التكنولوجيا والثورة السورية: حوار مع دلشاد عثمان و وائل علواني

الكاتب : شيرين الحايك و حسين الشيخ

التاريخ : ٢٢ يوليو ٢٠١٢ م

وائل علواني : مدون من سوريا. مهتم بمجالات تحليل البيانات والتعامل معها وأمن المعلومات. مدونته الشخصيه: wa2el.net.

دلشاد عثمان: ناشط تقني , أو خبير امن معلومات، شغل منصب مدير الـ New Media في المركز السوري للإعلام و حرية التعبير. حاصل على زمالة حرية الإنترنت 2012 من وزارة الخارجية الأميركية و مجلس حقوق الإنسان.

منذُ زمن، حتّى قبل الثورة، كثيرا ما كان السوري يعاني من التدقيق الرقابي على تصفح الإنترنت، ما هي أكثر الطرق أماناً بتصفّح الإنترنت في سوريا هذه الأيام دون التعرّض لمشاكل؟

دلشاد: يوجد العديد من الطرق التقنية التي ما تزال تعمل في سوريا , بالرغم من الضغط الشديد و التكنولوجيا المتطورة كـ DPI (التي تستطيع تحليل جميع الاتصالات الخارجة برغم تشفيرها و معرفة جهتها و تفاصيلها الداخلية) حيث ان تطبيق TOR الشهير مازال يعمل و هو مشروع مجاني يعتمد على مجموعة من المتطوعين من حول العالم يقومون بتشغيل حواسيبهم بشكل دائم من اجل منح الناشطين الذين يعانون من انترنت مقيدة – كما في سوريا – من الدخول بحرية , بالاضافة لتطبيق الاكسبات شيلد expatshield الذي هو تطبيق مجاني تقوم بتوفيره شركة AnchorFree , الذي بدوره يؤمن – قناة – اتصال مشفرة لجميع البرامج , تصفح , سكايب , ماسنجر.. الخ الخ

بالإضافة لبروتوكول الـ SSH, حيث انه بروتوكول يستخدم من اجل إدارة المخدمات عن بعد إلا أن السوريين استغلوه من أجل استثمار ما يسمى بالـ SSH tunnel و هي عبارة عن قناة تؤمن تبادل الملفات عبر الانترنت بطريقة مشفرة و بعض انواع اتصال الـ VPN المعدل, و الذي يستطيع فتح قناة اتصال مشفرة , تقوم بنقل حاسوبك الشخصي نظرياً – تبادل بيانات – الى خارج الدولة و التحول لجزء من شبكة موجودة في مكان ما خارج سوريا.

وائل:الطرق الأكثر أماناً بتصفّح الإنترنت في سوريا هذه الأيام دون التعرّض لمشاكل؟

يمكن القول بأن هناك ٣ طرق رئيسية عالية الأمان يمكن تصفح المواقع من خلالها بحرية ودون الخوف من التتبع والملاحقة الأمنية.

** الأولى، هي عبر بروكسي باتصال مشفر بشرط الوثوق بمزودي البروكسي (لأن هناك بروكسيات مشفرة تنشر عناوينها على أنها موثوقة، ولكنها في الواقع تعود للحكومات التي تريد مراقبة المستخدمين). طريقة استخدام البروكسي المشفر مستخدمة بكثرة في سوريا، وقد كتب أحد المدونين متهكما على الموضوع، وكان هذا قبل الثورة بفترة طويلة نسبيا، أن إيجاد بروكسي مشفر بات جزءا من عادات المستخدم السوري اليومية التي يمارسها كل صباح مع القهوة وصوت فيروز.

**الطريقة الثانية هي استخدام مشروع "تور" وهو مشروع متاح للعموم يهدف إلى إخفاء هوية المتصفح على الانترنت عبر تمرير أي طلب يطلقه جهاز المستخدم لزيارة صفحة معينة من خلال شبكة من الخوادم المنتشرة حول العالم قبل وصول الطلب لخادم الصفحة المطلوب زيارتها. الاتصالات عبر تور مشفرة، وفي حال قامت الحكومات بحجب الاتصال بالخوادم الشهيرة التي يستخدمها تور، فإن هناك قوائم تتحدث بشكل دوري تحمل عناوين خوادم أخرى تجعل من الصعب جدا على الحكومات الاستمرار بالحجب وستكون العملية منهكة جدا لهم.

