# الإرهاب عن بعد:
## نمط تنظيمي جديد لاستهداف الدول الغربية والآسيوية

د. شادي عبدالوهاب
رئيس وحدة تقدير الاتجاهات الأمنية، المستقبل للأبحاث والدراسات المتقدمة، أبوظبي

شهد عدد من الدول الغربية والآسيوية ظاهرة أطلق عليها "الإرهاب الموجه عن بعد"، وهو نمط من الإرهاب ابتدعه "داعش" لاستهداف هذه الدول، من خلال قيام أحد أعضاء التنظيم بتجنيد وتوجيه المتعاطفين عبر المجال السيبراني لتنفيذ عمليات إرهابية داخل هذه الدول.

تكشف التحقيقات المتعلقة بالعمليات الإرهابية، التي قام بها "داعش" في عدد من الدول الغربية والآسيوية، أن عدداً من العمليات التي نظر إليها في البداية على أنها تندرج ضمن "إرهاب الذئاب المنفردة" اتضح أنها، بعد مزيد من التحقيقات، تمت بتوجيه وإرشاد كامل من قبل عناصر "داعش" في سوريا والعراق.

ويسعى هذا التحليل إلى إلقاء الضوء على هذه الظاهرة، وبيان عناصرها الأساسية، وكذلك الوقوف على أبرز الإجراءات الأمنية التي شرعت الدول الغربية تحديداً في اتخاذها لمواجهة هذا النمط الجديد من الإرهاب.

### أولاً: أبعاد الإرهاب الموجه

ذكر عدد من الأدبيات المعنية بدراسة الإرهاب ظاهرة "الإرهاب الموجه عن بعد" منذ أواخر عام 2016، وأشار إليها باستخدام مصطلحات متعددة أبرزها "العمليات الإرهابية عن بعد" (Terror Plots from Afar)[1]، أو "التخطيط الافتراضي" (Virtual Planners)[2]، بينما أشارت السلطات الأمنية الفرنسية والألمانية إلى هذا النمط الجديد من العمليات الإرهابية باستخدام مصطلح "المؤامرات الإرهابية الموجهة عن بعد" (Remote Controlled Plots)[3]. وسوف يعتمد هذا التحليل مصطلح "الإرهاب الموجه عن بعد".

وقد استخدم "داعش" هذا النمط من العمليات الإرهابية بدءاً من أوائل عام 2014[4]، إذ إنه من بين حوالي 38 عملية إرهابية قام بها "داعش" في الولايات المتحدة خلال الفترة الممتدة بين 1 مارس 2014 و1 مارس 2017، وجد أنه على الأقل ثماني هجمات منها (أي حوالي 21% من إجمالي هذه الهجمات) تضمنت وجود نوع من التواصل عبر الفضاء السيبراني بين منفذ العملية وأحد العناصر المرتبطة بـ"داعش"[5].

وبالمثل، فإن الظاهرة نفسها يمكن رصدها في عدد من الدول الأوروبية والآسيوية، إذ كشف تحليل حديث لحوالي 38 عملية إرهابية تبناها "داعش"، ووقعت في الفترة بين عام 2014 وأكتوبر 2016، أن حوالي 19 عملية منها (أي حوالي 50% من إجمالي العمليات) تضمنت توجيهات من "داعش" عبر الفضاء السيبراني[6]. وقد كان أحد أبرز الأمثلة في هذا السياق العملية التي تمت في ربيع 2015،

عندما قام طالب في تكنولوجيا المعلومات يسمى "سيد أحمد غلام" بإطلاق النار على كنيسة في باريس بعد أن تلقى توجيهات من قبل أحد عناصر "داعش" عبر الإنترنت[7].

أما فيما يتعلق بالدول الآسيوية، فيلاحظ تكرار النمط الإرهابي نفسه هناك. ففي ماليزيا، وجد أن سبعة من ثلاث عشرة عملية إرهابية لـ"داعش" تم إحباطها ما بين 2013 وسبتمبر 2016، يعتقد أنها تمت بتوجيه من أحد عناصر "داعش" في سوريا، والمنتمي إلى الجنسية الماليزية، وبالمثل، سعى "داعش" لتنفيذ سبع عمليات إرهابية في إندونيسيا باتباع الأسلوب نفسه[8].

