تداعيات الاختراقات السيبرانية المحتملة لمواقع التعليم الالكتروني الخاصة باساتذة الجامعات

أ.م.د. رغد زكي غياض أ.د. محمد هادي ارحيم

الجامعة المستنصرية – كلية التربية الاساسية

المستخلص:

يهدف البحث الحالي الى تسليط الضوء على اهمية العلم السيبراني وعالميته وميادين توظيفه والاختراقات التي يحدثها على الصعد كافة وتداعيات هذه الاخراقات لمواقع الاساتذة الجامعيين حصريا. شاعت عالميا مصطلحات (السيبرانية – الحرب السيبرانية – الاختراقات السيبرانية – الامكانات السيبرانية – الهجمات السيبرانية وغيرها) في الاونة الاخيرة الامر الذي استرعى انتباه الباحثين لاسيما وان موضوع البحث يقع في مساحة اختصاصهما واهتماماتهما ما دفعهما للبحث الحالي. تتجلى اهمية هذا البحث فيما يوفره من معلومات في ميدان تجنيد الذكاء الصناعي والروبوتات وبرامج الحواسيب وتشفيراتها وكودات الذكاء الانساني واليات تحويلها الى المكائن وما يمثله كل ذلك من تداعيات محتملة. قد يتعرض الاساتذه الجامعيين لهذه الاختراقات من خلال مواقعهم الالكترونية التي ينشؤونها باسماءهم او المنصات الالكترونية التي يدخلونها لاغراض التدريس او المؤتمرات عن بعد في اثناء الحظر الوبائي الذي تسبب به تفشي الفايرس العالمي (19covid) وانعكاسات هذا الحظر التي القت ظلالها على طبيعة العمل في المؤسسات الجامعية. سيتم تبويب الاختراقات السيبرانية المحتملة وتداعياتها ضمن نتائج البحث في ضوء تحليل معطيات الواقع الماخوذ من اجابات اساتذة الجامعات انفسهم على اداة البحث المتمثلة باستبانتين مفتوحة تارة ومغلقة تارة اخرى كونها الاداة الاكثر اتساقا مع منهجية البحث الحالي .وسيقدم البحث مجموعة من التوصيات في صوء النتائج.

الفصل الاول / مدخل الى البحث

1 . اهمية البحث والحاجة اليه:

تتجلى اهمية البحث العلمي عموما في ما يضيفه من معلومات واكتشافات تفيد المنظومة الانسانية وتوفر للافراد نوعا من الامان الصحي – النفسي – الاقتصادي وغيرها من جوانب الامان كان اخرها الامان الالكتروني كون الجانب الالكتروني اصبح نسخة افتراضية للبشر كونه يحوي بيانات كاملة عن الافراد (صوت، صورة، بصمة اصابع، بصمة وجه، بصمة عين ومعلومات شخصية خاصة وعامة) . يعتبرمصطلح (السيبرانية) هو المصطلح الرئيس في البحث الحالي كونه من العلوم التي تشغل العالم اليوم وتدير حركة محاوره العلمية والعسكرية والسياسية والاقتصادية من خلال قواعد البيانات الالكترونية الكونية للافراد، الامر الذي حدى بالباحثين لدراسة جانب من جوانب تداعيات هذا العلم في جزئية صغيرة من الجزئيات التي يمكن لاختراقاته ان تحقق اثارا كبيرة وخطيرة تشكل تهديدا لامن فئة مهمة من فئات المجتمع العلمي وهم فئة العلماء (الاكاديميون) او (اساتذة

الجامعات). شكلت الاختراقات السيبرانية تهديدا مقلقا على امن الدول كونها لا تمتلك شرعية قانونية دولية مع صعوبة تحديد وقت او كيفية حصولها لانها تعتمد على اليات العمل الالكتروني وتحريك البيانات (Data) عبر الفضاء الكوني الالكتروني فضلا عن عدم القدرة على تحديد كنية الاشخاص القادرين على هذا التحريك لانهم غالبا من المحترفين الذين ياخذون اجورا طائلة مقابل حرفتهم هذه وبتكتم وسرية عاليين لضرورة الحفاظ على امنهم وسلامتهم كونهم يمثلون ثروة بشرية – ان احسن استخدامها. وجراء هذه الاختراقات وما تمثله من " تهديدات على امن الدول واسرار امنها القومي تم تسمية هذه الاختراقات بالحرب السيبرانية واصبح يسمى المنفذين لها بالمتسللين، فيقومون بشن هجمات على شكل افراد او مجموعات في عالم غامض تحكمه السيرفرات والخوادم الالكترونية في فضاء الكتروني مفتوح يصعب احتواءه او رسم حدوده في ظل انعدام القانون القيمي والاخلاقي تحت مظلة حماية الدول المستفيدة " (Madline, 2011 , p 43)

تتمثل الوسائط التي تتحقق بها الاختراقات السيبرانية بمجموعة من " اجهزة الكومبيوتر والخوادم واجهزة التوجيه والمحولات والكابيلات الضوئية المتصلة بشكل يسمح للبنى التحتية الحيوية بالعمل بفعالية ويعمل بمثابة الجهاز العصبي للاقتصاد العالمي والصحة المجتمعية والتعليم "

(webster's , 2010, p 133)

