الهاكتفيزم :
استخدام الشبكات الحاسوبية في تعزيز الاجندة السياسية

أ.م.د. باسم علي خريسان (*)

المقدمة:

شكل التحول نحو الفضاء السيبراني أحد التطورات الحديثة التي تسهم بشكل كبير في إعادة تشكيل مختلف جوانب الحياة، مما يؤثر بشكل عميق في حياة الأفراد والمجتمعات. نعيش اليوم مرحلة حضارية جديدة تختلف عن سابقاتها في طرق التفاعل وأدواته وأطرافه ومدياته وأشكاله وعوامله الفاعلة. من بين هذه العوامل البارزة يظهر مفهوم «الهاكتيفيزم» (Hacktivism)، الذي وجد في الفضاء السيبراني مجالاً واسعاً للنشاط، لا سيما في المجالات السياسية، حيث يسعى الناشطون لتحقيق أهدافهم من خلال استخدام التكنولوجيا الرقمية.

إن أهمية وحداثة موضوع الهاكتيفيزم تستدعي دراسة متأنية وتعريفاً شاملاً به، منطلقين من فرضية أن الشبكات الحاسوبية يمكن أن تُوظف من قِبَل جماعات مختلفة لتحقيق أهداف سياسية واجتماعية متنوعة. هذه الفرضية تعكس واقعاً جديداً حيث أصبحت التكنولوجيا أداة قوية للتأثير والتغيير في العالم الحديث، مما يبرز ضرورة فهم هذه الظاهرة واستكشاف تأثيراتها المحتملة في المجتمع والسياسة.

اولاً: مفهوم الهاكتفيزم:

الهاكتفيزم (أو hactivism) هو استخدام الهجمات السيبرانية لزيادة الوعي بالقضايا الاجتماعية أو السياسية أو غيرها. المصطلح عبارة عن مزيج من كلمتين ،"Hack" و "Activism"،"اختراق" و نشاط"[1]. وتعني لغويا القرصنة يمكن إرجاع أصول القرصنة إلى الأيام الأولى لأجهزة الكمبيوتر والإنترنت وقد تطورت جنبًا إلى جنب مع التبني العالمي للتكنولوجيا. لقد صيغت في الأصل على أنها مصدر للقرصنة والنشاط ، مع تعريفها بشكل فضفاض ، فإن القرصنة هي إساءة استخدام أجهزة الكمبيوتر أو الإنترنت للقيام بهجمات

مركز الدراسات الاستراتيجية والدولية - جامعة بغداد
alibasim٦٤٩٢@gmail.com

إلكترونية لإصـدار بيان سياسـي أو اجتماعي أو دينـي أو فضـح الظلم [٢]. كذلـك هي عملية قرصنـة أو اقتحـام نظام كمبيوتـر ، لأغراض سياسـية أو اجتماعيـة. يُقال إن الشـخص الذي يقوم بعمل من أعمال القرصنة هو أحد نشـطاء القرصنة السـيبرانية. ناشط القرصنة الذي يقوم بمثـل هـذه الأعمال ، مثل تشـويه موقع الويب الخاص بمؤسسـة ما أو تسـريب معلومات تلك المنظمة ، يهدف إلى إرسـال رسـالة من خلال أنشـطته والحصـول على رؤيـة لقضية يروج لها[٣].بسـبب تنوع معاني المصطلح ، قد يكون من الصعب تعريـف الهاكتفيزم. غالبًا ما يُنظر إليه علـى أنه نوع من الإرهاب السـيبراني أو القرصنـة. علاوة على ذلك ، يصبح الأمر أكثر إرباكاً عندما «تعمـل بعض الدول تحت غطاء القرصنـة» من أجـل تحقيق أهدافهـا الخاصة فيما يلي بعض التعريفات الأكثر انتشاراً والتي تسـاعد على فهم الظاهرة:١-»الاسـتخدام غير العنيـف لـلأدوات الرقميـة غيـر القانونية أو الغامضـة قانونًا لتحقيق غايات سياسـية» .٢-»مزيـج مـن الاحتجاج السياسـي الشـعبي مع قرصنة الكمبيوتر» .٣-»إجراء عبر الإنترنت لحادث فـردي ذي دوافع سياسـية ، أو حملة ، اتخذته جهات فاعلة غير حكومية انتقاما للتعبير عن الرفض أو لفت الانتباه إلى مشكلة [٤].يمكن أن تتخذ القرصنة أشكالًا عديدة - بعضها قانوني والبعـض الآخر غير قانوني. في حين أن حجم وطرق هذه الأنواع مـن الحركات قد تختلف ، فإن الهدف العام يظل كما هو - لتعزيز رسـالة أو سـبب معين واكتساب رؤية لما يروجون له.

