوم الاجتماعية ، قسم الاعلام ، تخصص اعلام

(41) ويليام مارسيلينو ، ميجان ل. سميث ، كريستوفوبول ، لورين سكرابالا ، (2017) ، رصد وسائل التواصل الاجتماعي عبر تحليلات وزارة الدفاع الامريكية لوسائل التواصل الاجتماعي في المستقبل دعما لعمليات المعلومات ، مكتب الدعم التقني لمكافحة الإرهاب ، **مركز سياسات الدفاع والامن الدولي** ، معهد أبحاث RAND للدفاع الوطني

(42) حمد حسن عبد العليم حسن الخطيب ، (2019) الجرائم المعلوماتية الواقعة عبر مواقع التواصل الاجتماعي ، قراءة في قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 ، ونظام مكافحة المعلومات السعودى 1428 ، **مجلة الدراسات الافريقية وحوض النيل** ، **المركز الديمقراطى العربى** ، العدد السادس أكتوبر 2019 ، برلين

(43) عبد المجيد مراد داد محمد احمد ، (2019) المسؤولية الجزائية عن إساءة استخدام وسائل التواصل الاجتماعى ، دراسة وصفية تحليلية للقانون والقضاء الإماراتي ، **رسالة ماجستير** ، كلية القانون ، جامعة الشارقة ، الامارات العربية المتحدة

(44) مجمد شومان (2003) ، اشكاليات في مسار اعلام الأزمات والكوارث ، **المجلة المصرية لبحوث الرأي العام** ، العدد الثالث ، المجلد الثاني ، يوليو – سبتمبر

(*) أد/ إبراهيم المسلمى / أستاذ الصحافة والاعلام جامعة الزقازيق جمهورية مصر العربية
أد/ صالح عراقي : أستاذ الإذاعة والتليفزيون جامعة الزقازيق جمهورية مصر العربية
أد/ محمد معوض : أستاذ الاعلام جامعة عين شمس جمهورية مصر العربية
أم د/ عرفة أبو زيد : أستاذ تكنولوجيا التعليم المساعد جامعة الزقازيق جمهورية مصر العربية

(45) عبد العزيز سلطان الضويحى ، (2004) ، التخطيط الإعلامي ودوره في مواجهة الكوارث والازمات ، **رسالة ماجستير غير منشورة** ، جامعة نايف للعلوم الامنية ، كلية الدراسات العليا ، قسم العلوم الادارية .

(46) الطيب أحمد الإمام ، (2015) ، دور التخطيط الإذاعي في ادارة الأزمات الأمنية ، **رسالة ماجستير** ، جامعة الرباط الوطني ، كلية الدراسات العليا والبحث العلمي .

(47) علم الدين بانقا ، (2019) ، مخاطر الهجمات الإلكترونية (السيبرانية) واثارها الاقتصادية : دراسة حالة دول مجلس التعاون الخليجي ، **سلسلة دراسات تنموية** ، المعهد العربي للتخطيط ، الكويت ، 2019

(48) محمد الشوا ، (1994) ، **ثورة المعلومات وانعكاساتها على قانون العقوبات** ، ط2 ، دار النهضة العربية ، ص 7

(49) عبد المؤمن صغير ، (2018) ، إشكالية تطبيق الحكومة الإلكترونية في الجزائر " المعوقات والافاق ، **مجلة الدراسات الإعلامية** ، المركز الديمقراطي العربي ، ع 1 ، ص 353

(50) عبد المؤمن صغير ، **مرجع سابق** ، ص 354

(51) محمد عبد العزيز درويش ، (2005) ، تطبيقات الحكومة الإلكترونية دراسة ميدانية على إدارة الجنية والإقامة دبى ، **رسالة ماجستير** ، جامعة نايف للعلوم الأمنية ، الرياض ، كلية الدراسات العليا ، ص ص 11-12

(52) جاسم محمد جرجيس ، مجدى زيادة ، (2001) ، واقع صناعة تكنولوجيا المعلومات في امارة دبى ، **ندوة المعلوماتية في الوطن العربي الواقع والافاق** ، مؤسسة عبد الحميد شومان ، عمان ، الأردن