** الطريقة الثالثة هي استخدام الساتالايت والأقمار الصناعية. يعيب هذه الطريقة أنها مكلفة جدا قياسا على الطرق الأخرى، ولكنها الأكثر أمنا، ويستخدمها الناشطون السوريون. وفي سوريا تحديدا، يستهدف النظام المباني التي يلحظ وجود الأجهزة الفضائية التي ترسل البث للأقمار الصناعية على أسطحها لعلمه أن الناشطين يستخدمونها لبث مقاطع المظاهرات وغيرها. إذ هي طريقة تتضمن المخاطرة.

هل يمكنُ لناشط مغترب أن يقدّم دعم في مجال الأمان و حماية الإنترنت للناشطين في الداخل؟ كيف ؟

وائل: بالطبع، وعلى عدة مستويات ومن أبرز الأمثلة لا على الحصر:

- تثقيف المستخدمين بأفضل الأساليب لحماية هويتهم وتقليل مخاطر التتبع والملاحقة (تثقيف عبر المدونات وشبكات التواصل الاجتماعي ومقاطع الفيديو(

- مساعدة مالكي مواقع المعارضة والناشطين في تحصين مواقعهم ضد الهجمات الغوغائية ومساعدتهم في استعادة السيطرة على المواقع والحسابات. كما نعلم العالم الرقمي مكننا من الاتصال بالخوادم والأجهزة حول العالم من أجهزتنا الشخصية، لذلك يمكن حل جميع المشاكل من هذا النوع من على بعد.

- تطوير آليات تواصل مشفرة عالية الأمان مثل برامج الكمبيوتر وتطبيقات الجوالات والمواقع

- الهاكتيفيزم وهو التهكير دعما لقضية معينة ولإضعاف قدرة الخصم الالكترونية. أبرز المجموعات التي تقوم بذلك هي أنونيموس التي تضم هاكرز كثر من بينهم هاكرز سوريين حول العالم ويقومون باختراق خوادم النظام السوري وتسريب الملفات الدقيقة بغرض إحراج النظام وكشف جرائمه. الانخراط في هذه المجموعات يجب أن يتم بحذر شديد لأنها دوما عرضة للاختراق تنظيميا من قبل آلاف بي آي والسي آي إيه وغيرها من وكالات الاستخبارات، وقد حصلت حالات سابقا لذلك.

كما أن التهكير عموما يمكن إساءة استغلاله ليتحول من موهبة موجهة لغرض سامٍ مثلا إلى تخريب غير مسؤول نابع عن أيديولوجية ضيقة فيصبح وسيلة لتصفية الحسابات السياسية والفكرية. هو خيار مطروح لمن يرى في نفسه القدرة ولكن التعاطي معه يجب أن يكون بشكل مسؤول ومحسوب العواقب والنتائج.

دلشاد: هذا ما أقوم به , وجدت نفسي خارج القطر منذ 6 أشهر أقوم بتقديم الدعم بشكل أكبر مما كنت به في سوريا, حيث أنه بسهولة أستطيع القيام بحجز مخدمات و إدارتها و توفير حسابات للناشطين , بالإضافة مساعدة الناشطين و مواقعهم التقنية , حيث أني أمتلك انترنت أسرع و مؤمن و متوافر بسهولة, في نفس الوقت نقوم بتنظيم دورات تقنية يستطيع الناشط حضورها في صفوف افتراضية.

