إستخدام الإنترنت في النشاطات الإستخباراتية – الفيسبوك نموذجاً

راسم بشارات

Rasem Bisharat

Coordinator of International Relations of the Universidade de Políticos do Movimento\ Popular UNIPOP- Brasilia

rasembisharat@gmail.com

ملخص:

وصل عدد مستخدمي الفيسبوك في العالم إلى عتبة الثلاثة مليار مستخدم، وهم في زيادة مستمرة يوميا، منهم في فلسطين أكثر من أربعة ملايين مستخدم في الضفة الغربية وقطاع غزة. وهذا يعني أن معلومات هائلة جدا- إقتصادية، سياسية، إجتماعية، شخصية، قد تكون ذات صلة بالموضوعات العسكرية; بعضها خطيرة دون قصد من صاحبها، قد تؤثر على الأمن القومي، وتكون معلومات إستخباراتية تتلقفها أجهزة الاستخبارات المعنية.

هذه الدراسة، تعتمد على المنهج التاريخي، وتتحدث عن استخدام الإنترنت، بشكل عام والفيسبوك بشكل خاص، من قبل وكالات الاستخبارات العالمية في أنشطتها الإستخباراتية، بإعتبارها إحدى الأدوات الحديثة للعمل الإستخباراتي، ويناقش السرية والخصوصية وشروط الإستخدام في الفيسبوك، بما في ذلك طبيعة المعلومات على صفحة المستخدم، ويشرح كيف تستخدم أجهزة الاستخبارات شبكة الإنترنت في الأغراض الإستخباراتية وكيفية إختراق أجهزة الحاسوب.

كلمات مفتاحية: الفيسبوك، الإنترنت، الإستخبارات، فلسطين، الأمن القومي.

The Use of the Internet in Intelligence Activities – Facebook as a Model

Abstract

The number of Facebook users in the world has reached the threshold of three billion users, and they are constantly increasing daily. In Palestine, there are more than four million users in the West Bank and Gaza Strip. This means that very enormous information - economic, political, social, personal, and may be related to security and military issues, some of which are dangerous - without the intention of its owner, may affect national security. This intelligence information is an easy target for the relevant intelligence services.

This study is based on the historical methodology and talks about the use of the Internet, in general and Facebook in particular, by global intelligence agencies in their intelligence activities, as one of the modern tools for intelligence work. It discusses confidentiality, privacy, and terms of use on Facebook, including the nature of information on a Facebook user page, and explains how intelligence services use the Internet for intelligence purposes and how to hack computers.

Keywords: Facebook, The Internet, Intelligence, Palestine, National Security.

https://journal.pass.ps « DOI: 10.36554/1796-007-001-003 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

مقدمة

وصل عدد مستخدمي الفيسبوك في العالم إلى عتبة الثلاث مليار مستخدم، وهم في زيادة مستمرة يوميا. وفي فلسطين وصل عددهم مع بداية العام 2022 إلى 3,615,100 مستخدم (Internet World Stats, 2022)، أي أكثر بقليل من نصف السكان في الضفة الغربية وقطاع غزة. وهذا يعني أن معلومات هائلة جدا– إقتصادية، سياسية، إجتماعية، شخصية، بعضها لها صلة بالموضوعات الأمنية، قد تؤثر على الأمن القومي دون قصد من صاحبها، وتكون معلومات إستخباراتية تتلقفها أجهزة الاستخبارات العدوة.

أغلبية مستخدمي الفيسبوك لا يدركون خطورة المعلومات التي يقدمونها عن شخصياتهم، مدنهم، علاقاتهم، أوطانهم. وهذا نابع من إعتقادهم بأن تلك المعلومات محدودة التداول ولا يطلع عليها سوى من يحددهم صاحب الحساب على الفيسبوك، كما إن الكثيرون لا يتمتعون بحس أمني يجعلهم قادرين على التمييز بين المعلومات العادية والمعلومات الخطيرة التي تمس الأمن القومي لبلدانهم أو حتى أمنهم الشخصي.

كما أن وسائل التواصل الاجتماعي، بما فيها الفيسبوك، تحتوي على جانبين استخباريين:

- الأول: المعلومات العلنية: تلك التي يقوم صاحب الحساب بوضعها في حسابه، ويمكن لأصدقائه على الفيسبوك الإطلاع عليها، وأحيانا تكون عامة يمكن لغير الأصدقاء الإطلاع عليها، وتشكل ما نسبته 90% من المعلومات التي توجد على الفيسبوك.
- الثاني: المعلومات الخاصة بصاحب الحساب (only me): وهي الرسائل التي يرسلها المستخدم أو يستقبلها، المعلومات التي يضعها ولا يطلع عليها أحد، وهي تشكل ما نسبته 5–10%. هذا النوع من المعلومات يحتاج إلى تقنيات وأساليب خاصة للوصول إليها، إما عن طريق اختراق الحساب أو عن طريق خادم الشركة.

مشكلة الدراسة

أجهزة الاستخبارات العالمية بدأت باستخدام الإنترنت في الأغراض الإستخباراتية منذ فترة طويلة لكنها نشطت بشكل كبير بعد أحداث الحادي عشر من سبتمبر 2001، وقد تمثلت تلك الاستخدامات في جمع المعلومات، المراقبة، التجنيد وإختراق أجهزة الحاسوب الشخصية للأشخاص المستهدفين باستخدام الفيسبوك كأحد أدوات التجسس. وبعد ظهور الفيسبوك عام 2004 أخذت مختلف الأجهزة الأمنية تولي الموقع اهتماما كبيرا بسبب توفر المعلومات العلنية لأصحاب الحسابات فيه. وعليه فإن هذه الدراسة تتناول طبيعة المعلومات الموجودة على صفحة مستخدم الفيسبوك، بالإضافة إلى مناقشة شروط إستخدام الفيسبوك وموضوعات السرية والخصوصية التي تقود في النهاية إلى وقوع صاحب حساب الفيسبوك تحت مصيدة الاستهداف الإستخباراتي دون دراية منه.

https://journal.pass.ps « DOI: 10.36554/1796-007-001-003 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

أهداف الدراسة

إثبات أن الانترنت، بما يشمل وسائل التواصل الاجتماعي، هي واحدة من المصادر العلنية الحديثة المهمة في الحصول على المعلومات الإستخباراتية التي تعتمد عليها أجهزة الاستخبارات المختلفة في عملها الأمني.