تميل أهداف القرصنة السـيبرانية إلى أن تكون منظمـات أو مجموعـات تدعم الاعتقـاد الذي تختلف معه مجموعة القرصنة بشـكل مباشـر ، والقرصنـة مـن جهة اخرى هي شـكل حديث من أشـكال العصيان المدني الـذي يرتبط غالبًا بقضايـا تتعلق بحقوق الإنسـان وحرية التعبير وحريـة المعلومات. عند العمـل لتحقيق هدف محدد ، قد يعمل نشـطاء القرصنة في شبكة من العديد من النشـطاء ، أو قـد يعمل الفرد بمفرده دون مساعدة أو شخصية ذات سلطة[٥].

دأت الهاكتفيزم كطريقـة للناس للاحتجاج عبر الإنترنـت للتأثيـر في التغيير. ناشـط القرصنة يكون مدفوعًا بالعصيان المدني ويسـعى لنشـر أيديولوجية. في بعـض الحالات ، تتضمن هذه الأيديولوجيـة فوضـى كاملة. لا يزال نشـطاء القرصنـة غيـر مدفوعيـن بنوايا خبيثـة. يقوم الهاكرز أيضًا بسـرقة الأمـوال أو البيانات في محاولة لنشـر أجندتهم. ومـع ذلك ، فإن دافعهم يشـبه دافع روبن هود. إنهم يسعون لأن يأخذوا من أولئك الذين يملكون ويعطون بحرية لمن لا يملكـون. عادة ما يرون أنفسـهم كأفراد يقظين يسـتخدمون القرصنـة لسـن عدالـة اجتماعية وتغييرات في السياسـة، يستخدم الهاكرز نفس الأدوات والتكتيـكات التي يسـتخدمها الهاكرز العاديون. على سـبيل المثال ، يمكن أن تتراوح تكتيكاتهم من نشـر رسـالة من خلال التشـويه البسـيط لموقع الويب أو الاسـتغلال من خلال اسـتخدام((Doxing[٦]. يمكنهـم حتـى شـن هجـوم رفـض الخدمـة المـوزع (DDoS)

لإسقاط شبكات كاملة. ولكن على عكس المتسللين العاديين ، لا يعمل نشطاء القرصنة دائمًا بمفردهم. يمكن أن يعمل الهاكرز أيضًا كجزء من مجموعة أو منظمة منسقة. يمكن أن تتراوح هذه المجموعات في الحجم من عدد قليل من الأصدقاء في الطابق السفلي ، إلى شبكة لامركزية كاملة من المتسللين في جميع أنحاء العالم [٧].

تمت صياغة مصطلح «Hacktivism" في ١٩٩٤ من قبل مجموعة الهاكرز الشهيرة(Cult of the Dead Cow). كما توحي الكلمة ، والهاكتفيزم هي وسيلة للنشاط السياسي أو الاجتماعي الجماعي الذي يتجلى من خلال اختراق أجهزة الكمبيوتر والشبكات. بدأت Hacktivism)) كثقافة فرعية للقرصنة والألعاب ومجتمعات الويب ، وسمحت للأفراد ذوي الميول الفنية باستخدام الاتصال وإخفاء الهوية على الويب للانضمام إلى الآخرين والعمل من أجل الأسباب المشتركة. على هذا النحو ، كان نشطاء القرصنة في الأصل من الشباب الذين استمتعوا بتصفح الويب وزيارة المنتديات ومجموعات الأخبار ومشاركة المعلومات على مواقع التنزيل غير القانونية ، والدردشة في "غرف خاصة" والتواطؤ مع المتسللين على الشبكة ممن لهم نفس التفكير. منحتهم الشبكة الفرصة لاستخدام أي اسم مستعار يريدونه ، واستخدام تلك الشخصية التي انخرطوا فيها في مغامرات مشتركة، من متابعة مواد إباحية ومشاركة النسخ المقرصنة من البرامج المرغوبة والمزح ، وأحياناً الأنشطة غير القانونية ". بعض المجموعات الأكثر شهرة والتي جذبت انتباه الجمهور فيما يتعلق بالقرصنة هي(Anonymous و Lulzsec)والجيش السوري السيبراني.هنا نأتي إلى السمة الثانية للهاكرز - الرغبة في "القتال" ضد عدو مشترك. عندما أصبح العالم أكثر ارتباطاً ، أدرك هؤلاء الأفراد أنهم يمكنهم التصرف (بأقل قدر من المخاطر الشخصية) ضد الآخرين. لكن هذه الأنشطة (التي سرعان ما أصبحت تُعرف باسم "العمليات") تطلبت أكثر من حفنة من الأصدقاء عبر الإنترنت. لقد احتاجوا إلى جيش. لذلك ولد المكون الأخير للهاكر - "الفيلق". كانت الرواية الجديدة ، التي تم إنشاؤها على مدى عقدين من الزمن ، هي قصة جيش مجهول الهوية يقاتل معاً كجماعة لكسر قيود العالم القديم[٨].