هل تعتبر بأنّه يجب أن يكون للمجلس الوطني و الهيئات و المنظمات المعارضة الأخرى قسم خاص بتأمين الحماية الأمنية أولاً و التقنيات و الدورات ثانياً أو أيّة طرق أخرى ؟ هل تعتبر بأنها لعبت أيّ دورٍ في هذا السياق ؟

دلشاد: من الضروري جداً أن يمتلكوا فريقاً تقنياً و لكن للأسف تعرض الكثير من السياسيين و الهيئات إلى عمليات قرصنة تسببت بتسريب معلومات هامة جداً , بالمقارنة مابين الأمان العالي الذي يمتلكه فريق لجان التنسيق المحلية بالمقارنة مع المجلس الوطني , نجد أن سجل لجان التنسيق المحلية بالاختراقات نظيف بسبب المتابعة و لكن بالمقابل تسريبات بريد برهان غليون و اختراق حسابه على الفيس بوك بالإضافة لحساب العديد من الأعضاء كان كفيلاً بان يقوموا بإيجاد حماية إضافية

وائل: من المهم جدا اتباع مثل هذه الخطوات من قبل المجلس والهيئات والتنظيمات لأن المعارضين والناشطين عموما مستهدفون باستمرار من النظام السوري، وهذا ينطبق على فترة تسبق الثورة السورية بكثير ومستمرة إلى يومنا هذا. النظام السوري منذ تلك الفترات كان واعيا لهذا الموضوع و بنى قدرة أمنية متقدمة تضم هاكرز ومخترقي مواقع لتعزيز قدرته الداخلية على مراقبة وملاحقة النشطاء. كما أنه وظف أناسا قد لا يملكون خبرة في مجال الأمن الالكتروني، ولكنهم يفيدون في أنواع معينة من الهجوم كهجوم الإغراق والإقصاء عن الخدمة (Distributed Denial of Service) والتي تتضمن إغراق خادم موقع ما بطلبات استعراض لصفحاته تجعل الخادم مشغولا وغير قادرا على تحمل كمية الطلبات هذه.

إذا بشكل آخر، توظيف الحشود لتنفيذ عملية تخريبية لموقع معارض.

لا نريد أيضا تضخيم قدرة النظام الأمنية وقدرة الهاكرز الذين نظمهم، فهناك اختراقات حصلت لمواقع المعارضة واكتشفنا أن من وراءها يجيد متابعة مواقع الهاكرز ويستخدم أدوات كتبها آخرون لتنفيذ هجماته، وربما استخدمها بغباء لا ينم إلا عن قلة معرفة بالمجال الأمني وأنه في النهاية كان له الفضل بتشغيلها فقط. هؤلاء يسمون بأطفال السكريبتات Script Kiddies وهم كثر.

ولم ألحظ أية مبادرة نابعة من المجلس وغيره لها ارتباط بهذا الخصوص.

ما هو باعتقادك أفضل طريقة لتقديم مساعده للداخل؟ و ما هي المواد التي تعتقد بأنها ستقدم خدمات كبيرة في الداخل – عدا الكاميرات و الكومبيوترات – ؟

وائل: الناشطون بحاجة دائما لوسائل اتصال آمنة وقادرة على الاستمرار في وجه الحجب والملاحقة. وسائل الاتصال تشمل التواصل فيما بينهم، بالإضافة إلى بث ما يسجلونه في المواقع والقنوات. من المهم أن نستمر بالتواصل معهم ومعرفة حاجاتهم الدقيقة وتزويدهم بها، إن كان على شكل نصائح، انتقاء برامج، تطوير برامج وتطبيقات، تزويدهم بأجهزة اتصال يصعب توفيرها بالظروف التقليدية كأجهزة اتصال فضائي بالساتالايت.

دلشاد: الانترنت الفضائي VSAT System ضروري جداً في هذا الوقت و هو أهم من أي شيء آخر ,النظام يقوم بقطع الانترنت في العديد من المناطق و خصوصاً تلك التي يسيطر عليها الثوار , بالمقابل نجد أن السوريين تأقلموا و تمكنوا من تركيب تلك الأجهزة في أماكن بعيدة و نقل الإشارة لغرف العمليات الخاصة بهم لذا فهي مهمة جداً.