ونظرا للانفتاح التكنولوجي للجامعات كمؤسسات تعليمية بمحتوياتها (المادية والبشرية) كافة في العالم عموما وفي الوطن العربي خصوصا وفي العراق تحديدا بشكل مكثف جدا تحت ضغط الحظر الوبائي الذي شاع في عام 2020 سبب تفشي الوباء العالمي الذي تسبب به فايرس (19covid) من اجل تحقيق ديمومة التعليم واستمرار دوران عجلته وذلك لشيوع حظر التجوال في العالم اجمع قبل نهاية العام الدراسي 2019 – 2020 الامر الذ تسبب بتعطيل الدروس وعملية تنفيذ المنهج وانشطته المصاحبة وتعطيل تقويمه الامر الذي لم يجعل امام تلك المؤسسات حلا سوى الالتجاء الى التعليم الالكتروني على الرغم من كل التحفظات التي تحيطه وعدم توفر الاستعدادات المادية والبشرية اللازمة له في كثير من الدول لاسيما النامية منها مثل دول الوطن العربية. مثل ذلك انعطافة تاريخية في مناهج التعليم العالي (تخطيطا – تنفيذا وتقويما) الانعطافة التي كانت تحديل للافراد المستخدمين مقابل الشركات المنتجة للتطبيقات التي نزلت بكم هائل من الاختيارات للتطبيقات المتاحة والتنافس بين المبرمجين في كم التسهيلات التعليمية التي تقدمها تلك التطبيقات التي هي مجانية غالبا ولا تكلف الفرد سوى مجموعة لمسات على شاشة هاتفه ولكن السؤال (مقابل ماذا ؟؟) الجواب (مقابل كم من البيانات الشخصية الخاصة والعامة التي يمثل تسربها او استخدامها في غير محلها خطرا على صاحبها).

ومن هنا جاءت اهمية البحث الحالي الذي يهدف الى لفت انتباه اساتذة الجامعات الى ما ياتي :

1. توضيح مفهوم العلم السيبراني .
2. تحديد مخاطر السيبرانية.
3. تبويب مجالات محتملة للاختراقات السيبرانية.

4. توضيح تداعيات الاختراقات السيبرانية لمواقع الاساتذة الجامعيين التي يستخدمونها في نشاطهم الاكاديمي الالكتروني .

2 . هدف البحث:

يهدف البحث الحالي الى دراسة تداعيات الاختراقات السيبرانية المحتملة لمواقع الاساتذة الجامعيين الاكثر ارتيادا .

3 . حدود البحث:

يتحدد البحث الحالي فيما ياتي :-

1. **الحدود الزمانية**: العام الدراسي 2019-2020 و 2020 – 2021 .
2. **الحدود البشرية**: الاساتذة بلقب استاذ مساعد صعودا في الجامعة المستنصرية و جامعة بغداد وجامغة ذي قار وجامعة واسط وجامعة تكريت وجامعة البصرة .
3. الحدود الموضوعية : الاختراقات السيبرانية ، المواقع الالكترونية المستخدمة في المهام الاكاديمية.
4 . **تحديد المصطلحات وتعريفها**:

تتحدد مصطلحات البحث الحالي ب (التداعيات، الاختراقات السيبرانية، المواقع الالكترونية) وفيما يلي تعريف لكل منها.

اولا: التداعيات:

عرفها الشحات 1983: "هي النتائج المترتبة على حدث ما " (الشحات ، 1983 ، ص60) .

ويعرفها الباحثان تعريفا نظريا: بانها الانعكاسات الفكرية والاجتماعية والصحية الحاصلة نتيجة لاختراقات سيبرانية محتملة للمواقع الالكترونية الخاصة باساتذة الجامعات .

ثانيا: الاختراقات السيبرانية

عرفها Martine 2013 بانها " الهجمات الرقمية المتمثلة بفيروسات و قرصنة من قبل جهة مستفيدة ما لتعطيل او سرقة انظمة الكومبيوتر الحيوية لدى جهات محددة او افراد بعينهم بهدف الاستغلال او العرقلة او حرف المسار عن وجهته " (73 martine , 2013 , p)

يعرفها الباحثان تعريفا نظريا: هي التسللات غير الملحوظة لمواقع الاساتذة الجامعيين التي يستخدموها في مختلف انشطتهم الاكاديمية التدريسية والتقويمية والمؤتمرات من اجل التجسس او سرقة البيانات او الابتزاز.

ثالثا : المواقع الالكترونية:

يعرفها المنصور2012 "هي مجموعة صفحات ويب مرتبطة مع بعضها البعض، ومخزنة على نفس الخادم. يمكن زيارة مواقع الويب عبر الإنترنت.. تختلف أهداف مواقع الويب، فمنها ما هو للإعلان عن المنتجات ومنها ما يبيعها، كما أن هناك مواقع للمحادثة (الدردشة) أو منتديات للنقاش والحديث بين مستخدمي الويب. ويوجد ما يعرف بالمدونات وهي مواقع ويب يسرد فيها مؤلفها ما يريد الكتابة عنه ومواضيع أخرى، كما يمكن للزوار الرد على ما يكتب". (المنصور ، 2012 ، ص82) يعرفها الباحثان تعريفا نظريا بانها مجموعة التطبيقات التي ينشئ عليها استاذ الجامعة حسابا باسمه الخاص وبياناته الرسمية الشخصية ليكون منصة للتواصل مع طلبته او زملائه لاغراض اكاديمية بحتة .

الفصل الثاني اطار نظري

يقدم الباحثان في هذا الفصل اطارا نظريا لمحاور البحث كي يتم الاستفادة منها في التاسيس لاداة البحث في الفصل التالي، وستتمثل محاور البحث فيما ياتي:

المحور الاول: السيبرانية ومدياتها

بدأ الاهتمام بهذا المجال من تسامي البشر مع الالة في حركة صناعة الروبوتات وتطور مايعرف بالذكاء الصناعي عندما تاسست حركة بحوث الذكاء الصناعي في مؤتمر كلية دارتموث عام 1956بحضور باحثين مثل جون مكارثي زمارفن مينسكاي وهربرت سايمن والاين نوييل الذين اصبحوا قادة في مجال الذكاء الصناعي في ارقى المعاهد المتخصصة والذين جعلوا من الحاسب الآلي متحدثا للغات مختلفة ومقتدرا على حل مسائل الرياضيات والمنطق، الامر الذي تم تجنيده من قبل وزارة الدفاع الامريكية في ستينيات القرن المنصرم فاصبحت تنفق ميزانيات ضخمة من المال لتمويل مثل هذه فنتج عن هذه الحركة نتاجات مهمة في تاريخ الذكاء الصناعي منها (روبوتات تقوم باعمال الانسان 1965) (معالجة المشكلات التي تسبب اخطاء في الحواسيب 1967) تعثرت ابحاث الذكاء الصناعي في السبعينيات ثم عادت للانتعاش في الثمانينيات بالنجاح التجاري فيما يعرف بالنظم الخبيرة وهي نظم تحاكي ذكاء البشر واستمر تطور هذه النظم واستمر معها الارباح العوائد المالية . حتى وصلنا في تسعينيات القرن العشرين واوائل القرن الواحد والعشرين الى استخدام الذكاء الصناعي في الامور اللوجستية والهكر على البيانات وبعض القضايا العلاجية طبيا وهي صور للسايبر الذي نهدف لدراسته في البحث الحالي وقد كان ويليام جيبسون 1982 قد استخدم المصطلح في خياله الروائي عام 1982 و 1984 والذي كان فيه يجسد الفضاء الالكتروني فكان سابقا للعلم في وضع رؤى المستقبل (ولد هذا الروائي في 17 مارس عام 1948 من اصل أمريكي كندي له طابع خيالي تأملي. ويُدعى"بالرسول الأسود" لنوع السيبربنك أدخل جيبسون مصطلح الفضاء الإلكتروني في قصته القصيرة "الكروم المحترق" التي صدرت عام 1982 ثم أشاع هذا المفهوم في روايته الأولى نيورومانسر التي صدرت في عام 1984. في تخيل الفضاء الإليكتروني، قام جيبسون بأول وصف لعصر المعلومات وذلك قبل ظهور الإنترنت في تسعينيات القرن العشرين. كان له الفضل أيضًا في التنبؤ بازدهار تلفزيون الواقع، وإرساء المفاهيم الأساسية المرتبطة بالنمو السريع للبيئات الافتراضية مثل ألعاب الفيديو، والشبكة العنكبوتية العالمية)
(https://ar.wikipedia.org/wiki/)

لقد توسعت التهديدات الامنية بجدية وانفتاح حتى وصلت مخاطرها لامن المليارات من الدولارات غندما لا يتم التعامل مع امن المعلومات بشكل صحيح ، ان الافتقار الى قواعد واضحة واطار قانوني يجعل من السيبرانية خطرا حقيقيا قد تستغله جماعات لا تقل خطورة عن الجماعات الارهابية لاسيما اذا تم تجنيدها لغايات منافية للاخلاق وقيم التعايش السلمي بين البشر .(federal office, 2005, website) تظهر الكثير من سيناريوهات الافعال التي توظف فيها العلوم السيبرانية وذلك لان مديات هذه العلوم لايحدها حد او قانون وقد استخدم مصطلح سايبر مع اي شيء يتعلق بالشبكات واجهزة الكومبيوتر خاصة في المجال الامني وهومجال ناشيء للدراسة يبحث في النزاعات ضمن الفضاء لدولة واحدة او مجموعة دول ورغم ذلك لايوجد اجماع بين الباحثين على ماهية الفضاء السيبراني او الاثار المترتبة عليه. (Ramon ,2017, p 33)

ان مفهوم السيبرانية مفهوم جديد غير خاضع لقانون الهي او وضعي، ومحاولات استحداث قانون لها نتج عنه قانو مجزء ومتناثر كان غالبا عرضة للتقسيم وقد ادى ذلك الى تكوين منطقة رمادية ترغب بعض الجهات استغلالها باختبار مستجدات تقنية مستمرة الامر الذي نلحظ اضطراده بتزايد عدد التطبيقات المستحدثة يوميا وباستمرار حتى تكونت عشرات الاختيارات امام الباحث عن تطبيق ما كلها متشابهة الغاية والالية الا انها تقدم في رزمة واحدة على شكل عروض في قوائم الاختيارات .

تسمى السيبرانية بالفضاء الالكتروني الذي هو شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات تشمل الانترنتوشبكات الاتصال السلكية واللاسلكية والمعالجات المدمجة و اجهزة التحكم في الصناعات الحيوية NSPD541HSPD – 23CNSS14009-215. والسيبرانية هي البيئة المعقدة الناتجة عن تفاعل الاشخاص والبرامج والخدمات على الانترنت عن طريق الاجهزة التكنلوجية والشبكات المتصلة بها والتي لا توجد باي شكل مادي . (7Nistir , 2015 ,p) وتنتشر السيبرانية على مساحة الكترونية مفاهيمية لا حدود لها .ومعظم تلك المساحة متعلق بالمال والتسليح والامن القومي وظهرت مصطلحات مثل مصطلح Stuxnet وهي دودة كمبيوتر تستهدف أنظمة التحكم الصناعية ، ولكنها الأكثر شهرة على الأرجح أنها أول سلاح إلكتروني حقيقي ، حيث تم تصميمه لإلحاق ضرر مادي ، تم تطويره من قبل الولايات المتحدة وإسرائيل (على الرغم من أنهم لم يؤكدوا ذلك أبدًا) لاستهداف البرنامج النووي الإيراني. استهدفت الدودة ، التي تم رصدها لأول مرة في عام 2010 ، أنظمة تحكم صناعية معينة من شركة سيمنز ، وبدا أنها تستهدف الأنظمة التي تتحكم في أجهزة الطرد المركزي في مشروع تخصيب اليورانيوم الإيراني - مما أدى على ما يبدو إلى إتلاف 1000 من أجهزة الطرد المركزي هذه وتأخير المشروع ، على الرغم من التأثير العام على البرنامج غير واضح . (kemp ,2012 , p 146) ومصطلح هجوم (Wanna Cry Ran somware)، الذي تسبب في فوضى في مايو 2017. ومصطلح (برامج الفدية) شديدة الضراوة كونها كانت مشحونة مع ثغرة يومzero تم تخزينها من قبل وكالة الأمن القومي ، ويفترض استخدامها في التجسس السيبراني . ولكن تم الحصول على الأداة بطريقة أو بأخرى من قبل مجموعة القرصنة. (website , 2019 , Dradis) كان عام 2007 عندما انتقلت الحرب السيبرانية من التنظير الى التطبيق وذلك عندما أعلنت حكومة دولة إستونيا شرق أوروبا عن خطط لنقل نصب تذكاري للحرب السوفيتية ، وجدت نفسها تحت قصف رقمي غاضب أطاح بالبنوك والخدمات الحكومية دون اتصال بالإنترنت سميت هجمات DDoS ومع ذلك لم يُنظر إليها على أنها ارتفعت إلى مستوى الحرب السيبرانية الفعلية ، كما أثبت مختبر أيداهو الوطني في العام نفسه أنه يمكن استخدام هجوم رقمي لتدمير الأشياء المادية عبر اختبار أورورا للمولدات. (devers , 2007 , p 23)

