التكنولوجيا الذكية والتهديدات الأمنية الجديدة

الطالب: بخدا عبد الكريم

جامعة قاصدي مرباح ورقلة

مقدمة :

سعت العديد من الدول الى إنشاء بنية تحتية متقدمة لتكنولوجيا المعلومات والاتصالات وتوفير بيئة قائمة على المعرفة وذالك من خلال استفادة الافراد والشركات من مزايا الانترنت بما يحقق الكفاءة في العمل ويسهم في تعزيز التنمية الاجتماعية . غير ان هذه البنية الجديدة افروت العديد من التهديدات الأمنية افرزها الواقع الجديد .في ظل تنامي التهديدات الأمنية الإلكترونية على الصعيدين الإقليمي والعالمي والتي تراوحت ما بين عمليات السطو الإلكتروني إلى عمليات التجسس برعاية الشركات وأجهزة المخابرات الدولية، وصولا الى ما أصبح يعرف بإرهاب الانترنت الذي بمكن من خلاله شن هجوم واختراق لأنظمة الأمن والشبكات ، او توزيع فيروس كمبيوتري قوي واختراق شبكات الأمان للدول .وبهذا الشكل فقد جاءت التكنولوجيا الحديثة والعولمة المعرفية لتعلن نهاية الجغرافيا ، مع تقدم وسائل الاتصالات الحديثة، وذالك بعد فكرة نهاية التاريخ التي طرحها فوكوياما ، فدول العالم اليوم في حالة فقدان مستمر لدعامتها الجغرافية لصالح وسائل الاتصال غير القارية .

وعلى ضوء ذلك تبرز الحاجة إلى تحليل مكثف لاتجاهات الأمن المعلوماتي والبحث عن استراتيجيات دفاع وسياسات فعّالة لمواجهة هذه التهديدات وهنا تبرز أهمية التكنولوجيا الذكية لحماية الحدود وتطوير المنظومة الدفاعية وحمايتها من التهديدات المحتملة.

وسنحاول من خلال هذه الورقة الوقوف على التهديدات الأمنية الجديدة وضرورة تبني منظومة تكنولوجية ذكية في تامين الحدود الجغرافية للدول .

✓ اولا : ماهية التكنولوجيا الذكية :

1-يمكن تعريف التكنولوجيا الذكية على أنها :

مجموعة الهواتف النقالة وأجهزة الحواسيب الحديثة والمتطوّرة التي ظهرت في الوقت الحاضر، تزامناً مع التطورات التي حدثت في العالم، وتحتوي هذه الأجهزة على أنظمة متطورة لتشغيلها كنظام الأندرويد ونظام الأيزو وغيرها من الأنظمة، وهناك الكثير من الشركات التي أنتجت العديد من الهواتف الذكية كشركة سامسونج وشركة أبل وغيرها من الشركات، ويمكن القيام بالعديد من الأمور بواسطة الهواتف الذكية، فهي لا تقتصر على الاستقبال والإرسال كما في الهواتف النقالة القديمة، بل يمكن من خلال هذه الهواتف الذكية القيام بعمليات التصفح المختلفة على شبكة الإنترنت، وتحميل

العديد من التطبيقات الخاصّة بكل جهاز، عن طريق المتجر المتوفر فيها، تعمل الهواتف الذكية على خاصية اللمس.[1]

تنطوي التكنولوجيا الذكية على ابتكارات مثل الحواسيب والأجهزة القابلة للارتداء؛ وتكنولوجيا الواقع المعزَّز؛ وتكنولوجيا الواقع الافتراضي. ويهيمن على سوق التكنولوجيا الذكية حاليًا عدد صغير من الأجهزة: النظَّارات الذكية والساعات وأساور اللياقة البدنية، والتي يتفاعل كثير منها مع الهواتف الذكية والحواسيب اللوحية عن طريق تطبيقات لتتبُّع فترات نوم المستخدمين وصحتهم وحركتهم، وهو ما يشكِّل اتِّجاهًا جديدًا يُعرف باسم "القياس الكمِّي للذات". وتصف شركة 'دلويت' (Deloitte) القطاع بأنَّه "سوق متخصص ضخم" سوف يدرُّ نحو 3 مليار دولار في هذه السنة وحدها.[2]

ويمكن تعريفها أيضا انطلاقا من مجال الخدمة التي تقدمها للجمهور بأنها : عبارة عن عمليات تعتمد في استخداماتها الاستراتيجية على أحدث تقنيات المعلومات والاتصالات، وعلى رأسها التقنيات الذكية، بهدف التحول النوعي في الطريقة التي تعمل بها الجهة الحكومية في تقديم خدماتها، وذلك تحقيقًا لرضى المتعاملين بالتعاون مع جميع الجهات ذات الصلة، ويتم ذلك عبر توفير وسائل تواصل سلسة وتفاعلية وذكية تعمل في أي وقت وأي مكان، عبر العديد من الاجهزة.

2- مجالات التحسين والتطوير التي تدعمها الخدمات الذكية

أولا : جودة الخدمات المعلوماتية من خلال الوصول الى المعلومات الحكومية بواسطة:

قنوات الرسائل النصية القصيرة (SMS)

وسائل الاستجابة الصوتية (IVR)

الاستجابة التفاعلية بالصوت والصورة (IVVR)

استخدام منصة الانترنت للهواتف المتحركة(mobile Web)

نظام التطبيقات اللاسلكية (WAP)

ثانيا : تعزيز تفاعل الخدمات مع الجمهور : من خلال توفير التقنيات اللازمة للجمهور وتشمل : التقنيات التي تعتمد على تحديد الموقع الجغرافي مثل التصوير، وتسجيل مقاطع الفيديو، والخرائط. استخدام وربط وسائل التواصل الاجتماعي مع الخدمة الذكية .

ثالثا : تطوير الخدمات الإجرائية والتفاعلية:

- تطوير خدمات إجرائية للجمهور قد تشمل تقديم الطلبات، أو الإعلان عن شاغر وظيفي، أو شراء تذاكر الحافلات، أو حجز موعد، أو التوقيع على المعاملات رقميًا .

- توفير الخدمات المعلوماتية في مجالات مختلفة مثل الخدمات الصحية ، معلومات عن المراقبة، والاختبارات، والفحوصات وخدمات التعليم ، ومعلومات الحساب، والمعلومات عن خدمات الجهات المسؤولة عن تطبيق القوانين،وغيرها.

رابعا : تكامل الخدمات :

تجميع خدمات أو بيانات من أقسام مختلفة داخل الجهة الحكومية الواحدة أو من جهات حكومية أخرى، ما يجعلها أكثر ملائمة للجمهور عبر إتاحة التكامل بين خدمات متنوعة في منصة واحدة .[3]

✓ **ثانيا : التهديدات الأمنية الجديدة لأمن الحدود :**

تعرَّضت وظائف الحدود الدولية، شأنها في ذلك شأن كل مكونات الدولة الوطنية، لتغير كبير خلال العقود الأخيرة نتيجة للتطور السريع في النظام العالمي الذي أصبح فيه الفاعلون غير الحكوميين ينافسون الدول في مختلف المجالات السياسية والاقتصادية والاجتماعية .كما أن التطور الذي شهده عالم الإعلام والاتصال بمختلف أشكالهما كان له أثر كبير في إعادة النظر في التعريفات التقليدية للإقليم والحدود والسيادة الوطنية .وكان يُنظر إلى الحدود، عند ظهور الدولة الوطنية أول مرة، من الزاوية العسكرية باعتبارها" خطوطاً استراتيجية ينبغيى تحصينها عسكرياً أو تُختَرَق"[4]. إن الإشكاليات السابقة لأمن الحدود كانت قائمة طوال الوقت، وقد أدت إلى إثارة موجات من الاهتمام بمسألة أمن الحدود فى فترات مختلفة ، ولا يزال بعضها يثير نقاشات داخل وخارج عديد الدول ، فيما يتعلق بتطوير أنظمة أمن الحدود، أو كيفية التعامل مع مناطق الحدود، لكنه تم التعايش معها بصفة عامة، وفق ترتيبات مختلفة، قبل أن تبدأ مخاوف حقيقية من فقدان السيطرة على الحدود، فى الظهور[5]. وقد يقود هذا الأمر إلى تغير شكل الحدود بين الدول، إذ تصاعدت التهديدات التقليدية، التي كان من المفترض أنها مشكلات أمنية معتادة، إلى حدود غير مسبوقة، وبدأ ت فئة جديدة من التهديدات الحادة في الظهور .[6]

من جهة أخرى، أعلن المنادون بالعولمة (globalists) أن الحدود الإقليمية تتعرض للتعرية بسبب الحضور المطَّرد للفاعلين غير الحكوميين على الساحة الدولية وللتفاعل بين العولمة وتقنيات الإعلام والتواصل الجديدة التي يُنظر إليها باعتبارها عملية إضفاء الطابع الافتراضي بشكل متزايد على التدفقات عبر الحدود .ويرى جيمس روزناو (James Rosenau) في هذا السياق أن الاتجاهات المتغيرة التي حدثت في مرحلة ما بعد الحرب الباردة قد" أضعفت من قدرات الدول وفاعليتها وجعلت حدودها أكثر اختراقاً وأقل أهمية ." تسجِّل ساسكيا ساسن (Saskia Sassen) أنه على الرغم من الإجماع المتنامي بين الدول المتقدمة حول تسهيل تدفقات السلع والأخبار ورأس المال، فإنه حينما يتعلق الأمر بالأشخاص فإن الدول الوطنية تستعيد عظمتها القديمة لتأكيد حقها السيادي في مراقبة الحدود .وبرغم أن العولمة قلصت الوظائف العسكرية والاقتصادية للحدود، فإنها في الآن ذاته أنشأت عملاً إضافياً للدولة في مراقبة الحدود، حيث تنفق ملايين الدولارات كل عام لتحصين حدودها الوطنية.[7]

اولا : التطور التكنولوجي كبيئة مساعدة للممارسات الإرهابية :

قدم تطور وسائل الاتصالات و أنظمة المعلومات خدمة غير مقصودة للتنظيمات الإرهابية؛

حيث قامت الأخيرة باستغلال هذا التطور في خدمة أغراضها غير المشروعة وفى إتمام عملياتها الإجرامية، فقد وفرت الاتصالات الحديثة عملية نقل الأفكار والبيانات والتوجيهات إلى خلايا الشبكات الإرهابية بأمان بعيدا عن أعين الرقابة الأمنية، كما أمنت أنظمة المعلومات الالكترونية أيضا تدفق سيل من المعلومات اللازمة لتنفيذ عملياتها الإرهابية .[8]

يمكن تعريف "الإرهاب الإلكتروني:" بأنه "نشاط أو هجوم متعمد، يملك دوافع سياسية ويسعى للتأثير في القرارات الحكومية والرأي العام العالمي، ويستخدم الفضاء الإلكتروني بوصفه عاملا مساعدا ووسيطا في عملية التنفيذ للعمل الإرهابي، أو الحربي. كما يسعى لإحداث تأثير معنوي ونفسي عبر التحريض على بث الكراهية الدينية وحروب الأفكار. ويأتي هذا العمل في صورة رقمية عبر استخدام آليات الأسلحة الإلكترونية الجديدة في معارك تدور رحاها في الفضاء الإلكتروني، وقد يقتصر تأثيرها على بعدها الرقمي، أو تتعداه لتصل إلى الإضرار بأهداف مادية تتعلق بالبنية التحتية الحيوية". كذلك يعني هذا المصطلح استخدام وسائل إلكترونية، في عدوان أو تخويف أو تهديد له طابع مادي أو معنوي، ويصدر من دول أو جماعات أو أفراد عبر الفضاء الإلكتروني. كما يعني أن يسعى ذلك العدوان للتأثير على الاستخدام السلمي للفضاء الإلكتروني. بحسب كتاب "الإرهاب الإلكتروني والقوة في العلاقات الدولية: نمط جديد وتحديات جديدة"[9]، ويمكن تعريفه أيضا بأنة جملة الأعمال والأنشطة التي يقوم بها أفراد أو جماعات باستخدام تكنولوجيا المعلومات والشبكة العنكبوتية، بقصد إحداث دمار للبنى التحتية المرتبطة والمدارة بواسطة مثل هذه التكنولوجيا، كشبكات توزيع المياه والكهرباء، أنظمة الخدمات المصرفية، السجلات الصحية، الأنظمة العسكرية، وغيرها من البنى التحتية التي من شأن تدميرها أن يحدث أضرارا مباشرة وغير مباشرة بالمواطنين والدول.

وعليه يقترح "أرغويلا و رونفلدت" توزيع الناشطين عبر الانترنت على ثلاث مجموعات، مع إقامة الفارق بينهم:

1- . الناشطون Activist: وهم الذين يستخدمون الانترنت للترويج لقضية سياسية معينة أو يدافعون عن أيديولوجية معينة.

2- القراصنة Hijackist: وهم الذين يهاجمون مواقع الانترنت لتعطيلها دون نية أو القدرة على إحداث دمار كبير فيها (يدخل فعلهم في خانة الجرائم الإلكترونية)

3- الإرهابيون Cyber-terrorist: وهم أشخاص يحركهم دافع سياسي، يهاجمون المواقع الإلكترونية وأنظمة معلومات البنية التحتية المرتبطة بالانترنت بغية إحداث دمار بشري أو مادي .[10]

إن خطر الإرهاب الإلكتروني يكمن في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بعمله الإرهابي وهو في منزله، أو مكتبه، أو في مقهى....الخ. ومع أن الإرهاب في خطره

وأضراره لا يعرف الحدود ، ولا يميز بين الأشخاص او المؤسسات او الأنظمة ، إلا أن إن أكثر الجهات.

استهدافا من الإرهاب المنظمات والمؤسسات الأمنية . ولا تقف خطورة الإرهاب الالكتروني عند هذا الحد ، ذلك أن الخطورة الأمنية والمجتمعية تأخذ بعدا اخطر إذا أدركنا أن الجماعات المتطرفة كانت من أوائل الجماعات الفكرية التي دخلت العالم الإلكتروني حتى قبل ان تظهر شبكة الانترنت بسنوات. ومما تشير إليه المصادر الغربية أن "توم ميتزقر " Tom metzger احد أشهر المتطرفين الأمريكيين العنصريين ومؤسس مجموعة "المقاومة الاريانية" White Aryan Resistance البيضاء كان من أوائل من أسس مجموعة بريد الكترونية ليتواصل مع إتباعه ويبث أفكاره عام 1958 م .[11]

هذا وقد ظهر التزاوج بين الإنترنت والإرهاب بشكل أكثر وضوحا بعد أحداث الحادي عشر من سبتمبر 2001م؛ حيث انتقلت المواجهة ضد الممارسات الإرهابية من المواجهة المادية المباشرة الواقعية إلى الفضاء الإلكتروني، وتشير الإحصاءات ان عدد المواقع الاليكترونية للتنظيمات الإرهابية ارتفع من 4 مواقع عام 2011 الى قرابة العشرين الف موقع عام 2011 حيث استخدم أرباب الفكر الضال والإرهاب الإنترنت للعمل الإرهابي التقليدي مساعدا في معركتهم على عدة محاور أهمها وأولها: أن يصبح الإنترنت عاملا المادي وذلك بتوفير المعلومات الضرورية عن الأماكن المستهدفة أو كوسيط في عملية التنفيذ اذ تعد الانترنت احد أدوات تحقيق الترابط التنظيمي بين الجماعات والخلايا التي تمكنهم من تبادل المقترحات والأفكار والمعلومات الميدانية حول كيفية إصابة الهدف واختراقه والتخطيط والتنسيق للعمل الإرهابي ، وثانيها يتمثل في استخدام الإنترنت لإحداث أ ثار نفسية من خلال التحريض على بث الكراهية والحقد وحرب الأفكار؛ حيث خدم الإنترنت الخلية الإرهابية من حيث تضخيم الصورة الذهنية لقوة وحجم تلك الخلايا والتي قد تتكون في واقع الأمر من عدد قليل الأفراد لديهم أو لدى أحدهم خبرة بالإنترنت وبرامج Multi Media لبث رسائل إعلامية تخدم أهدافهم لشن حرب نفسية ضد مستهدفيها والدعاية لأهدافها وأنشطتها بعيدا عن وسائل الإعلام التقليدية ، فالتنظيم الإرهابي لا يهمه كم من الناس قتلوا في الحدث الإرهابي بقدر ما يهمه كم من الناس شاهدوا وتفاعلوا مع الحدث الإرهابي، وثالثها يتمثل في الإمكانات التكنولوجية التي تتيحها الإنترنت؛ فمن خلال استخدام آلياته الجديدة يتمكن أعضاء الخلية الإرهابية من تحديد صورة رقمية يمكن من خلالها ان تدار رحى معاركهم في الفضاء الإلكتروني، ومن ثم لا يقتصر تأثيرها على بعدها الرقمي فقد بل تتعداه لإصابة أهداف أخرى كتدمير مواقع الإنترنت المضادة واختراق مؤسسات حيوية أو حتى تعطيل خدماتها الإلكترونية.[12]

ثانيا : تهديد الاستقرار وإشاعة ثقافة إسقاط الأنظمة :

برزت شبكات التواصل الاجتماعية "تويتر" و "فيس بوك" "يوتوب" عام 2011م في الربيع العربي كعامل فاعل و محفز للتغيرات السياسية كما واكبت مختلف الحركات الاحتجاجية في العالم، و بعد ما

كانت شبكات التواصل هذه ذات غايات ترفيهية و اجتماعية، صارت اليوم تلعب دورا إعلاميا و سياسيا و في هذا السياق كان موقع "فيس بوك" رائد في الميدان حيث ارتفع عدد مشتركي الموقع بشكل ملحوظ و حقق .

شهرة كبيرة بعد أن أصبحت صفحاته نوافذ إعلامية هبت عبرها رياح الثورة على البلدان العربية الكثيرة بل و حتى الغربية كما هو الحال في أوكرانيا.

و بحسب تقرير معهد التنبؤ الاقتصادي لعالم البحر الأبيض المتوسط فإن أكثر من 20 مليون عربي يستخدمون شبكة التواصل الاجتماعية "فيس بوك" و عن الانترنيت كان بمثابة أرضية للمقاومة في خدمة الثورات التي شهدتها بعض الدول العربية.و إن الفيس بوك لعب دورا لا يستهان به حيث سمح بالانتشار الشامل للمعلومة الغير المراقبة مستمدة من مستخدمي الانترنت أنفسهم. [13]

ففي عودة إلى أبرز أحداث "الربيع العربي" و بداية من تونس، يمكن تلخيص الدور الذي لعبته مواقع التواصل الاجتماعي في الانتفاضة الشعبية التونسية بالقول أن جزء من تاريخ "ثورة الشباب" في تونس كتب على الحائط الافتراضي لموقع "فيس بوك" . فقد كان نظام زين العابدين بن علي يحكم بقبضته على الاتصالات الالكترونية و يضيق على الصحافيين و الإعلاميين و منع المراسلين المحليين و الأجانب من السفر إلى سيدي بوزيد لتغطية الأحداث. فمع القمع و التضييق الإعلامي الذي كان يعيشه التونسيون كان البديل شبكة الانترنت و بالتحديد موقع التواصل الاجتماعي "فيس بوك" الذي تمكن من خلاله التونسيون الالتفاف على الرقابة و على التعتيم الإعلامي و سمحت للكثيرين بنقل كم هائل من المعلومات من صور و فيديو إلى العالم وإلى التونسيين عبر موقع "فيس بوك" و عبر الانترنت ، مما ساعد في إقناع التونسيين بأن الوقت قد حان للانتفاضة و التحرك للخروج إلى الشارع و الانضمام إلى الشباب في ثورتهم.

كما في تونس كذلك في مصر فقد نشطت مواقع التواصل الاجتماعي و تحديدا خدمة "تويتر" للدعوة للتظاهر ولتنسيق الاحتجاج. فالانترنت غيّر مفاهيم الناس من خلال حملات التوعية التي يقوم بها النشطاء المصريين للتعريف بحقوق الإنسان و بحقوق" المواطن" السياسية.[14] و يرى الناشط المصري أيمن صلاح أن شبكات التواصل الاجتماعي كانت "اختراعاً جيداً بالنسبة للناشطين المصريين." وكان الناشطون المصريون يتناقلون المعلومات عبر التويتر، وأغلبهم من المدونين لينقلوا صورة ما يحدث إلى العالم الخارجي، فقد كان هناك تعاون بين الناشطين على شبكات التواصل الاجتماعي والناشطين على الأرض،"[15] و كان لمواقع التواصل الاجتماعي الدور الأكبر في تنظيم النشطاء و في نقل نبض الشارع و نقل وقائع الأحداث بشكل آني من قلب التظاهرات، و لتبادل المعلومات عن أماكن التجمعات بالإضافة للنصائح المختلفة لمواجهة حالات الاعتقال أو كيفية تفادي القنابل المسيلة للدموع و غيرها من الأمور لحماية المتظاهرين.

و أهمية هذا الوسيط كانت أيضا من خلال التفاعل بين المواطنين المصريين في الداخل و الخارج و أيضا في كيفية نقل وقائع الإحداث بدل الإعلام العالمي و الوطني المكبل حتى تنحي حسني مبارك . وما زال الإعلام الاجتماعي ناشطا في مصر اليوم في مواجهة المجلس الأعلى للقوات المسلحة .

في ليبيا عند اندلاع ثورة 17 فبراير ، أسس المدون الصحفي محمد نبوس "قناة ليبيا الحرة" التي تعد أول محطة تلفزيونية إخبارية خاصة ومستقلة أنشئت في الأراضي التي يسيطر عليها "المجلس الوطني الانتقالي" تبث عبر الانترنت. حيث تناقلت وسائل الإعلام العالمية الصور الأولى التي نقلها نبوس عن الدمار و المعارك في مدينة بنغازي. قتل محمد نبوس في 19 مارس/ آذار 2011 برصاص قناصة عندما حاول التقاط صور عن الدمار الذي لحق بمدينة بنغازي جراء قصف كتائب القذافي لها في معركة بنغازي الثانية. في سوريا مع تصاعد نبض الاحتجاجات ضد نظام بشار الأسد في سوريا، تصاعدت أيضا حدة المواجهات في الفضاء الالكتروني حيث تحولت الشبكة العنكبوتية إلى ساحة حرب حقيقية، فبرزت مجموعة على موقع "فيس بوك" أطلقت على نفسها اسم «الجيش السوري الإلكتروني» و فيما بعد كان لها موقعها الالكتروني الخاص.

فقد دشنت هذه المجموعة أسلوبا جديدا في التعاطي مع الاحتجاجات ومع المعارضة عن طريق قرصنة الصفحات الشخصية لبعض المعارضين أو المناهضين للنظام السوري و أيضا اختراق مواقع وسائل الإعلام العربية والغربية و مواقع غربية و إسرائيلية . و مع منع النظام السوري عمل مراسلي وسائل الإعلام العالمي على الأراضي السورية ،لجأت وسائل الإعلام تلك إلى ما يتم تداوله على مواقع التواصل الاجتماعي "يوتيوب" و"فيس بوك" و "تويتر" التي تنشر عليها أفلام فيديو من المظاهرات أو المعارك مصورة بالهاتف الخلوي، دون التأكد من صدقيه ما يورد في تلك الملفات.[16]

أما ما أوردته وكالة «إنترافاكس»، فهو إن صدق يعد دليلا قاطعا لا مراء فيه على أن تلك الشبكات الاجتماعية مسلطة على الشعوب لخدمة أهداف استخباراتية خاصة بدول غربية على رأسها الولايات المتحدة الأمريكية؛ حيث نقلت تلك الوكالة عن رئيس أكاديمية العلوم العسكرية الروسية الجنرال محمود غاريف قوله: «إن الاضطرابات التي تشهدها منطقة الشرق الأوسط وشمال أفريقيا في الآونة الأخيرة . يقصد المظاهرات التي حدثت في تونس، مصر، ليبيا مطلع عام . (2011م) . ناتجة عن تجريب الغرب لأحدث التكنولوجيا الإعلامية التخريبية، وقد تم إنشاء مئات الآلاف من تلك الصفحات في تلك البلدان على مدى سنتين؛ حيث تم تجريبها في البداية في بث دعوات للقيام بأعمال غير منافية للقانون، وحين لوحظ فاعليتها، جرى في اللحظة المناسبة عبر الشبكات كافة توجيه أمر بالقيام بمظاهرات.

وفي تقرير نشرته صحيفة الحقيقة الدولية أشار إلى ما قاله : جيرالد نيرو الأستاذ في كلية علم النفس بجامعة بروفانس الفرنسية، وصاحب كتاب مخاطر الانترنت: إن هذه الشبكة الفيس بوك يديرها مختصون نفسانيون إسرائيليون مجندون لاستقطاب شباب العالم الثالث وخصوصا المقيمين في دول

الصراع العربي الإسرائيلي إضافة إلى أمريكا الجنوبية. ويشير التقرير إلى أن الشباب العربي ما يجد نفسه كثيرا مضطرا بتفاصيل مهمة عن حياته وحياة أفراد أسرته ومعلومات عن وظيفته وأصدقائه والمحيطين به وصور شخصية له لا بأس به لأي جهة ترغب في معرفة أدق التفاصيل عن عالم الشباب العربي. ومعلومات يومية تشكل قدرا وهذا يمكن جهات أجنبية من الاستفادة من تلك المعلومات والحوارات لمعرفة ما يدور من حراكات فكرية. وبعد أقل من أربعة أشهر من نشر ذلك التقرير، نشرت مجلة لوما غازين ديسرابيل الفرنسية ملفا واسعا عن هذا الموقع جمعته . بحسب قولها . عبر مصادر إسرائيلية وصفتها بالموثوقة، أكدت خلاله بأنه موقع استخباراتي مهمته تجنيد العملاء والجواسيس لصالح الكيان الصهيوني، ورغم أن أولئك الأشخاص عاديين لا يعرفون انهم يقومون بمثل هذه المهمة الخطيرة .[17]

ثالثا :التهديدات المتعلقة بإثارة النعرات الطائفية والمذهبية :

يتعرض المواطن العربي العادي الى شتى أنواع غسل الأدمغة، ويتلقى تبسيطات اختزالية إعلامية للأوضاع المعقدة في الأقطار العربية التي تمرّ بموجة ثورية ضخمة، أصبحت تُلهم بعبقريتها وجرأتها انتفاضات شعبية في بلدان عديدة. وإذا كانت من ميزة في هذه الحركات الشعبية فهي جمع فئات الشعب العمرية والاجتماعية والمهنية في حراة واحدة، مطالبها الرئيسية هي الكرامة والعدالة والخبز والقضاء على الفساد وتأمين الحريات العامة الأساسية والتداول السلطة. و أمام هذه الأحداث التي أصبحت تنتشر في أقطار عربية عديدة، اذ نرى بعد أشهر قليلة تعميم التحليلات المغرضة حول الظواهر القبلية والإقليمية داخل القُطر، والدينية عند وجود ديانتين في المجتمع الواحد كالإسلام والمسيحية، أو مذهبية في ما بين الطوائف الإسلامية نفسها، هكذا يتمّ اختزال أوضاع معقّدة ذات أبعاد اقتصادية واجتماعية وسياسية، أكثر مما هي دينية أو مذهبية، خاصة في المجتمعات التي تتميز بالتنوع الديني .[18]

هناك من يتساهل مع الدور الذي يلعبه الإعلام الجديد في إثارة النعرات القبلية والطائفية، ولكن الحقيقة أن الموضوع خطير جدا ووصل إلى درجة انتقلت معها المناوشات من ساحات القنوات الفضائية الشعبية والعوالم الافتراضية إلى الأحياء وحتى المدارس حيث يشترك الأطفال في جدالات حول القبيلة وأفعالها وأمجادها التليدة، وبالطبع كل ذلك يدور في ثنايا الشبكات الاجتماعية وغرف الدردشة ، وما يسمع يدمى له الجبين، وفيه خطر شديد على الوحدة والأمن الوطني.

وتشير بعض الإحصاءات إلى وجود أكثر من ثلاثة آلاف موقع ومنتدى خاصة بالقبائل، بل ويفاخر بعض المنتمين لتلك القبائل بكثرة المواقع التي تحكي عن قبيلتهم وتنافح عنها وتتغنى بأمجادها وتروج لشيوخها، بل إن بعض القبائل قد وصل عدد المواقع الخاصة إلى أكثر من ثلاثمائة موقع .[19]

ويشدد الدكتور على عبدالرحمن العسيري، عضو هيئة التدريس في كلية العلوم الاجتماعية، على أن النعرات الطائفية أشد خطرا وحدة الوطن من الإرهاب؛ ويعزو ذلك إلى أن الإرهاب ينحصر في فئة

يمكن تحديدها والقضاء عليها، لكن العصبية القبلية سرطان ينتشر بسرعة في جسد الوحدة الوطنية ، بدعم وتأييد من أطياف المجتمع المتعددة. ويحدد معاول هدم الوحدة الوطنية في عدة أمور على رأسها القنوات الفضائية الشعبية، المنتديات ، القبلية، الألعاب الرقمية والذهنية .[20]

وكنماذج حول ما يبث من مساعي لبث الفتنة الطائفة؛ فقد دعا موقع طائفي عراقي على الانترنت صراحة الى قتل المواطنين السنة وتكرار مجزرة حي الجهاد، وعلى الصعيد المصري انتشر مقطع فيديو على العديد من المواقع الرقمية يدعو إلى مهاجمة نصارى مصر وحرق جميع الكنائس بإمبابة وذلك بعد الأحداث التي وقعت هناك في شهر جماد ثاني1432هـ (مايو 2011م) وأسفرت عن مقتل 12 شخصا وإصابة 240 آخرين. وكان هناك من نسب نشر ذلك المقطع إلى الموساد الإسرائيلي بغرض إشعال الفتنة الطائفية في مصر.[21] وعلى الصعيد المصري أيضا أطلقت مجلة "الإيكونومست" الهجوم على مصر، بفتح ملف ما أسمته "معاناة الأقلية المسيحية في العالم العربي"، زاعمة أن الظاهرة ممتدة، من الموصل في العراق إلى صعيد مصر.[22]

رابعا : التحديدات المتعلقة بالجريمة الالكترونية :

أن مسالة توفير الأمن من الأمور العسيرة والصعبة في العصر التقني، إذ يشكل مجرمو الانترنت ومجموعات التجسس والميلشيات الالكترونية والقراصنة السياسيون خطراً مباشراً يهدد مسيرة التقدم . تؤكد هذه الهجمات والجرائم الالكترونية أن الحماية منها يتطلب مشاركة فاعلة للعديد من الجهات والمؤسسات المعنية. بالإضافة إلى ذلك، يحتاج المواطنون عامة، والمجموعات المسؤولة عن الأمن الالكتروني خاصة، إلى إدراك التهديدات التي تواجه البيانات والبنية الأساسية. يقول ريتش ديميلو، كبير العلماء في معهد قطر لبحوث الحوسبة: "يتحرك القراصنة بسرعة فائقة، فإذا كانت عملياتك تهدف إلى الدفاع عن الدولة، فعليك التفكير بجدية في تحسين سرعة استجاباتك."[23]

تتسم جرائم تقنية المعلومات بنفس سمات الجرائم العادية من حيث إلحاق الضرر بالآخرين ، ولذالك يمكن تصنيفها حسب طبيعة الجهة او الشخص المتضرر منها ، حيث تتدرج هذه الجرائم تحت جرائم النصب والاحتيال او جرائم سرقة المعلومات .وتنحصر أهم جرائم تقنية المعلومات في ما يلي :

1-الجرائم المرتكبة ضد التقنية ومستخدميها :

ا-جرائم الاختراق والتعدي ودخول الحواسيب دون تصريح واستخدامها دون تصريح بهدف قراءة البيانات او اتلافها او مسحها وهذه الجرائم في ازدياد مستمر كما ان الهاكرز او قراصنة الحاسب الآلي والانترنت يقومون باختراق أنظمة وقواعد المعلومات وسرقتها كما كشفت الدراسة التي أجرتها الأمم المتحدة في عام 2005 م ان 37 بالمئة من جرائم الاختراق والتعدي داخلي وان 23 بالمئة يرجع الى مصادر خارجية وبلغ حجم الخسائر الاقتصادية لهذه الجرائم عام 2004 م فقط حوالي 3,5 مليار دولار ، كما كشفت الدراسة ان حالات الاختراق التي وقعت على الحكومة الأمريكية كحالة خاصة لعام 2004 بلغت 354000 حالة اختراق 64 بالمئة منها ناجحة ، ولم يكشف سوى عن 4 بالمئة منها .

أ- جرائم سرقة الحقوق الفكرية :وسرقة معلومات التسويق او سجل العملاء او خطط التسويق مما يترتب عليه تدمير الإنتاج الفكري لشخص معين وكذالك محاولات الوصول السجلات الحكومية الأمنية وسجلات المنظمات العسكرية او الحصول على معلومات استخباراتية او ابتزاز أشخاص بناء على معلومات تم الحصول عليها عن طريف الحاسب الآلي .

ج-جرائم إنشاء او نشر برامج معادية مثل فيروسات عن طريق البريد الالكتروني لالحاق ضرر فعلي بالبيانات المخزنة او إضعاف قدرة النظم الحاسوبية على الحوسبة .

د-جرائم تخريب الحواسيب مثل العمليات الهجومية لتعطيل الخدمة الحاسوبية بإغراق الحواسيب بوابل من البيانات العشوائية التي تحمل الحاسب الحاسب الآلي حمولة مفرطة تتسبب في تعطيله عن العمل .

2-الجرائم التي ترتكب باستخدام تقنية المعلومات :

أ- جرائم الاحتيال المالي : تضمن الجرائم من هذا النوع الاحتيال واستعمال أجهزة الصرف الآلي وحسابات مزورة وسرقة بطاقات الائتمان وتضمن أيضا السرقات المالية من حساب البنوك ومراكز التعامل المالي . بلغت الخسائر الناتجة عن الاختراقات غير المشروعة 6078 شكوى تلقاها مركز شكاوى احتيال الانترنت الأمريكي في عام 2000م حوالي 4,6 مليار دولار ، وبلغ حجم خسائر الشركات الأمريكية حوالي 540 مليون دولار بسبب الاحتيال المالي وسوء الاستخدام لبطاقات الائتمان.

ب- جرائم استخدام النظم الحاسوبية لإنتاج او توزيع صور او نصوص او معلومات مخالفة للقانون الجنائي .

ت- جرائم الاختطاف ذات الصلة بالانترنت مثل إغراء الأطفال عبر مواقع الدردشة واستدراجهم وبعد تدبير مقابلة شخصية يتم اختطافهم لاستغلالهم جنسيا .

ث- جرائم المخدرات من خلال نشر كيفية زراعتها وأساليب ترويجها وطرق تصنيعها واستعمالها.[24]

أحد أشكال الجرائم الرقمية :الابتزاز من خلال الجاني ضحيته بنشر صور خاصة جداً لها في مواقع الإنترنت المختلفة، وعبر البلوتوث أو أجهزة البلاك بيري أو البرامج المختلفة المرفقة بأجهزة الهواتف الذكية مثل برنامج الواتس آب؛ إن لم ترضخ له وتستجيب لمطالبه سواء كانت تلك المطالب مادية أو معنوية. ومنه قيام أحد المخربين بسرقة بيانات البريد الرقمي لإحدى الفتيات ومساومتها على تزويده بمبالغ مالية وفي حال رفضت ذلك سيقوم بنشر صورها في مواقع الإنترنت بعد أن يقوم بعمل دبلجة للوجه مع أجساد عارية من خلال برنامج الفوتو شوب، وفي حال استجابتها لطلبه فسوف يعيد لها كلمة المرور الخاصة بعنوانها البريدي .[25]

✓ **ثالثا : التكنــولوجيا الذكيـــة لامن الحــدود :**

أصبحت إدارة أمن الحدود اليوم المستندة إلى التكنولوجيا أم را حتميا، لما تقدمه التكنولوجيات الحديثة و الرقمنة الإلكترونية و كذا المعلومة الجغرافية من معطيات أمنية و خدمات معلوماتية ضرورية لمتابعة حالة أمن الحدود، كالاعتماد على أنظمة تحديد المواقع (نظام "الج بي اس" GPSوغيره)، تحديد الخطوط و المساحات الجوارية، متابعة التمركز السكاني و العمراني على الحدود، إضافة إلى رسم الطرق و توضيح المسالك الرئيسية و الفرعية الرابطة بين المناطق و غيرها، الأمر الذي يسهل التعامل مع المسائل الأمنية على الحدود و مواجهة التهديدات الأمنية العابرة لها والحد منها بشكل مرن و أكثر احترافية، و كل هذا يتم بناء على يسمى بالحدود الذكية " Smart Borders ". [26]

تسعى العديد من الدول بالإضافة إلى الأسوار والسياجات الى تبني أيضاً نظاماً افتراضياً لمراقبة حدودها الوطنية .وشهد النظام الأخير، الذي يُعرف بالجدار أو السياج الافتراضي، تطوراً ملحوظاً خلال مرحلة ما بعد أحداث 11 سبتمبر، باعتباره سياسة مفضلة من قبل الدول الأوروبية وأمريكا الشمالية لمواجهة التهديدات الأمنية العابرة للحدود .ويميز جوزياح هايمن (Josiah Heyman) بين مَعنَيين لهذا الجدار الافتراضي :

المعنى الأول للجدار الافتراضي : ضيق ويُحيل إلى استعمال تكنولوجيا متطورة في مجالي الحاسوب والمراقبة لتطبيق قانون الحدود، من خلال استعمال رادار دائري المستوى round–level) (radar، على سبيل المثال، للكشف عن حركة الأشخاص وتحديد اتجاههم في محيط الحدود .[27]

و تتمتع نظم المراقبة الإلكترونية التي تنشر سواء على الحدود الطويلة أو عند أي طوق خارجي قصير المدى، ببعض المزايا المشتركة ونذكر منها:

* القدرة على كشف الدخلاء والتعرف إليهم، مع غربلة التحركات غير المهددة أو الطبيعية التي(تتنقل مثل الطيور المحلقة أو الحيوانات) تقليصاً للإنذارات الخاطئة.

24في الساعة في أحوال الرؤية الضعيفة

*ينبغي على كل نظام أن يكون قادراً على العمل والطقس القاسي، خصوصاً ذلك الذي تصحبه مواد تعتيمية (مثل الرمال والدخان والغبار) كما هو الحال في الحدود الصحراوية.

* إقامة قطاعات للإنذار محددة مسبقا لمستويات التهديد ولتصنيف الأهداف تستند إلى حجم الهدف وحركته وارتفاعه عن الأرض، ويمكن أن يكون هذا النظام محمولاً فردياً أو بحجم أكبر.

* ينبغي أن تمتد النظم على مئات آلاف الأمتار لتتلاءم مع أية تدابير أمنية مادية مع إمكانية إخفاء مكان وضع المستشعرات ، الرواصد و المتقفيات .

* أن تكون قادرة على التمييز و الكشف ما بين المسافرين لأغراض تجارية والمجرمين والمهربين بالإضافة إلى التهديدات الإرهابية والعسكرية مثل فرق الاستطلاع والقوات الخاصة .[28]

المعنى الواسع للجدار الافتراضي: فيشير إلى حشد قوات الشرطة، بما في ذلك الوكالات العسكرية والاستخباراتية، في المنطقة الحدودية .ويمثل الجدار الافتراضي بمعناه الضيق الجيل الأول لتطبيق

التكنولوجيا العسكرية في نظام مراقبة الحدود الذي أظهر عدم فعالية، وخاصة مع الاستخدام الذكي للتكنولوجيا المتطورة وأساليب مختلفة من التمويه من قبل المهربين والمهاجرين غير النظاميين. أما التعريف الواسع فيحيل إلى عسكرة افتراضية شاملة للحدود للكشف بدقة عالية عن كل الاختراقات غير القانونية على مدار الساعة، وبغض النظر عن أحوال الطقس السائدة.

ظل البحث عن الحلول التكنولوجية لمراقبة الحدود حاضراً بقوة في الولايات المتحدة خلال العقد الماضي .ويتضمن كل من" قانون حماية الحدود ومكافحة الإرهاب ومراقبة الهجرة غير الشرعية "الذي أقره مجلس النواب الأمريكي في ديسمبر 2005 ، و"قانون الإصلاح الشامل للهجرة "الذي أقره مجلس الشيوخ في ماي 2006 ، أحكاماً تتطلب توظيف تكنولوجيات جديدة لدعم جهود مراقبة الحدود بين منافذ الدخول المختلفة، وخاصة على طول الحدود الأمريكية – المكسيكية . يرتبط الجدار الافتراضي الأمريكي إلى حد كبير ب" مبادرة تأمين الحدود (Secure Border Initiative–SBI) التي أطلقتها وزارة الأمن الداخلي في نوفمبر . 2005 وتهدف وزارة الأمن الداخلي من خلال هذه المبادرة إلى تعزيز تقنيات المراقبة، ورفع مستوى أهلية العنصر البشري، وتطبيق قوانين الهجرة، وتحسين البنية التحتية المادية على طول حدود الولايات المتحدة مع كل من المكسيك وكندا، بهدف منع التهديدات الأمنية العابرة للحدود والحد من الهجرة غير النظامية.

أما في السياق الأوروبي، فقد اتخذ الاتحاد الأوروبي، خلال العقدين الماضيين، مبادرات لرقمنة نظام مراقبة الحدود بهدف مراقبة حركة التنقل عبر الحدود ومنع التهديدات الأمنية الخارجية .وقد تم دمج تكنولوجيا المعلومات والاتصالات من قبل الاتحاد الأوروبي في مجال مراقبة الحدود على مستويين اثنين على الأقل، ففي المستوى الأول استُعملت هذه التقنيات لتعزيز الأمن وتحصينه على الحدود الخارجية للاتحاد الأوروبي .ويُعدُّ نظام شنجن للمعلومات (Schengen Information System–SIS) والنظام المتكامل للمراقبة الخارجية .SIVE . اما المستوى الثاني فقد تضمن نشر أنواع أخرى من تكنولوجيا المعلومات والاتصالات ل" إخراج " (externalisation) مراقبة الحدود خارج محيط الاتحاد الأوروبي 57 .وفي إطار الاسراتيجية الثانية، اعتمد مجلس الاتحاد الأوروبي وهو نظام يهدف إلى تسجيل في عام 2004 ، نظام معلومات التأشيرة–Visa Information System) (VIS، المعلومات البيومترية لطالبي التأشيرة لتسهيل تبادل البيانات بين الدول الأعضاء، بما كُميِّن السلطات الوطنية المختصة من الدخول وتحديث بيانات التأشيرة والتشاور إلكترونياً حول هذه البيانات.[29]

كما دعت المفوضية الأوروبية "سيسيليا مالستروم " الدول الأعضاء إلى الاستثمار في التقنيات المتطورة لتحسين عبور الحدود من اجل جذب سياح ورجال أعمال الى الاتحاد الأوروبي. واقترحت إجراءان لجعل الحدود الخارجية لشينغن "ذكية" هما برنامج لتسجيل المسافرين ونظام للدخول والخروج .[30] وتقول الخبيرة في الشؤون الأوروبية "كيارا دي فيليشي" بالنسبة **لنظام سجل المسافرين** أن الغرض

منه هو تبسيط الإجراءات التي يخضع لها رعايا البلدان الأجنبية الذين يسافرون بشكل متكرر إلى الاتحاد الأوروبي، وهذا يشمل رجال الأعمال والعمال والمقيمين في المناطق الحدودية للاتحاد الذين يعبرون الحدود عدة مرات في السنة.[31] **أما نظام الدخول والخروج** فسيسد ثغرة في النظام الأوروبي العاجز اليوم عن متابعة تحركات الأجانب الذين يدخلون بتأشيرات ومعرفة ما اذا كان غادروا البلاد. وأوضحت المفوضية أن الإجراءات الجديدة "ستسجل تاريخ ومكان دخول وخروج مواطني الدول أخرى الذين يتوجهون إلى الاتحاد وستحتسب بطريقة الكترونية مدة الإقامة المسموح بها.[32]

خاتمة :

وأخيرا يمكن القول ان عودة كلمة " الحدود "إلى الظهور مرة أخرى فى أنحاء مختلفة من مناطق العالم، لكنها لا ترتبط هذه المرة بتلك الموجة العاتية من النزاعات التى تفجرت خلال التسعينات حول " خطوط

الحدود "بين الدول، وإنما بنوعية أخرى من المشكلات التى تتعلق بتهديدات لاتقل حدة فى" مناطق الحدود" ذاتها، بحيث تحولت الحدود إلى " خطوط ساخنة" ، تثير إشكاليات تتجاوز ما ارتبط بعمليات التأمين المعتادة ضد المخاطر التقليدية، إلى إقامة نظم أمن حدودية معقدة، لمواجهة موجة الاختراقات الراهنة،والتحديات الأمنية الجديدة .

من هذا المنطلق فانه لابد من مواكبة التطورات العلمية والتقنيات الحديثة التي تمكننا من تحقيق أفضل المستويات الأمنية لحدود أي دولة باعتبارها خط الدفاع الأول عن أمنها، كما أنه أي (التقنيات الحديثة) تساعد في تقديم خدمة أفضل للمسافرين عبر هذه الحدود، سواء من حيث توفير الوقت أو الجهد أو حتى تقليل الاحتكاك مع العنصر البشري في عمليات التفتيش وما ينجم عنه من مشاكل فردية

ويمكن إجمال أهم استنتاجات البحث في الخلاصات الآتية :

– على الدول البحث عن كيفية التوصل إلى حلول معلوماتية مبتكرة وفعالة من خلال الدمج بين "كاميرات المراقبة الأمنية" (CCTV) وأجهزة الاستشعار بالأشعة تحت الحمراء والليزر وتقنيات رسم الخرائط والمسح و"نظم المعلومات الجغرافية" (GIS) بهدف تعزيز فعالية وكفاءة عمليات المراقبة والاستطلاع والتحكم وحماية الحدود.