عندما تمّ استهداف الصحفيين الأجانب في بابا عمرو في شباط الماضي، أذيعَ أنّه تمّ استهداف المركز الإعلامي عن طريق الأجهزة الإنترنتيّة اللاسلكية التي كانت تستخدم من قبلهم، هكذا تمّ التعرّف على مكانهم و استهدافهم، هل يمكن أن يكون هذا الكلام صحيحاً ؟ و هل هناكَ طرق تحايل على مثل هذه المعطيات حتّى لا تكشف مكان الناشطين؟

دلشاد: بالطبع , ما كان يستخدمه الصحفيين الأجانب في بابا عمرو كان جهاز ما يسمى بالبيغان و الثريا اي بي , مشكلة هذه الأجهزة أنها لا تمتلك (انتينة) لاقط موجه على شكل Dish) صحن) بل تقوم بتوزيع الإشارة بزاوية منفرجة , لذا فطاقتها أكبر من طاقة جهاز الانترنت الفضائي الذي يمتلك (صحن) و إبرة , و الذي تكون زاويته أقل بالإضافة للطاقة

البث الأقل Uplink لذا , وجود هذه العناصر يعتبر مهماً جداً و مع ذلك , طلعات الطيران تستطيع كشف جميع الأجهزة الفضائية.

وائل: مع الأقمار الصناعية تحتاج وضع طبق الإرسال والاستقبال على أسطح المباني. وهذه يسهل تمييزها من قبل القناصة أو طائرات الاستطلاع، وربما عن طريق أجهزة أخرى تلتقط وجود إشارات بث قوية من جهات معينة (ولكنها لا تتعرف طبعا على محتوى الاتصال) ويمكن عبرها تحديد أماكن أجهزة البث. لا أعلم إذا كان النظام السوري يملك مثل هذه الأجهزة. ربما تكون أفضل طرق التحايل مرتبطة بطريقة تنصيب أجهزة البث على الأسطح بشكل موارب لا يثير الانتباه. أيضا عدم التمركز في مكان لفترة طويلة، أي التحرك باستمرار والانتقال من موقع لآخر.

ما هي أأمن وسيلة لتبادل المعلومات على النت بين الناشطين على الأرض؟

وائل: هناك عدة وسائل اتصال مشفرة يمكن استخدامها ولكن من المهم دائما اللجوء للوسائل مفتوحة المصدر التي تعرف قوتها التشفيرية والتي لا تتبع لشركات لا تنتهج مبدأ الشفافية من ناحية الطلبات التي تصلها من حكومات تطلب الاطلاع على بيانات الناشطين، وكون هذه الشركات لا توضح البنية التشفيرية التي استندت إليها ما يجعل معلومات الناشطين مهددة دوما بالكشف عنها.

الأمثلة على البرامج والوسائل عديدة ويتوجب تحديد الغرض الدقيق المراد منها والبحث عنها في المواقع البارزة والتي تهتم بالناشطين وتشرح لهم كيفية تنصيب البرامج واستخدامها بدقة.

دلشاد: إن كانت موبايل أو حاسوب , استخدام الاتصال الآمن VPN – SSH ...etc بالإضافة لتوخي الحذر باستخدام برمجيات مضمونة و فعالة و القيام بوضع الإعدادات بشكل صحيح يفي بالغرض .

يعتقد الكثير بأنّ إجراءات الأمان معقدة جدّاً ، كيفَ يمكنها أن تكون أبسط؟

دلشاد: كتقنيون سوريين نتفهم ما معنى أن تقتحم الانترنت منازل أغلب المواطنين , و أن تتحول التقنية حاجة ملحة من أجل بقاء التواصل و نشر الأخبار , لذا نعمل بشكل كامل للتعامل مع كافة المستويات التقنية , بالإضافة لقيام التقنيين السوريين بتدريب مدربين يقومون بنفس المهام و بحسب اختصاصات مختلفة.

كتجربة شخصية أعاني أحياناً و خصوصاً من ناحية تفهم القوانين الخاصة بخصوصية الفيس بوك , مثلاً موضوع الاسم الوهمي , أو تواجد صور تحض على العنف أو التعليقات الطائفية التي تسبب بإغلاق الصفحات على الفيس بوك.