ثم وقع هجوم البرامج الضارة Stuxnet في عام 2010 ، مما أثبت أن البرامج الضارة يمكن أن تؤثر على العالم المادي .(89borkovich , 2012 , p) ومنذ ذلك الحين والاحداث السيبرانية تتوالى ففي عام 2013 ، قالت وكالة الأمن القومي أنها أوقفت مؤامرة من قبل دولة غير مسماة - يعتقد أنها الصين - لمهاجمة رقاقة BIOS في أجهزة الكمبيوتر، مما يجعلها غير قابلة للاستخدام تلاها في عام 2014 الهجوم الذي حصل على Sony Pictures Entertainment ، الذي حمل الكثيرون

مسؤوليته على كوريا الشمالية ، واتخذ الناتو في نفس العام خطوة مهمة لتأكيد أن الهجوم السيبراني على أحد أعضائه سيكون كافياً للسماح لهم بالاستناد إلى المادة 5 ، آلية الدفاع الجماعي في قلب الحلف وقد تمكن المتسللون قبل عيد الميلاد في عام 2015 ، من تعطيل إمدادات الطاقة في أجزاء من أوكرانيا ، باستخدام حصان طروادة المعروف Black Energy ، تلاها في مارس 2016 اتهام سبعة متسللين إيرانيين بمحاولة إغلاق سد في نيويورك وذلك ضمن لائحة اتهام من قبل هيئة محلفين كبرى . (70Curiel, 2019 , p) وعلى اساس هذه الاحداث التاريخية توجهت الدول بسرعة نحو بناء قدرات الدفاع السيبراني والهجوم ،ونتج عن ذلك تحديد الفضاء الإلكتروني ب "المجال التشغيلي" لخلق منطقة يمكن أن يحدث فيها الصراع ، فأصبح الإنترنت رسميًا ساحة معركة .

ومن خلال ماجمعه الباحثان من بيانات تم عرضها انفا يتضح لنا مديات هذا العلم و خطورة تداعياته لو تركت دون انتباه من افراد المجتمع عموما و الاكاديميين خصوصا.

المحور الثاني : الاختراقات السيبرانية والهكر

غالبًا ما تُعتبر أنظمة التحكم الصناعية الكبيرة أو الشبكات العسكرية الأهداف الرئيسية في الحرب السيبرانية ، لكن إحدى نتائج صعود إنترنت الأشياء قد تتمثل في إحضار ساحة المعركة إلى منازلنا.

" قال موجز إخباري لمجتمع المخابرات الأمريكية في كانون الثاني / يناير 2017: يمتلك خصومنا قدرات على تحمل البنية التحتية الحرجة للولايات المتحدة بالإضافة إلى النظام البيئي الأوسع للأجهزة الاستهلاكية والأجهزة الصناعية المعروفة باسم إنترنت الأشياء". يتم استخدامها جميعًا إما للتجسس على مواطني دولة أخرى ، أو لإحداث فوضى إذا تم اختراقهم. ليست جميع أجهزة إنترنت الأشياء في المنازل ؛ تمتلئ المستشفيات والمصانع والمدن الذكية الآن بأجهزة استشعار وأجهزة أخرى ، مما يعني أن التأثير الحقيقي لانقطاع إنترنت الأشياء يمكن الشعور به على نطاق واسع".
(CNBC , 2017, website)

قد يكون من الصعب إيقاف الاختراقات السيبرانية عند حدود ما وستكون هناك حاجة إلى استثمارات إضافية للأمن السيبراني مثل:

1. تشفير قوي
2. مصادقة متعددة العوامل
3. مراقبة متقدمة للشبكة

وهي اساليب قد لا تمنع الاختراق ولكن تقلل الضرر المحتمل ، وتعمل الدول على تطوير ستراتيجيات الدفاع السيبراني الخاصة بها مثل الاتحاد الأوروبي عندما أعلن مؤخرًا عن خطط للعمل على خطة للدفاع الإلكتروني ستستدعيها إذا واجهت هجومًا إلكترونيًا كبيرًا عبر الحدود ، وخطط للعمل مع الناتو في تدريبات للدفاع الإلكتروني . ومع ذلك ، لا تعطي جميع الدول أولوية عالية للامن السيبراني . (Borys , 2017 ,p33) ومن اهم سبل تحقيق الامن السيبراني ردع المنافسين من مهاجمة الأسلحة التقليدية ، وذلك من خلال تطور مفهوم الردع السيبراني للمساعدة في منع حدوث الهجمات الرقمية بجعل تكلفة الهجوم باهظة للغاية بالنسبة لأي مهاجم محتمل واحد طرق القيام بذلك هو تأمين وتصلب أنظمة الكمبيوتر الخاصة بالمتسللين السيبرانيين بحيث يصبح الأمر صعبًا للغاية ومكلفًا للغاية بتصعيب ايجاد نقاط ضعف ممكنة الاختراق .