كما ويهدف البحث إلى التوعية من مخاطر الإستخدام الخاطئ للفيسبوك، وتوضيح مخاطره على الأمن القومي الفلسطيني، من خلال استخدامه في العمليات الإستخباراتية من قبل مختلف أجهزة الاستخبارات العالمية.

أهمية الدراسة

تزداد أهمية هذه الدراسة مع الانتشار الواسع لاستخدام الفيسبوك وما رافقه من عولمة للإنترنت وانتشار واسع للمعلومات المجانية التي يمكن إختزالها وتحليلها وتحويلها إلى معلومات أمنية تؤثر على الأمن القومي. وعلى الرغم من تلك الأهمية إلا أننا نلاحظ ندرة في الدراسات التي تبحث في موضوع الفيسبوك وخطورته الأمنية.

فضلا عن ذلك، فان غالبية شركات الانترنت العملاقة وعلى راسها غوغل وفيسبوك، والشركات المختصة في التجسس الإلكتروني وأهمها شركة إن اس او NSO Group Technologies مالكة برنامج بيغاسوس للتجسس، هي شركات يملكها يهود موالون لدولة إسرائيل أو إسرائيليون يقيمون فيها، وهو ما يعني تسخير إمكانات تلك الشركات لخدمة أهداف إسرائيل ومحاربة معارضيها ومن تصفهم بالأعداء.

أسئلة الدراسة

هذه الدراسة سوف تجيب على الأسئلة التالية:

- هل الإنترنت، بما يشمل وسائل التواصل الاجتماعي، هو هدف للاستخبارات العالمية في أنشطتها الإستخباراتية؟
- هل يعتبر الفيسبوك مصدرا لجمع المعلومات من قبل أجهزة الاستخبارات العالمية؟

الفرضيات

تأتي نتيجة هذا البحث لتأكيد أو نفي الفرضيات التالية:

- وسائل التواصل الاجتماعي، وخاصة الفيسبوك، هي نوع من المصادر المفتوحة الحديثة للإستخبارات الإستراتيجية التي يتم إستخدامها كبديل عن وسائل الإعلام التقليدية.
- يتم إستخدام الفيسبوك في عمليات الاستخبارات لجمع المعلومات، الاختراق، التجنيد والرصد. واستخدام النتائج في وضع خطط إستراتيجية للعمل في المستقبل.

منهجية الدراسة

تعتمد هذه الدراسة على المنهج التاريخي الذي يهتم بإختيار المشكلة وتوضيحها، ومن ثم وضع فرضيات البحث وجمع المعلومات وتحليلها للوصول إلى النتائج التي تخدم البحث. كما وسيتم إستخدام المنهج التحليلي في تحليل الفيسبوك كمحتوى من خلال تحليل طبيعة المعلومات التي يجب على صاحب الحساب إدراجها حتى يتم تفعيل حسابه، ثم تحليل شروط الإستخدام والسرية والخصوصية التي يوافق عليها صاحب الحساب.

إستخدام الإنترنت في النشاطات الإستخباراتية

يؤكد الخبراء المختصون في شؤون الإنترنت بأن استخدامه بدأ بشكل سري في الستينيات من القرن الماضي في الأغراض العسكرية، حيث لعبت القطاعات العسكرية دورا بارزا في تطوره، وكان أساس نشاطها في أواخر الستينات من القرن الماضي للأغراض العسكرية وحفظ مراكز المعلومات من الدمار حال وقوع هجمات حربية تهدف إلى تدمير تلك المراكز، ثم توسع إستخدام الانترنت ليشمل قطاعات عريضة من الأشخاص والشركات والمؤسسات الحكومية والخاصة، وتعمل هذه القطاعات على تحقيق أهداف سياسية وإجتماعية وإقتصادية مختلفة. إستخدام الإنترنت من قبل أجهزة الاستخبارات في العالم سبق ظهور مواقع التواصل الإجتماعي بسنين طويلة، وكانت الولايات المتحدة الأمريكية وإسرائيل من أوائل الدول التي إستخدمت الإنترنت في العمل الإستخباراتي منذ ما قبل أحداث الحادي عشر من أيلول عام 2001، ونشط بشكل أوسع بعد ذلك التاريخ، وكان تحت مسمى مكافحة الإرهاب، وهو ما تؤكده عدد من الدراسات والأبحاث والتقارير الصحفية المتخصصة في شؤون الاستخبارات (الحارثي، 2014).

شموئيل ايفن ودايفيد سيمون . توف، الباحثان في معهد دراسات الأمن القومي في جامعة تل أبيب، أكدا على أن إستخدام الفضاء الإلكتروني لجمع المعلومات الإستخباراتية بدأ منذ تاريخ طويل عندما تم إدخال أجهزة الحاسوب والبرمجيات لأول مرة في أنظمة الإتصالات المختلفة. وفي تلك الدراسة نوه الباحثان إلى ميزات الفضاء الإلكتروني (Cyberspace) كمجال قتال، وأبرزها التمكن من العمل بسرعة واحد من الألف من الثانية ضد أعداء يبعدون آلاف الآميال دون تعرض المهاجمين أو المقاتلين للأخطار. والميزات التي يتمتع بها الفضاء الإلكتروني تجعله عامل جذب للإستعمال في القتال خلال الحرب إلى جانب الأسلحة التقليدية، مثلما فعلت روسيا . كما يقول المؤلفان . في حربها ضد جورجيا في سنة 2008 (Even and Simon-Tov, 2012) .

ويمكن أيضا إستخدامه أثناء الحرب ضد أهداف استراتيجية، مثل الهجوم الذي تعرض له المفاعل النووي الإيراني في سنة ٢٠٠٩، والإنفجار في محطة نطنز الذي دمر نظام الطاقة الداخلي الذي يزود أجهزة الطرد المركزي في باطن الأرض، حيث أعتبر المؤلفان أن هذا الهجوم (الذي قامت به إسرائيل وفق العديد من المصادر الإعلامية) كان حدثا تأسيسيا في مجال حرب الفضاء الإلكتروني، وشكل مرحلة جديدة في تطور إستعمال الفضاء الإلكتروني في مجالات القتال (دافيد، وشموئيل، ٢٠١١؛ وشفيق، ٢٠٢١).

https://journal.pass.ps « DOI: 10.36554/1796-007-001-003 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