(53) ايمان محمد عيسى ، منى داخل السريحى ، (2019) ، منصة البيانات المفتوحة وتفعليها عبر بوابات الحكومة الإلكترونية لدول مجلس التعاون الخليجي ، دراسة مقارنة ، **بحث منشور** ، جامعة الملك عبد العزيز ، قسم علم المعلومات ، دار جامعة حمد بن خليفة للنشر ،

(54) العربي العربي ، الحكومة الإلكترونية والبعد الأمني ، **مقال منشور** ، مركز الشرق العربي للدراسات الحضارية والإستراتيجية بالمملكة المتحدة لندن
http://www.asharqalarabi.org.uk/
(55) Choi,h,park,m.,j.,rho,j,j,&zo,h ,(2016),**rething the assessment of government implementation in developing countries from the perspective of design** – reality gap : application in the Indonesian e-procurement system telecommunications policy 40,644-660
دعاء الحسبان ، وئام الحايك (2017) ، التحديات والفرص المؤثرة على نجاح الحكومة الإلكترونية بالأردن ، **مجلة العلوم الهندسية وتكنولوجيا المعلومات** ، 1(2) 58-71
خيرى كتانة ، سحر أبو جارو ، (2016) ، الحكومة الإلكترونية في الأردن : التحديات والفرص ، **مجلة رماح للبحوث والدراسات** ، العدد 17 ، ص ص 115-129
(56) ندى جراح ، شيماء محمود ، (2012) ، الحكومة الإلكترونية الاقع ومشاكل التطبيق في العراق ، **مجلة الخليج العربي** ، العدد 40 ، ص ص 91-134
(57) محمد سالم المحمدي (2010) ، مشروع الحكومة الإلكترونية في سلطنة عمان : دراسة حالة وزارة التجارة والصناعة ، **رسالة ماجستير غير منشورة** ، جامعة السلطان قابوس ، عمان
(58) محمود محمد إبراهيم ، بسمة محرم الحداد ، (2018) ، منشات الأعمال والتحول الرقمي ، **المجلة المصرية للمعلومات** ، الكمبيوتر ، (21) ص ص 25-32
(59) العربي العربي ، **مرجع سابق**
(60)Ubaldi, B. (2013). Open government data: Towards Empirical Analysis of Open Government Data Initiative. OECD **Working Papers on Public Governance**, (22), 0_1.
(61) Kumar , sachan, nukherjee& kumar,(2018) , factors influencing e-government adoption in India , a qualitative approach , **digital policy** , regulation and governance ,1-21 , dol
(62) عبد الفتاح مراد (1991) ، **المدن والقرى الذكية** ، الإسكندرية ، جمهورية مصر العربية ، دار أجيال المستقبل ، للطباعة والنشر
(63) ICF (2006) , intelgent community forum , what is an intelligent community , retrieved from ,
http**://www.intelligentcommunity.org/displaycommon**.cFm?an=1&subariticlenbr=18
(64) خلود رياض صادق (2013) ، مناهج تخطيط المدن الذكية ، حالة دراسية دمشق ، **رسالة دكتوراه غير منشورة** ، كلية الهندسة ، جامعة دمشق ، سوريا
(65)Walid, t (2009) , RFID – intelligent cities , **intelligent cities conference** , Umm AL-Qura University , Makah /Saudi Arabia
(66) احمد نجيب القاضي ، محمد إبراهيم العراقي ، (2014) ، خصائص المدن الذكية ودورها في التحول الى استدامة المدينة المصرية ، **المجلة الدولية في العمارة والهندسة والتكنولوجيا** ، بحث منشور ، 2014 ، ص 7
(67) جاسم محمد جرجيس ، مجدى زيادة ، **مرجع سابق**
(68) EMC information infrastructure (EMC II) VMWare , pivotal , virtualized computing environment (VCE) **, RSA , virtustream**

(69) اى ام سى ، (2015) **بناء مدن كية ترتكز على البيانات** ، لمحة عامة عن الحل ، : IDC analze future ، أكتوبر

(70) محمد الشوا ، **مرجع سابق** ، ص 7

(71) عبد الكريم على جبر الدبيسي ، زهير ياسين الطاهات ، (2012) دور وسائل الاتصال الرقمي في تعزيز التنوع الثقافي ، بحث منشور ، **مجلة الاتصال والتنمية** ، دار النهضة العربية ، بيروت ، العدد 6 ، ص 25

(72) لطفى بلفرد امين ، (2016) ، الفضاء السيبرانى : هندسة وفواعل ، **المجلة الجزائرية للدراسات السياسية** ، ص ص 149-159