وقد تلجأ الدول الى فرض تكاليف على المهاجمين من خلال العقوبات أو التحقيقات الجنائية أو حتى التهديد بالرد كما حصل في الآونة الأخيرة عندما حاولت الولايات المتحدة إنشاء ردع من خلال سياسة التشهير واستخدام لوائح الاتهام لتسمية أفراد معينين تعتقد أنهم مسؤولون عن تنفيذ هجمات إلكترونية مدعومة من دول معادية لها . (LaValle , 2011 , p 98)

والتجسس السيبراني من ضمن المخاطر والتداعيات التي يجب الالتفات لها اذ يتسلل المتسللون إلى أنظمة وشبكات الكمبيوتر لسرقة البيانات او الملكية الفكرية كما حصل مؤخرا في الاختراق على مكتب إدارة شؤون الموظفين الأمريكي الذي شهد سرقة 21 مليون مواطن أمريكي ، بما في ذلك خمسة ملايين مجموعة من بصمات الأصابع والتي قام بها على الارجح قراصنة مدعومين . (Denning , 2016 , interview)

إن الخط الفاصل بين الاختراقات السيبرانية والتجسس السيبراني غير واضح وذلك لان السلوك متشابه لكليهما وهو(التسلل إلى الشبكات) والبحث عن عيوب في البرامج ولكن النتيجة مختلفة ففي التجسس النتيجة سرقة وفي الاختراقات تدمير وابتزاز ، من الصعب تحديد الفرق بين عدو يبحث في شبكة عن عيوب لاستغلالها وعدو يستقصي شبكة للعثور على الأسرار.(LaValle ,2011,p 99) إن إدراك الخطر السيبراني خطوة اولى لتحقيق الحماية ، حتى إذا لم تكن مؤسستك ذات اهمية ملحوظة لتكون هدفًا واضحًا للمتسللين بدافع الجشع مثال ذلك مؤسسات الصرف الصحي فقد يسأل غير المكترثين (من يخترق الصرف الصحي مقابل المال؟) ولمدرك لخطر السيبرانية يجيب (نعم يخترقها المتسللون الطامحون لخلق الفوضى فتكون هذه المؤسسة اولوية في اهميتها ضمن جدول اعمالهم). تستمر الهجمات السيبرانية في النمو من حيث العدد والتطور كل عام كما توضحها سلسلة الاحداث الاتية:

1. بدأت شبكة الأعمال الروسية الروسية (MBN) التابعة لمجموعة المافيا الروسية في عام 2006 باستخدام البرامج الضارة لسرقة الهوية.
2. بحلول عام 2007 ، احتكر RBN سرقة الهوية عبر الإنترنت.
3. بحلول سبتمبر 2007 تم تقدير تشغيل Storm Worm على ما يقرب من مليون جهاز كمبيوتر ، وإرسال ملايين رسائل البريد الإلكتروني المصابة كل يوم.
4. في عام 2008 انتقلت الهجمات السيبرانية من أجهزة الكمبيوتر الشخصية إلى المؤسسات الحكومية.
5. في 27 أغسطس 2008 ، أكدت وكالة ناسا العثور على دودة على أجهزة الكمبيوتر المحمولة في محطة الفضاء الدولية. بعد ذلك بثلاثة أشهر ، تم اختراق أجهزة الكمبيوتر التابعة لوزارة الدفاع الأمريكية (البنتاغون) ، من قبل قراصنة روسيين.
6. تعرض بنك الدولة في الهند (أكبر بنك في الهند) للهجوم من قبل قراصنة في باكستان في 25 ديسمبر 2008 حينها لم يتم فقدان أي بيانات ، أجبر الهجوم SBI على إغلاق موقع الويب مؤقتًا وحل المشكلة.(Barnum, 2014 , p 45)

في معرض الحديث عن المخاطر السيبرانية يجب ان نشير الى مصطلح المناورات السيبرانية فما هي هذه المناورات ؟ عندما نذكر المناورات السيبرانية نذكر فريق Locked Shields Green وهم فريق الدفاع الإلكتروني المدعوم من الناتو ، وهم مسؤولون عن المناورات السيبرانية من خلال توظيف ما يصل إلى 900 خبير في الأمن السيبراني يشحذون مهاراتهم لتحقيق المدافعة من الهجمات الإلكترونية المتزايدة من قبل الدولة المنافسة كما ورد على لسان عضو حلف شمال الاطلسي .(Bailey ، 2014 ، 88)

كانت أول ممارسة لإشراك السياسيين على مستوى وزراء دفاع الاتحاد الأوروبي في تمرين على الطاولة يسمى EU Cyberid. في سبتمبر 2017 ، اذ تم تصميم التمرين لاختبار ستراتيجيتهم في صنع القرار لمواجهة هجوم إلكتروني كبير محتمل على المنظمات العسكرية للاتحاد الأوروبي او ما يعرف ب (الاختراق السيبراني). هدف التمرين إلى مساعدتهم في تطوير المبادئ التوجيهية لاستخدامها في مثل هذه الأزمة الواقعية . (96 Gertner , 2019 , p)

وقد نكون هنا مضطرين للمرور على مصطلح (هكر) الذي يحدث في "الفضاء الإلكتروني " الذ هو المكان ظهور محادثة هاتفية تخص شخص ما لكن ليس على هاتفه الشخصي فقط، أو جهازحاسوبه المحمول او على مكتبه. بل على هاتف شخص آخر او جهاز حاسوبه المحمول او المكتبي ، في أي مدينة اذن هو مايحدث في المكان غير المحدد بين الهواتف out there ، من حيث لايعلم صاحب المكالمة الاصلية بمن يخترق مكالمته ويطلع على اسراره ليستغلها وفق اهواءه ومصالحه . (16Borys , 2017 , p)

من هنا يعصف ذهن الباحثين مجموعة من التساؤلات والافكار التي تمثل خطا للشروع في تحسس تداعيات الاختراقات السيبرانية – هدف البحث الحالي – وهي :

1. يعيد المتصيدون والمتسللون والجواسيس السيبرانيون اليوم كتابة قواعد الصراع من داخل سباق التسلح الرقمي السري .
2. الحرب السرية على أسرارالإنترنت الخاصة المتمثلة بالمراقبة عبر الإنترنت من خلال ما يعرف بالجيش السيبراني قوضت الثقة في المواقع الالكترونية والمنصات والتطبيقات .
3. الاختراقات السيبرانية منطقة رمادية تشمل الجريمة السيبرانية والحرب السيبرانية بما فيها التجسس السيبراني .
4. لماذا تضع وكالة المخابرات المركزية الاختراقات في(نظم IOS و Android و Windows) في دائرة الضوء ؟
5. هل وفر القانون الدولي غطاءا قانونيا لضبط الاختراقات السيبرانية ؟
6. تم تصنيف أكبر 15 تهديدًا عبر الإنترنت من خلال البرامج الضارة التي يعمل عليها الجواسيس الإلكترونيين.
7. عندما تحذر المملكة المتحدة القراصنة الروس من استهداف البنية التحتية الحيوية والديمقراطية فان مؤشر الخطر واضح للاخرين لاسيما في الدول النامية .

