



الحروب الناعمة بين البعد الثقافي والواقع الأمني

Soft Wars, Amid Cultural Dimension and the Security Reality

خيرالدين بوهدة¹

¹ جامعة يحي فارس، المدية (الجزائر)، khiri99@gmail.com

ملخص

عادة ما تتجنب القوة الناعمة أدوات السياسة الخارجية التقليدية المتمثلة في الجزرة والعصا فهي ترفض استعمال تلك الأساليب الكلاسيكية، فهي تسعى وراء التأثير من خلال بناء الشبكات الرقمية، ونقل الأخبار المقنعة، ووضع القواعد الدولية، والاعتماد على الموارد التي تجعل بلدًا ما جذابًا بشكل طبيعي للعالم. يؤثر انتشار التقنيات الرقمية في كل مكان في وسائط الاتصال الجديدة بشكل متزايد على عمل صانعي السلام، مما يغير ممارسات بناء السلام وديناميكيات الصراع. لكن يشكل الاستخدام الضار لتكنولوجيا الاتصالات تهديدات جديدة للمجتمعات المسالمة ويدفع بناء السلام إلى التفكير في مجالات عمل جديدة في الفضاء الإلكتروني. وعليه فإن سؤال إشكالية هذه الورقة: ما هي الأساليب التقنية التي يمكن استخدامها لمواجهة الحروب الناعمة في وسائط الاتصال الجديدة؟ إبراز أهمية الرقمنة في تغيير ديناميكيات الصراع في وسائط الاتصال الجديدة.

الكلمات المفتاحية: وسائط الاتصال الجديدة؛ الرقمنة؛ الحروب الناعمة؛ أمن المعلومات.

Abstract

Usually, soft power eschews the traditional carrot-and-stick foreign policy tools of these classic tactics. It seeks influence by building digital networks, conveying persuasive news, setting international rules, and relying on the resources that make a country naturally attractive to the world. The ubiquity of digital technologies in new media of communication is increasingly affecting the work of peacemakers, altering peacebuilding practices and conflict dynamics. But the harmful use of communication technology poses new threats to peaceful



societies and is prompting peacebuilders to consider new areas of work in cyberspace. The problematic question of this paper is: What are the technical methods that can be used to confront soft wars in the new means of communication? Highlighting the importance of digitization in changing the dynamics of conflict in the new means of communication.

Keywords: new media; digitization; soft wars; information security.

مقدمة

هناك طرق وأدوات مختلفة لتوفير الأمن وهي تتأثر بثلاثة أنواع من القوة: العسكرية والاقتصادية وقوة الجذب. الأمن الناعم هو نوع من الأمن يمكن إنشاؤه من خلال قوة الجذب في المجتمع. القوة الناعمة هي القدرة على الحصول على النتائج المفضلة عن طريق الجذب بدلاً من الإكراه أو الدفع. (Jr, 1990) تتجنب القوة الناعمة أدوات السياسة الخارجية التقليدية المتمثلة في الجزرة والعصا، وتسعى بدلاً من ذلك إلى تحقيق التأثير من خلال بناء الشبكات، وتوصيل الاخبار المقنعة، ووضع القواعد الدولية، والاعتماد على الموارد التي تجعل بلدًا ما جذابًا بشكل طبيعي للعالم. اليوم يؤثر الانتشار الواسع للتقنيات الرقمية في وسائط الاتصال الجديدة بشكل متزايد على عمل صناعات السلام، مما يغير ممارسات بناء السلام وديناميكيات الصراع. حيث يشكل الاستخدام الضار للتكنولوجيا الاتصال تهديدات جديدة للمجتمعات المسلمة ويحث بناء السلام على التفكير في مجالات عمل جديدة في الفضاء الإلكتروني. وعلى هذا الأساس فإن هذه الورقة البحثية تطرح الإشكالية التالية: ماهي الاساليب التقنية التي يمكن استخدامها لمواجهة الحروب الناعمة في وسائط الاتصال الجديدة؟ مبرزاً أهمية الرقمة في تغير ديناميكية الصراع في وسائط الاتصال الجديدة.

مفاتيح البحث.