(73) Solomon jonathan cyber deterrence between nation(2011) – states : plausible strategy or pipe dream **strategic studies quarterly** 5,no 1 ,

(74) Rawashdeh , m . s, & al-maj , s (2017) , **the phenomenon of conflict in international relations , the international journal of social sciances and humoanities invention** 4 (5) :, pp 3488-3502,

(75) عادل عبد الصادق ، (2016) ، **أسلحة الفضاء الإلكتروني في ظل القانون الدولي** ، الإسكندرية ، وحدة الدراسات المستقبلية ، مكتبة الإسكندرية

(76)Stevens , tim ,(2017) , acyberwar of ideas ? deterrence and norms in **cyberspance contemporary security policy** vol . 33 . no1 pp 148-170

(77) خالد دخليز ، خالد وليد ، (2017) ، مقومات نجاح تطبيق الحكومة الإلكترونية في فلسطين : دراسة استكشافية ، **مجلة جامعة النجاح للأبحاث** ص ص 1111-1156

(78) طوربيا نذير (2019)،الحكومة الإلكترونية ومحاولة التأسيس المبدئي للإدارة الإلكترونية في الجزائر(تحليل للواقع واستشراق للمستقبل) **مجلة البشائر الإقتصادية** ، ص ص 537-558

(79) نضال ناجى بدوى بريوش ، (2020) **الصراع السيبرانى مع العدو الصهيوني** ، دبلوم الدراسات الفلسطينية ، أكاديمية دراسات اللاجئين ، قسم الأبحاث والمشاريع ، دبلوم الدراسات

(80) المبادئ التوجيهية المتعلقة بالبنية التحتية للإنترنت في الدول العربية ، **مجتمع الإنترنت** ، مارس 2020، ص ص 36-37

(81) (https://www.tra.gov.ae/aecert

(82) حكومة دبى ، **مرجع سابق**

(83)securitycyber/government/uae/news/com.gulfnews://http dubai-in-established-centre- html.621167--percent-23rises-cybercrime-

(84) على فياض الربيعات ، (2017) ، دور الموسيقى والمؤثرات الصوتية في تعزيز الإحساس الفلمي ، بحث منشور ، **المجلة الأردنية للفنون** ، مجلد 8 ، عدد1 ص ص 81-85

(85) احمد نجيب القاضي ، محمد إبراهيم العراقي ، **مرجع سابق** ، ص ص 8-9

(86) Argenti, P. (2002), December). Crisis communication**:** Lessons from 9/11. **Harvard Business Review**, 80(12), 103-109

(87) رحاب مالك العزة ، (2017) ، استخدام التقنيات التليفزيونية الحديثة وتأثيرها على زيادة متابعة مشاهدة البرامج الإخبارية في التليفزيون الأردني ، **رسالة ماجستير غير منشورة** ، جامعة الشرق الأوسط ، قسم الاعلام ، ، ص ص 16-18

(88) اسراء جبريل رشاد مرعى ، **مرجع سابق** ، ص ص442-443

(89) بارنى دارن ، **المجتمع الشبكي** ، (2015) ترجمة أنور الجمعاوى ، ط 1 ، المركز العربي للأبحاث ودراسات السياسة ، ص 39

(90) على حداده ،(2019) **تحديث المناهج التعليمية لمواكبة متطلبات الثورة الرقمية الثانية** ، اتحاد الغرف العربية ، دائرة البحوث الاقتصادية ، ص ص 2-3

(91) علم الدين بانقا ، **مرجع سابق**

(92) الأمم المتحدة ، المجلس الاقتصادي والاجتماعي ، اللجنة الاقتصادية والاجتماعية لغربي اسيا ،(2011) **إرشادات الاسكوا لتنسيق التشريعات السيبرانية في المنطقة العربية** ، بيروت ، 13-15 ، ص 7

(93) الاتحاد الدولي للاتصالات ، مكتب تنمية الاتصالات ، (2018) ، **مجموعة أدوات المهارات الرقمية** ، ص xi

(94) World economic forum ,(2016) the future of jobs :employment , skills and workforce strategy for the fourth industrial revolution , January . **https://reports.weforum.org/furture-of-jobs-2016**