8. المتسللون الذين لم يختفوا أبدًا مستعدون لمزيد من الهجمات المدعومة من دول مختلفة مستهدفين التسريبات والمحاكاة هذا العام .

9. من مصادر المخابرات الأمريكية 30 دولة تبني قدرات الهجوم الإلكتروني . (LaValle ، 2011، 100)

10. الاختراقات السيبرانية هي دليل الشخص الذكي (Tech Republic)

المحور الثالث : مواقع التعليم الالكتروني

تخللت التقنيات الرقمية مهامنا وتفاعلاتنا اليومية في القرن الحادي والعشرين اذ تغيرت طريقة التعلم والعمل والاختلاط لاسيما في نمط الحياة الذي فرضه الحجر المنزلي الذي اصبح امرا واقعا بسبب تفشي الوباء العالمي المتسبب من فايرس كورونا (covid 19) وما نتج عنه من اعتماد كلي على الوسائل التكنولوجية في التواصل وتسيير امور المال والاعمال والتعليم . هذا كله كان ارضا خصبة للمتسللين واختراقاتهم غير المرئية لكثرة تسجيل الافراد على المنصات وظهور افراد جدد ممن لم يدخلوا سابقا ولم يمتلكوا تسجيلا على مواقع التواصل مضطرين بحكم عملهم كما حصل في سلك التعليم الجامعي .

هذا الامر أدى إلى ضرورة النظر في العواقب المترتبة على المجتمع فيما يتعلق بكيفية تأمين تفاعلنا مع بعضنا البعض وكيفية استخدام هذه الأدوات الرقمية وقنوات الاتصال.

عند التفكير في المجتمع الرقمي ، نحتاج أولاً إلى التفكير في مجتمع المعلومات وهو مرتبط إلى حد كبير بتقدم المعلومات الرقمية وتكنولوجيا الاتصالات اذ يشير مجتمع المعلومات إلى المجتمعات التي أصبح فيها إنشاء المعلومات ونشرها واستخدامها ومعالجتها أمرًا متاحا وسهلا ومهما في المساعي السياسية والاقتصادية والاجتماعية والثقافية. لقد أتاح مجتمع المعلومات العديد من الفرص بشكل أوسع من أي وقت مضى تتاح لنسبة كبيرة من سكان العالم للوصول إلى مصادر المعلومات والتقنيات التي تمكنهم من الانخراط عبر الإنترنت في عدد كبير من الأنشطة ، سواء كانت اقتصادية أو اجتماعية أو سياسية أو تعليمية فيمكن التحكم في التعلم من خلال المشاركة في دورات مجانية او بدء عمل تجاري عبر الإنترنت دون الحاجة إلى الكثير من رأس المال مثل بيع الحرف اليدوية او بث آراء ووجهات نظر لجمهور عالمي اضافة الى التواصل الاجتماعي عبر الحدود الجغرافية. ومن خلال ذلك ظهر لدينا مصطلح " المواطن الرقمي " وهو شخص يطور المهارات والمعرفة لاستخدام الإنترنت والتقنيات الرقمية بشكل فعال و يستخدم التقنيات الرقمية والإنترنت بطرق مناسبة ومسؤولة من أجل الانخراط والمشاركة في المجتمع والعمل والسياسة.

يمكن تعريف المواطنة الرقمية بانها القدرة على الوصول إلى التقنيات الرقمية مع الحفاظ على البقاء آمنًا. من خلال فهم ما قد يعنيه ذلك في المجتمع الرقمي. (إنجين ، 2015 ، ص 168)

تعرف المواقع الإلكترونية بانها مجموعة صفحات متصلة على الشبكة العالمية ، وتكون بنية واحدة يمتلكها شخص أو عدة اشخاص او مؤسسة ما، وقد يغطي هذا الموقع موضوع او عدة مواضيع . (dictionary , 2017 , website)

والمواقع الالكترونية توحد روابط الخوادم والعملاء ماحقق قبولاً سريعاً عند إنشاء المنصة وهناك عدة أنواع للمواقع الإلكترونية (تجارية ،رموز البلدان، مواقع تعليمية، مواقع ترفيه، مواقع حكومية، مواقع عسكرية،مواقع إخبارية، مواقع منظمات، مواقع شخصية) .

الفصل الثالث / اجراءات البحث

اولا: منهجية البحث:

اعتمد البحث الحالي منهجية البحث الوصفي كونها الاقرب لمتطلبات البحث باعتباره بحثا مستندا للبيانات النظرية والتجارب السابقة ومسح اراء المعنيين للوصول الى النتائج .

ثانيا : مجتمع البحث وعينته:

نظرا لضرورة اعتماد وجهات نظر اساتذة الجامعات كونهم الفئة المحددة في البحث الحالي فقد اعتمد الباحثان مجتمع التدريسيين في مجموعة من الجامعات العراقية فقط موزعة في (شمال ووسط وجنوب) العراق محددة بمن هم بلقب استاذ مساعد واستاذ وذلك وفق ما يسهل عليهما التواصل من خلال توزيع وجمع اداة البحث ، لكون البحث الحالي قد كتب في فترة اجتياح الوباء العالمي كورونا انحاء العراق وتفشي الاصابات بما يقيد حرية الحركة لاجراء البحوث العلمية وقد كان المجتمع وفق المتاح مكونا من (3435) استاذ جامعي بلقب (استاذ واستاذ مساعد). اخذت عينة عشوائية من الاساتذة المنتسبين لعينة قصدية من الجامعات العراقية وكان السبب من وراء اختيار هذه الجامعات هو توفر مجموعة من الاصدقاء المستعدين للتعاون مع الباحثين في توزيع ادوات البحث وجمعها الكترونيا عبر سلسلة من العلاقات العنقودية وفيما يلي جدولا يوضح توزيع افراد العينة :

الجامعة	عدد التدريسيين بلقب استاذ	عدد التدريسيين بلقب استاذ مساعد	المجموع
بغداد	68	64	132
المستنصرية	90	87	177
واسط	44	32	76
البصرة	76	41	117
ذي قار	23	34	57
تكريت	20	40	60
الموصل	67	55	122
ميسان	43	56	99
الكوفة	35	78	112
بابل	69	68	137
السليمانية	30	23	50
المجموع			1139

وقد مثل مجموع افراد العينة نسبة 33% من المجتمع الاصلي . تم التواصل معهم الكترونيا عبر وسائل التواصل الاجتماعي (what's app , viber , Massinger) وذلك رضوخا لقوانين

حظر التجول وتعميم تجربة التعليم الالكتروني رسميل في وزارة التعليم العالي والبحث العلمي العراقية للعام الدراسي 2019 – 2020 شاملا كل الانشطة الاكاديمية التي يقدمها الاساتذة بما فيها من مؤتمرات وندوات وورش عمل وبحث ونشر علمي .

ثالثا: اداة البحث:

اعتمد الباحثان الاستبانة اداة للبحث وكانت بنوعيها (المفتوحة والمغلقة) تم صياغتها بصورة اولية وعرضت على مجموعة من الخبراء لاخذ صدق الاداة ظاهريا .

كانت الاستبانة المفتوحة لغرض معرفة ماحددته عينة البحث من تداعيات للاختراقات السيبرانية المحتملة لمواقعهم الالكترونية. ثم جمعت الاجابات وتم تفرغها على خمسة محاور كل محور منها تضمن من 5 الى 7 فقرات وفق ما جاء في الاستبانة المفتوحة ، وضعت الفقرات في استبانة مغلقة واعيد توزيعها على الافراد ذاتهم لغرض اخذ موافقتهم على ما جاء فيها .

جمعت الاستبانات وكانت هناك موافقة على جميع الفقرات ، وبغية التحقق من ثبات الاداة اعيد توزيع الاستبانة ذاتها على الافراد ذاتهم بعد مرور شهر لاخذ الاتساق بين اجابتهم الاولى واجابتهم الثانية وكان هناك اتفاق بالاجماع ايضا .

رابعا :الوسائل الاحصائية:

حيث ان البحث بحثا وصفيا فهو بطبيعته لا يحتاج كثيرا من المعادلات والاحصائيات للوصول الى نتائجه لذلك لم يستخدم الباحثان سوى معادلة النسبة المئوية و الاختبار التائي لفحص الارتباط بين اجابتي العينة لاغراض الثبات .

خامسا / نتائج البحث:

توصل البحث الى تشخيص للتداعيات الناتجة عن الاختراقات السيبرانية للمواقع الالكترونية الخاصة باساتذة الجامعات يمكن ايجازها بما ياتي :

1- ان تغيير كلمات المرور الافتراضية وجعل كلمات المرور صعبه الاختراق من شأنه جعل عملية اختراق المواقع الالكترونية صعبة المنال خاصة في الدول التي لا تستغني عن الانترنت في تعاملاتها كافة كالمصارف والبنى التحتية وغيرها.

2- عدم استخدام كلمة المرور لانظمة مختلفة يعقد عملية اختراق وتهكير المواقع الالكترونية التي تهدف الى الاطلاع على خصوصيات العلاقات الشخصية كالمدونات والصور الخاصة والفيديوهات وغيرها من البيانات الخاصة.

3- الجيوش السيبرانية والالكترونية في عمل دؤوب بغية الاختراق وتدمير للعديد من الانظمة الخاصة بالدول والاشخاص يقابله عملية تحديث وتصويب ومعالجة ومكافحة البرامج المطورة من الفيروسات التي اخذت حيزاً تدميريا يضاهي الاسلحة الفتاكة للجيوش النظامية في الدول المتطورة .

4- لقد اصبح الانترنت جزء لا يتجزأ من المنظومة الحياتية لكل البشر ولا يمكن الاستغناء عنه لذلك من الضروري ان يكون الاتصال بالانترنت عند الضرورة التي يقتضيها الاحتياج للانترنت.

5- اصبح من بديهيات العمل الالكتروني ضرورة مراعاة توفير النسخ البديلة للبيانات الاساسية التي يتم العمل فيها تحوطا لكل طارئ قد ينتج عن هجوم سيبراني او خلل خاصة نحن نعيش في عالم كل

شئ مقصود فيه فقد نتج عن مفاهيم العولمة والمعلوماتية والسيبرانية ان زمن البراءة ولى وانتهى الى غير رجعة.

وفيما يلي جدولا بمحاور الاختراقات وتداعياتها التي تم كشفها من خلال اجراءات البحث :

محاور الاختراقات	التداعيات
المحور الشخصي	الاطلاع على اسرار العلاقات الشخصي سرقة الصور الخاصة تشفير الصور والفيديوات تسريب الفيديوات والمحادثات الشخصية سرقة البيانات الخاصة
المحور الفكري والعقائدي	نشر في الظل عن الفكر او المعتقد تبني وجهات نظر مناقضة لايمان الفرد التشهير والسب للرموز الدينية او المذهبية بث الافكار الطائفية باسم شخص ما دون معرفته. التجاوزات الاخلاقية المناهضة لفكر الفرد وعقيدته الترويج للتمييز العنصري دون قناعة الفرد بذلك التضارب والتناقض فيما يتم نشره او مشاركته
المحور الاكاديمي	سرقة بيانات متعلقة بالامتحانات الالكترونية الدخول على نظام الحاسب الشخصي او الهاتف الشخصي لتسريب محادثات . الاطلاع على مناقشات خاصة بين الاستاذ وطلبته او زملائه اختراق كروبات الاساتذة الرسمية او الشخصية حذف ملفات المحاضرات او التبليغات. تشفير ملفات المحاضرات والاختبارت التلاعب بالاسئلة والدرجات الالكترونية
المحور الاخلاقي	فبركة صور شخصية فبركة صوت وصورة بمقاطع فيديوية محاربة المرشحين من الاكاديميين لمناصب قيادية بحملات تسقيط الكترونية تغيير محتوى الملفات الدراسية المرسلة للطلبة بمحتويات لا اخلاقية تغيير ملامح الحوار الاكاديمي باخر متفسخ اخلاقيا .
المحور المادي	الابتزاز الاخلاقي التجسس على الاسرار المتعلقة بالتعاملات الشخصية المالية اختراق الحسابات البنكية والاطلاع على كودات الصرف الالكتروني انشاء حلقة ابتزاز للافراد الموجودة بياناتهم ضمن منظومة بيانات الفرد. كشف اسرار الممتلكات المادية والعينية الخاصة بالفرد.

توصيات البحث: يوصي الباحثان استنادا لنتائج البحث بالتوصيات الاتية :

1. تغيير كلمات المرور الافتراضية وجعل كلمات المرور صعبة الاختراق.
2. عدم استخدام نفس كلمة المرور لأنظمة مختلفة.
3. التأكد من أن جميع الأنظمة مصححة ومحدثة (بما في ذلك استخدام برامج مكافحة الفيروسات)
4. التأكد من أن الأنظمة تتصل بالإنترنت عند الضرورة فقط .
5. التأكد من عمل نسخة احتياطية من البيانات الأساسية بشكل آمن.

مقترحات البحث:

يقترح البحث في ضوء معطيات البحث الحالي المقترحين الاتيين :

1. اجراء دراسة تبحث في كم الحسابات المخترقة سيبرانيا في الجامعات العراقية .
2. اجراء دراسة الكترونية تفحص المنصات الهشة الاختراق لتجنب انشاء حسايات عليها .

مصادر البحث :

اولاً:- المصادر العربية

Al-Shahat, Ismail Metwally, Terminology in Political Science, Dar al-Ghad Printing and Publishing, Cairo, 1983(

Mansour, Muhammad. The impact of social networks on the audience of recipients is a lesson compared to social media and Arab websites model, 2012

Ingen Essen and Robert Evelyn, (2015). Being a digital citizen. London: RLI. University of New York

ثانياً:- **References**

Bailey, Tucker, Andrea Del Miglio, Wolf Richte. 2014. The rising strategic risks of

cyberattacks. Industry Research, New York: McKinsey Quarterly.

Barnum, Sean. 2014. 'Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).' MITRE Corporation.

Borkovich, D. J. (2012). When corporations collide: Information overload. Issues in Information Systems, 13(2), 269-284.

Borys, Christian. 2017. The day a mysterious cyber-attack crippled Ukraine. 4 July. http://www.bbc.com/future/story/20170704-the-day-a-mysterious-cyber-attackcrippled-ukraine.

CNBC. 2017. There are 20 billion cyber attacks every day: Cisco.https://www.cnbc.com/video/2017/there-are-20-billion-cyber-attacks-every-daycisco-.html.

Curiel, Johanna. 2019. Malware Information Sharing Platform MISP - A Threat Intelligence Sharing Platform. Accessed 11 06, 2019. https://www.circl.lu/services/misp-malwareinformation-sharing-platform/.

10-Denning, Dorothy. 2016. 'Cybersecurity's Next Phase: Cyber Deterrence.' The Conversation, 13 December.

Devers, C. J. (2007). Literacy in the information age. Unpublished Interview. University of Illinois at Urbana-Champaign.
Dradis. 2019. Dradis Pro. Accessed 11 07, 2019. https://dradisframework.com/ce/.
Eurofighter Typhoon - About. Accessed 11 07, 2019.
Gertner, J. (2019). The idea factory: Bell Labs and the great age of American innovation. New York, NY: The Penguin Press.
Kemp, 'Cyberweapons: bold steps in a digital darkness?', in Bulletin of the Atomic Scientists, 7 June 2012,available at: http://thebulletin.org/web-edition/op-eds/cyberweapons-bold-steps-digital-darkness
LaValle, S., Lesser, E., Shockley, R., Hopkins, M. S., &Kruschwitz, N. (2011). Big Data, analytics and the path from insights to References
(Madline Philip, Cyber electronic space, Scientific American, new York , vol : 233 no. 68, 2011)
Martine .d.jon, Cyber breaches of capital states , university of Colorado . journal of human and innovation , vol.52 no.41 , 2013)
Nistir, layman j Erik .social cines magazine , 8074 , vol.2, Iso / iec27032 .
Ramon ,D , Addison , Cyber Science in U.S. National Security, a paper for World Conference of National Security Advisors After 9/11, Washington d c , 2017)
(Webster's new world hacker dictionary , copy right , Bernadette Schell and Clemens Motrin published by Wiley , Indiana police , 2010)
المواقع الالكترونية
https://ar.wikipedia.org/wiki/
http://www.bsi .de/English/gshb/manual/index. htm (31 Oct. 2005).
[VRR8] Secure Communication in E-Government. Federal Office for Information Security
www.dictionary.com, Retrieved 21-11-2017

Ramification of Potential Cyber Penetrations For E-Learning Sites Of Universities Professors

Ass. Prof. Dr. Raghed Z. Ghayadh
Prof. Dr. Mohammed HadiIrhaim
Al-Mustansiriyah University - Faculty of Basic Education

Abstract:
The current research aims to highlight the importance of cyber science and its universality and the fields of employment and the breakthroughs it causes at all levels and the implications of these implications for the sites of university professors exclusively
The terms "cyber-warfare" and "cyber warfare" have been widely popular ized in recent times, which has attracted the attention of researchers, especially since the subject of the research falls into their area of competence and interests, which prompted them to research the current research.
The importance of this research is reflected in the information it provides in the field of the recruitment of artificial intelligence, robots, computer programs, encryption, human intelligence codes, and machinery and potential implications. The implications that university professors are likely to be exposed to through their websites, which they create with their names or the electronic platforms they enter for teaching purposes. or the electronic platforms they enter for teaching purposes or teleconferences during the epidemic ban caused by the global outbreak of fire (covid19) And the implications of this ban, which cast its shadow on the nature of work in university institutions what the university professors themselves answer edited Potential cyber breaches and their implications will be classified in search results in light of the analysis of reality data which The search tool of two Questionnaire open and closed as it is the most consistent tool with the current research methodology. The research will provide a set of recommendations in the results.