ويعد أحد الأسباب وراء عدم اكتشاف هذا النمط قبل نهاية عام 2016 هو أنه كان ينظر إلى العديد من الهجمات الإرهابية في البداية باعتبارها "إرهاب الذئاب المنفردة"، غير أن التحقيقات التي أجرتها أجهزة إنفاذ القانون اكتشفت فيما بعد أنه كان يتم توجيهها عن بعد من خلال عناصر "داعش".

ويمكن تعريف "الإرهاب الموجه عن بعد" بأنه "تلك الهجمات التي لم يسبق لمنفذيها أن سافروا إلى مناطق الصراعات، أو انضموا إلى تنظيم إرهابي، ولكنهم مع ذلك، كانوا على تواصل دائم مع عناصر الجماعات الإرهابية من خلال استخدام منصات وسائل الاتصال المشفرة، وذلك لتوفير الدعم والنصيحة للمهاجم في كل مرحلة من مراحل الإعداد للعملية الإرهابية"[9]، كما أنه لوحظ أنه في بعض الحالات تم توفير الدعم المالي للقيام بعملية إرهابية، بل وفي انتقاء المناطق التي سيتم استهدافها.

وفي ضوء التعريف السابق، يمكن القول إن الإرهاب الموجه عن بعد هو شكل هجين لنمطين سابقين من الإرهاب في الدول الغربية، وهما الإرهاب الشبكي وإرهاب الذئاب المنفردة. فهي تتشابه مع الأشكال الشبكية من الإرهاب في وجود بعض الصلات بين منفذي الهجوم الإرهابي والتنظيم الإرهابي، غير أنه يختلف عنها في محور واحد، وهو أن هذه الصلات ليست تنظيمية، بل افتراضية، أي أن العنصر الإرهابي تم توجيهه من خلال الفضاء السيبراني.

وبالمثل، فإن الإرهاب الموجه عن بعد يتشابه مع إرهاب الذئاب المنفردة في بعد وحيد، وهي أن أغلب الهجمات يقوم بها فرد واحد. غير أنه بخلاف إرهاب الفرد الواحد، فإنه يوجد اتصال مع جماعة إرهابية قائمة، وإن كان عبر الفضاء السيبراني، كما أن الجماعة الإرهابية تساعد منفذ الهجوم الإرهابي في كل المراحل بدءاً من التطرف وانتهاءً بتجنيده لتنفيذ عملية إرهابية محددة[10]، وهو ما سيتم توضيحه لاحقاً.

## ثانياً: كيفية توجيه العمليات الإرهابية

يتم توجيه عمليات "الإرهاب الموجه عن بعد" من خلال الاعتماد على عنصرين أساسيين، وهما: المخطط الافتراضي (Virtual Planners)، والفضاء السيبراني، وهو ما يمكن تفصيلهما على النحو التالي:

**1- المخطط الافتراضي (Virtual Planners):** يعد جزءاً لا يتجزأ من "قسم العمليات الخارجية" داخل تنظيم "داعش"، وكانت مسؤولية الجهاز تتمثل في اختيار وتدريب العناصر الخارجية، وتنفيذ عمليات إرهابية خارج مناطق سيطرة التنظيم في سوريا والعراق. ويعتقد أن مدير "قسم العمليات الخارجية" هو المواطن الفرنسي "أبو سليمان الفرنسي".

ويمد المخطط الافتراضي أنصار "داعش" بالخدمات نفسها التي يجب أن يقدمها التنظيم الإرهابي لأتباعه، وبصورة أكثر تحديداً، ينتقي المُخطط الأهداف التي سيتم مهاجمتها، وتوقيت الهجوم الإرهابي وكيفية تنفيذه. وفي كل الحالات تقريباً، فإن منفذي العمليات الإرهابية لم يسبق لهم أن قابلوا شخصياً المخططين الذين يتآمرون معهم لتنفيذ العملية الإرهابية.

وتجدر الإشارة هنا إلى أن المخططين الافتراضيين داخل "داعش" كان يتم توزيعهم على المناطق الجغرافية المختلفة وفقاً لجنسياتهم، ومهاراتهم اللغوية[11]، وذلك للاستفادة من معرفتهم الجيدة بالأماكن المحتمل تنفيذ العمليات الإرهابية بها داخل الدولة المستهدفة، وتوظيف هذه المعرفة في توجيه المتعاطف مع التنظيم، أي أنهم غالباً ما ينتمون إلى الدولة نفسها التي يجري التخطيط فيها لتنفيذ عمل إرهابي[12].