(95) Vuorikari,R,Punie,Y,carretero Gomez S,Van den Brande , G (2016) Digital Comptence Framework for citizen Update phase 1: the conceptual Reference Model . Luxembourg 11517 / **publication office of the eurpean union** . EUR 27948 EN . doi:10.2791

(96) نزهة حانون ، (2008) الأساليب الإقناعية في الصحافة المكتوبة ، **رسالة ماجستير غير منشورة** ، قسم علوم الإعلام والاتصال ، كلية الخدمة الاجتماعية الإنسانية ،جامعة منثورى ، قسطنتنية ، ، ص 37

(97) على شدوان ، (2005) ، **الإعلان ، المدخل والنظرية** ، دار المعرفة الجامعية ، الإسكندرية ، ص 145

(98) كريمة زلماطى ، (2014) استخدامات أساليب الاقناع في تناول ظاهرة حوادث المرور ، **رسالة ماجستير غير منشورة** ، قسم علوم الإعلام والاتصال ، كلية العلوم الاجتماعية ص 77

(99) عادل عبد الصادق ، **مرجع سابق**

(100) ذيب عايض القحطاني ، (2015) ، **امن المعلومات** ، مدينة الملك عبد العزيز للعلوم والتقنية ، الرياض ، ص 23

(101)https://**www.escwa.un.org.**/information/meetingdetails.asp?referenceNum-1427E

(102) الاستراتيجية الوطنية للأمم السيبراني ، **رئاسة مجلس الوزراء** ، المجلس الأعلى للأمن السيبرانى ، جمهورية مصر العربية ، 2017-2021

(103) الاستراتيجية الوطنية للأمم السيبراني ، **مرجع سابق**

(104) نيال ادلبى ، (2017) الأمان في الفضاء السيبراني ومكافحة الجرائم اليسبرانية في المنطقة العربية ، توصيات سياسية ، ورقة عمل ، **مؤتمر الأمن السيبراني والدفاع السيبراني** ، الجامعة اللبنانية والوكالة الجامعية للفرنكوفرنية AUF ، ص 73

(105) الاستراتيجية الوطنية للأمم السيبراني ، **مرجع سابق**

(106) LTU, arco Grecke ,(2012) Understanding cybercrime : phenomena , challenges and legal response , September , p 18

(107)https://www.goc.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final-pdf,p18

(108) Secretariat of security and defense committee, finland is cyber security strategy **http://www.defmin.fi/files/2378/finland_scyber_security-strategy.pdf,p9**

(109) الاستراتيجية الوطنية للأمم السيبراني ، **مرجع سابق**

(110) صبري المبارك (2014) ، المعلومات ودورها في التنمية ، **مجلة المعلوماتية الإلكترونية** ، العدد 25 ، 2014/2/18 . informatics.gov.old/details.php?id=295

(111) عايد الحميدان (2004) **اهوال المخدرات في المجتمعات العربية** ، مطبعة الحكومة، 45

(112) ابن فارس ، **معجم مقاييس اللغة** ، ، 124/6

(113) عمر صالح عمر ، مفهوم الوعى والتوعية وأهميتها ، **ندوة الحج الكبرى** ، كلية الشريعة والدراسات الإسلامية ، الامارات العربية المتحدة ، جامعة الشارقة ، ص 39

(114)اديب خضور (2007) ، **البحوث الإعلامية دراسات في المنهجية والسيميولوجيا وتحليل المضمون** ، دمشق ، مطبعة خالد بن الوليد

(115) حكومة دبى ، مركز دبى للأمن الإلكتروني ، **مرجع سابق**

(116) ملقى سيفين ، محمد مصطفى إبراهيم (2011) ، فعالية استراتيجية قائمة على التفاعل بين الرياضيات والعلوم والتكنولوجيا لتمية الثقافة والوعى التكنولوجي لدى المعلمين ، **المؤتمر العلمي العاشر لكلية التربية** ، جامعة الفيوم ، مصر

(117) وداد الجمل ، محمد امين ، (2017) تطوير أسس تربوية لتمية الوعى التكنولوجي لدى طلبة الجامعات الأردنية الرسمية في مواجهة تحديات الثورة المعلوماتية ، المجلد العاشر ، ، **المجلة العربية لضمان جودة التعليم الجامعي** ، العدد 12

(118) عايد الحميدان ، **مرجع سابق** ، ص16- 19

(119) عايد الحميدان ، (2004) ،**مرجع سابق** ، ص 26