1-1 وسائط الاتصال الجديدة:

إنه مصطلح شامل ظهر لأول مرة في الثمانينيات من القرن الماضي ويشير إلى الوسائط المعتمدة على الكمبيوتر. ولقد عرفت بأنها تلك الوسائط الجديدة (من مقالات صحفية، مدونات، فيديوهات...) التي يتم تسليمها رقمياً. (Cote, 2020) ينطبق المصطلح أيضاً على مجموعة واسعة من الظواهر والممارسات: أنواع



جديدة من الأشكال النصية ومنتعة الترفيه (ألعاب الفيديو ، الإنترنت ، العالم الافتراضي) ؛ أنماط جديدة لاستهلاك الوسائط (التقارب ، النص التشعبي) ؛ طرق جديدة لتمثيل العالم (المدونات، الرقمنة، التصوير الفوتوغرافي) ، الذات (الصورة الرمزية ، الصفحة الرئيسية الشخصية) ، والمجتمع (لوحات الإعلانات غرف الدردشة، الشبكات الاجتماعية)؛علاقات جديدة بين منتجي وسائل الإعلام المستهلكين (مشاركة الملفات ، اقتصاد الهدايا ، الثقافة التشاركية ، المحتوى الناتج عن المستخدم)، والتجارب الظواهر الجديدة(التجسيد، الانغماس، الحضور). تميل وسائل الإعلام الجديدة إلى طمس التمييز بين التواصل بين الأفراد والاتصال الجماهيري (النشر المكتبي، البث المحدود، المجالات العامة والخاصة) (Communication, 2021).

2-1 الرقمنة:

مما لا شك فيه تعني الرقمنة (Digitization) بشكل أساسي إلى أخذ المعلومات التناظرية وترميزها إلى الصفر والواحد حتى تتمكن أجهزة الكمبيوتر من تخزين هذه المعلومات ومعالجتها ونقلها.(Bloomberg, 2018) ويشير أيضا قاموس المصطلحات لتكنولوجيا المعلومات من Gartner "الرقمنة هي عملية التغير من النموذج التناظري إلى الشكل الرقمي". وهناك تعريف آخر قريب من الأول (Digitalisation) ليس تقنيا، حيث عرف Scott Brennen و Daniel Kreiss من جامعة نورث كارولينا بالولايات المتحدة الأمريكية حيننا قلا: "نشير إلى الرقمنة على أنها الطريقة التي يتم بها إعادة هيكلة العديد من مجالات الحياة الاجتماعية حول الاتصالات الرقمية والبنى التحتية لوسائل الإعلام." (Bloomberg، 2018) وبالتالي، يبني برينن وكريس تعريفهما للرقمنة على الحياة الاجتماعية، وبعبارة أخرى، كيف يتفاعل الناس. مع انتقال هذه التفاعلات بعيدًا عن التقنيات التناظرية (البريد العادي والمكالمات الهاتفية) إلى التقنيات الرقمية (البريد الإلكتروني والدردشة والوسائط الاجتماعية)، تصبح مجالات العمل والترفيه على حدٍ سواء رقمية. (Bloomberg، 2018)

3-1 الحروب الناعمة

يقصد بالحرب الناعمة ذلك انه عندما تستخدم دولة ما النفوذ الثقافي والاقتصادي لإقناع الدول الأخرى بفعل شيء ما بدلاً من استخدام القوة العسكرية. عندما يتعلق الأمر بالقوة الناعمة، تعد ألمانيا الآن واحدة من أقوى الدول على وجه الأرض.(Dictionary, 2021) حيث تمت الإشارة إلى القوة الناعمة على أنها شكل



من أشكال القوة الوطنية التي تقوم على الجاذبية الفكرية والثقافية، والتي يتم استخدامها عن قصد أو عن غير قصد من قبل الجهات الفاعلة في العلاقات الدولية لتحقيق الضرورات الاستراتيجية. (Nye, 2017)

حدد جوزيف ناي مبتكر المفهوم، في البداية ثلاثة مصادر رئيسية للقوة الناعمة أثناء تطويره للمفهوم. الركائز الثلاث للقوة الناعمة لدى ناي هي: القيم السياسية، والثقافة، والسياسة الخارجية. (Portland, 2021). ولكن ضمن هذه الفئات الثلاث، فإن المصادر الفردية للقوة الناعمة متعددة ومتنوعة. (Portland, 2021)

