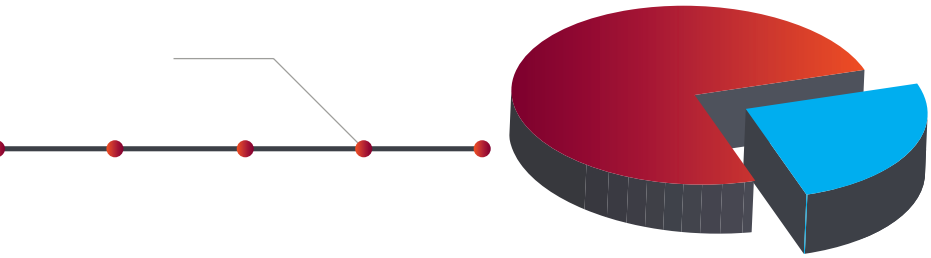
AL SHARQ
STRATEGIC
RESEARCH
الشرق
للأبحاث الاستراتيجية

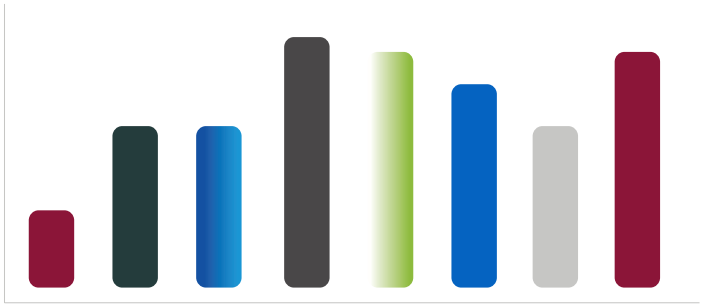
العمليات السيبرانية في الحرب الروسية الأوكرانية طبيعتها وأنماطها

تحليلات

نبيل عودة

20 سبتمبر 2022





المحتوى

ملخَّص

تسلِّط هذه الورقة الضوءَ على الجبهة السيبرانية في الحرب الدائرة بين روسيا وأوكرانيا التي اشتعلت في 24 فبراير/شباط 2022، وذلك من خلال تناول الاستراتيجيات العامة للعمليات السيبرانية وطبيعتها وأبرز التكتيكات التي اتبعها الجانبان. وقد تناولت الورقة البحث من خلال تقسيمه إلى قسمَيْن رئيسَيْن: القرصنة الخشنة التي تستهدف الشبكات الإلكترونية للبنية الحيوية العسكرية والمدنية على حدٍّ سواء من خلال تعطيلها وإخراجها عن الخدمة أو التحكُّم بها، والقرصنة الناعمة التي تستهدف التأثير في معنويات الخصم وقناعاته وتصوراته.

وقد بات موضوع العمليات السيبرانية يحظى بالمزيد من الاهتمام في الدوائر السياسية والأكاديمية والاستراتيجية بسبب الاعتماد المتزايد على شبكة الإنترنت وانتشارها، فضلًا عن انتشار تطبيقاتها، مثل منصات التواصل الاجتماعي، بحيث باتت البنية الحيوية المدنية والعسكرية وحتى الاجتماعية لأي دولة معتمدةً اعتمادًا كاملًا على شبكة الإنترنت في عمليات التشغيل والتنفيذ والاتصال. وبناءً على هذه الأهمية، باتت كل دولة تحظى بجيش سيبراني أو وحدات سيبرانية تختصُّ بالهجوم والدفاع. وبات الفضاء السيبراني المجال الخامس في الحروب مضافًا إلى المجالات التقليدية الأخرى: البرية والبحرية والجوية والفضائية.

وتثير الورقة تساؤلَين جوهريَّين: هل لجأت الأطراف المتحاربة إلى توظيف العمليات السيبرانية في عملياتها الحربية؟ وما هي طبيعة هذه العمليات السيبرانية، والاستراتيجيات والتكتيكات التي اتبعتها هذه الأطراف؟

وقد أظهرت الدراسة الاهتمامَ الذي أولته الجهات المتحاربة للجبهة السيبرانية، وهو ما يعزز من أهمية هذه الجبهة في المجهودات الحربية. وعلى عكس ما شاع في بداية الحرب من أن الجبهة السيبرانية لم تكن حاضرة، فإن الورقة تثبت أن العمليات السيبرانية قد شُنَّت على نطاق واسع، واستخدمت العديد من الاستراتيجيات والتكتيكات، سواء الهجومية منها أو الردعية، لتحقيق الأهداف المرجوة.