**2- الفضاء السيبراني:** لجأت التنظيمات الإرهابية، خاصة "داعش"، إلى الإنترنت، وذلك للقيام بوظائف متعددة، منها تزويد اتباعهم بالمعلومات اللازمة، ونشر التطرف، وتجنيد العناصر المتعاطفة وتحويلهم لتنفيذ عمليات إرهابية، بالإضافة إلى نشر الدعاية، وجمع التبرعات من الداعمين للتنظيم، وأخيراً تنسيق العمليات الإرهابية[13]، وهو ما يمكن توضيحه تفصيلياً على النحو التالي:

**أ- الإمداد بالأسلحة:** فقد قام "المخطط الافتراضي التابع لتنظيم "داعش" الإرهابي بالتواصل مع عصابات الجريمة المنظمة داخل الهند، وذلك لشراء الأسلحة للخلية الإرهابية، التي تم تجنيدها لتنفيذ عملية إرهابية في مدينة "حيدرأباد" الهندية، كما أن المخطط اتفق مع العصابة على المكان الذي سيتم وضع السلاح فيه، وتواصل مع أحد المنفذين لكي يذهب إلى المنطقة نفسها لتسلم السلاح. ولعل ما ساعد المخطط على ذلك هو أنه كان "هندياً" يتحدث اللغة الهندية بطلاقة، ولديه خبرة جيدة بالمناطق المحلية في الهند[14].

**ب- إعطاء التوجيهات لتنفيذ العملية الإرهابية:** فقد تواصل المخطط الافتراضي مع الخلية الهندية، وأعطاهم توجيهات لاستخدام مادة "ترياسيتون تريبيروكسيد" لصنع المتفجرات[15]. وفي بعض الأحيان، قام المخطط الافتراضي بتعريف عدد من العناصر المتطرفة ببعضها البعض، ليكون خلية إرهابية صغيرة، وذلك لدفعهم لتنفيذ عمليات إرهابية. ففي سبتمبر 2016، ألقت السلطات الفرنسية القبض على خلية من النساء، حاولن وضع سيارة مليئة بالمتفجرات قرب كاتدرائية "نوتردام"، وقد كان المخطط المسؤول عنهم هو "راشد قاسم"، وهو المخطط المسؤول عن تنفيذ العمليات الإرهابية في أوروبا. وفي بعض الحالات، قام المخطط الافتراضي بتزويد متطرف أمريكي يدعى "منير عبدالقادر" بعنوان جندي أمريكي لكي يقتله ذبحاً، وهو المخطط الذي لم ينجح[16].

**ج- توظيف العملات الافتراضية:** إذ يشير عدد من المؤشرات إلى قيام تنظيم "داعش" تحديداً باستخدام العملات الافتراضية في تمويل العمليات الإرهابية، فقد أكدت السلطات الإندونيسية قيام إرهابيين مرتبطين بـ"داعش" لديها بالتواصل مع أفراد في سوريا، وأجريت تحويلات مالية باستخدام عملة البيتكوين. وقام متطرف متعاطف مع تنظيم "داعش" بإعطاء تعليمات على توتير لإرشاد المتطرفين حول كيفية التبرع لـ"داعش" باستخدام عملية بيتكوين الإلكترونية[17].

**د- استخدام عدة تطبيقات مشيفرة للتواصل:** استفادت التنظيمات الإرهابية، خاصة "داعش" من خدمات التواصل الاجتماعي، خاصة تطبيق "تليجرام"، والذي كان أحد أوائل التطبيقات، التي تستخدم "نظم التشفير من الطرف إلى الطرف" (End-to-End Encryption) [18]، أي أن هذه التطبيقات تقوم بتشفير الرسالة من المرسل وحتى جهاز المتلقي، بحيث لا يمكن لأجهزة إنفاذ القانون اعتراض الرسالة وقراءتها[19].

وفي حالة خلية "حيدر أباد"، قام أحد عناصر الخلية، ويدعى "يزداني" باستخدام عدة تطبيقات مشيفرة، سواء على الموبايل، أو اللاب توب، وكان الهدف الأساسي من ذلك هو ضمان عدم قدرة الأجهزة الأمنية على معرفة تفاصيل التخطيط الإرهابي، حتى لو تمكنت من فك تشفير الاتصالات التي تمت على أحد هذه التطبيقات[20].