– تحتاج أجهزة الأمن إلى كثير من العمل لتطوير قدراتها للتعامل مع جرائم الكمبيوتر والوقاية منها، وتطوير إجراءات الكشف عن الجريمة ، وأيضًا يلزم نشر الوعي العام بجرائم الكمبيوتر، والعقوبات المترتبة عليها، واستحداث الأجهزة الأمنية المختصة القادرة على التحقيق في جرائم الكمبيوتر، والتعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم.

في ظل بروز تهديدات الأمنية المستحدثة عبر أدوات رقمية متطورة وذكية استوجب على الدول تطوير منظوماتها الدفاعية ونقل استراتيجياتها في مجال امن الحدود من بناء الأسوار والسياجات إلى ما صبح يعرف بالحدود الذكية او الحدود الافتراضية .

الهوامش :

1. الموقع الالكتروني : http://mawdoo3.com تاريخ الاطلاع 2017/01/10
2. إيما بول ، التكنولوجيا القابلة للارتداء وعالمها الرائع الجديد ، مجلة المنظمة العالمية للملكية الفكرية،يونيو 2014 .
3. إرشادات التحول الذكي للخدمات الحكومية ، حكومة عجمان ، ص 1 .
4. سعيد الصديقي ،تشديد الرقابة على الحدود وبناء الأسوار لمحاربة الهجرة : مقارنة بين السياستين الأمريكية والاسبانية ، مجلة رؤى استراتيجية ، جامعة العين للعلوم والتكنولوجيا ، يونيو 2013. ص91.
5. محمد عبد السلام ،" أمن الحدود "فى المنطقة العربية" ،شركة التنمية بحوث استشارات تدريب ،ص 6 .
6. نفس المرجع ، ص 7 .
7. سعيد الصديقي ، مرجع سبق ذكره ، ص 92 .
8. رائد العدوان ، المعالجة الدولية لقضايا الإرهاب الإلكتروني ،الدورة التدريبية :توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب ،2013 ، الرياض ، 2013 ، 7.
9. امجد المنيف ، الإرهاب الإلكتروني ..المعركة الحديثة ، العربية ، 30 يوليو 2015 ، ص 2 .
10. رائد العدوان ، مرجع سبق ذكره ، ص 8 .
11. أيسر محمد عطية ، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الالكتروني وطرق مواجهته ، الملتقى العلمي حول : الجرائم المستحدثة في ظل المتغيرات والتحولات الالفليمية والدولية ايام 2-2014/9/4 ، ص 10، 11 .
12. إيمان عبد الرحيم السيد الشرقاوي ، جدلية العلاقة بين الإعلام الجديد و الممارسات الإرهابية ، مؤتمر دور الإعلام العربي في التصدي لظاهرة الإرهاب ،جامعة نايف العربية للعلوم الأمنية ، 16-2014/12/18 ، ص16 .
13. محمد عجم ، تويتر وفيسبوك زعيما ثورات الربيع العربي ، القاهرة ، 2011، الموقع الالكتروني www.aawsat.com تاريخ الاطلاع 2017/01/10 .
14. الشبكات الاجتماعية في الربيع العربي ، الموقع الالكتروني : www.douliya.com تاريخ الاطلاع 2017/01/13.
15. مها فالح ساق الله ، دور الإعلام الجديد في الثورات العربية ،قسم الصحافة ، الجامعة الإسلامية غزة ، 2013 ،
16. الشبكات الاجتماعية في الربيع العربي ، مرجع سبق ذكره .
17. فهد بن عبد العزيز الغفيلي ، الإعلام الرقمي ماهيته ..أنواعه..أثاره ، ص 25-26 .
18. جورج قرم ، دور الإعلام والمثقفين العرب في تحويل الثورات إلى فِتَن دينية ومذهبية، جريدة" السفير – "العد 12017 ، أكتوبر 2011 ، ص 1 .
19. فهد بن عبد العزيز الغفيلي ، مرجع سبق ذكره ، ص 27 .

20. ندوة بمناسبة اليوم الوطني السعودي ، بعنوان " المواطنة الصالحة ...المفهوم والمقومات " ، جامعة الإمام محمد بن سعود الإسلامية ، 2007،
21. فهد بن عبد العزيز الغفيلي ، مرجع سبق ذكره ، ص 28-29 .
22. الموقع الالكتروني : www.cairoportaile.com اطلع عليه بتاريخ 2017/01/15.
23. تقرير التهديدات الالكترونية الجديدة ، معهد قطر لبحوث الحوسبة ، 2014 ،ص 3- 4 .
24. منصور بن سعيد القحطاني ، مهددات الأمن المعلوماتي وسبل مواجهتها ، رسالة مقدمة للحصول على شهادة الماجستر في العلوم الإدارية ، قسم العلوم الإدارية ، جامعة نايف العربية للعلوم الأمنية ،2008 ، ص28 الى 30 .
25. فهد بن عبد العزيز الغفيلي ، الإعلام الرقمي أدوات تواصل متنوعة ومخاطر أمنية متعددة ، ب د ن ،ب س ن ،ص 28- 29 .
26. الحامدي عيدون ،امن الحدود وتداعياته الجيو سياسية على الجزائر ،مذكرة مقدمة لنيل شهادة الماجستر في العلوم السياسية والعلاقات الدولية تخصص الدراسات السياسية المقارنة ،جامعة محمد بوضياف المسيلة ،2015 ، ص 148.
27. سعيد الصديقي ، تشديد الرقابة على الحدود وبناء الأسوار لمحاربة الهجرة : مقارنة بين السياستين الأمريكية والاسبانية ، مرجع سابق ، ص 104 .
28. الحامدي عيدون ، مرجع سبق ذكره ، ص 149 .
29. سعيد الصديقي، مرجع سبق ذكره ، ص 105-106 .
30. مقال على الانترنت اقتراح من المفوضية الأوروبية لجعل الجدود الخارجية لدول الشنغن اذكي ، www.alkompis.se اطلع عليه بتاريخ 2017/01/18 .
31. مقال على الانترنت الاتحاد الأوروبي يطلق حزمة الحدود الذكية ، www.aljazeera.net/news اطلع عليه بتاريخ 2017/01/18 .
32. مقال على الانترنت اقتراح من المفوضية الأوروبية لجعل الجدود الخارجية لدول الشنغن اذكي ،مرجع سبق ذكره.