وائل: اكتساب المهارات الأساسية في تعزيز الأمان قد تكون صعبة في البداية ومعقدة، لكن مع التعود والممارسة، تصبح الأمور أكثر سهولة لأن المفاهيم الأساسية والتفصيلية تكون قد اكتسبت، وما يبقى هو الاطلاع المستمر على آخر البرامج والتطبيقات وأخذ الاحتياطات بشكل دوري كتغيير كلمات السر وتحديث برامج الحماية. يتوجب على الناشطين استيعاب أن الأدوات عالية الأمان تبقى أدوات، وأن التعويل هو على الحس الأمني لدى الناشط، والبقاء متيقظا لما يطلب منه، والروابط التي يفتحها، ومع من يتواصل. هناك مجال يسمى الهندسة الاجتماعية وهو علم يدرس كيفية التلاعب بالشخص بغرض أن يكشف الأخير معلومات حساسة. من المهم الاطلاع على أبرز أساليبه والاستفادة من تجارب الآخرين لتحصين النفس. ...

الجيش الالكتروني السوري، ماذا تشعر عندما تسمع بهذا الاسم ؟

وائل: يأتيني دفق من المشاعر السلبية السوداء وأتذكر فورا بعض مواقع المعارضة التي شاركت وأحد الأصدقاء في صد الهجمات عليها قبل وبعد الثورة، وأتذكر كم تعادي هذه المجموعات وأسيادها الفكر والثقافة والحرية.

دلشاد: مجموعة من الشباب السوري يمتلكون خبرة تقنية و لكن للأسف تم تجنيدها لمحاربة حرية الانترنت , لم يحصل لحد هذه اللحظة أي تماس مباشر بيننا كتقنيين اتخذنا من الحماية عملاً لنا و بين الجيش السوري الالكتروني..

يؤلمني أن أحد أصدقائي المقربين تحول لأحد أعضاء الجيش السوري الالكتروني و في إحدى المرات أخبرني ساخراً بأنه على استعداد لتنظيف) صفحتي (بالمقابل أن أقدم لهم العون, مؤلم جداً أن تستخدم معرفتك و علمك للحرب.

هل تعتبر أنك – مع آخرين – تشكلون الجيش الالكتروني السوري الحر؟

دلشاد: لم أتجه باتجاه الاختراق أو العمليات الهجومية الالكترونية بتاتاً لأني لا أؤمن بها , لذا لا أعتبر نفسي أنا و من يعمل بنفس الاتجاه أننا لسنا جيش إلكتروني , بل نحاول العمل على تثبيت حق الإنسان بالحصول على إنترنت حرة و نظيفة.

وائل: لا.. ما أقوم به بالتعاون مع شباب ضليعين في المجال الأمني ليس جزءا من أي تنظيم.

هل يمكن لكافة الجيوش أن تصبح الكترونية في يومٍ ما في المستقبل، إذا أخذنا بعين الاعتبار أن الحروب تنحو باتجاه كونها لا تحتاج إلى أسلحة مباشرة؟

وائل: لا لا أعتقد ذلك.. الحرب الالكترونية هي معركة وجبهة من جبهات الحروب الحديثة التي تهدف إلى ضرب قدرة الخصم الالكترونية والبنية التحتية التقنية. وما نشهده من حرب إلكترونية بين إيران وإسرائيل وأميركا يعتبر من أكثر هذه الحروب تقدما، إذا ما نظرنا إلى كمية الاستثمارات في برمجة الفيروسات والبرامج التجسسية الموجهة.

دلشاد: طبعاً و هذا ما نراه في سوريا و الصين و إيران , كما النزاع العنيف الالكتروني بين السعودية و إسرائيل و الذي يتداخل في اختراقات قد تهز بنية اقتصادية أو حتى عسكرية , الجيوش الالكترونية لن تكون بديلاً و لكن ستصبح جيشاً متوازياً , التجربة السورية كانت خير بيان لمصطلح الجيش الالكتروني.....

يقوم الفيس بوك – ضمن اتفاق – بإغلاق صفحات من يتم اعتقالهم بشكلٍ موثوق لتأمين الحماية لأصدقائهم، و انضمّ السكايب إلى قائمه من يتعاونون و يتفهمون ظروف الاعتقال السورية و يغلقون – ضمن شروط – الحسابات التي تعود لمعتقلين في سوريا، ما رأيك في هذا و هل تعتقد أنه قد يكون هناك مجال أكبر للدعم من قبل مؤسسات كهذه و غيرها من الشبكات الإجتماعية كالتويتر و غوغل و غيرها؟

دلشاد: بذلنا الكثير من الجهد لإقناع مايكروسوفت و من بعدها ياهو للقيام بعمل مماثل , في النهاية وجدنا تفهماً كاملاً للظرف السوري . الكثير من الأصدقاء تم إنقاذ حياتهم بكل معنى الكلمة و إنقاذ جميع من يتواصل معهم عن طريق إغلاق حساباتهم , لا تتخيل ما لذي يعنيه وصول خبر بان صديقك تم إطلاق سراحه لعدم توافر أي أدلة ضده في غضون يوماً ..