1-4 أمن المعلومات

أمن المعلومات، الذي يُختصر أحياناً بـ infosec، عبارة عن مجموعة من الممارسات التي تهدف إلى الحفاظ على البيانات آمنة من الوصول أو التعديلات غير المصرح بها، سواء عند تخزينها أو عند نقلها من جهاز أو موقع مادي إلى آخر. قد ترى أحياناً أنه يشار إليه بأمان البيانات. نظراً لأن المعرفة أصبحت واحدة من أهم أصول القرن الحادي والعشرين، فقد أصبحت الجهود المبذولة للحفاظ على أمن المعلومات ذات أهمية متزايدة في المقابل. (Fruhlinger, 2020) وغالباً ما يتم تلخيص المكونات الأساسية لأمن المعلومات من خلال ما يسمى القواعد الثلاثة لوكالة المخابرات المركزية: السرية والنزاهة والتوافر.

1-4-1 السرية.

ربما تكون السرية هي عنصر الثالوث الذي يتبادر إلى الذهن على الفور عندما تفكر في أمن المعلومات. تكون البيانات سرية عندما لا يتمكن من القيام بذلك سوى الأشخاص المصرح لهم بالوصول إليها؛ لضمان السرية، يجب أن تكون قادرًا على تحديد من يحاول الوصول إلى البيانات وحظر المحاولات من قبل أولئك الذين ليس لديهم تصريح. كلمات المرور والتشفير والمصادقة والدفاع ضد هجمات الاختراق كلها تقنيات مصممة لضمان السرية. (Brathwaite, 2021)

1-4-2 النزاهة

لحماية المعلومات من التعديل من قبل أشخاص غير مصرح لهم ولضمان أن المعلومات جديدة بالثقة ودقيقة. قد يتم تعديل المعلومات في أي وقت بواسطة شخص غير مصرح له بذلك، سواء كان شخصاً داخل الشركة أو خارجها، فهذا يعد انتهاكاً لسلامة المعلومات. على سبيل المثال، إذا أرسل رئيس المكتب المالي وثيقة



لفحصها أو مراجعتها من قبل مدير المالية. قد يحاول مدير المالية التلاعب بالمعلومات دون علم المدير المالي من أجل جعل إدارته تبدو أفضل، وغسل الأموال، إلخ. (Brathwaite, 2021)

1-4-3 التوافر

التوافر هو صورة طبق الأصل للسرية: بينما تحتاج إلى التأكد من أن بياناتك لا يمكن الوصول إليها من قبل مستخدمين غير مصرح لهم، فإنك تحتاج أيضًا إلى ضمان إمكانية الوصول إليها من قبل أولئك الذين لديهم الأذونات المناسبة. يعني ضمان توفر البيانات مطابقة موارد الشبكة والحوسبة مع حجم الوصول إلى البيانات الذي تتوقعه وتنفيذ سياسة نسخ احتياطي جيدة لأغراض التعافي من الكوارث. (Fruhlinger, 2020)

2- واقع منصات وسائل التواصل الاجتماعي

قبل التحدث عن أهم الأخطار الأمنية في العالم الافتراضي لا بد من التحدث عن منصات وسائل التواصل الاجتماعي منذ ظهورها. فبالإضافة إلى ما يتعلق بأعداد المستخدمين على هذه الوسائط فهي جد مرتفعة، وهذه بعض هذه الأرقام: (work, 2021)

2.45 - مليار مستخدم نشط شهريًا على Facebook

300 مليون مستخدم نشط شهريًا على Twitter

مليار مستخدم نشط شهريًا Instagram

شعبية مثل هذا تعني أن وسائل التواصل الاجتماعي مثل العسل بالنسبة للدبور حيث يتعلق الأمر بالجرائم الإلكترونية. يرى المحتالون مستخدم وسائل التواصل الاجتماعي على أنهم جمهور أسير وموثوق، يمكن التلاعب به لأداء أعمال يكونون عادة أكثر يقظة حيالها. قامت وسائل التواصل الاجتماعي ببناء منصة فعالة، ليس فقط لمشاركة الأفكار وصور القطط، ولكن كملعب للجرائم الإلكترونية. (work, 2021)

3- الثقافة في العالم الافتراضي



الواقع الافتراضي، كأداة تكنولوجية، لا يمتلك في حد ذاته أي سمات ثقافية أو اجتماعية. إنها أداة يستخدمها المستخدمون ومنشئوها لتحقيق أهداف معينة بما في ذلك الترفيه والتعليم والتدريب وخلق تجربة افتراضية للسلامة والسياحة وغيرها. (Buliva, 2018)

يعود اهتمام فنان الفيديو بيل فيولا بفكرة "مساحة البيانات" منذ الثمانينيات كوسيلة لتسجيل التاريخ الثقافي في الفضاء الإلكتروني أو الافتراضي، المستوحى من "قصص الذاكرة" للمعابد اليونانية والكاتدرائيات القوطية. (Packer, 2021) قارن فيولا هذه الأوعية المعمارية القديمة للمعرفة بالكمبيوتر الشخصي المعاصر بقدرته على التخزين واسترجاع المعلومات والوصول الفوري. وفقًا لفيولا، فإن الزخرفة الرمزية واللوحات والنوافذ ذات الزجاج الملون للكاتدرائيات الأوروبية قد تكون بمثابة نموذج للمسارات المتفرعة والبيئات شديدة التوسط لأعمال الفيديو التي يتم التحكم فيها بواسطة الكمبيوتر، مما ينتج عنه ما يشير إليه بـ "مساحة الفكرة" - الأساس المفاهيمي لتطبيقات الواقع الافتراضي الحديثة التي تستخدم محاكاة ثلاثية الأبعاد لمساحة المعلومات. (Packer, 2021)

من جانب آخر صاغ ويليام جيبسون مصطلح الفضاء الإلكتروني في روايته الخيال العلمي عام 1984 نيورومانسر بإضافة هذا المصطلح إلى المفردات المعاصرة ، أعطى جيبسون معنى أدبيًا للأسلاك والمحاور والشبكات وأجهزة الكمبيوتر التي تشكل المظهر المادي لفضاء المعلومات الافتراضي الأكثر تجريداً (Packer, 2021). فيما بعد طور عالم الكمبيوتر بافيل كيرتس واحدة من أولى البيئات متعددة المستخدمين في Xerox PARC (مركز بالو ألتو للأبحاث) في أوائل التسعينيات ، بعنوان LambdaMOO ، وتم تصميمها كواقع افتراضي قائم على النص. كان الهدف من بحثه هو استكشاف الظواهر الاجتماعية في الفضاء الافتراضي في الوقت الفعلي ويعتبر رائد "غرفة الدردشة". (Packer, 2021)

عند النظر إلى التطور التاريخي للواقع الافتراضي وتأثيره الثقافي، نرى الطبيعة الخالدة والدورية للتعبير البشري من الأحلام والتمثيلات كما تم تصويرها في كهوف ما قبل التاريخ في لاسكو؛ لتجربة الشمولية لـ *Gesamtkunstwerk*؛ إلى الأشكال الرقمية الحديثة للتجربة المتعددة الأبعاد وحالات الوعي المتغيرة. (Packer, 2021)

4- أهم الأخطار الأمنية التي يواجهها المجتمع الافتراضي



قبل التحدث عن الأخطار الأمنية التي يصادفها المجتمع الافتراضي والاشكالية المطروحة و المتمثلة عن الأساليب الأمنية التي تحد من انتشار و توسع التهديدات الامنية، لا بد من الإشارة الى أهم التهديدات عبر الفضاء الافتراضي. أكثر من 90٪ من التهديدات المتقدمة التي تستهدف الشركات تأتي من البريد الإلكتروني، ومع ذلك يتم تخصيص جزء صغير جدًا من ميزانية الأمان لتأمين قناة الاتصال الحيوية هذه. لا يزال أمان الشبكة ونقطة النهاية يحصل على نصيب الأسد من ميزانيات الأمن السيبراني اليوم. (paper, 2021) تكمن المشكلة في أن غالبية التهديدات الإلكترونية المتقدمة تستهدف الأشخاص الذين يستخدمون البريد الإلكتروني ووسائل التواصل الاجتماعي وتطبيقات الهاتف المحمول كوسيلة للوصول إلى مؤسسة ما، وسرقة المعلومات والمال، وربما الإضرار بسمعة المؤسسة. Katie Yun هي مستشارة رقمية لها خبرة تزيد عن 10 سنوات في التسويق ووسائل التواصل الاجتماعي والاستراتيجية الرقمية. تري خمس تهديدات شائعة لوسائل التواصل الاجتماعي. (Yun, 2020) هنا نذكر فقط أنها سوف تعرض فقط الحيل والانتهاكات عبر الوسائط الاجتماعية.

4-2-1 إهمال الحساب؛

المحادثات الاجتماعية حول نشاطك التجاري والتي لا تعرفها تمثل ثغرة أمنية. عندما لا تتحقق بانتظام من الحسابات الاجتماعية لوكالتك، فإنك تخاطر بفقدان الشكاوى والأسئلة التي تتطلب ردك. يمكن أن يؤدي ذلك أيضًا إلى فتح الباب أمام البريد العشوائي، والأسوأ من ذلك، أن يجعلك أكثر عرضة للمتسللين الذين يستغلون الحسابات غير النشطة.

4-2-2 خطأ بشري

من بين جميع التهديدات الاجتماعية، يمكن أن يتسبب الخطأ البشري في إحداث أكبر تأثير اقتصادي سلبي. يحدث ذلك عندما يقوم شخص ما عن طريق الخطأ بتحميل صورة خاطئة لمنشور اجتماعي، أو يشارك معلومات من حساب خاطئ، أو يشارك بيانات حساسة عن غير قصد. خذ كلمات المرور على سبيل المثال، تستخدم العديد من مواقع الويب أسئلة المعلومات الشخصية كآليات أمان لإعادة تعيين كلمات المرور والسماح بالوصول. ليس من المستغرب أن الأشخاص لا يربطون بين أسئلة الأمان التي يجيبون عليها لموقع ويب الشركة والمحتوى الذي يضعونه على مواقع التواصل الاجتماعي التي يشاركون فيها. ولكن، قد توفر المعلومات الموجودة على وسائل التواصل الاجتماعي عن غير قصد الإجابات اللازمة المخترق لانتحال صفتهم



من أجل الوصول إلى حساباتهم على مواقع أخرى. يمكن أن تكون النتائج مدمرة. يحدد مكتب التحقيقات الفيدرالي (FBI) مخاطر الشبكات الاجتماعية عبر الإنترنت على موقعه على الويب، وقد أوضحوا ذلك بإيجاز إلى حد ما: "بمجرد نشر المعلومات على موقع شبكة اجتماعية، فإنها لم تعد خاصة. كلما زادت المعلومات التي تنشرها، كلما أصبحت أكثر ضعفًا". لا يمكنني توضيح الأمر أكثر من ذلك بكثير. (Frank, 2016)

3-2-4 التصيد

تستخدم حيل التصيد الاحتيالي وسائل التواصل الاجتماعي لخداع الأشخاص لتقديم معلومات شخصية مثل التفاصيل المصرفية وكلمات المرور. لقد أثبت موقع Facebook أنه مورد واضح هنا، حيث يشكل أحد أهم 3 أهداف لهجمات التصيد الاحتيالي في عام 2017 - وهو مؤشر واضح على وعي مجرمي الإنترنت بالقوة التضخمية لوسائل التواصل الاجتماعي باعتبارها صومعة للحصول على البيانات الشخصية. (Gregory Webb, 2019)

4-2-4 اختراق الحساب

يحدث هذا عندما يستولي أحد المجرمين الإلكترونيين على حساب الوسائط الاجتماعية الخاص ويرسل رسائل غير مناسبة أو خارجة عن العلامة التجارية. قدمت حوالي 30-40٪ من مواقع التواصل الاجتماعي التي تم فحصها شكلاً من أشكال خدمة القرصنة. في كثير من الأحيان كان هناك تركيز على خدمات القرصنة "الأخلاقية"، على الرغم من عدم وجود طرق واضحة، لتأكيد هذا. تضمنت بعض الأمثلة التي تم الكشف عنها أثناء البحث: أدوات اختراق مواقع الويب، واستئجار المتسللين، والبرامج التعليمية الخاصة بالقرصنة. (Gregory Webb, 2019)

4-2-5 انتهاكات الامتثال

الامتثال لوسائل التواصل الاجتماعي ليس مخيفًا كما يبدو. نعم، تم وضع العديد من القواعد واللوائح من قبل العديد من الهيئات التنظيمية، مثل FINRA و FTC و FDA و SEC. تحتاج الشركات في الصناعات الخاضعة للتنظيم إلى فهم التزامات الامتثال الخاصة بها من أجل استخدام وسائل التواصل الاجتماعي كأداة تسويقية فعالة ومناسبة. إن إنشاء سياسة وسائط اجتماعية واضحة مع الإشراف على الامتثال لما



يمكن وما لا يمكن قوله من خلال وسائل التواصل الاجتماعي سيساعد شركتك على الامتثال للوائح بنجاح. تعرف على كيفية الحفاظ على امتثالك لوسائل التواصل الاجتماعي.

5-الادوات المستخدمة للحد من الهجمات الالكترونية

في أغلب الأحيان، تكون هجمات الأنظمة الأساسية الاجتماعية قادرة على اختراق حسابات المستخدمين عن طريق سرقة بيانات اعتماد المصادقة الخاصة بهم عند تسجيل الدخول. تُستخدم هذه المعلومات بعد ذلك لسحب البيانات الشخصية بشكل سري من أصدقاء المستخدمين وزملائهم عبر الإنترنت. تشير دراسة حديثة أجريت على موقع Stratecast إلى أن 22٪ من مستخدمي وسائل التواصل الاجتماعي وقعوا ضحية حادث متعلق بالأمن، وأن الهجمات الموثقة مؤخرًا تدعم هذه الأرقام. أثرت Pony botnet على Facebook و Google و Yahoo ومستخدمي الوسائط الاجتماعية الآخرين، حيث سرقت أكثر من مليوني كلمة مرور للمستخدم. يقدر موقع Facebook أن ما بين 50 مليون إلى 100 مليون من حسابات المستخدمين النشطين شهريًا هي نسخ مزيفة، وما يصل إلى 14 مليون منهم "غير مرغوب فيهم" على الموقع. (McAfee, 2021)

هناك العديد من الادوات التي يمكن أن تكون حاجزا منيعا للتصدي لمثل هذه الهجمات وبين أهم هذه الهجمات يمكننا ان نحدد أهمها، وهذا من قبل بعض الاختصاصيين في هذا المجال:(Sarangam, 2021)

-يعد إنشاء كلمات مرور قوية هو الخيار الأساسي لضمان خصوصية معلوماتك.

-تأكد من أن كلمات المرور معقدة ، بما في ذلك الأحرف الكبيرة والصغيرة والأرقام والأحرف الخاصة. يجب حفظها وعدم كتابتها على الورق.

- نحتاج إلى أن نكون حاسمين فيما نحملة / نشاركه في حساباتنا على الشبكات الاجتماعية وأن نتجنب مشاركة المعلومات الشخصية مثل تاريخ الميلاد وتفاصيل الضمان الاجتماعي وأرقام الهواتف والأسماء وصور أفراد العائلة.

-استخدم خيارات الأمان والخصوصية التي توفرها منصات الوسائط الاجتماعية : نظام مصادقة ثنائي ، التحكم في الوصول.



-قم بتوصيل أجهزتنا فقط بوصول wifi المصرح به، واستخدم خيارات الخصوصية التي توفرها أنظمة تشغيل الأجهزة المحمولة المختلفة، واستخدم ميزات القفل التلقائي، وقم بتنزيل التطبيقات فقط من متاجر التطبيقات المعتمدة.

-حافظ على نظام التشغيل محدثاً بأحدث التصحيحات ، وقم بتشغيل جدار الحماية ، وتجنب تثبيت البرامج المكسورة.

-تأكد من تحديث برنامج مكافحة الفيروسات الخاص بنا وإجراء عمليات الفحص بشكل متكرر.

-نحن بحاجة إلى أن نكون أذكياء في استخدام الإنترنت وأن نتجنب زيارة المواقع غير الموثوق بها ؛ لا يتم النقر فوق روابط الإحالة لزيارة مواقع الويب ؛ بدلاً من ذلك ، اكتب عنوان URL الخاص بالمتصفح.

-يجب توخي الحذر لقبول طلبات الصداقة فقط من الأشخاص الذين نعرفهم وحظر أولئك الذين ينشرون محتوى أو تعليقات مزعجة.

الخاتمة

تعد منصات وسائل التواصل الاجتماعي قصة بداية القرن الحادي والعشرين هذا راجع بدون أدنى شك، إلى شبكة اتصالات قوية، مرتبطة بشبكة الكمبيوتر متجانسة، و اقمار صناعية مُتحكم بها بمحطات أرضية منتشرة وفق دراسات استراتيجية بعيدة المدى، و مغذيات بشبكة نت عالمية. كل هذا الزخم التكنولوجي المتسارع ساهم بشكل مباشر او غير مباشر في انتشار نوع جديد من القلق المرتبط بالأمن المجتمعي والإنساني بالدرجة الاولى. والذي كثيرا ما يهدد خصوصيات الافراد و حتي المؤسسات الحكومية، حيث أثارت حوادث خرق البيانات قلق العديد من المستخدمين وأجبرتهم على إعادة التفكير في علاقاتهم بوسائل التواصل الاجتماعي وأمن معلوماتهم الشخصية.المجرمون بارعون في خداع مستخدمي وسائل التواصل الاجتماعي لتسليم المعلومات الحساسة، وسرقة البيانات الشخصية، والوصول إلى الحسابات التي يعتبرها المستخدمون خاصة.لهذا كان من الضروري ايجاد أدوات رديعة لإيقاف هذه الهجمات الالكترونية والتي غالبا ما تكون سببا في اهتزاز العلاقة بين مستخدمي وسائل الاتصال واصحاب منصات التواصل الاجتماعي.



المراجع:

Bloomberg, J. (2018, 04 29). *Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril*. Récupéré sur <https://www.forbes.com:https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril>

Brathwaite, S. (2021, 12 23). *What are the 3 principles of Information Security?* Récupéré sur <https://www.securitymadesimple.org:https://www.securitymadesimple.org/cybersecurity-blog/what-are-the-3-principles-of-information-security>

Buliva, N. (2018, 03 18). *Does Culture Impact Learning For Students Who Use Virtual Reality (VR) Tools? A Review of Literature*. . Récupéré sur https://members.aect.org:https://members.aect.org/pdf/Proceedings/proceedings18/2018/18_03.pdf

Communication, A. D. (2021). *new media*. Récupéré sur <https://www.oxfordreference.com:https://www.oxfordreference.com/view/10.1093/oi/authority.2011080310023183>

6

Cote, J. (2020, 02 24). *What is New Media?* Récupéré sur <https://www.snhu.edu:https://www.snhu.edu/about-us/newsroom/liberal-arts/what-is-new-media>

Dictionary, E. (2021, 10 27). *soft power*. Récupéré sur <https://dictionary.cambridge.org:https://dictionary.cambridge.org/dictionary/english/soft-power>



Frank, G. S. (2016, 07 11). *Human Error and the Risks of Social Media*. Récupéré sur <https://www.linkedin.com/pulse/human-error-risks-social-media-gregory-s-frank-pmp-cism>

Fruhlinger, J. (2020, 01 17). *What is information security? Definition, principles, and jobs*. Récupéré sur <https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html>

Gregory Webb. (2019, 02). *Social Media Platform the Cybercrime Economy*. Récupéré sur <https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf>

Jr, N. J. (1990). *Bound to Lead: The Changing Nature of American Power*. . New York.: Basic Books.

McAfee. (2021, 11 21). *How Cybercriminals Target Social Media Accounts*. Récupéré sur <https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybercriminal-social-media>.

Nye, J. (2017, 02 21). *Soft power: the origins and political progress of a concept*. Récupéré sur <https://www.nature.com/articles/palcomms20178#article-info>

Packer, R. (2021, 11 11). *Virtual Reality, Cultural Implications*. Récupéré sur <https://science.jrank.org/>



paper, w. (2021, 11 21). *Flipping The Script On Security Spending*. Récupéré sur <https://www.proofpoint.com>: <https://www.proofpoint.com/us/resources/white-papers/flipping-script-security-spending>

Portland. (2021, 10). *what is the soft power?* Récupéré sur <https://softpower30.com>.

Sarangam, A. (2021, 02 18). *Social Media Cyber Security: An Overview in 3 Easy Points*.

Récupéré sur <https://www.jigsawacademy.com/>:

<https://www.jigsawacademy.com/blogs/cyber-security/social-media-cyber-security/#Solutions-On-Social-Media-Threats>

work, T. d. (2021, 11 20). *How Social Media is Used in Cybercrimes*. Récupéré sur <https://thedefenceworks.com/>: <https://thedefenceworks.com/services/cyber-and-security-awareness/guides/how-social-media-is-used-in-cybercrimes>

Yun, K. (2020, 11 04). *5 Common Social Media Security Threats for Agents*. Récupéré sur

<https://agentblog.nationwide.com/>: <https://agentblog.nationwide.com/agency-management/sales-and-marketing/social-media-security-threats/>