> لجأت التنظيمات الإرهابية، خاصة "داعش"، إلى الفضاء السيبراني، وذلك للقيام بوظائف متعددة، منها تزويد أتباعهم بالمعلومات اللازمة، ونشر التطرف، وتجنيد العناصر المتعاطفة وتحويلهم لتنفيذ عمليات إرهابية، بالإضافة إلى نشر الدعاية، وجمع التبرعات من الداعمين للتنظيم، وأخيراً تنسيق العمليات الإرهابية.

وبالإضافة إلى ما سبق، فإن تطبيقات، مثل "تليجرام" و"ويكر" تمتلك خاصية بها، تسمح بأن يتم حذف الرسائل القديمة تلقائياً بعد مرور ساعة أو يوم من قراءتها، فضلاً عن إمكانية حذفها يدوياً، وهو ما يعني أنه عندما تتم مصادرة جهاز الموبايل أو اللاب توب الخاصة بالإرهابي، فإن أغلب الأدلة المتوفرة عليه، سوف تكون قد حذفت[21]، وهو ما يعيق الأجهزة الأمنية عن التوصل لأطراف المخطط الإرهابي.

## ثالثاً: الإجراءات الأمنية المضادة

قامت الدول الغربية، خاصة الولايات المتحدة بتبني عدد من الإجراءات لمواجهة هذا النمط الإرهابي الجديد، وهو ما يمكن تفصيله على النحو التالي:

**1- استخبارات الإشارة (Signal Intelligence):** إذ باتت الأجهزة الأمنية في الدول الغربية تعتمد على استخبارات الإشارة لمواجهة التهديدات النابعة من التنظيمات الإرهابية، بالإضافة إلى التجسس على الاتصالات التي تتم في "الإنترنت المظلم" (Dark Web). وقد قامت " وكالة مشاريع البحوث المتطورة الدفاعية" (Defense Advanced Research Projects Agency) بتطوير مشروع عرف باسم "ميمكس" (MEMEX) منذ عام 2014، والذي يقوم برصد وتعقب مستخدمي الإنترنت المظلم، بما في ذلك العناصر الإرهابية. وتعد وكالة مشاريع البحوث المتطورة الدفاعية هي إحدى الإدارات التابعة لوزارة الدفاع الأمريكية، والمسؤولة عن تطوير التكنولوجيات الحديثة لصالح الجيش الأمريكي[22].

**2- تصفية المخططين الافتراضيين:** إذ شرعت الاستخبارات الأمريكية والبريطانية منذ ربيع 2015 بتعقب المخططين الافتراضيين، بعدما أدركوا التهديدات الأمنية النابعة منهم، وقامت بتصفيتهم من خلال الضربات الجوية، وهو ما ترتب عليه مقتل عدد كبير منهم[23]. وأحد الأمثلة البارزة في هذا الإطار، هو تصفية الجيش الأمريكي لثلاثة مخططين افتراضيين باستخدام الطائرات بدون طيار في مدينة الرقة، عندما كانت تحت سيطرة "داعش"، وذلك خلال عامي 2015 و2016. وقد كان الثلاثة يقومون بتوجيه المتعاطفين لتنفيذ عمليات إرهابية في الولايات المتحدة[24].

**3- وقف الرسائل المشيفرة:** ففي مواجهة توظيف الجماعات الإرهابية للتطبيقات المشيفرة، شرعت الحكومات الغربية، خاصة البريطانية والأمريكية، في البحث عن طرق لاختراق الرسائل المشيفرة. وقد سعت في البداية إلى الضغط على شركات التكنولوجيا المنتجة لهذه التطبيقات. وعلى سبيل المثال، فإن جيمس كومي، مدير مكتب التحقيقات الفيدرالية السابق، وغيره من رؤساء الأجهزة الأمنية أبلغوا اللجنة القضائية في مجلس الشيوخ في يوليو 2015 أن "نظام التشفير من الطرف إلى الطرف" يمنع أجهزة إنفاذ القانون من جمع الأدلة الإلكترونية لجعل أمريكا آمنة. وطالب كومي صراحة بأن يتم إعطاء الأجهزة الأمنية "باباً خلفياً" للأجهزة الأمنية يتيح لها تجاوز نظم التشفير. وقد تجددت هذه المطالبات بعد العمليات الإرهابية التي شهدتها كل من باريس وسان بيرناردينو في أواخر عام 2015، وبروكسل في مارس 2016[25].

وقد طالبت وزيرة الداخلية البريطانية "أمبر رود" بمطالب مماثلة عقب هجمات لندن الإرهابية في مايو 2017، إذ صرحت بأن نظم التشفير من الطرف إلى الطرف في تطبيقات مثل الـ "واتس آب" غير مقبولة تماماً"[26].

ونظراً للمشاكل الفنية التي تثيرها هذه المطالب، فإن الحكومات شرعت في البحث عن وسائل أخرى، منها تطوير وسائل وأدوات للتجسس على الرسائل والمكالمات المشيفرة. وقد كشفت تسريبات ويكيليكس مؤخراً عن قيام وكالة الاستخبارات المركزية (CIA) بالتجسس على تطبيقات الرسائل الشهيرة (مثل الواتس آب وسيجنال ..) من خلال اختراق النظام التشغيلي للهواتف الذكية، والتجسس على الرسائل النصية والصوتية قبل إرسالها من خلال التطبيق وتشفيرها. ومن جهة ثانية، فإن وكالة الاستخبارات المركزية استغلت ثغرة موجودة في كافة نظم التشغيل للأجهزة الكمبيوترية مثل "ويندوز" و"ماك أو إس" و"لينكس"، والتي تتيح لها اختراق الأجهزة والتجسس عليها، بل والتحكم فيها[27].

## الخاتمة

كشف تطوير "داعش" أسلوب الإرهاب الموجه عن بعد عن نجاحه في تنفيذ عمليات ضد عدد كبير من الدول مثل الولايات المتحدة والدول الأوروبية الرئيسية، وهو ما مكنه من الاستمرار في تصدر المشهد الإرهابي على الرغم من انحسار سيطرته على مناطق نفوذه في سوريا والعراق. ولذلك يرجح تزايد اعتماد "داعش" على هذا النمط في الدول الغربية[28].

ولعل من المؤشرات في هذا الإطار أن التنظيم بدأ في استئناف نشاطه الإعلامي الناطق باللغة الإنجليزية، والذي يحرض أتباعه على تنفيذ عمليات إرهابية في الغرب، خاصة مع استئناف وكالة أنباء "أمواج" التابعة لـ"داعش" أول بياناتها باللغة الإنجليزية في أواخر يناير 2018، وذلك بعد توقف أكثر من أربعة أشهر[29].

ومع ذلك، فإن قدرة "داعش" على الاستمرار في تبني هذا النمط من العمليات الإرهابية يتوقف في جانب منه على امتلاكه عناصر أجنبية منتمية للدول التي يستهدفها، وهو ما يتوقف على مصير المقاتلين الأجانب في صفوف "داعش"، وهل سيعودون إلى بلدانهم الأم، أما أنهم سينتقلون إلى أحد التنظيمات الفرعية المرتبطة بـ"داعش"، ويقومون بإعادة توجيه المتعاطفين لتنفيذ عمليات إرهابية، كما لا يمكن إغفال إمكانية لجوء التنظيمات الأخرى المرتبطة بالقاعدة إلى محاكاة التكتيكات التي اتبعها "داعش".

وعلى الجانب الآخر، فإن هناك عدداً من التحديات التي تواجه هذا النمط من الإرهاب، إذ إن العناصر المتعاطفة التي يتم تجنيدها غالباً ما تفتقد إلى الخبرة الإجرامية الكافية، ومن ثم لا تستطيع تنفيذ الأوامر التي يعطيها لهم بكفاءة، وهو ما قد يترتب عليه فشل العملية الإرهابية، كما أن الأفراد الذين يتم توجيههم عبر الفضاء الإلكتروني قد يتم اعتراض اتصالاتهم من قبل الأجهزة الأمنية، ومن ثم إحباط المخطط الإرهابي. غير أن هذا الأمر مردود عليه بأن الهجمات الإرهابية التي شهدتها مؤخراً كل من فنلندا وبرشلونة وروسيا في أغسطس 2017، تكشف أن تكتيكات الإرهاب غير المعقدة مثل الطعن والدهس، قد يتم تنفيذها بسهولة نسبية، ولكن نتائجها تكون كارثية، خاصة فيما يتعلق بعدد الضحايا.

وفي الختام، يمكن القول إن هذا النمط من الإرهاب مرجح للانتشار بدرجة أكبر في الدول الأوروبية من العربية، والتي يشهد بعضها وجود التنظيمات الإرهابية المحلية الموالية لـ"داعش"، فلا يجب إغفال أن "الإرهاب الموجه عن بعد" جاء نتيجة لإخفاق تنظيم "داعش" في الاحتفاظ بخلايا نائمة في الدول الأوروبية.

1- Rukmini Callimachi, Not “lone Wolves” after all: How ISIS guides world’s terror plots from afar, **The New York Times**, February 4, 2017, accessible at: https://goo.gl/P3ZPEb

2- Andrew Zammit, The role of virtual planners in the 2015 Anzac day Terror plot, **Security Challenges**, Vol. 13, no. 1, 2017, p. 45.

3- Thomas Joscelyn, Terror plots in Germany, France were ‘remote-controlled’ by Islamic State operatives, **Long War Journal**, September 24, 2016, accessible at: https://goo.gl/Z4Wdyu

4- Andrew Zammit, **op.cit**., p. 41.

5- Seamus Hughes and Alexander Meleagrou-Hitchens, The Threat to the United States from the Islamic State’s Virtual Entrepreneurs, **CTC sentinel**, Volume 10, Issue 3, March 2017, p. 1.

6- **Ibid**., p. 6.

7- Rukmini Callimachi, **op.cit**.

8- Andrew Zammit, **op.cit**., p. 45.

9- Andrew Zammit, **op.cit**., p. 42.

10- Rukmini Callimachi, **op.cit**.

11- Daveed Gartenstein-Ross and Madeleine Blackman, Isil’s Virtual Planners: A Critical Terrorist Innovation, **War on the rocks**, January 4, 2017, accessible at: https://goo.gl/uJMZFK

12- Bridget Moreng, ISIS' Virtual Puppeteers, How They Recruit and Train "Lone Wolves", **Foreign Affairs**, September 21, 2016, accessible at: https://goo.gl/ZsGeZw

13- Gabriel Weimann, Terrorist Migration to the Dark Web, **Perspectives on Terrorism**, Vol. 10, no. 3, 2016, (p. 36), accessible at: http://www.iacis.org/iis/2016/4_iis_2016_36-41.pdf

14- Rukmini Callimachi, **op.cit.**

15- Andrew Zammit, **op.cit**., p. 43.

16- Andrew Zammit, **op.cit**., p. 43.

17- Levi Maxey, Terror Finance in the Age of Bitcoin, **The Cipher Brief**, June 11, 2017, accessible at: https://www.thecipherbrief.com/terror-finance-in-the-age-of-bitcoin

18- Robert Graham, How Terrorists Use Encryption, **CTC SENTINEL**, June 2016, Volume 9, Issue 6, p. 20.

19- Jasper Hamill, How terrorists use encrypted messaging apps to plot, recruit and attack, **New York Post**, March 28, 2017, accessible at: https://goo.gl/QFwYK2

20- Rukmini Callimachi, **op.cit**.

21- Robert Graham, **op.cit**.

22- Ryan Ehney and Jack D. Shorter, Deep Web, Dark Web, Invisible Web and The Post ISIS World, **Issues in Information Systems**, Volume 17, Issue IV, 2016, p. 39.

23- Rukmini Callimachi, **op.cit**.

24- Seamus Hughes and Alexander Meleagrou-Hitchens, **op.cit**., p. 5

25- Darrell M. West and Jack Karsten, A brief history of U.S. encryption policy, **Brookings**, April 19, 2016, accessible at: https://goo.gl/z7GyrW

26- Timothy Revell, Theresa May’s repeated calls to ban encryption still won’t work, **New Scientist**, June 5, 2017, accessible at: https://goo.gl/KsPNHY

27- Swati Khandelwal, 10 things you need to know about “Wikileaks CIA Leak”, **The hackers news**, March 8, 2017, accessible at: https://goo.gl/JAC7A1

28- Bridget Moreng, **op.cit**.

29- تقرير أميركي: «داعش» يعلن «الحرب الافتراضية» على الغرب بعد سقوط عاصمته، **الشرق الأوسط**، 24 يناير 2018، موجود على الرابط التالي: https://goo.gl/heQt7S