وائل: يعتبر أمرا جيدا مع الأخذ دائما بعين الاعتبار أن فيس بوك وسكايب لا تحققان مراتب متقدمة في مقاييس شفافية الأداء بما يتعلق بتعاملها مع الحكومات. بغض النظر عن التفاصيل حول هذا الموضوع، أرى أنه أمر جيد ومن المهم أن يكسب النشطاء السوريون دعم شركات أخرى كتويتر التي تحقق مرتبة متقدمة جدا في شفافية التعامل مع الحكومات.

كثيرا ما يذاع عن أنّ الفيس بوك غير آمن حتى في الغروبات السرية و ينصح عادهً بعدم تبادل أيّة معلومات عليه، ما رأيك ؟

وائل: نعم يبقى مستخدم فيس بوك عرضة للاختراق دائما بمجرد الضغط مثلا على روابط ضارة تسحب معلومات حسابه، أو أن يضيف شخصا ينتحل هوية صديق له. الفيس بوك بات مستهدفا بشكل كبير من الهاكرز الذين يمكنهم النفاذ لمعلومات الشخص من جهات عدة (روابط ضارة، تطبيقات تنتهك الخصوصية، انتحال الشخصيات،...)

يجب التعامل به بحذر شديد واللجوء لطرق أخرى لتبادل المعلومات الحساسة والسرية.

دلشاد: لا يوجد شيء آمن 100% أنواع الاختراقات متعددة, ففي حال تم اختراق الحاسوب الشخصي لمستخدم ما , فان جميع الغروبات السرية و الصفحات و الرسائل الخاصة ستصبح مكشوفة , إلا انه بالمقابل , لعبت دوراً هاماً في التنسيق وخصوصاً بعد ارتفاع مستوى إدراك ماهية امن المعلومات و كيفية الحماية الشخصية.

الأسماء الوهمية؟ هل تفيد في تمويه شخصية المستخدم و ما رأيك باستخدامها تقنيا و فكريا؟

دلشاد: في ظرف مثل الظرف السوري ليس مطلوباً من أحد أن يظهر باسمه الحقيقي ,في ظل وجود الجيش السوري

الالكتروني المنتشر في جميع الصفحات , إلا أنه بالمقابل وجود الأسماء الحقيقية يعني قيام الشعب السوري بكسر حاجز الخوف الرئيسي على الانترنت , استخدم السوريين شبكات التواصل الاجتماعية للتنسيق و نشر الأخبار , لذا في ظل الأسماء الوهمية تعتبر تلك الأخبار غير موثقة بشكل كامل , هذه أيضا ضريبة !

وائل: قد تكون مفيدة للبعض وهي تعود للشخص واختياراته وظروفه. ولكنها من الناحية الأمنية ليست ذات تأثير كبير فمن الممكن تتبع أثر الشخص والوصول إلى مكانه. طبعا يتطلب الموضوع مراقبة وجهدا للوصول إلى الشخص بعينه، ولكن كلما برع الشخص بإخفاء هويته (باستخدام برنامج تور مثلا) فإن التعرف والوصول إليه سيكون صعبا جدا.

أيّ شيء آخر؟

دلشاد: تقييد حرية الانترنت بتضييق الخناق بالمراقبة و نشر الفيروسات يعتبر خرقاً للقوانين و للأخلاق العامة , أن تجد عنصر مخابرات يمتلك خبرات تقنية هو أمر طبيعي أما أن يتحول الإنسان التقني لعنصر مخابرات ، هو الأكثر ألما و الذي نتمنى أن لا نجده في سوريا المستقبل..

شكراً لكم

موقع الانتفاضة الشعبية في سوريا

المصادر: