



إيهاب خليفة

منسق برنامج التطورات التكنولوجية
بمركز المستقبل للأبحاث والدراسات
المتقدمة - أبوظبي - الإمارات العربية
المتحدة

تحولت مواقع التواصل الاجتماعي إلى سلاح إعلامي فعال، وباتت إحدى الأدوات الرئيسية التي يتم توظيفها في المعارك السياسية والعسكرية والإعلامية، لتحقيق الأهداف الاستراتيجية لدولة أو جماعة ما، وذلك بما تمتلكه من عدد مستخدمين يقرب من ملياري مستخدم، وبما تتميز به من سرعة في نقل المعلومات في الوقت الحقيقي للحدث، وقدرتها على التشبيك المباشر بين مختلف المستويات الرسمية وغير الرسمية.

وقد وضعت العديد من دول العالم استراتيجية إعلامية وعسكرية للتعامل مع هذه المواقع في ضوء ما تطرحه من تحديات تتعلق بصعوبة التحقق من هوية المستخدمين، أو التأكد من صحة المعلومات المتداولة من خلالها؛ لتتشكل ظاهرة جديدة يمكن أن يطلق عليها «حروب مواقع التواصل الاجتماعي»: إذ أنشأت بعض الدول كتائب إلكترونية، مهمتها الدفاع عن صورة الدولة، والمساهمة في تحقيق أهدافها، لتتشكل جبهة حرب حقيقية موازية، ساحة القتال فيها هي مواقع التواصل الاجتماعي، وأدوات القتال هي الفكرة والمعلومة والصورة والفيديو وبرامج الكمبيوتر العملاقة، والخسائر فيها تمثل خصماً من اتجاه الرأي العام المؤيد لأحد أطراف الصراع. كما عمدت العديد من التنظيمات والجماعات الإرهابية والمتطرفة وشبكات الجريمة المنظمة وغيرها إلى تشكيل مثل هذه الكتائب الإلكترونية لأغراض مختلفة.

الكتائب الإلكترونية:

الملاحم العامة لحروب مواقع التواصل الاجتماعي في الشرق الأوسط



الإقليمي أو الدولي، عبر وسائل التواصل الحديثة، سواء كان ذلك من خلال مواقع الإنترنت أو عبر التطبيقات الهاتفية للتواصل الاجتماعي، خلال فترة زمنية معينة، تصاحبها تطورات سياسية أو عسكرية".

ومن أبرز الأمثلة على ذلك، الحرب على مواقع التواصل الاجتماعي بين حركة حماس وإسرائيل خلال العدوان المتكرر على غزة، حيث يسعى كل طرف دائماً إلى إبراز اعتداءات الطرف الآخر عليه، ومحاولة الظهور أمام الرأي العام الإلكتروني المتشكك على مواقع التواصل الاجتماعي باعتباره ضحية تدافع عن نفسها.

وتظهر هذه الحرب في السياسة أيضاً، سواء كانت داخلية أو إقليمية، وتجد - وبصورة فورية - طريقاً لها عبر مواقع التواصل الاجتماعي، مثل الانتخابات والاستفتاءات والاستطلاعات والقوانين وغيرها من الأحداث، حيث تبدأ الهاشتاجات (Hashtags) في الانتشار، ما بين مؤيد ومعارض، ويحاول كل طرف أن يبرر وجهة نظره ويستقطب الطرف الآخر لها.

2- أبرز خصائص حروب التواصل الاجتماعي:

تتسم حروب مواقع التواصل الاجتماعي ببعض الخصائص، أبرزها:

- ساحة القتال فيها افتراضية، وبالتالي لا توجد لها حدود جغرافية أو إقليمية يمكن احتلالها أو طرد عدو منها.
- الحرب فيها من دون رصاص أو حطام، والخسائر ليس بها أشلاء أو ركام، والأسلحة المستخدمة ليس لديها قدرة على تدمير العدو أو إزالته.
- تلعب التكنولوجيا الدور الرئيسي في هذه الحرب؛ فالطرف الذي يمتلك البرامج المتطورة القادرة على تحليل مواقع التواصل الاجتماعي، وتحقيق التفاعل بين المستخدمين عبرها، واختيار أفضل الأوقات لبث الأفكار والحجج التي تؤيد رأيه، هو الذي تكون له الغلبة في النهاية.

- مرتبطة بالتطورات السياسية والعسكرية على أرض الواقع.
- يشارك فيها المدنيون بصورة أكثر من العسكريين.
- ليس بها هدنة، حتى لو تحققت على أرض الواقع، ولا يمكن إيقافها.
- لا يمكن فيها تدمير العدو كلياً أو إزالته.

3- فواعل حروب التواصل الاجتماعي:

يشارك في حروب مواقع التواصل الاجتماعي العديد من الفواعل، تبدأ بالأفراد، وتنتهي بالدول، مروراً بالحركات الإرهابية والأحزاب السياسية وجماعات الضغط والمصالح والناشطين السياسيين، ويشترك في إدارة هذا النوع من الحروب العديد من الجهات منها:

ويمكن تعريف مواقع التواصل الاجتماعي بأنها "خدمات تتوافر من خلال شبكة الإنترنت، تسمح للأفراد بتقديم لمحة عن حياتهم العامة من خلالها، وإتاحة الفرصة للتواصل مع الآخرين من أصدقائهم، والمشاركة المتبادلة للمعلومات المتاحة بينهم" وتختلف طبيعة عملية الاتصال من موقع لآخر⁽¹⁾؛ فقد تتم عملية الاتصال من خلال مواقع مبادلة الصور مثل إنستجرام، أو الفيديوها مثل يوتيوب، أو الرسائل القصيرة مثل تويتر، أو قد تشمل جميع هذه الأدوات مثل الفيسبوك.

لقد أصبحت جميع هذه المواقع وغيرها أدوات رئيسية ليس فقط لمشاركة الأحداث الاجتماعية، والخواطر الشخصية، والأفكار الفردية، في إطار جمعي بين المستخدمين، أو التعبير عن الأفكار السياسية والتوجهات الأيديولوجية للمستخدمين، بل تحولت كذلك إلى أدوات لصناعة الأحداث والأخبار والحشد وتنظيم التظاهرات والاحتجاجات، أو جمع توقعات لأهداف ما، أو تسويق أفكار ومنتجات. والأخطر من ذلك أنها تمثل منصة سياسية وأيديولوجية لنشر الأفكار المتطرفة، وتجنيد الأعضاء، والحصول على التمويل، كما يحدث من قبل التنظيمات الجهادية المتطرفة والإرهابية والإجرامية؛ وهو ما جعل هذه المعارك الافتراضية أقرب ما تكون لحرب حقيقية تؤثر في العالم الواقعي، الأمر الذي أبرز ضرورة التعامل الجدي مع هذه الظاهرة الجديدة التي تمس الأفراد والمجتمعات والدول.

في هذا الإطار تستهدف هذه الدراسة إلقاء الضوء على ماهية وخصائص حروب التواصل الاجتماعي، باعتبارها جزءاً مما يطلق عليه الحرب الإلكترونية، وتحديد أهم الفواعل الأكثر استخداماً لمواقع التواصل الاجتماعي لتحقيق أهداف مختلفة، كما تناقش أبرز أدوات هذه الحرب خاصة برامج الكمبيوتر المستخدمة على وجه خاص من قبل الإدارة الأمريكية، والهاشتاج باعتباره أصبح من أكثر الأدوات شيوعاً داخل هذه المواقع، وتنتهي الدراسة بتحليل أولي للأنماط الأكثر شيوعاً لهذه الحرب بمنطقة الشرق الأوسط، سواء على مستوى الدولة الواحدة، أو على المستوى الإقليمي.

أولاً: ماهية وخصائص حروب مواقع التواصل الاجتماعي

تعتبر حروب مواقع التواصل الاجتماعي من الظواهر الحديثة المرتبطة بتزايد دور هذه المواقع في التأثير على التفاعلات اليومية، ليس فقط على المستوى الاجتماعي، بل أيضاً على المستوى السياسي والأمني. ولما كانت هذه الظاهرة حديثة، فهي تطرح عدداً من الأسئلة الرئيسية الخاصة بماهية هذه الحروب، والعناصر المشتركة فيها، وكيفية إدارتها، وهل يمكن تحقيق الانتصار فيها؟

1- تعريف حروب التواصل الاجتماعي

لا يوجد تعريف محدد لحروب مواقع التواصل الاجتماعي، نظراً لحدائتها، وعدم اكتمال أبعادها، فهي ظاهرة لاتزال قيد التشكل، ولكن يمكن النظر إليها على أنها "تحدث حينما تتنافس جهتان متصادمتان أو أكثر، على جذب اهتمام الرأي العام، المحلي أو



التواصل الاجتماعي تدعم النظام الإيراني وقادة الجمهورية الإسلامية، وتعمل على مهاجمة المعارضين السياسيين.

وقد تم إنشاء الجيش الإلكتروني الإيراني، وهو جهة غير رسمية، ويتكون من مجموعة من القراصنة المحترفين، وتوجد تكهنات بأن المشغلين الحقيقيين للجيش الإلكتروني الإيراني هم مجموعة من القراصنة والمطورين (developers) الروس، ويقومون بتقديم الدعم للجيش الإلكتروني الإيراني، وتصل بعض التقديرات إلى أن الجيش الإلكتروني الإيراني يضم ما يقرب من 120 ألف متسلل متطوع. ولعل هذا الرقم مبالغ فيه، إلا أنه قد يشمل متطوعين من كتائب حزب الله ومن الجيش السوري.

من جانب آخر لم يعد إنشاء الكتائب الإلكترونية حكراً على الدول وحدها، فقد اعتمد تنظيم "داعش" على كتائبه الإلكترونية في عمليات التجنيد من خلال مواقع التواصل الاجتماعي، والمساهمة في إيجاد صورة ذهنية عن التنظيم تميزت بالوحشية من خلال عرض المجازر التي يرتكبها عبر هذه المواقع.

وبالمثل تؤسس العديد من الجماعات هذه الكتائب للدفاع أو الهجوم السياسي، فقد اشتهرت كتائب جماعة الإخوان المسلمين في مصر باسم "كتائب خيرت الشاطر"، نائب مرشد جماعة الإخوان في مصر، وتورطت هذه الميليشيات الإلكترونية الإخوانية في شن هجمات إلكترونية عديدة، منها محاولة الهجوم على مواقع حكومية إماراتية في أعقاب ثورة 30 يونيو وعزل الرئيس "الإخواني"، نظراً لدعم الإمارات لثورة 30 يونيو.

4- معايير الانتصار في الحرب الإلكترونية

لا يوجد في حروب مواقع التواصل الاجتماعي منتصر ومهزوم بشكل مطلق، فالانتصار نسبي لكل منهما، والطرف الذي يمتلك التكنولوجيا والقدرة على تسويق حججه وأفكاره، يتفوق على الطرف الآخر، ولكن من دون أن يخرج من هذه الحرب كلياً.

ولمعرفة إلى أي مدى استطاع أحد طرفي الحرب أن يحقق انتصاراً نسبياً على الآخر، يمكن الرجوع إلى عدة معايير، منها معايير كمية وأخرى كيفية، وتتمثل في التالي:

• **المعايير الكمية:** ويتم خلالها الاعتماد على عدد المؤيدين

• **الدول والأجهزة السيادية،** بما تمتلكه من برامج مراقبة وتحليل المواد المنشورة على مواقع التواصل الاجتماعي، ومتابعة الحسابات الشخصية النشطة، أو إيجاد حسابات وهمية، أو إنشاء كتائب إلكترونية لبحث أفكار معينة، وإيجاد اتجاه رأي عام إلكتروني على مواقع التواصل، حتى وإن كان غير حقيقي.

• **الشركات التي تمتلك مواقع التواصل الاجتماعي،** بما تمتلكه من قدرة على إدارة الحسابات الشخصية أو غلق بعض الحسابات أو الصفحات أو تغيير معدلات ظهورها في نتائج البحث الخاص بها، أو عقد اتفاقات مع بعض الدول لتسهيل حصولها على معلومات حول المستخدمين.

• **قادة الرأي العام،** بما لديهم من مصداقية لدى الرأي العام، وعدد مشاركين ومتابعين على مواقع التواصل الاجتماعي قد يصلوا إلى الآلاف، وفي بعض الأحيان ملايين من المتابعين الذي يساهمون في نشر أفكارهم وآرائهم حول القضايا المثارة.

• **المستخدمون التقليديون،** بما لديهم من قدرة على ترجيح كفة أحد الأطراف من خلال المشاركات التي يتبنونها وقدرتهم على إيجاد اتجاه عام حقيقي داخل مواقع التواصل الاجتماعي.

• **الكتائب الإلكترونية،** وتتنوع ما بين مجموعات تشكلها دولة ما للدفاع عن مصالحها أو الإضرار بطرف آخر، وتنظيمات إرهابية تستخدم وسائل التواصل الاجتماعي لعرض أفكارها ومحاولة تجنيد عناصر لها.

ويمكن تعريف "الكتائب الإلكترونية" (Cyber Militias) على أنها مجموعة من المتطوعين، الذين يتصلون بصورة أساسية من خلال الإنترنت، ويستطيعون إخفاء هويتهم كقاعدة عامة، ويمتلكون القدرة والرغبة على شن هجمات إلكترونية من أجل تحقيق هدف سياسي، ومن الملحوظ أن الكتائب الإلكترونية لا تخضع للسيطرة المباشرة للدولة، ومن الممكن أن تصبح إضافة مهمة لقوة الدولة الإلكترونية، ولكنها في الوقت ذاته من الممكن أن تتحول لتهديد للأمن القومي للدولة⁽²⁾.

وتتبع بعض هذه الكتائب الدولة، إذ تجند العديد من الدول مجموعة من الأشخاص المنظمين والمدربين على استخدام التكنولوجيا الحديثة ووسائل الاتصال، ويتميزون بكثافة نشاطهم ووجودهم على مواقع التواصل الاجتماعي، ويتم إمدادهم بالمعلومات بهدف نشرها عبر متابعيهم ومستخدمي هذه المواقع، وتكون مهمتهم الرئيسية هي الدفاع عن مصالح الدولة ومواقفها تجاه الأحداث، سواء من خلال اختراق الحسابات الإلكترونية والتجسس عليها أو الدفاع عن وجهة نظر الدولة تجاه بعض القضايا الرئيسية.

ولعل النموذج الأبرز في منطقة الشرق الأوسط هو كتائب الباسيج الإلكترونية، التي أنشأتها إيران بعد تعرضها لهجمات من فيروس (Stuxnet) الذي أصاب برنامجها النووي، كما تم تدريب مجموعة من الشباب الإيراني على استخدام أدوات الاتصال الحديثة بهدف المساهمة في عمليات التعبئة والحشد والمدافعة عن رموز الدولة، من خلال كتابة موضوعات عبر المدونات ومواقع

مواقع التواصل الاجتماعي بما يؤثر على الاتجاهات (Trends) السائدة حول موضوع أو قضية ما، ويغير من نتائج ظهورها على محركات البحث الخاصة بها. ويمكن لها أيضاً مراقبة كافة أنشطة المستخدمين على مواقع التواصل في زمنها الحقيقي (Real Time) والتجسس على تحركاتهم الافتراضية ومكالماتهم الهاتفية عبر الإنترنت.

وقد كشفت تسريبات إدوارد سنودن (Edward Snowden) الموظف السابق بوكالة الاستخبارات الأمريكية (CIA) ووكالة الأمن القومي الأمريكية (NSA) عن العديد من البرامج التي صممتها الإدارة الأمريكية واستخدمتها في حروب التواصل الاجتماعي، وبات معلوماً أن الإدارة الأمريكية لديها مجموعة كبيرة من البرامج الخاصة بالتجسس وجمع المعلومات ومتابعة المستخدمين على مواقع التواصل الاجتماعي، من أبرزها:

• برنامج بريزم (PRISM):

بموجب قانون حماية أمريكا (Protect America Act of 2007) الصادر في عام 2007، تم إنشاء برنامج سري يدعى (US-984XN) ويسمى أيضاً (PRISM)، وهو أحد البرامج التي تم تصميمها في إطار مكافحة الإرهاب. ويعمل برنامج "بريزم" على جمع معلومات من أشخاص داخل الولايات المتحدة وخارجها⁽³⁾.

وبموجب هذا القانون، فإنه بمجرد موافقة أحد القضاة السريين بـ "محكمة مراقبة الاستخبارات الخارجية" التي تم إنشاؤها بموجب القانون ذاته؛ يحق لوكالة الأمن القومي الأمريكي (NSA) أن تطلب من الشركات العاملة في مجال الإنترنت، مثل ياهو وفيسبوك وجوجل وأبل ومايكروسوفت وغيرها، بيانات تتعلق بمستخدمين لها حول العالم⁽⁴⁾.

وقد قام إدوارد سنودن بتسريب معلومات لصحيفة الجارديان البريطانية حول برنامج بريزم في يونيو 2013، موضحاً أنه برنامج تجسس رقمي أمريكي مصنف بأنه "سري للغاية" يُشغل من قبل وكالة الأمن القومي الأمريكية (NSA) بدأ منذ عام 2007، ويتيح مراقبة الاتصالات الحية والمعلومات المخزنة، واستهداف أي عميل (Client) لأي شركة منخرطة في البرنامج مثل شركة جوجل وفيسبوك وتويتر وغيرها، حيث يستطيع هذا البرنامج الحصول على معلومات تتضمن رسائل البريد الإلكتروني، ومحادثات الفيديو والصوت، والصور، والاتصالات الصوتية بروتوكول الإنترنت، وعمليات نقل الملفات، وإخطارات الولوج وتفاصيل الشبكات الاجتماعية⁽⁵⁾.

• برنامج (SMISC)

أعلنت وكالة مشروعات البحوث الدفاعية المتطورة (DARPA) في عام 2011 عن برنامج لاستخدام مواقع التواصل الاجتماعي في تحقيق التواصل الاستراتيجي (Social Media in Strategic Communication program (SMISC))، والذي يهدف لتطوير آليات لتحديد المعلومات الزائفة أو الحملات الخادعة، التي يتم نشرها عبر مواقع التواصل الاجتماعي،

لطرف المنتصر، سواء بمشاركة أفكاره أو أخباره أو الدفاع عن مواقفه عبر مواقع التواصل الاجتماعي. ويمكن الاستناد إلى معدل المشاركات (Content Sharing) على مدار اليوم، وعدد المشتركين (Subscribers) والمعجبين (Like) والمتابعين (Followers)، والاتجاه السائد على مواقع التواصل (Website Trending).

• **المعايير الكيفية:** وتتمثل في نوعية المشاركين في هذه الحرب، والوزن النسبي لهم داخل المجتمع، فكلما تعدد المشاركون، بمعنى عدم اقتصرهم فقط على المستخدمين العاديين، وإنما دخول قادة الرأي العام والمؤثرين فيه محلياً وإقليمياً ودولياً كذلك كان الطرف أقرب للانتصار.

ثانياً: أبرز الأدوات المستخدمة في حروب التواصل الاجتماعي

تتلاءم الأدوات التي يتم استخدامها في هذا النوع من الحروب مع طبيعتها وخصائصها السابقة، فبعضها له طبيعة افتراضية Virtual، ويتم داخل مواقع التواصل الاجتماعي، مثل المعلومات والصور والفيديوهات والهاشتاجات؛ وبعضها له طبيعة افتراضية أيضاً، ولكن خارج هذه المواقع، مثل برامج الكمبيوتر العملاقة التي تعمل على تحليل البيانات ومراقبة النشاطات على مواقع التواصل.

وفيما يلي أبرز هذه الأدوات التي يتم استخدامها في حروب التواصل الاجتماعي:

1- المعلومة والصورة والفيديو:

تعد المعلومة هي الأداة الأهم في هذا النوع من الحروب، أما الصورة والفيديو فيمثلان المؤثرات البصرية الأكثر تأثيراً وقدرة على الإقناع وجذب مشاركين، هذا علاوة على السبق بالنشر، لأن الموضوعات التي يتم نشرها أولاً غالباً ما تحظى بأكثر قدر من المشاركات، سواء أكانت صحيحة أم خاطئة، ولذلك فإن الطرف الذي يسبق بنشر فكرة أو معلومة، غالباً ما يجد صدى لدى مستخدمي مواقع التواصل الاجتماعي بصورة أكبر من الطرف اللاحق.

2- برامج إدارة حروب مواقع التواصل الاجتماعية:

تعمل هذه البرامج على تحليل البيانات والمعلومات المتاحة على



واسعة مؤخراً نظراً لقدرتها على الوصول إلى أكبر عدد من المستخدمين، وذلك بعد أن اتجهت العديد من مواقع التواصل إلى إدخال خاصية الهاشتاج (#Hashtag)، التي تعتبر أكثر الأدوات استخداماً في الوقت الحالي، إذ تضاعف عدد مستخدمي الهاشتاج عبر موقع تويتر، ثم اتجهت مواقع الفيسبوك وجوجل بلس وإنستغرام لاستخدام هذه الخاصية، لتصبح من أقوى أدوات التأثير داخل هذه المواقع.

وتتمثل السمة الرئيسية للهاشتاج في عدم وجود إدارة مركزية تتحكم في الرسائل التي يتم بثها من خلاله، فالجميع لهم المساحة المتساوية نفسها للتعبير عن رأيهم، ويحظون بفرص الظهور نفسها أمام الأصدقاء والباحثين عن الهاشتاج؛ مما جعله وجهة لكثير من مستخدمي مواقع التواصل خلافاً لصفحات الفيسبوك التي تعتمد على المركزية في الإدارة والتحكم.

وللهاشتاج سمات رئيسية، من أبرزها:

- الانتشار السريع، من أهم خصائص الهاشتاج قدرته على الانتشار السريع والوصول إلى أكبر عدد من الأفراد في زمن قياسي، فبمجرد إطلاق هاشتاج يحمل رسالة أو يتناول قضية أو خبراً عاجلاً، فإنه ينتشر بسرعة بين مستخدمي مواقع التواصل الاجتماعي.

- مؤشر أولي لقياس الرأي العام الإلكتروني، فعلى الرغم من أنه مؤشر غير دقيق إحصائياً إلى حد كبير، فإنه يعكس اتجاهاً عاماً سائداً داخل فئة معينة من المجتمع خلال فترة زمنية معينة.

- الهاشتاج المسيء هو الأسرع انتشاراً، فقد ظهرت بعض الهاشتاجات المسيئة، وانتشرت أسرع من غيرها في زمن قياسي داخل مواقع التواصل.

- العمر الافتراضي للهاشتاج قصير، لأنه غالباً ما يكون رد فعل على موقف قد يتغير، أو حملة دعائية مرتبطة بفترة زمنية معينة، فالهاشتاجات تتغير وفقاً للأحداث اليومية.

- القدرة على الوصول إلى الجمهور المستهدف في الوقت الحقيقي، لأن الآلية التي يعمل بها الهاشتاج تتيح الوصول إلى الجمهور المستهدف، ويتم عرض الهاشتاج في نفس وقت التعبير عنه على مواقع التواصل الاجتماعي.

ونتيجة لذلك، فقد ظهرت العديد من الاستخدامات، الإيجابية والسلبية، للهاشتاج، من أبرزها:

- القدرة على إيجاد تعاطف دولي مع بعض القضايا المحلية، حيث يمكن للهاشتاج الذي يتناول قضايا محلية أن يحظى باهتمام وتعاطف دولي، خاصة عند كتابته بلغات مختلفة.

- منصة إعلامية أثناء الأحداث الكبرى، فقد تم توظيف الهاشتاج بصورة فعالة أثناء تنظيم كأس العام 2014، مما أتاح الفرصة

ومواجهتها من خلال نشر المعلومات الصحيحة، ومن ثم تقليل قدرة الخصوم على الترويج لمعلومات خاطئة، كما يهدف هذا البرنامج لتمكين وزارة الدفاع من استخدام مواقع التواصل في بث رسائل إعلامية تخدم مصالحها الاستراتيجية⁽⁶⁾.

• برنامج (Sock Puppet)

هي عبارة عن حسابات شخصية وهمية يتم تدشينها من خلال برنامج إلكتروني على مواقع التواصل الاجتماعي بلغات مختلفة، بهدف بث رسائل تدعم رؤية ما خلال فترة الأزمات، وهو ما قد يُمكن الدولة من إيجاد اتجاه عام زائف أو غير حقيقي نحو قضايا معينة، بما يمكن أن يؤثر في الأحداث السياسية⁽⁷⁾.

• برنامج (SOCMINT):

استخدمت الحكومة البريطانية استراتيجية ("SOCMINT" Social Media Intelligence) بهدف تحليل البيانات الموجودة على مواقع التواصل الاجتماعي والخروج بمؤشرات إحصائية حول المستخدمين النشطين والمؤثرين عليها، ووضع مؤشرات معلوماتية خاصة بعمليات الحشد والتعبئة التي تقوم بها بعض الحركات الجهادية على هذه المواقع.

• تطبيقات اختراق الهواتف المحمولة:

أصبح استهداف الهواتف المحمولة والحواسيب اللوحية أداة لجمع المعلومات حول ملايين الأفراد في أنحاء العالم، حيث يمكن لبعض الجهات الرسمية وغير الرسمية اختراق بعض تطبيقات هذه الأجهزة وسرقة المعلومات الموجودة عليها، ومعرفة كافة

البيانات المُخزنة في حسابات المستخدم، مثل العمر والجنس والميول ومكان التواجد والمستوى العلمي وغيرها.

وكشف تقرير نشرته صحيفة "الجارديان" البريطانية، أن وكالة الأمن القومي الأمريكي تقوم بتطوير تقنيات تسمح لها باستغلال تطبيقات الهواتف الذكية للوصول إلى معلومات خاصة بالمستخدمين، مشيراً إلى أنه بمجرد قيام المستخدم برفع صورة إلى وسائل التواصل الاجتماعي باستخدام هاتفه الذكي، تستطيع الوكالة جمع معلومات، مثل جهات الاتصال في هاتف المستخدم، وعناوين البريد الإلكتروني، ومكان أو موقع المستخدم⁽⁸⁾.

كما سرب سنودن وثائق تؤكد استهداف وكالة الاستخبارات الأمريكية بيانات الهواتف المحمول، وذلك لجلب معلومات عن الإرهابيين وأهداف استخباراتية أخرى، حيث أنفقت الولايات المتحدة ما يزيد على مليار دولار لصالح برامج التجسس الخاصة باستهداف الهواتف الذكية.

3- الهاشتاج:

تقوم هذه الأداة بتصنيف الموضوعات المثارة عبر مواقع التواصل الاجتماعي، وتسهيل عملية الوصول إليها. وقد اكتسبت شهرة

البروكسي (Proxy) للدخول على المواقع المحجوبة في ليبيا⁽⁹⁾.

ويمكن تناول الملاح العامة لحروب التواصل الاجتماعي في منطقة الشرق الأوسط، بإيجاز، كما يلي:

1- على المستوى الداخلي للدول:

تتميز حروب مواقع التواصل الاجتماعي في منطقة الشرق الأوسط على المستوى الداخلي للدول بعدة سمات، أبرزها تنظيم الفعاليات الجماهيرية وغلبة الطابع الأمني، حيث تستخدم هذه المواقع في تنظيم التظاهرات والاحتجاجات الواقعية أو الافتراضية، أو في تشكيل جبهات حرب افتراضية بين أنصار ومعارض أحد التيارات السياسية أو الفكرية، ومن أبرز أشكال الاستخدام الأكثر شيوعاً، ما يلي:

أ- التشويه السياسي الإلكتروني:

يقصد به تشويه الرموز السياسية، شخصيات كانت أم دولاً أم مؤسسات، من خلال الإنترنت، لاسيما بعد الاستخدام الفعال لخاصية "الهاشتاج" بموقع تويتر، والذي يتم استخدامه من قبل العديد من التيارات الفكرية في معاركها السياسية والانتخابية، ويتضح ذلك في:

• **الإساءة للشخصيات:** فقد تم استخدام هاشتاج مسيء من قبل بعض شباب الإخوان المسلمين والمعارضين لترشح الرئيس عبدالفتاح السيسي للانتخابات المصرية، وتم الرد عليهم بهاشتاج مسيء أيضاً يتناول الرئيس السابق وجماعته.

• **الإساءة للدول:** ظهر ذلك عند انتقاد دولة قطر والأسرة الحاكمة على مواقع التواصل الاجتماعي على خلفية موقفها الداعم للإخوان المسلمين، وموقفها من الثورة المصرية.

• **الإساءة للمؤسسات:** من خلال انتقاد وزارة الداخلية المصرية حينما صرحت بمراقبة مواقع التواصل الاجتماعي، فامتلات المواقع بالسخرية من القرار كرد فعل عكسي من الناشطين الإلكترونيين.

ب- الاحتجاجات والتظاهرات الإلكترونية:

يتم في هذه الحالة استخدام الفضاء الإلكتروني باعتباره وسيطاً للتعبئة والحشد للاحتجاج على سياسات أو خدمات مدنية. وتبدأ العديد من الحملات الإلكترونية بعرض مطالب تهم عدداً كبيراً من المواطنين داخل الدولة، بما يساهم في زيادة عملية الترويج الإلكتروني لهذه المطالب، وإذا لم تتعامل الدولة بجدية مع هذه المطالب، فإنها تجد طريقها للتصعيد سريعاً، فتتحول خلال أيام قليلة إلى احتجاجات أو إضرابات فتوية.

ومن ظواهر الاحتجاج الإلكتروني قيام بعض الشباب في مصر عبر مواقع التواصل الاجتماعي بالاحتجاج على خدمات الإنترنت، وظهور بعض الحملات الإلكترونية في زمن قصير، نادت بالتصعيد ضد بعض الشركات التي تقدم خدمات الإنترنت؛ الأمر الذي دفعها إلى الاستجابة بصورة مباشرة إلى هذه المطالب بتخفيض أسعار الخدمة والعمل على تحسينها.



متابعة أخبار الحدث الرياضي الأهم بصورة فورية وتفاعلية.

• حملات إلكترونية للتوعية العامة، حيث ظهرت العديد من الحملات الإلكترونية لمواجهة ظواهر سلبية في المجتمعات، مثل ظاهرة التحرش وبعض الحملات التي يمكن تنظيمها لتوعية المجتمع بقضية مهمة أو بسلوك معين.

• استطلاع الآراء حول قضايا مثارة، بهدف معرفة اتجاه قطاع من الرأي العام، أو مشاركة الشباب ومستخدمي مواقع التواصل الاجتماعي في قضايا معينة أو سياسات تتبعها الدولة.

• تشويه الرموز السياسية، إذ يتم توظيف الهاشتاج لتوجيه إساءات لبعض القادة السياسيين ورؤساء الدول والرموز السياسية أو الدينية أو المجتمعية.

• تنظيم تظاهرات افتراضية، من خلال استخدام الهاشتاج لعرض مطالب سياسية أو فتوية عبر إطلاق هاشتاج ينتشر في مواقع التواصل الاجتماعي يحتوي هذه المطالب.

ثالثاً: حروب التواصل الاجتماعي في منطقة الشرق الأوسط

برزت مواقع التواصل الاجتماعي بقوة خلال فترة الثورات العربية؛ مما دفع بعض الأنظمة الحاكمة إلى إغلاق هذه المواقع في بعض الأحيان، وإبرام مناقصات لشراء برامج عملاقة لمراقبتها وتحليلها ورصد تحركات الناشطين عليها.

ومن أمثلة ذلك ما حدث في أعقاب 25 يناير 2011، حيث عثر بعض الناشطون على وثائق خاصة تشير إلى عزم الحكومة المصرية على التعاقد مع شركة (Gamma International UK Limited) للحصول على نسخة من برنامج (FinSpy) الذي تبلغ قيمته 287,000 يورو، وهو أحد برامج مراقبة الاتصالات عبر الإنترنت بداية من برامج الدردشة الفورية (Chatting) حتى مواقع التواصل الاجتماعي.

وفي الفترة نفسها أمدت شركة (Amesys) الفرنسية معمر القذافي، بناء على طلبه، بحزمة من البرامج الفنية تدعى (EAGLES) لكي تمكنه من مراقبة المحادثات الهاتفية وبرامج المراسلات الفورية وغيرها من مواقع التواصل الاجتماعي على الإنترنت في ليبيا، بالإضافة إلى برامج لمنع الليبيين من استخدام

للموقف القطري، ومنها مثلاً هاشتاج "#قطر_تدعم_الإرهاب"، وهو الأمر الذي رفضه أنصار قطر خاصة من الإسلاميين، ليتخذوا موقف المدافع عنها باعتبارها داعماً رئيسياً للثورات العربية.

ب- مواجهة التنظيمات الإرهابية:

يمثل تنظيم "داعش" محور اهتمام مواقع التواصل الاجتماعي، خاصة بعد الاستراتيجية الإعلامية التي اتبعتها التنظيم من خلال مواقع التواصل الاجتماعي، ونجح من خلالها في تجنيد العديد من الأفراد في المنطقة العربية، ونجح أيضاً في إيجاد صورة ذهنية عن بشاعة أفعاله، ساعدته في دخول بعض القرى العراقية من دون مقاومة تذكر.

وتشهد مواقع التواصل حرباً حقيقية ومنظمة بالتزامن مع الضربات الأمريكية لمواقع "داعش"، حيث كشفت جريدة التليجراف عن أن "الخارجية الأمريكية دشنت عدة حسابات على مواقع التواصل الاجتماعي لمواجهة حملة "داعش" لتجنيد مزيد من الأفراد، حيث تعمل هذه الحسابات بلغات عدة منها الإنجليزية والعربية والأوردو والصومالية، وتقوم ببث صور ومقاطع فيديو تكشف الدمار الذي تخلفه الغارات الجوية، التي تستهدف ما تقول إنه مواقع "داعش" في العراق وسوريا كتحذير للشباب الذين يفكرون في الانضمام إليه"⁽¹⁰⁾.

وتعتبر حروب التواصل الاجتماعي بين الولايات المتحدة والجهاديين في منطقة الشرق الأوسط من أبرز النماذج على تلك الحرب الدائرة بين الكتل الجهادية والدول، فقد أنشأت وزارة الخارجية الأمريكية في عام 2011 مركز "الاتصالات الاستراتيجية لمكافحة الإرهاب"، بهدف التواصل مع الجهاديين والأصوليين، خصوصاً من تنظيم القاعدة وتنظيم "داعش" في المنطقة العربية، ومحاولة بث رسائل باللغة العربية والإنجليزية على موقعي تويتر والفيسبوك، بهدف توعية الشباب، فضلاً عن انخراط موظفي هذا المركز داخل مندييات وصفحات هذه التنظيمات، في محاولة منهم للإيقاع ببعضهم من ناحية، أو استقطابهم من ناحية أخرى.

ج- أداة رئيسية في الصراعات الإقليمية:

عادة ما تصاحب الصراعات الإقليمية في المنطقة العربية حروب افتراضية على مواقع التواصل الاجتماعي، خاصة في الصراع العربي الإسرائيلي، حيث تشهد هذه المواقع حملات إعلامية يشنها الناشطون الفلسطينيون والعرب لفضح انتهاكات الاحتلال الإسرائيلي. ولعل المواجهة الأخيرة التي دارت في سبتمبر 2014، شهدت وجوداً مكثفاً للشبكات الاجتماعية لفضح هذه الانتهاكات، حيث بادر الناشطون بنشر صور وفيديوهات للقصف الإسرائيلي على غزة.

وفي المقابل قام الجيش الإسرائيلي بنشر صور وفيديوهات مضادة توضح تعرض إسرائيل للقصف من قبل الفلسطينيين وحق

وتعتبر مواقع التواصل الاجتماعي مجالاً افتراضياً للتشجيع على التظاهر، كما حدث خلال الثورات العربية، حيث كانت هذه المواقع هي الوقود المغذي للتظاهرات، وهو ما يظهر أثره، إلى جانب عوامل أخرى واقعية، لاسيما في الدول كثيفة السكان مثل مصر؛ إذ ساعدت هذه المواقع على الحشد والتشبيك والتنظيم والانتقال من المجال الافتراضي إلى المجال الواقعي، وخرج ملايين المواطنين رافعين مطالب ثورية انتهت بانهيار النظم الحاكم.

ويتم تنظيم التظاهرات الافتراضية من خلال الاتفاق على موعد محدد وهاشتاج محدد على صفحات تويتر أو الفيسبوك، يتجمع عليه أكبر عدد من المشتركين في لحظة معينة، لعرض مطالب ذات طبيعة سياسية. ومن أبرز الأمثلة على التظاهرات الافتراضية قيام عدد من الشباب القطريين تحت مسمى "حركة أحرار قطر" بالدعوة إلى ثورة شعبية عبر مواقع التواصل الاجتماعي.

ج- حرب افتراضية بين تيارات سياسية:

عادة ما يتم استخدام مواقع التواصل الاجتماعي في المنطقة العربية للسجلات الفكرية بين التيارات السياسية والفكرية. وقد حدث هذا مراراً في أعقاب الانتخابات البرلمانية أو الرئاسية والاستفتاءات التي شهدتها عدة دول عربية. ففي مصر هناك دائماً معارك افتراضية مشتتة بين أنصار الرئيس الأسبق مبارك ومعارضيه، وبين أنصار الإخوان ومعارضيه، وبين التيارات السياسية كافة، وفق مجريات ما يحدث على الساحة، وثمة معارك بين مؤيدي ومعارضين النظام في سوريا، وهو الأمر نفسه، الذي حدث في أعقاب الانتخابات الرئاسية الجزائرية، التي شهدت جدلاً بين مؤيدي ومعارضين الرئيس عبدالعزيز بوتفليقة، بل إن الأمر انتقل لمستويات أقل من ذلك، فشمّل الجدل حول القوانين الداخلية والقرارات السياسية والتصريحات الرسمية، التي عادة ما تلقى ردود فعل ساخرة أو مهاجمة لها.

2- على المستوى الإقليمي:

سيطر على حروب التواصل الاجتماعي إقليمياً عدد من القضايا الرئيسية، أهمها - على سبيل المثال لا الحصر - انقسام المنطقة العربية حول الدور السياسي للتيار الإسلامي، بالإضافة إلى تصاعد دور الحركات الإرهابية في منطقة الشرق الأوسط، خاصة بعد تمدد تنظيم "داعش"، فضلاً عن الاعتداءات الإسرائيلية المتكررة على الفلسطينيين، وهو ما يتضح فيما يلي:

أ- حروب فكرية بين التيارات السياسية:

سادت خلال الفترات الماضية، ولاتزال، حرب افتراضية على مواقع التواصل الاجتماعي، كان محورها الإسلاميين عموماً، ودولة قطر خصوصاً. فقد مثل الموقف القطري الداعم للإسلاميين وجماعة الإخوان مجالاً للنقد والهجوم على مواقع التواصل الاجتماعي، وظهرت العديد من الهاشتاجات ما بين تأييد أو رفض

لم تكن أبداً في حسبانهم.

وتكمن المشكلة الأساسية في الوقت الراهن في كيفية التعامل مع هذه الظاهرة في أن محاولة مراقبة هذه المواقع والسيطرة عليها من قبل الدول تطرح إشكالية تهديد الخصوصية الفردية للمستخدمين، وتركها ساحة مفتوحة أمام مختلف المستخدمين، سواء كانوا أفراداً أو جماعات أو تيارات، كما يطرح ذلك مشكلات تتعلق بتهديد الأمن القومي للدول، بل والأمن الشخصي للأفراد أيضاً، في معضلة لا تقبل الحلول الوسط؛ فالدول لن تتهاون في الحفاظ على أمنها القومي، ولن يتهاون الأشخاص في الحفاظ على خصوصياتهم الفردية، إلا أن الغلبة في النهاية ستكون للدول، بما تمتلكه من قدرات لإدارة ومراقبة هذه المواقع، وبما توفره التكنولوجيا المتقدمة من برامج لرصدها وتحليلها.

ولن تلعب الشركات المشغلة لهذه المواقع دور المحاييد، فهي لن تستطيع تحدي إرادة الدول حفاظاً على استثماراتها، بما يفتح أبواباً خلفية بينها وبين الدول، يكون ضحيتها مستخدمو مواقع التواصل الاجتماعي، فهي حرب غير محدودة ومفتوحة المصدر ومتاحة ومؤثرة على جميع الأفراد من قريب أو بعيد.

وإذا كان الوضع الحالي هو وجود حرب افتراضية على مواقع التواصل الاجتماعي، فإن التطور القادم سيكون حرب تطبيقات الهواتف الذكية الخاصة بالمحادثات الفورية، مثل واتس أب (Watsapp) ووي شات (Wechat) وفيبير (Viber)، فإذا كانت المعلومات على مواقع التواصل في معظمها عامة ومتاحة للجميع، فهي غير ذلك على تطبيقات الهاتف الذكي، وإذا كان من السهل مراقبة مواقع التواصل وتحليل ما بها من بيانات ومعلومات وأفكار واستراتيجيات، فإن الأمر قد يصبح أصعب في تطبيقات الموبايل، الأمر الذي يجعل التحدي القادم للدول هو السيطرة على المحادثات الخاصة التي تحدث عبر هذه التطبيقات، وليس مجرد مراقبة مواقع التواصل الاجتماعي والسيطرة على الأحداث التي تدور بداخلها.

الإسرائيليون في الدفاع عن أنفسهم، وتبارى كل فريق لكسب تأييد الرأي العام الدولي لصالحه، وانطلق على موقع تويتر وغيره من المواقع هاشتاغان رئيسيان هما (#GazaUnderAttack) و(#IsraelUnderFire)، وحاول كل فريق منهم توضيح المعاناة التي يتعرض لها جراء القصف، حيث ألفت الحرب بظلالها على مواقع التواصل الاجتماعي ونسبت حرب افتراضية توازي الحرب الحقيقية.

خاتمة:

يوضح العرض السابق أن حروب مواقع التواصل الاجتماعي تعد ظاهرة جديدة انطلقت خلال السنوات القليلة الماضية، لكن معالمها النهائية لم تتشكل بعد، وهي في الأغلب سوف تستمر وتأخذ وقتاً طويلاً حتى تتضح كافة ملامحها، ليس فقط لحدثة الظاهرة أو لأنها لا تزال قيد التشكل، ولكن أيضاً لأن تسارع التطور التكنولوجي وظهور أجيال جديدة في وقت قصير من مواقع التواصل الاجتماعي، بل وكذلك من الأجهزة المحمولة أو اللوحية، يقودان إلى بروز أشكال جديدة، وربما غير معروفة، من المعارك الإلكترونية، لاسيما على مواقع التواصل الاجتماعي.

وما يُهم في هذا السياق أنه لا يمكن غض الطرف عن تداعيات هذه الحرب، فالجميع يشارك فيها، بدءاً من الدول، مروراً بالحركات والمؤسسات المدنية، والتنظيمات والحركات الإرهابية والإجرامية، وصولاً إلى مجموعات صغيرة من الأفراد التقليديين، بعضهم محترف ولديه مهارات غير تقليدية يستخدمها بشكل غير مشروع، وبعضهم مستخدمون عاديون، وكافة هذه الأنواع من المستخدمين لا توجد عليهم سلطة قانونية واحدة، ولا حدود جغرافية يعترفون بها، وبالتالي يصعب السيطرة عليهم؛ الأمر الذي لم يحول مواقع التواصل الاجتماعي فقط لأن تصبح مواقع للإزعاج الاجتماعي، ولكن بمثابة مواقع باتت تؤثر على سياسات دول ومؤسسات وتنظيمات، ويصل إزعاجها إلى الفرد العادي الذي لم يعد بعيداً عن الحرب ضد خصوصيته أو أن تطله أضرار

1- Danah m. boyd, Nicole B. Ellison, Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication, vol 13, issue 1. Dec 2007, p. 210.

2- Rain Ottis, "Proactive Defense Tactics Against On-Line Cyber Militia", 8th European Conference on Information Warfare and Security, 01-02.07.2010, Thessaloniki, Greece, p. 223.

3- هو تطوير لقانون مراقبة الاستخبارات الخارجية Foreign Intelligence Surveillance Act، بهدف تمكين الولايات المتحدة من مراقبة أنشطة الجماعات الإرهابية بعد أحداث 11 سبتمبر، يمكن مطالعة نص القانون على الرابط التالي: <http://www.justice.gov/archive/ll/>

4- Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data , Access Date, August 25th, 2014, on

<http://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism/in/4167369>

5- NSA Prism program slides, On Nov 5th, 2013, <http://goo.gl/GXW4D8>

6- Pentagon Seeks to Manipulate Social Media for Propaganda Purposes, On April 21th, 2014, <http://www.globalresearch.ca/pentagon-seeks-to-manipulate-social-media-for-propaganda-purposes/25719>

7- Nick Fielding and Ian Cobain, Revealed: US spy operation that manipulates social media, the Gardian. On 21 March 2014, <http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks>

8- Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, 28 January 2014, <http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data>

9- Sarah Lange, The End of: Social Media Revolution, the fletcher forum of world affairs, vol.38:1 winter 2014 , P59 http://www.fletcherforum.org/wp-content/uploads/2014/04/38-1_Lange1.pdf

10- Raf Sanchez, US wages social media war against Isil, Telegraph, 25 Sep 2014,

<http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11122490/US-wages-social-media-war-against-Isil.html>