مجلس الاستخبارات القومي في واشنطن العاصمة، في عام 2004، وفي تقريره حول وضع العالم بعد خمسة عشر عاما، خلص إلى أن الغضب المتزايد من قبل الجهات الفاعلة على الساحة الدولية والإقليمية، بما فيها الجماعات الإرهابية، قد يؤدي إلى إكتساب وتطوير القدرات لتنفيذ هجمات مادية وإلكترونية على حد سواء ضد مراكز البنى التحتية للمعلومات، بما فيها مراكز الإنترنت، شبكات الإتصالات السلكية واللاسلكية، وأنظمة الحاسوب التي تتحكم في عمليات التصنيع الهامة مثل شبكات الكهرباء، المصافي، وآليات السيطرة على الفيضانات. ويشير التقرير إلى أن الجماعات الإرهابية قد حددت بالفعل البنى التحتية للمعلومات التي تديرها الولايات المتحدة الأمريكية كهدف، وهي قادرة على تنفيذ إعتداءات مادية من شأنها أن تسبب، لفترة وجيزة على الأقل، اضطرابات وعزل لتلك المراكز. ونوه التقرير إلى أن القدرة على الإستجابة لمثل هذه الهجمات تتطلب تقنية فائقة لسد الفجوة بين المهاجم والمدافع (National Intelligence Council, 2004).

أما يورام شوايتزر، رئيس برنامج الإرهاب والصراع في معهد دراسات الأمن القومي التابع لجامعة تل أبيب (INSS)، فيرى ضرورة العمل على إختراق الشبكات ومواقع الدردشة والرسائل، بالإضافة إلى اختراق الحواسيب الشخصية لأهداف إستخباراتية ولأهداف تعطيل قدرة الجماعات الإرهابية « من الضروري، عند محاربة المنظمات الإرهابية، تفعيل عنصرين معينين هما الاستخبارات والتعطيل، بالإضافة إلى القيام بعملية جمع جيدة ودقيقة للمعلومات بإستخدام مجموعة من المصادر المفتوحة والوصول إلى مادة من حواسيب شخصية للإرهابيين ومن شبكاتهم ومواقع الدردشة والرسائل الخاصة بهم» (Schweitzer et al. , 2011).

وأما ستانسفيلد تيرنر، مدير وكالة المخابرات المركزية (CIA) 1977-1981، فقد أكد في مقال نشر عام 1991 في مجلة فورين أفيرز بعنوان «المخابرات في ظل نظام عالمي جديد»، على ضرورة الإهتمام بالمصادر المفتوحة، مشيرا إلى أن أجهزة الاستخبارات الأمريكية تولي قضية الرأي العام والمصادر المفتوحة إهتمامها. ويشير إلى أن هذا الاهتمام جاء بعد فشل الاستخبارات الأمريكية في توقع إنتصار الثورة الإيرانية عام 1979، إذ أن الاستخبارات الأمريكية كان لديها المعلومات عن خطط آية الله روح الله الخميني لإسقاط نظام حكم الشاه في إيران، الحليف القوي لإسرائيل والولايات المتحدة الأمريكية، لكنها كانت تفتقر إلى معرفة رأي الشارع الايراني، فهي لم تكن متصلة برجال الدين لتعرف أنهم كانوا يقولون للفلاحين بأن الشاه يدنس الإسلام، ولم يكونوا على صلة مع المثقفين في السياسة الذين كانوا ساخطين على الشاه لعدم إستعداده لتقاسم السلطة، كما أنهم لم يكونوا متصلين بالتجار الذين كانوا ساخطين لسيطرة النظام على الإقتصاد. وهذا ما دفع أجهزة الاستخبارات الأمريكية للإهتمام بموقف الرأي العام والاهتمام بالمصادر المفتوحة، التي أصبحت مواقع التواصل الاجتماعي فيما بعد من أهم مصادرها (Tumer, 1991) .

د. محمد الحارثي (الحارثي،2014) يقول بأن حركة التجسس قد نشطت على الإنترنت بعد الحادي عشر من سبتمبر 2001، عندما كثفت أجهزة الأمن الأمريكية التجسس على شبكة الإنترنت وبدأت عمليات موسعة لإصطياد من أسمتهم بالجماعات الإرهابية، حيث اعتقدت أجهزة الاستخبارات الأمريكية أن الجماعات المعادية للولايات المتحدة الأمريكية تستخدم شبكة الإنترنت في إصدار الأوامر إلى الخلايا النائمة لضرب الأهداف الأمريكية .

وتتلخص أهداف الإختراق التي تقوم بها أجهزة الاستخبارات بما يلي:

- جمع المعلومات حول الأشخاص المستهدفين ومعرفة تنقلاتهم وتحركاتهم.
- محاولة سرقة كلمات المرور وغيرها من وثائق التفويض.
- مراقبة البريد الإلكتروني والرسائل الفورية (SMS).
- التعطيل وضرب البنى التحتية للمؤسسات المستهدفة، كما حصل مع مفاعل بوشهر الإيراني.
- إستخدام البيانات التي يتم جمعها ضد الشخص المستهدف بهدف تجنيده.

فيسبوك تتعاون مع اسرائيل إلى أبعد الحدود، وتجاوز التعاون في المسائل الأمنية إلى محاربة المحتوى الفلسطيني وإسكات الأصوات الداعية إلى العدل والحرية وإنهاء الاحتلال، وقامت الفيسبوك بطلب إسرائيلي بحذف صفحات كثيرة لصحفيين وناشطين فلسطينيين وأجانب، بحيث بلغ عدد الطلبات الإسرائيلية التي قدمت لإدارة الفيسبوك لحذف حسابات نشطاء 20 ألف طلب في العام الماضي 2021 (Baroud, 2022). ومع إرتفاع حدة الإعتراضات على الفيسبوك، ومن أجل إسكات الأصوات المحتجة، قامت الشركة نهاية العام الماضي بحظر أربع شركات إسرائيلية إلكترونية إتهمت بمراقبة نشطاء حقوق الإنسان وصحفيين، حيث تورطت شركات Cobwebs Technology, Cognyte, Black Cube, Blue Hawk CI في عمليات إستطلاع على الملفات الشخصية على الفيسبوك لعدد من نشطاء حقوق الانسان وصحفيين، وقامت الشركة بحذف اكثر من 200 حساب وهمي تدار من قبل تلك الشركات (Alyshai, 2021)

طبيعة الفيسبوك

الفيسبوك هو موقع ويب للتواصل قام بتصميمه الأمريكي مارك زوكربرغ Mark zuckerberg عام 2004 عندما كان طالبا في جامعة هارفارد في الولايات المتحدة الأمريكية، وأعلن عنه كشركة تحول إسمها لاحقا إلى ميتا Meta، ومنذ انطلاق الموقع على شبكة الإنترنت، شهد إقبالا عالميا كبيرا، بحيث وصل عدد المشتركين فيه إلى عتبة الثلاثة مليار مشترك.