على عكس العديد من الجهات الفاعلة في التهديد التي تحركها مكاسب مالية بحتة ، ينخرط نشطاء القرصنة في نشاط تخريبي أو ضار نيابة عن قضية ، سواء كانت سياسية أو اجتماعية أو دينية بطبيعتها. غالباً ما يرى هؤلاء الأفراد أو الجماعات أنفسهم على أنهم «حراس فعليون» ، يعملون على فضح الاحتيال أو المخالفات أو جشع الشركات ، أو لفت الانتباه إلى انتهاكات حقوق الإنسان ، أو يحتجوا على الرقابة أو يسلطون الضوء على مظالم اجتماعية أخرى،زادت هجمات القرصنة بشكل كبير في السنوات الأخيرة، يرجع الارتفاع في

هذا النشـاط جزئياً إلى اعتمادنا الجماعي على الإنترنت ووسائل التواصل الاجتماعي وغيرها من أشكال الاتصال الرقمي ، فضلاً عن المشهد السياسي العالمي المشحون عاطفياً.على الرغم مـن أن العديد من نشـطاء القرصنة يدعون أن لديهـم نوايـا نبيلة ويعملـون غالباً في السـعي لتحقيـق المسـاواة أو العدالة أو تحسـين حقوق الإنسـان ، فمن المهـم أن نتذكـر أن القرصنة السـيبرانية تقع ضمـن فئة الجرائم السـيبرانية وإنهـا غير القانونيـة بغض النظـر عن دوافع المخترق أو نتائج الهجوم [٩].

ثانياً:انواع الهاكتفيزم.

تحـدث القرصنـة عندمـا يسـتخدم النشـطاء السياسـيون أو الاجتماعيـون تكنولوجيـا الكمبيوتـر لـلإدلاء ببيـان يدعم أحد أسـبابهم. فـي معظم الحـالات ، تركز أنشـطة القرصنة السـيبرانية على أهـداف حكومية أو شـركات ، ولكنهـا يمكن أن تشـمل أي مؤسسـة مهمة ، مثـل الجماعات الدينية أو تجـار المخدرات أو الإرهابيين أو المتحرشـين بالأطفال. القرصنة تعنـي اختـراق جهـاز كمبيوتـر لشـخص ما. يشـير النشـاط إلـى تعزيز منظـور اجتماعي. «القرصنة» هـي مزيج من الاثنين.على الرغم مـن أن جميع هجمات الناشـطين في القرصنة تهـدف إلـى تعزيـز أيديولوجيـة أو مواجهـة واحدة يراها نشـطاء القرصنـة تهديدًا لقضيتهم ، إلا أن أوجه التشـابه غالبًا ما تتوقف عند هذا الحد. تختلف الأسـاليب التي يستخدمها نشطاء القرصنة بشـكل كبير ، كما هو الحال بالنسـبة لشدة وشرعية أفعالهم.على سبيل المثال ، عندما ينظـم نشـطاء القرصنة حركة عبـر الإنترنت للترويـج للاسـتخدام المجانـي للإنترنت ، فلا يتعيـن عليهم خرق أي قوانين أو مهاجمة جهاز كمبيوتر أي شخص. من ناحية أخرى ، يمكن أن تتحول أنشـطة القرصنة السيبرانية إلى جريمة السيبرانية عند اسـتخدام الهجمات السيبرانية ، مثـل هجمات رفض الخدمـة (DoS) ، لتدمير أجهـزة الكمبيوتر والسـمعة وتكبد الشـركات أضـرارًا بملايين الـدولارات. فـي كثير من الحالات ، لا تشكل النشأة السيبرانية سوى تهديد للمنظمات أو الأشـخاص الذين يعتنقون اعتقادًا يتعارض مع موقف نشطاء القرصنة [١٠].

وتعد القرصنة كذلك شـكل من أشـكال النشاط الرقمـي غير العنيف حيث لا يكون الدافع ، في المقام الأول ، مكسباً مالياً شخصياً. بدلاً من ذلك ، تهدف حملات القرصنة السيبرانية إلى تحقيق العدالة السياسـية أو الاجتماعيـة أو الدينية بما يتماشى مع قضية المجموعة. يستخدم المتسللون تكتيكات مثل اسـتقصاء المعلومات والتشـويه ورفـض الخدمـة لاقتحـام أنظمة المؤسسـات الحكوميـة أو الخاصة.يقوم المتسـللون بخرق البيانات لأكثر من مجرد مكاسب مالية. بدلاً من ذلك ، تشـن أجندتهم المتميزة حرباً إعلامية من أجل الميل السياسـي أو العدالـة الاجتماعية أو النية الدينية أو الفوضى.اما اهم انواع القرصنة فهي كالتالي:

١-القرصنة السياسـية: تهدف القرصنة كشكل من أشكال التعبئة السياسية إلى إقناع السكان أو

التأثير عليهم لصالح أجندة الهاكرز.

٢-القرصنة الاجتماعية: تهدف العدالة الاجتماعية في القرصنة إلى إحداث تغيير مجتمعي.

٣-القرصنة الدينية: تهدف القرصنة من أجل أجندة دينية إلى تجنيد كيان ديني أو التنصل منه.

٤- القرصنة الفوضوية: يمكن أن يكون للقراصنة أجندة فوضوية للوصول إلى البنية التحتية المدنية أو المعدات العسكرية أو عامة السكان أو التحكم فيها[١١].

ثالثاً:طرق القرصنة:

لتحقيق أهدافهم ، يستخدم نشطاء القرصنة نفس الأساليب التي يستخدمها مجرمو الجرائم السيبرانية العاديون. وتعد الأكثر شيوعا هي:

١-التشويه - تغيير محتوى موقع الويب المستهدف ، وعادةً ما يتم نشر محتوى يروج لأفكار ناشطي القرصنة .

٢-Doxing - جمع معلومات سرية عن شخص أو منظمة لغرض مزيد من الإفصاح ؛

٣-DDoS - استخدام هجمات متزامنة من أجهزة متعددة لتعطيل مورد معين. يدعي الهاكرز عادة مسؤوليتهم عن مثل هذه الهجمات ويعبرون علانية عن دوافعهم ؛

٤-القصف الجغرافي - استخدام العلامات الجغرافية على (YouTube) لربط مقاطع فيديو متعددة حول قضية اجتماعية معينة بنقطة محددة على الخريطة. تظهر مقاطع الفيديو التي تحمل علامات جغرافية على(Google Earth) في الموقع المقابل.

يتخصص نشطاء القرصنة الآخرون في إنشاء وتوزيع الأدوات ، مثل المتصفحات الآمنة وتطبيقات المراسلة ، ومجهولي الهوية ، ووسائل تجاوز قيود المحتوى ، لمشاركة المعلومات غير الخاضعة للرقابة[١٢].

ثالثاً:مجموعات الهاكتفيزم.

يعمل بعض نشطاء الهاكتفيزم بمفردهم ، والبعض الآخر في فرق. يمكن أن يكون نشطاء القرصنة الأفراد جزءاً من عدة مجموعات في وقت واحد. أصبح عدد قليل من الجماعات الناشطة في مجال القرصنة مشهورا نسبيا ولعل ابرزها.

١-المجهول(Anonymous).

واحدة من أكثر مجموعات الاختراق شهرة ، أعلنت(Anonymous) مسؤوليتها عن العديد من الهجمات السيبرانية ، بما في ذلك تلك التي استهدفت كنيسة السيانتولوجيا ومنظمات مكافحة القرصنة. و(Anonymous) هي مجموعة لامركزية تعمل في جميع أنحاء العالم.

٢-عبادة البقرة الميتة.

يعود الفضل إلى أحد أعضاء المجموعة الملقب (بأوميغا) في صياغة مصطلح hacktivism))مرة أخرى في العام ١٩٩٦. في عام ١٩٩٩ شكلت المجموعة فرعاً لها (Hacktivismo

)، متخصص في تقنيات مكافحة الرقابة ويدعو إلى النشر المجاني لأي معلومات. طورت طائفة البقرة الميتة وأصدرت العديد من الأدوات لكل من القرصنة ومشاركة المعلومات من خلال إخفاء المعلومات والتشفير [١٣].

رابعا: كيف تعمل الهاكتفيزم؟

تسعى الهاكتفيزم عادة إلى تحقيق واحد أو أكثر من الأهداف التالية[١٤]:

١- وقف تمويل الإرهاب.

٢-تجاوز قوانين الرقابة التي وضعتها الحكومة.

٣-التحدث ضد الحرب.

٤-استخدم وسائل التواصل الاجتماعي لمساعدة الأشخاص الخاضعين للرقابة أو أولئك الذين يتم انتهاك حقوقهم.

٥-التحدث ضد الرأسمالية.

٦-مهاجمة المواقع الحكومية التي تحاول قمع الاضطرابات السياسية.

٧-تعزيز الديمقراطية وحرية التعبير.

٨-مساعدة المهاجرين على تجاوز حدود البلد.

٩-مساعد الانتفاضات المحلية

١٠-تقويض قوة الشركات

خامساً: تاثيرات الهاكتفيزم.

يكشف التحليل أن ممارسات الهاكتفيزم لها تأثير إيجابي وسلبي في الأمن القومي وعملية صنع القرار وذلك من خلال التالي .

١- التأثير في الأمن القومي

توضح حالة المتسللين النزعة المتزايدة للحكومات لتصوير العصيان المدني الإلكتروني (ECD) على أنه نشاط إرهابي. على سبيل المثال ، أعرب مدير وكالة الأمن القومي الامريكي عن قلقه من أن يكون لدى (Anonymous) قريبًا القدرة على التسبب في انقطاع محدود للتيار الكهربائي من خلال الهجمات السيبرانية. ومع ذلك ، ليس من الصحيح الادعاء بأن القرصنة ليست سوى تهديد للأمن القومي أو أمن الشركات. يساعد الهاكرز الدول والشركات على إيجاد نقاط ضعف في أنظمتها المعلوماتية لحماية خصوصية المستهلك وأمان الإنترنت. هناك العديد من الحالات التي ساعدت فيها هجمات وأدوات نشطاء القرصنة على تحسين حماية بيانات العملاء وبرامجهم.

٢- تأثير في عملية صنع القرار.

الاعتقاد أن تنمية الطفولة المبكرة على وجه الخصوص يمكن أن يعيد المواطنين المهمشين إلى وضعهم كمشاركين في العمليات التشريعية ، ويزيل الإجراءات الديمقراطية الرسمية التي قد يشعرون بأنهم مستبعدون منها. يجب أن تتعود الهيئات الحكومية على نوع جديد من النشاط ، مجهول الهوية ولا مركزي ، لذلك لن يتم استخدام التدفق النقدي أو التهديد

بالعقـاب أو العنف كآلية للسـيطرة على الدولة. بفضـل تكنولوجيا المعلومـات الجديدة وظهور مفهـوم القرصنة السـيبرانية ، حصل الشـباب على فرصة ليس فقط للترويج لآرائهم السياسية الخاصة ولكـن أيضًا لأداء بعض الأعمال ذات الدوافع السياسـية. ومع ذلك ، تكشف العديد من الاعتقـالات والإدانـات الجنائيـة للمتظاهرين عبر الإنترنت أن الافتراض الرسـمي العام هو اعتبار القرصنة جريمة ، وليس ممارسة لحقوق المشـاركة وحرية التعبيـر. الهاكتفيزم ، الذين يلتزمون عمومًـا بالقيم التحرريـة الإلكترونية أو الفوضويـة ، يسـاهمون فـي لامركزيـة السـلطة وزيادة المساءلة ، بالإضافة إلى عملية صنـع قرار تكـون أكثر اسـتنارة وديمقراطية ونتيجـة لذلك تكـون عملية صنع القـرار أكثر كفـاءة. ومع ذلك ، فمن المشـكوك فيه أن تكون "النزعة التنظيمية اليومية لأصحاب المصلحة المتعددين" التي تشـير إلى تفاعلات ديناميكية تواتـراً بين الجهـات الفاعلـة الحكومية وغير الحكومية قد تكون راسخة بالكامل[١٥].

سادساً: هاكتفيزم القبعات البيضاء والسوداء.

١- هاكتفيزم القبعات البيضاء.

قراصنـة القبعة البيضاء أولئك الذين يسـعون لتحقيق أهداف مشـروعة وقد حصلوا على إذن لأنشـطتهم. غالبًا ما يتم توظيف هؤلاء الأفراد بواسـطة شـركات مختلفـة لاختبـار أنظمتهم الأمنية والعثور على نقاط الضعف الأمنية. على سبيل المثال ، فيما يتعلق بمشكلة أمنية محتملة ، قد تستخدم مجموعة من قراصنة القبعة البيضاء أساليب مماثلة يسـتخدمها المتسللون الضارون من أجل العثور علـى الثغرات المحتملة. ولكن بدلاً من التسـبب في ضرر أو سرقة البيانات ، سـيتم القيام بذلك من أجـل تحديد نقاط الضعف ووضع إرشـادات حـول كيفيـة معالجتها. من المسـاهمات المهمة للمتسللين البيض في مجال الأعمال تأثيرهم في تأمين شبكات الشركة وبهذه الطريقة حماية الأسـرار التجارية والممارسات التجارية. علاوة على ذلك يساعد قراصنة القبعة البيضاء فـي ضمان أمان منتج البائع،من المهم ملاحظـة أنه يمكـن توظيف قراصنـة القبعات البيضـاء فقط من قبل شـركة واحـدة أو العمل كمسـتقل ومسـاعدة العديد من الشركات. ومن المثيـر للاهتمـام ، أن هناك مواقـف يقدم فيها قراصنة القبعات البيضاء خدماتهم مجانًا لبعض المؤسسات أو الهيئات الأخرى المحتاجة. على سـبيل المثال ، خلال جائحـة (COVID-١٩)، كان هناك ارتفاع فـي الهجمات الإلكترونية ضد المستشـفيات ، مما أدى إلى قيام مجموعة مـن المهنيين بإنشـاء(Cyber Alliance to Defend Our Healthcare)، والذي يهدف إلى مسـاعدة المستشـفيات على تقويـة أنظمة الأمن السـيبراني وتجنـب المخاطر والهجمات المضادة.

٢-هاكتفيزم القبعات السوداء.

قراصنـة القبعـات السـوداء من ناحيـة أخرى يتصرفـون بطريقة غير القانونيـة ، في كثير مـن الأحيـان عندما نفكر في المتسـللين ، فإننا

نفكر في هذه المجموعة الفرعية التي في السعي لتحقيق مكاسب مالية ، على سبيل المثال ، تسبب ضررًا لنا ولمجتمعاتنا. تتضمن بعض الأساليب التي يستخدمها هؤلاء المخترقون غالبًا .التصيد-برامج الفدية-الديدان-الفيروسات-هجمات DoS / DdoS-سرقة ملفات تعريف الارتباط.

٣-هاكتفيزم القبعات الرمادية.

يجلس هؤلاء المخترقون على تقاطع بين القبعات البيضاء والسوداء ، وبالتالي فإن أنشطتهم تثير أكثر النقاشات الأخلاقية. يمكن أن يكونوا يسعون وراء أهداف أيديولوجية أعلى ، أو يمكن أن يتأثروا مرة أخرى بحوافز شخصية بحتة مثل البحث عن الترفيه. قد يكسرون بعض القيود القانونية ، لكنهم في النهاية لن يسعوا إلى التسبب في ضرر. تلتزم معظم القبعات الرمادية بفهمها الشخصي للأسئلة الأخلاقية ومبادئها الأخلاقية الراسخة[١٦].

سادساً: اخلاقية الهاكتفيزم.

هناك قضية أخلاقية مهمة أخرى تتعلق بوجود ما يسمى ب «النشطاء»، ينفذ هؤلاء الأفراد عمليات اقتحام إلكترونية غير قانوني في إطار السعي المزعوم لهدف أيديولوجي و / أو حماية القيم الأخلاقية مثل حرية التعبير والمساواة وما إلى ذلك. يتم استخدامها فيما يتعلق ببعض الأجندة السياسية أو الاجتماعية التي ينفذها الأفراد لأغراض سياسية خاصة بهم ، وغالبًا ما يكون هذا العنصر السياسي بمثابة تبرير مركزي للاختراق. يثير هذا العديد من المعضلات الأخلاقية [١٧].

يجادل المدافعون عن القرصنة بأنهم حراس ، متمردون ولهم سبب وجيه. يستخدمون نفس الأدوات والبرامج والأساليب والأجهزة التي يستخدمها المتسللون الفعليون من أجل الوصول إلى الشبكة أو قاعدة البيانات أو الأجهزة الخاصة بمؤسسة ما. يقوم المتسللون بمهاجمة أنظمة الكمبيوتر الآمنة واختراقها. غالبًا ما يكون هدف نشطاء القرصنة شركات كبيرة أو هيئات حكومية. نظرًا لأن نشطاء القرصنة يتصرفون بحس من الضمير السياسي ، فقد يهاجمون أيضًا الشركات والمنظمات الأصغر. يهدف الهاكرز إلى تحقيق مكاسب مالية ، ولهذا السبب يستهدفون في الغالب مؤسسات أكبر ، ولكن لا يسعى نشطاء القرصنة لتحقيق مكاسب مالية ، ولهذا السبب يمكن لأي مؤسسة تقريبًا ، بغض النظر عن حجمها ، أن تكون هدفًا للقرصنة.يستخدم الهاكرز الأدوات والأساليب والبرامج نفسها التي يستخدمها المتسللون: البرامج الضارة والفيروسات وأحصنة طروادة وديدان الكمبيوتر والتصيد الاحتيالي والعديد من البرامج الضارة الأخرى بالإضافة إلى هجمات DDoS وهجمات القوة الغاشمة والأساليب المماثلة

ومرة أخرى ، على غرار المتسللين ، يهدف نشطاء القرصنة إلى جمع أو كشف معلومات حساسة. ومع ذلك ، على عكس المتسللين ، يقوم نشطاء القرصنة بمثل هذه الإجراءات

بغرض كشف الحقيقة القبيحة ، أو مساعدة المجتمع المدني أو اكتساب نفوذ في الدفاع عن معتقداتهم وأيديولوجيتهم[١٨].

سادسا: الحد من تاثير هجمات الهاكتفيزم.

للحد من التاثيرات السلبية للجمات مجموعات الهاكتفيزم لابد من اعتماد استراتيجيات :

١-الاستثمار في توظيف فريق خبير في تكنولوجيا المعلومات و / أو الأمن السيبراني.

٢-تحديد أولويات الأصول الخاصة وخطط لاستراتيجية الأمن السيبراني الخاصة حول العناصر الأكثر أهمية.تثقيف موظفي تكنولوجيا المعلومات وغيرهم ، حتى تتمكن المؤسسة من الحصول على واجهة أقوى ضد التصيد الاحتيالي والهجمات المماثلة.

٣-تحديث أنظمة التشغيل وجدران الحماية وبروتوكولات الأمان وبرامج مكافحة الفيروسات والأدوات المماثلة بانتظام.

٤-وضع جدولة وإجراء اختبارات منتظمة لاكتشاف نقاط الضعف في أنظمه والتخفيف منها.

٥-وضع خطة طوارئ في حالة حدوث هجوم. والتأكد من أن أعضاء فريق تكنولوجيا المعلومات و / أو فريق الأمن السيبراني يعرفون دورهم في مثل هذا الحدث [١٩].

ثامنا: مستقبل الهاكتفيزم.

يبقى السؤال هو ماذا يحدث للمتسللين الذين اكتسبوا خبرة كبيرة طوال الصراع وهم يقومون في كثير من الأحيان بهجمات سيبرانية معقدة؟ نظرًا لأن الحكومات قد تتطلع إلى تجنيد الأفراد ، فمن المرجح جدًا أن يتطلع الفاعلون المعنيون بالتهديد الإجرامي إلى فعل الشيء نفسه. إن مجموعات برامج الفدية التي تتطلع باستمرار إلى تجنيد «شركاء تابعين» لعملياتها ستجذب بالتأكيد أفرادًا مؤهلين بوعود بتحقيق مكاسب مالية وسمعة سيئة ، وهو أمر طالما كان العديد من نشطاء القرصنة يتوقون إليه. ومن المحتمل أيضًا أن نسبة كبيرة من العناصر الناشطة في مجال القرصنة المتورطة في النشاطات الحالية لهم روابط بالفعل بالنشاط الإجرامي السيبراني ، وبالتالي من المرجح أن يعودوا إلى «وظائفهم اليومية» مع انتهاء الصراع [٢٠].

الخاتمة:

العمل على دراسة الابعاد السياسية للتطور الكبير في مجال الحاسوب من الدراسات المهمة التي تفرض الاهتمام بها ، خاصة بعد ان تم استخدام الحاسوب والتطور في مجال الاتصالات للتأثير في الظاهرة السياسية التي اصبحت ميدان من ميادين الهاكتفيزم من خلال التاثير في الراي العام وممارسة الضغط على الحكومات والقوى السياسية لتحقيق اهداف سياسية وحماية حقوق الانسان .ولاهمية الموضوع لابد من الاهتمام بالتوصيات التالية في العراق.

١-يعد موضوع الهاكتفيزم من الموضوعات

المهمــة والتي لاتزال كتابــات عنها في العراق نادرة الامر الذي يفرض الاهتمام به خاصة في مجال الامن السيبراني.

٢-اســهم التطــور الكبيــر في مجــال توظيف الحاســبات واســتخدامها فــي ان تكــون احدى الفواعــل غيــر المرئيــه في مختلــف مجالات وميادين الحياة ومنها المجال السياسي والامني والعســكر، وفــي العــراق نجد زيــادة واضحة للتاثيــر ذلك التوظيف خاصة مع تشــكل فضاء سيبراني عراقي .

٣- لابد من بناء وحدة امنية سيبرانية ترتبط باحد الاجهــزة الامنية العراقية يقع عليها مســؤولية التعامل مع تهديدات مجموعات الهاكتفيزم.

٤-العمل على تأســيس مجموعات من هاكتفيزم ترتبط بصورة غير المباشرة باحدى المؤسسات الامنية الرسمية يمكن الاعتماد عليها للرد على هجمــات الهاكتفيزم التي تســتهدف مؤسســات الدولة الرســمية وبالاخص المؤسســات الامنية ـدفاع-داخلية-مكافحــة الارهاب-الحشــد الشعبي...الخ.

٥-تعــد التشــريعات القانونية من اســس حماية المؤسسات والمجتمع لذلك لابد تضمينها قوانين تكون مسؤولة عن معاقبة اي سلوك يمارس من مجموعــات الهاكتفيزم يحمل تهديد للاســتقرار السياسي والاجتماعي والاقتصادي في العراق.

الهوامش

1-https://encyclopedia.kaspersky.com/glossary/hacktivism/.

2- SecAlliance, The Changing Landscape of Hacktivism, April 21, 2022, https://www.secalliance.com/blog/the-changing-landscape-of-hacktivism,28-2-2023.

3- https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hacktivism/.

4- Aydelia Gareeva,Kira Krylova,Olga Khovrina, Hacktivism: a new form of political activism, JOURNAL OF SOCIETY AND THE STATE

SCHOOL OF GOVERNANCE AND POLITICS, MGIMO UNIVERSITY, RUSSIA, noverber 2020, https://sgp-journal.mgimo.ru/2020/2020-7/hacktivism,17-1-2023.

5-What is Hacktivism, https://www.sangfor.com/glossary/cybersecurity/what-is-hacktivism-in-cybersecurity20 -7-2022-24-6-2023.

6 - Doxing هــي ممارســة جمــع ونشــر معلومات شــخصية أو خاصة عن شــخص مــا علــى الإنترنت. إنها مشــتقة مــن كلمة »document«/»dox« وقــد ظهــرت “ كتكتيــك انتقامــي فــي ثقافــة القرصنة في

التسـعينيات. تتراوح طرق الحصول على معلومات حول الشـخص الذي يتم التشهير به بين استخدام قواعد البيانات العامة القابلة للبحـث ومنصـات الوسـائط الاجتماعيـة واختـراق الحسـاباتFacebookمثـل الشـخصية. https://www.cybersmile.org/advice-help/doxing

7- Patrick Putman, What is a Hacktivist?, https://www.uscybersecurity.net/hacktivist/,5-1-2023.

8-https://www.sentinelone.com/cybersecurity-101/hacktivism/.

9 - HACKTIVISM: WHAT YOU NEED TO KNOW

May 6, 2021, https://www.crowdstrike.com/cybersecurity-101/hacktivism/.

10 - Hacktivism—A Cyberattack? Meaning, Types, and More, https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism,5-1-2023.

11 - What is Hacktivism? Campaigns That Shaped the Movement, June 23, 2020, https://www.pandasecurity.com/en/mediacenter/technology/what-is-hacktivism/.

12 - https://encyclopedia.kaspersky.com/glossary/hacktivism/.

13 - https://encyclopedia.kaspersky.com/glossary/hacktivism/.

14 - Hacktivism—A Cyberattack? Meaning, Types, and More,Op[,Cit.

15 - Aydelia Gareeva,Kira Krylova,Olga Khovrina, Hacktivism: a new form of political activism,Op,Cit.

16 -Denitsa Kozhuharova, Atanas Kirov & Zhanin Al-Shargabi, Home Cybersecurity of Digital Service Chains Chapter

Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them?, https://link.springer.com/chapt

er/10.1007/978-3-031-04036-8_9.

17 -Ibid.

18 - What is Cyber Hacktivism?, https://www.logsign.com/blog/what-is-cyber-hacktivism/,5-1-2023.

19 -Iide, Op, Cit.

20 -The Changing Landscape of

Hacktivism, 21April, 2022, https://www.secalliance.com/blog/the-changing-landscape-of-hacktivism.

الملخص:

التحول نحو الفضاء السيبراني أعاد تشكيل جوانب الحياة، مؤثرًا بعمق على الأفراد والمجتمعات، حيث نعيش مرحلة حضارية جديدة تتميز بطرق تفاعل وأدوات وأطراف وعوامل فاعلة مختلفة. من بين هذه العوامل البارزة يظهر مفهوم "الهاكتيفيزم" الذي وجد في الفضاء السيبراني مجالاً واسعاً للنشاط، خاصة في المجالات السياسية لتحقيق أهداف باستخدام التكنولوجيا الرقمية. أهمية موضوع الهاكتيفيزم تستدعي دراسة متأنية وشاملة، حيث تُوظف الشبكات الحاسوبية لتحقيق أهداف سياسية واجتماعية. أصبحت التكنولوجيا أداة قوية للتأثير والتغيير في العالم الحديث، مما يبرز ضرورة فهم هذه الظاهرة وتأثيراتها.

الكلمات الافتتاحية:الهاكتفيزم-الشبكات الحاسوبية-القبعات السود والبيض والرمادية-اخلاق الهاكتفيزم.

The shift towards cyberspace has significantly reshaped various aspects of life, affecting individuals and communities deeply. We are now in a new cultural phase characterized by different methods of interaction, tools, participants, and active factors. One notable factor is "hacktivism," which thrives in cyberspace, especially in political realms, where activists use digital technology to achieve their goals. Studying the political dimensions of this technological advancement is crucial, as computers and communications developments have been utilized to influence political phenomena. Hacktivism has become a means to sway public opinion and pressure governments and political forces, aiming to achieve political goals and protect human rights.

Hacktivism:

Using computer networks to promote political agendas

DR.Basim Ali KHarisan