في فلسطين، كان عدد مستخدمي الفيسبوك في نهاية عام 2011 قد بلغ 712.260 مستخدما، 61% منهم من الذكور، وقد تراوحت اعمار 91% من المستخدمين من كلا الجنسين ما بين 13 .

https://journal.pass.ps « DOI: 10.36554/1796-007-001-003 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

29 عام، فيما كان 40% من مستخدمي الإنترنت من الفلسطينيين يستخدمون شبكات إسرائيلية (Internet World Stats, 2011) . وبعد عقد من الزمن تجاوز العدد ثلاثة ملايين ونصف مع نهاية عام 2021، بحيث بلغ 3,615,100 مستخدم بنسبة 68,2 بالمائة من عدد السكان البالغ 5,302,778 نسمة (Internet World Stats, 2022).

طبيعة المعلومات التي تحتوي عليها صفحة المستخدم في الفيسبوك

الخطوة الاولى لعمل حساب على الفيسبوك هي الضغط على التسجيل، لتبدأ الصفحة الشخصية بالتشكل، ثم يتبعها عدة خطوات ينبغي على المشترك القيام بها، وهي تعبئة البيانات الشخصية واختيار صورة فوتوغرافية.

البيانات الشخصية الواجب تعبئتها تشمل الجوانب التالية:

- المعلومات الشخصية : البيانات الشخصية، العلاقات، العمل والمهنة، مكان الإقامة، الأصدقاء، أفراد العائلة، الصور الشخصية والعامة.
- النشاطات التي يقوم بها المشترك بالوقت والتاريخ والمكان.
- تحديد وتحليل سلوك وشخصية صاحب الحساب من خلال:
  - تسجيل الإعجاب (Like).
  - المجموعات التي يشارك فيها المستخدم (Groups).
  - التوجهات الدينية والسياسية والميول الثقافية(Political, Religious and Cultural Views) .
  - المحادثات التي يجريها المستخدم (Chat) .
  - عمليات البحث التي قام بها المستخدم على جهازه وفي الفيسبوك (Search) .
- معرفة تحركات صاحب الحساب وتنقلاته والأماكن التي يزورها سواء داخل وطنه أو في الخارج، من خلال تحديد الأماكن التي قام صاحب الحساب بتسجيل الدخول منها، ومن خلال الصور التي يتم إضافتها ويتم فيها تحديد المكان والزمان لإلتقاط تلك الصور، وإضافة أسماء من في الصور.
- تحديد العنوان الإلكتروني وأرقام الهواتف الخاصة بالمشترك، بالإضافة إلى الرسائل التي يرسلها أو التي يستقبلها.
- تحديد التوجهات السياسية والفكرية والثقافية والمزاج الشخصي لصاحب الحساب من خلال نشاطه اليومي في الفيسبوك.

شروط الاستخدام (Terms and Policies): أول خطوة للتجسس

زاد عدد مستخدمي الفيسبوك عن ثلاثة مليار مستخدم، لكن السؤال المطروح هو كم شخص منهم قرأ شروط إستخدام الفيسبوك التي وضعتها إدارة الموقع. إذ أن إنشاء إي حساب على الفيسبوك يعني أن صاحبه قد وافق على شروط الإستخدام حتى ولو لم يقرأها أو يطلع عليها، لأن الدخول على الحساب يأتي بعد تصريح المستخدم بأنه قرأ واطلع على شروط الإستخدام ووافق عليها.

وعند قيام المستخدم بالضغط على التسجيل، فإنه يقر ويعترف بأنه قرأ ووافق على شروط وسياسة الفيسبوك، بما في ذلك إستخدام ملفات تعريف الارتباط « بالضغط على التسجيل، توافق على شروطنا وأنك قرأت سياسة استخدام البيانات لدينا، بما في ذلك استخدام ملفات تعريف الارتباط».

شروط الاستخدام التي وضعتها إدارة الفيسبوك، ولا يمكن للمستخدم الدخول إلا بعد الإقرار بها والموافقة عليها، تتكون من تسعة عشر بندا. البند الثاني من شروط استخدام الفيسبوك يتحدث عن مشاركة المحتوى والمعلومات الخاصة بالمستخدم، وتنص المادة رقم (1) من هذا البند على أن تسجيل الحساب في الفيسبوك يعطي إدارة الفيسبوك الصلاحيات باستخدام ما ينشرة المستخدم على حسابه « بالنسبة إلى المحتوى الخاضع لحقوق الملكية الفكرية، مثل الصور والفيديو (المشار إليه لاحقًا بـ «المحتوى الخاضع لحقوق الملكية الفكرية»، فإنك تعطينا الإذن التالي ذكره بشكل محدد، الخاضع لـ إعدادات الخصوصية والتطبيقات: انت تمنحنا ترخيصًا دوليًّا غير حصري وقابلاً للنقل وللترخيص من الباطن وغير خاضع لأية رسوم امتياز لاستخدام أي محتوى خاضع لحقوق الملكية الفكرية تنشره على فيس بوك أو له صِلة به» (فيسبوك، شروطنا، مشاركة المحتوى والمعلومات الخاصة بك).

أما المادة رقم (5) من نفس البند، فهي تفويض من المستخدم لإدارة الفيسبوك باستخدام معلوماته دون الرجوع إليه ودون أي التزام بالتعويض عليه « قد نستخدم تلك المعلومات . معلومات المستخدم . من دون أي التزام من جهتنا بالتعويض عليك عنها (تمامًا مثل عدم إلزامنا لك بتقديمها)».

البند رقم (3) من شروط الإستخدام يؤكد أن إدارة الفيسبوك لا تستطيع ضمان المحافظة على أمان فيسبوك، مما يعني أنها تخلي مسئوليتها عن أي إنتهاك لخصوصية المستخدمين أو أي استخدام لمعلوماتهم من طرف ثالث. أما البند السابع عشر . المادة الاولى، فيوضح أن كافة بيانات ومعلومات مستخدمي الفيسبوك، المقيمين خارج الولايات المتحدة الأمريكية، تنقل الى الولايات المتحدة ويتم معالجتها هناك، حيث مقر الشركة.

يستطيع الفيسبوك تجميع كافة المعلومات عن المستخدم، سواء التي قام بتحديثها شخصيا، من حيث الدخول وإضافة بيانات، والمشاركات في التعليقات، وإضافة مقاطع فيديو أو صور أو مقالات. أو من المعلومات التي قام آخرون بإضافتها على الفيسبوك عن المستخدم. أو من خلال إرسال أو استقبال رسائل. وتحديد الجهاز الذي قمت بتسجيل الدخول منه وتحديد عنوان IP ومكان الدخول من خلال نظام تحديد المواقع العالمي (Nieva, 2018) (GPS)» .

https://journal.pass.ps « DOI: 10.36554/1796-007-001-003 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

السرية والخصوصية (Secrecy vs Privacy)

إن شروط الاستخدام التي يوافق عليها المستخدم تنفي السرية عن حسابه طالما أن الشركة تقوم بتجميع بيانات المستخدم تحت عدة مستخدمات، كما أنها تدرك أن لا سرية مضمونة، فهي تخلي مسؤوليتها عن أي إنتهاك أو إستخدام لمعلومات المستخدم من قبل طرف ثالث أو من طرفها.

الفيسبوك بدأت منذ فترة قليلة في طرح المعلومات المتعلقة بمستخدمي الشبكة علنا على محركات البحث على الانترنت مثل غوغل وياهو، ويهدف من هذه الخطوة إلى الدخول في سباق لبناء دليل إلكتروني عالمي يحتوي على أكبر قدر ممكن من المعلومات والتفاصيل الشخصية مثل السير الذاتية، وأرقام الهواتف، الهويات ومعلومات تفصيلية عن اهتمامات الأشخاص.

زيادة على ذلك فإن عدد من المختصين في شؤون الإنترنت يؤكدون بأن إدارة الفيسبوك على إطلاع كامل بكل ما يقوم به المستخدم، على حسابه أو على الإنترنت، من حيث المواقع التي تصفحها والصفحات التي زارها حتى بعد أن يقوم بتسجيل الخروج.

الأسترالي نيك كوبرلوفيكNick Cubrilovic ، قرصان ومدون، يقول بأن الفيسبوك يبقى على إطلاع على ما يقوم به المستخدم، ويمكنه تعقب جميع الصفحات التي يزورها على الإنترنت، حتى وإن قام بتسجيل الخروج. ويضيف كوبرلوفيك بأن البيانات المتعلقة بصاحب الحساب، بما فيها رقم حسابه، يتم إرسالها بشكل مستمر إلى فيسبوك. شركة فيسبوك أنكرت ذلك مدعية بأنها غير مهتمة بجمع البيانات حول المواقع التي يزورها مستخدمي الفيسبوك. ويفسر كوبرلوفيك بأن مواقع التواصل الإجتماعي تستخدم ملفات تعريف الارتباط التي لا تحذف عند تسجيل الخروج، وبدلا من ذلك يتم تعديل هذه الملفات ليتم ارسال المعلومات عن الاشخاص الذين يزورون مواقع تحتوي على زر الفيسبوك «أعجبني»، زر « مشاركة» أو أزرار اخرى. لذا فإن أحد المواقع المتخصصة في الإنترنت والمطلع على شؤون الفيسبوك يقترح على مستخدمي الفيسبوك التفكير جيدا بما سيقومون بتنزيله على صفحاتهم " فكر أولا، نزل ثانيا» «Think first, post second"، حيث يرى الموقع أن فيسبوك يستخدم بيانات المشتركين التي يتم تنزيلها على صفحاتهم، بما في ذلك ما تم تنزيله قبل تسعة عشر عاما، أي منذ تأسيس الفيسبوك وانطلاقه إلى العلن (Café feel secure plog, 2011). كما أن مواقع متخصصة في الشؤون الإلكترونية وشبكات التواصل الإجتماعي بحثت في موضوع السرية والخصوصية، وخرجت بنتائج أن لا خصوصية في الانترنت (Cerna, 2019).

كما يركز الفيسبوك عمليات المسح في الحسابات الشخصية التي لا تملك أصدقاء مشتركين أو الأشخاص الذين انفصلوا منذ فترة قريبة عن بعضهم، أو الأشخاص الذين أصبحوا أصدقاء مع وجود فارق كبير في السن، وكل ما يمكنه إثارة الشبهات بشكل عام دون أن يكون تعبير ‹›مثير للشبهة›› واضحا أو محددا للمستخدمين.

حقيقة أن لا خصوصية ولا أمن للمعلومات عبر الإنترنت هي حقيقة تناولها جوليان أسانج خلال لقائه مع ثلاثة من أشهر المختصين في عالم الإنترنت في العالم، وهم آندي مولر . الالماني، جيريمي زيمرمان . الفرنسي وجاكوب ابلباوم . الأمريكي، عندما التقى بهم في برنامج خاص بثته قناة روسيا اليوم . فقد أكد جوليان أسانج « أن اتصالاتنا وتفاعلاتنا على الإنترنت يتم التجسس عليها، ويتم تخزينها، وربما يتم استخدامها ضدنا» (Assange, 2012a). فيما أكد جيريمي أن محرك البحث جوجل، الذي نستخدمه في الوصول إلى موقع الفيسبوك، يعرف فيما إذا كان المستخدم شخص عادي أم لا، ويعرف مع من يقوم بالاتصال، ومن هم معارفه، وما هي المجالات التي يبحث عنها، التوجهات الجنسية، الديانة والفلسفة، مؤكدا أن جوجل يعرف أكثر من أمهاتنا وربما أكثر مما نعرفه عن أنفسنا (Assange, 2012b) .

جاكوب يرى بأن هناك علاقة تحالف ما بين الفيسبوك والدولة، وهذا التحالف جعل الفيسبوك جزء من عالم الإستخبارات، ويقول بأن «الهدف من انشاء الفيسبوك هو اقتصادي يهدف للربح، فلا غرابة أن يقوم ببيع المستخدمين لتحقيق ربح مضاعف. ومن أجل الربح قرر الفيسبوك التعاون مع الدولة ببيع المستخدمين وإنتهاك خصوصيتهم، ورضي بأن يكون جزأ من نظام الرقابة، بحيث تدفع لهم الحكومات لكونهم أصبحوا جزءا من عالم الاستخبارات» (Assange, 2012b) .

أما قضية إدوارد سنودن، الموظف السابق في الاستخبارات الأمريكية، فقد كشفت حقائق كثيرة لها علاقة بالتجسس على شركات الإنترنت العملاقة والوصول إلى مستخدمي تلك الشركات، ومنها الفيسبوك وجوجل وتويتر. فهي أكدت المعلومات التي كان قد صرح بها جوليان أسانج وضيوفه في «روسيا اليوم» بما يخص الفيسبوك، وفتحت المجال أمام الشركات لتقوم بالرد وفضح العلاقة ما بينها وبين أجهزة الاستخبارات الأمريكية.

وقد كشفت صحيفتا الغارديان والواشنطن بوست، نقلا عن سنودن، في يونيو 2013، حول قيام وكالة الأمن القومي NSA ومكتب التحقيقات الفدراليFBI بالوصول إلى خوادم تسعة من شركات الإنترنت العملاقة في الولايات المتحدة الأمريكية، من بينها شركة الفيسبوك، والتجسس على مستخدمي تلك الشبكات الذين يعيشون خارج الولايات المتحدة، من خلال برنامج يسمى «بريزم» PRISM. كما وذكرت صحيفة الغارديان بأن وكالة مقر الإتصالات الحكومية البريطاني تقوم بجمع المعلومات بشكل سري من خلال شركات الإنترنت نفسها وعبر بريزم الذي صممته الاستخبارات الأمريكية (Gallo, 2013; Gellman and Piotras, 2013) .

برنامج بريزم، وفقا لوثائق سنودن، هو المساهم الأكبر في التقارير الإستخباراتية لوكالة الأمن القومي، ويطلق عليه تسمية «المصب». وهذا يعني أن وكالة الأمن القومي الأمريكية تقوم بجمع البيانات من جوجل، الفيسبوك، وأبل وياهو وغيرها من عمالقة الإنترنت في الولايات المتحدة. إحدى الشرائح التي سربها سنودن تؤكد بأن وكالة الأمن القومي لها وصول مباشر لخوادم شركات

https://journal.pass.ps « DOI: 10.36554/1796-007-001-003 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

الإنترنت، وهو ما عارضته تلك الشركات، حيث ادعت بأنها تتعامل مع طلبات مشروعة بموجب القانون عند تزويد الوكالة ببيانات المستخدمين.

كنتون وغريغ، الصحفيين في صحيفة الغارديان، وضحا خطورة برنامج بريزم والقدرة الهائلة في التجسس على حسابات الفيسبوك، بغض النظر عن علاقة أصحاب تلك الحسابات بالإرهاب أم لا. يقول الصحفيان بأنك لست بحاجة إلى أن تتحدث إلى مشتبه به بالإرهاب ليتم تحليل بيانات الاتصالات الخاصة بك من قبل وكالة الأمن القومي الأمريكية. فالوكالة سمحت لنفسها بالإبتعاد عن أهدافها التي تتابعها بمقدار « ثلاث درجات « خارج النطاق المرسوم، بحيث إذا كنت هدفا للوكالة، فانها من خلالك قد تصل إلى سلسلة من الأشخاص الذين يتحدثون إلى أشخاص آخرين، وأولئك الأشخاص الآخرون يتحدثون إلى أشخاص يتحدثون معك على الفيسبوك، بحيث أنه ومن خلال مستخدم عادي للفيسبوك الذي له 190 صديق على سبيل المثال، تستطيع الوكالة عبر القفزات الثلاث التجسس على شبكة من مستخدمي الفيسبوك تزيد عن خمسة ملايين مستخدم، بمعنى أن الوكالة ومن خلال برنامج بريزم تستطيع التجسس على كافة سكان الأراضي الفلسطينية من خلال الدخول إلى حساب مستخدم واحد.

ومن أجل التوضيح، حساب على الفيسبوك لديه 190 صديق (المستوى الأول)، في المستوى الثاني تدخل وكالة الأمن القومي NSA على أصدقائك المائة وتسعون في الفيسبوك فتصل من خلالهم إلى 31،046 مستخدم، وفي المستوى الثالث ومن خلال أصدقاء أصدقائك تصل الوكالة إلى 5،072،916 مستخدم على الفيسبوك ، أي ما يقارب عدد سكان فلسطين في الضفة الغربية وقطاع غزة (Powell and Chen, 2013).

نماذج سهلة للتجسس على الفيسبوك دون إستخدام تقنيات خاصة

هناك العديد من الطرق البسيطة والسهلة للتجسس على الفيسبوك، يمكن أن تتم من قبل أناس عاديين ليس لديهم مهارات ولا يحتاجون إلى تقنيات خاصة في التجسس. ومن الممكن أيضا أن تقوم بها وكالات الإستخبارات، لا سيما في عمليات مراقبة الفيسبوك، وتصيد المرشحين للإستهداف. اس أناغا (Anagha, 2021) أخصائية التسويق على الفيسبوك تورد سبعة طرق للتجسس على حسابات المنافسين، وذلك باستخدام بعض التقنيات، وهي:

- مصادقة المنافس Befriending the Competitor
- متابعة إعلانات المنافس Following Competitor's Ads
- الإعلان في المكان المناسب Advertising at the Right Place
- تحليل الارتباط بالمحتوى Analysing Content Engagement
- متابعة تعليقات المنافس Following the Comments of the Competitor

https://journal.pass.ps « DOI: 10.36554/1796-007-001-003 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

- تحليل مصادر الحركة Analysing Sources of Traffic
- إستخدام الأدوات الصحيحة Using the Right Tools

أما كريستين كين، الخبيرة في شؤون الفيسبوك، فقد عرضت عشر طرق تعتبر سهلة ولا تحتاج تقنيات وبرامج، هي على النحو التالي (Kane, 2012):

- الحسابات العلنية (التي تمكن العامة من الاطلاع عليها): ما لم يكن حسابك خاص، يمكن فقط للأصدقاء الإطلاع على بياناتك الشخصية، فإن أي مستخدم يستطيع الوصول لبياناتك الشخصية.
- الصداقة: كافة أصدقائك يطلعون على بياناتك الشخصية، وعند قبولك لأي صديق جديد، فانك تمنحه تلك الميزة أيضا وتخوله الاطلاع على كل ما تكتب وما تقوم بتنزيله.
- الحسابات المزيفة: إذا أراد شخص ما التجسس على حساب شخص آخر، ولا يتوقع أن يتم قبول طلب صداقته على الفيسبوك، فإنه يقوم بعمل حساب مزيف لشخص آخر يثير إهتمام صاحب الحساب الذي ينوي إرسال طلب الصداقة له، فمثلا يقوم بعمل حساب مزيف لفتاة جميلة لجذب الإنتباه أو حساب لشخص ذو إهتمامات مشتركة مع صاحب الحساب المستهدف، مما يسهل عملية قبوله كصديق على الفيسبوك.
- إستخدام إسم صديق للمستخدم موجود على قائمة الأصدقاء: عندها يعتقد المستخدم أن لصديقه حساب آخر فيضيفه تلقائيا دون فحص هل هو نفس الشخص أم غيره. وفي هذه الحالة يتم إختيار صديق مشاركاته قليلة في الفيسبوك ومعلوماته قليلة أيضا كي لا يتم كشفه، فيقوم بإنتحال إسمه وإرسال طلب صداقة.
- إضافة أصدقاء مشتركين وبعدها يتم ارسال طلب صداقة، إذ أن غالبية مستخدمي الفيسبوك يطمئنون للشخص الذي لديه أصدقاء مشتركين معه دون التدقيق في حقيقتهم.
- إضافة تعليقات على مشاركات الشخص في حسابات الآخرين، فيصبح مع الوقت مألوفا لصاحب الحساب، وعند إرسال طلب صداقة يتم قبوله.
- إرسال رسالة: الفيسبوك يوفر إمكانية إرسال الرسائل إلى حساب المستخدمين دون أن يكون صديقا على قائمة الأصدقاء، وبهذا يتمكن من التأثير على صاحب الحساب.
- الإشتراك في نفس المجموعة، سواء مجموعة سياسية أو إقتصادية أو فنية أو علمية ... الخ.
- الدخول إلى حساب المستخدم من خلال التطبيقات والبرامج أو الأخبار: فالفيسبوك يتيح لمستخدميه تسجيل الدخول إلى المواقع المختلفة مثل المواقع الإخبارية وذلك بإستخدام الملف الشخصي، ويتم من خلال ذلك إضافة تعليقات على المقالات على سبيل المثال، وهذا التطبيق يتيح للآخرين الوصول إلى الملف الشخصي للمستخدم.

https://journal.pass.ps « DOI: 10.36554/1796-007-001-003 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

– إضافة التحديثات الخاصة بالمستخدم تمكن الآخرين من متابعته والاطلاع على تحديثاته.

لهذا، يرى المحللون والخبراء في مجال شبكات التواصل الإجتماعي بأن هذه الشبكات قادرة على القيام بثلاثة أشياء (Fitsanaks, 2012):

– تعكس اتجاهات الرأي وقناة العمل السياسي الشامل؛
– تمكن من القيام بعمليات أمنية ضد الجماعات المستهدفة . عمليات فعالة ومثيرة للجدل؛
– توفير المعلومات الإستخباراتية التكتيكية للتنفيذ

النتائج

من خلال ما تقدم، نستطيع القول أن الانترنت أصبح من المصادر المهمة للإستخبارات الإستراتيجية في عملياتها الإستخباراتية، من خلال كم المعلومات المختلفة التي يتم نشرها على الصفحات الشخصية والمجموعات المختلفة، سواء على صفحات الفيسبوك او الإنستغرام او التويتر وغيرها، وهو ما يسهل مهام الأجهزة الإستخباراتية في الحصول على تلك المعلومات بالمجان، وبعد دراسة وتحليل تلك المعلومات، تأتي عمليات المراقبة، التجنيد وإختراق أجهزة الحاسوب الشخصية للأشخاص المستهدفين حسب رؤية وأهداف تلك الأجهزة.

والفيسبوك، مع ما يحتوي من معلومات شاملة، يتيح لأي جهاز إستخباراتي القدرة في الحصول على المعلومات الأساسية عن الشخص المستهدف، وتمكنهم من متابعة نشاطاته وتنقلاته، كما وتمكنهم من تحليل سلوكياته ومزاجه الشخصي، والتنبؤ بحركاته المقبلة، بالإضافة إلى إختراق حاسوبه الشخصي والإطلاع على ملفاته الخاصة وسرقتها، مع إمكانية استخدامها ضده في المستقبل. وهو ما يعطي أجهزة الاستخبارات المختلفة القدرة على الإختراق، ومن ثم تمكنها من إستغلال نقاط الضعف لدى الشخص المستهدف التي تم إستنتاجها من خلال تحليل ملفه على موقع التواصل الاجتماعي الفيسبوك، فتقوم بتحييده إما بتهديده أو بتجنيده أو بتصفيته.

الخاتمة

الفيسبوك تخطى أهميته كموقع للتواصل الاجتماعي والتعارف بين الناس، وأصبح له وقع سياسي وإجتماعي وإقتصادي، كما وأصبح عامل ضغط سياسي على العديد من الأنظمة السياسية في العقد الأخير، وقد ظهر ذلك بشكل واضح في الشرق الأوسط عند إندلاع ثورات الربيع العربي في تونس ومصر، حيث أصبح الفيسبوك أداة للتواصل والدعوة للإحتجاجات التي طالبت برحيل نظام زين العابدين بن علي في تونس وحسني مبارك في مصر.

ومن خلال ما تقدم، نستطيع القول أن الفيسبوك أصبح من المصادر المهمة للإستخبارات الإستراتيجية في عملياتها الإستخباراتية، من خلال جمع المعلومات، المراقبة، التجنيد، وإختراق أجهزة الحاسوب الشخصية للأشخاص والشركات والحكومات والدول المستهدفة.

ومع الإنتشار الواسع لإستخدام الفيسبوك في الأراضي الفلسطينية، قامت إسرائيل، كسلطة قائمة بالإحتلال، بتجاوز الفيسبوك كموقع للتواصل الإجتماعي، وعملت على إستخدامه في أنشطتها الإستخباراتية المختلفة ضد الشعب الفلسطيني ومكوناته السياسية والعسكرية والإقتصادية، بدءا من إنشاء صفحات باللغة العربية موجهة للدول العربية بهدف تحسين صورة إسرائيل، إلى محاربة المحتوى الفلسطيني بهدف إسكات الأصوات الداعية إلى العدل والحرية وإنهاء الإحتلال، فضلا عن إستخدامه في عمليات التجنيد والإعتقال.

التوصيات

على مراكز الأبحاث المتخصصة في فلسطين تسليط الضوء في دراساتها على موضوع وسائط التواصل الاجتماعي، وخاصة الفيسبوك، من خلال نشر الأبحاث والدراسات التي تحذر من خطورة الإندفاع في نشر البيانات الشخصية، والإندفاع العاطفي خلف الفعاليات الوطنية بنشرها على صفحاتهم الشخصية وإضافة الموقع الذي يشهد تلك الأحداث، مما يتيح لأجهزة الاستخبارات الإسرائيلية سهولة الحصول عليها، وبالتالي الوصول لمعلومات خطيرة بكل سهولة تؤدي إلى إحباط أي نشاط موجه للإحتلال.

وعلى الحكومة الفلسطينية، والأجهزة الأمنية الفلسطينية تحديدا، العمل على نشر الوعي الأمني والمعرفة بين المواطنين، على أساس أن توعية المواطن هو جزء من مكافحة التجسس. هذا الهدف له إرتباط مع جوهر العمل الإستخباراتي، الذي يسعى دوما لحماية الوطن من الأعمال الإستخباراتية الخارجية، تلك التي تعمل على منع وتعطيل أي عمل تجسسي. وبما أن من حق الدولة محاسبة وإعتقال أي مواطن يثبت تورطه في أعمال تجسسية على مواطنيه ودولته، فإن من حق المواطن على الدولة تثقيفه من النواحي الأمنية ليكون على وعي بكافة الطرق والوسائل التي تتبعها الأجهزة الإستخباراتية العدوة من حيث الإختراق والتجنيد وغيره من الطرق والوسائل.

https://journal.pass.ps « DOI: 10.36554/1796-007-001-003 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

قائمة المراجع:

أولا: المراجع العربية

الحارثي، محمد، (2014). الحرب الالكترونية على الانترنت، المعركة – شبكة انتفاضة فلسطين، منشور على موقع: http://www.alma3raka.net/spip.php?page=article&id_article=114&lang=ar تم الدخول 2022 .

شفيق، كريم. (2021)، ما خيارات ايران للرد على ضرب محطة «نطنز»، سكاي نيوز عربية، منشور على موقع: https://www.skynewsarabia.com/world/1429333 . تم الدخول 2022.

ايفن، شموئيل، وبن سلمان، دافيد (2011). قراءة في كتاب حرب الفضاء الالكتروني: اتجاهات وتأثيرات على إسرائيل، قطر: المركز العربي للأبحاث ودراسة السياسات.

ثانيا: المراجع العربية المترجمه

Al-Harthy, M. (2014). Electronic warfare online, The Battle - Palestine Intifada Network. Retrieved on 2022, from http://www.alma3raka.net/spip.php?page=article&id_article=114&lang=ar

Even, Sh., & Bin Salman, D. (2011). Reading in the book Cyberspace War: Trends and Effects on Israel, Qatar: The Arab Center for Research and Policy Studies.

Shafiq, K. (2021). What are Iran's options to respond to the attack on the "Natanz" station, Sky News Arabia. Retrieved on 2022, from https://www.skynewsarabia.com/world/1429333

ثالثا: المراجع الاجنبية

Alyshai. (2021), Facebook Disables Accounts of Israeli companies Spying on People of Interest, Propakistani, Retrieved on 2022, from https://propakistani.pk/2021/12/28/facebook-disables-accounts-of-israeli-companies-spying-on-people-of-interest/

Anagha, S. (2021). 7 Amazing Ways to Spy Your Competitor on Facebook, StartupTalky. on 2022, from https://startuptalky.com/facebook-competitor-spying-techniques/

Assange, J. (2012a). The Julian Assange Show. Entrevistas com Julian Assange, on 2022, from https://assange.rt.com/ar/assange_8/

Assange, J. (2012b). Cypherpunks: Freedom and the future of the internet, New York, London, OR Books, New York – London.

Baroud, R. (2022), Israel's 'Facebook Law', Retrieved on 2022, from https://www.thenews.com.pk/print/928129-israel-s-facebook-law

café feel secure blog, (2011). Facebook Privacy – Not so private: Important news every teen must know!, Retrieved on 2022 from http://blog.wefeelsecure.com/2011/06/facebook-privacy-not-so-private-important-news-every-teen-must-know/.

Cerna, P. (2019). There's no privacy on the internet, The Temple News, Retrieved on 2022, from https://temple-news.com/theres-no-privacy-on-the-internet/

Even, Sh., & Simon-Tov, D. (2012). Cyber Warfare: Concepts and Strategic Trends, Memorandom 117, Tel-Aviv University, the Institute for National Security Studies (INSS).

Fitsanaks, J. (2012). Spies increasingly using facebook, twitter to gather data, Intelnews.org. Retrieved on 2022, from http://www.intelnews.org/2012/02/13/01-927/more-8172 .

Internet World Stats, (2022). Internet Usage in the Middle East, Retrieved on 2022, from: https://www.internetworldstats.com/middle.htm#ps

Gallo, W. (2013). US Spy Chief Slams Leaks on Surveillance Program, Global Security. Retrieved on 2022, from http://www.globalsecurity.org/intell/library/news/2013/intell-130607-voa02.htm?_m=3n%2e002a%2e825%2ebr0ao04sx6%2er3h.

Gellman, B., & Poitras, L. (2013). British intelligence mining data from nine U.S. Internet companies in broad secret program, Retrieved on 2022, from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Kane, Ch. (2012). 10 Ways People Use Facebook to Spy on Others, Retrieved on 2022, from http://www.internetserviceproviders.org/blog/2012/10-ways-people-use-facebook-to-spy-on-others/.

National Intelligence Council (NIC), (2004). Mapping the Global future, NIC 2004-13.

Nieva, R. (2018). Here's how Facebook collects your data when you're logged out, Retrieved on 2022, from https://www.cnet.com/news/privacy/heres-how-facebook-collects-your-data-when-youre-logged-out/

Powell, K. & Chen, G. (2013). Three degrees of separation. Retrieved on 2022, from http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

Schweitzer, Y., Sibani, G., & Yogev, E. (2011). Cyper space and terrorist organizations, Military and strategic affairs, 3(3): 44.

Tumer, S. (1991). Intelligence for a new world order, Foreign Affairs, 70(4): 150-166.

https://journal.pass.ps « DOI: 10.36554/1796-007-001-003 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854