ونظرًا لهذا التنوع الواسع في استخدام هذه الاستراتيجيات والتكتيكات المتبعة من الأطراف المتحاربة، فقد خلصت الورقة إلى أن الحرب السيبرانية لا ينبغي إخضاعها لشروط الحروب الأرضية ومقاييسها، لتجنُّب الوقوع في الاختزال وسوء التقييم. فالحرب السيبرانية هي مجال قائم بحدِّ ذاته. وهذا لا ينفي جواز توظيف الهجمات السيبرانية في دعم مجهود الحرب الأرضية. كما أن الحرب السيبرانية لا تقتصر على الهجمات الإلكترونية ضد الشبكات، بل تشمل أيضًا حروب الدعاية والتضليل وبثّ الأخبار الكاذبة للتأثير في معنويات الخصم وقناعاته. فالحرب السيبرانية هي طيفٌ يشمل جميع العمليات التي تقع بين طرفَيْن: حرب الشبكات، وحروب الدعاية.

المقدمة

اندلعت الحرب الروسية على أوكرانيا في الرابع والعشرين من شهر فبراير/شباط 2021، لتضع العالم أمام حقائق جديدة. فمنذ نهاية الحرب العالمية الثانية، لم تحدث حربٌ بين دولتَيْن كبيرتَيْن متجاورتَيْن في أوروبا. وستدفع هذه الحرب العديد من منظري العلوم السياسية والعلاقات الدولية إلى التفكير من جديد في الكثير من الحقائق والمسلَّمات التي سادت في العقود الأخيرة. ولن تكون الحرب السيبرانية بمعزلٍ عن عملية إعادة التفكير هذه. والسبب في ذلك يعود إلى أن هذه الحرب الدائرة بين روسيا وأوكرانيا تكتسب أهميةً خاصةً من حيثُ العمليات السيبرانية، لامتلاك البلدين عددًا كبيرًا من المتخصِّصين في تكنولوجيا المعلومات والأمن، ومراكمتهما الخبرة في مجال العمليات السيبرانية على مدار سنوات طويلة. فروسيا تُعَدُّ واحدة من أبرز الدول في العالم توظيفًا للعمليات السيبرانية في سياستها الخارجية، في حين عملت أوكرانيا بشكلٍ حثيثٍ على تطوير بنيتها التحتية الرقمية لمواجهة المخاطر الروسية، خصوصًا بعد الهجمات التي ضربت شبكة الكهرباء في عام 2015.

إن جوهر العمليات السيبرانية هو المعلومات، فهي عمليات تُشَنُّ باستخدام الشبكات المعلوماتية للحصول على البيانات أو إتلافها أو حجبها، أو هي عمليات تُشَنُّ بواسطة المعلومات لحرمان الخصم من الاستفادة من مصادر قوته والنيل من عزيمته. وفي الوقت الذي كانت العديد من منطلقات فهم العمليات السيبرانية تُبنى على افتراضات وسيناريوهات متوقَّعة، فإن الحرب الدائرة بين روسيا وأوكرانيا توفر مثالًا تجريبيًا لاختبار هذه الافتراضات ومعرفة مدى أهليتها النظرية.

على مدار سنوات، برزت أوكرانيا كواحدة من أكثر الجهات التي استهدفتها روسيا بعملياتها السيبرانية التي شملت اختراق الشبكات الإلكترونية الحيوية وإخراجها من الخدمة، ومحاولة التأثير في الانتخابات الأوكرانية من خلال عمليات التضليل وبثِّ الأخبار الكاذبة. وقد أدى وقوع أوكرانيا تحت التهديد السيبراني المتواصل من قِبَل روسيا إلى تطوير آليات الردع السيبرانية، التي أسهمت إسهامًا كبيرًا في توفير بيئة رقمية أكثر مرونةً في التعامل مع الهجمات السيبرانية من ناحية تحييدها أو التخفيف من أضرارها الجانبية من ناحية أخرى.

وقد برزت الحرب الدائرة حاليًا بوصفها مثالًا واضحًا على توظيف كلٍّ من روسيا وأوكرانيا للعمليات السيبرانية في تحقيق أهدافهما الاستراتيجية. وقد تنوَّعت هذه العمليات بين عملياتٍ هجومية وأخرى دفاعية. كما برز مفهوم الردع الشامل بوصفه واحدًا من أهم الاستراتيجيات في التصدي للبرمجيات الخبيثة وعمليات التلاعب والتأثير.

ونظرًا لأن روسيا كانت الطرف الذي بدأ الحرب، فقد كانت أكثر توظيفًا للعمليات السيبرانية الهجومية. وقد شملت هذه العمليات استهداف شبكات البنية الحيوية المدنية والعسكرية، والمواقع الإلكترونية لقطاعات واسعة في أوكرانيا، هذا فضلًا عن عمليات التلاعب والتأثير وبثِّ الأخبار الكاذبة، التي حاولت الإتيان على الروح المعنويَّة للأوكرانيين من خلال تصويرهم ضعفاء وينشدون الاستسلام.

وفي الوقت الذي لجأت فيه أوكرانيا إلى بعض الاستراتيجيات الهجومية، كما هو الحال في إنشاء جيش أوكرانيا السيبراني، فإن غالبية عملياتها أخذت طابعَ الدفاع والردع. وقد أثبتت أوكرانيا أن مفهوم

الردع الشامل، الذي يتبنَّى تكتيكات تعزيز قدرات الدفاع الذاتية، وبناء تحالفاتٍ بين القطاعات الخاصة والحكومية من جهة، وتحالفاتٍ مع حكومات ومنظمات دولية من جهة أخرى، قابلٌ للتطبيق ويمنح الأطراف مرونةً في التعاطي مع الهجمات السيبرانية.

وقد برعت أوكرانيا أيضًا في تكتيكات حروب الدعاية والتأثير، حيث وظَّفت هذه التكتيكات في دعم سرديتها عن الحرب من جهة، وبثِّ روح العزيمة والصمود في الحاضنة الأوكرانية من جهة أخرى. وقد كان ذلك واضحًا من خلال الدخول الكثيف للرئيس الأوكراني على خطِّ هذه التكتيكات من خلال الفيديوهات التي كان يخرج بها على شعبه بشكل مباشر من شوارع العاصمة كييف عبر تطبيقات منصات التواصل الاجتماعي، مثل تيك توك. هذا فضلًا عن عدد المتطوعين السيبرانيين الذي أبدوا استعدادهم للإسهام في تنفيذ هجماتٍ سيبرانية نيابةً عن الجانب الأوكراني.

إن دراسة العمليات السيبرانية في الحرب الدائرة بين روسيا وأوكرانيا تُعَدُّ أمرًا جوهريًّا لتعزيز فهمنا لظاهرة الحرب في عصر الإنترنت، حيث باتت الوسائل والأدوات الإلكترونية مرتبطةً بشكلٍ عضويٍّ في أي عملٍ حربيّ. وقد اعتمدت الورقة، التي ركَّزت على الفترة الممتدَّة منذ انطلاق العمليات العسكرية في 24 فبراير/شباط 2022 حتى منتصف شهر نيسان/إبريل 2022، على منهجية التحليل المقارن بين العمليات العسكرية التي شنَّتها روسيا، وتلك التي شنَّتها أوكرانيا، من أجل التعرف إلى طبيعة هذه العمليات وأنماطها، والاستراتيجيات والتكتيكات التي اتُّبِعَت في تنفيذها. وقد تجنَّب التحليلُ البحثَ في نتائج هذه العمليات والآثار التي ترتَّبت عليها، وذلك لأسباب أهمها أن الحرب لم تنتهِ بعدُ، حيث ما زال هناك نافذة لتصعيد العمليات السيبرانية على صعيدَي النطاق والأهداف. فالعمليات العسكرية على الأرض ما زالت قائمةً، وهو ما يُصعب من عملية رصد التأثيرات المحتملة للعمليات السيبرانية. هذا من جانب، أما من جانبٍ آخر فالأمر يعود إلى طبيعة العمليات السيبرانية التي تحدث عادةً في الخفاء ولا يتم الكشف عن المدى الذي وصلت إليه وحجم الضرر الذي أوقعته في الخصم، وهو ما يجعل قياس تأثير هذه العمليات أمرًا في غاية الصعوبة.

تذهب الورقة في اتجاه افتراض رئيس، هو أنه على عكس ما ادعى العديد من الخبراء والمراقبين بأن العمليات السيبرانية كانت هامشيةً في الصراع الجاري حاليًّا بين روسيا وأوكرانيا، فإن الورقة تجادل -على العكس من ذلك- بأن الاعتماد على شنِّ الهجمات السيبرانية كان اعتمادًا كبيرًا وواسعًا، وفي صلب الاستراتيجية الحربية لدى الطرفَيْن. والشاهد على ذلك:

١- **كثافة شن العمليات**: حيث بلغ حجم العمليات المئات في الفترة القصيرة التي ترصدها الورقة، والتي لا تتعدى الشهرين من عُمر الحرب.

٢- **توقيت العمليات**: حيث شُنَّت العديد من العمليات قبيل العمليات العسكرية الأرضية ومع بدايتها.

٣- **تنوع العمليات**: حيث شملت العمليات السيبرانية العديد من أوجه الحرب السيبرانية، سواء تلك التي تتعلَّق بقرصنة الشبكات الحيوية أو المواقع الرسمية والمالية، أو تلك التي تستهدف التأثير في تصورات الأشخاص وعقولهم عبر عمليات التلاعب وبثِّ الأخبار الكاذبة.

تتضمَّن الورقة بالإضافة إلى المقدمة ثلاثة أجزاء وخاتمة. يناقش الجزء الأول المفاهيم الرئيسة للحرب السيبرانية من خلال إبراز التعريفات الأكثر شمولًا في الموضوع، وذلك جنبًا إلى جنب أبرز المقاربات

النظرية للحرب السيبرانية بين أولئك الذين يدرجونها ضمن العمليات التكتيكة للحرب الأرضية، وأولئك الذين يرون أنها نوع جديد تمامًا من الحروب. ويناقش الجزء الثاني الهجمات السيبرانية وطبيعتها وتنوعها، التي شنَّت روسيا معظمها، كما يناقش الردع السيبراني الشامل الذي برعت فيه أوكرانيا إلى حدٍّ كبير. أما الجزء الثالث فيناقش العمليات السيبرانية من نوع حروب الدعاية والتضليل ونشر الأخبار الكاذبة، التي هدفت بالأساس إلى رفع معنويات الحاضنة الشعبية من جهة، وكسر إرادة الخصم والتشويش على قدرته في اتخاذ القرارات من جهة أخرى.

الكلمات المفتاحية: الحرب السيبرانية، الحرب الإلكترونية، الفضاء السيبراني، روسيا، أوكرانيا، الناتو

الجزء الأول: مفهوم الحرب السيبرانية ومقاربتها النظرية

يشير نيلز ميلزر إلى أن الحرب الإلكترونية/السيبرانية هي تلك التي «تجري في الفضاء السيبراني من خلال الوسائل والأساليب السيبرانية». ويرى أنه في الوقت الذي يشير فيه مصطلح «الحرب» بشكل عام إلى الأعمال العدائية العسكرية في حالات النزاع المسلح، فإن الفضاء السيبراني/الإلكتروني يأخذ بُعدًا آخر، ويشير إلى «شبكة مترابطة عالميًّا من المعلومات الرقمية والبُنى التحتية للاتصالات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعلومات المتوفر بداخلها». ومن ثَمَّ حسب ميلزر، فإن إصابة شبكة كمبيوتر تابعة لأحد الخصوم ببرمجيات خبيثة -على سبيل المثال- «تشكِّل عملًا من أعمال الحرب الإلكترونية»، في حين أن «القصف الجوي بناءً على أمر عسكري إلكتروني» لا يمثِّل عملًا من أعمال الحرب السيبرانية[1].

وهناك تعريف آخر يرى أن الحرب السيبرانية «هي أعمال هجومية ودفاعية، متكافئة وغير متكافئة، تحدث في الشبكات الرقمية من قِبَل الدول أو جهات فاعلة شبيهة بالدولة (أو ما دون الدولة)، وتشتمل على مخاطر تصيب البنية التحتية الوطنية المهمَّة والأنظمة العسكرية»[2]. ويتطلب هذا الشكل من الحروب «درجة عالية من الترابط بين الشبكات الرقمية والبنية التحتية من جانب المدافع، والتقدُّم التكنولوجي من جانب المهاجم»[3]. ويمكن فهم هذه الحروب على أنها «تهديد مستقبلي وليس تهديدًا حاليًّا، وتتناسب تمامًا مع نموذج حرب المعلومات»[4].

وتختلف العمليات السيبرانية عن العمليات المعلوماتية (Information Operation)، التي تهتمُّ اهتمامًا خاصًّا باستخدام القدرات المتعلِّقة بالمعلومات في أثناء العمليات العسكرية للتأثير في عملية صُنع القرار لدى الخصوم. وقد تستخدم العمليات المعلوماتية الفضاء الإلكتروني كوسيط، ولكنها قد تستخدم أيضًا إمكانات من المجالات المادية[5]. وهذا يعني أن الحروب المعلوماتية أهمُّ من الحروب السيبرانية، حيث تختصُّ الحروب السيبرانية باستهداف الشبكات والبيانات التي تتضمَّنها هذه الشبكات، في حين تذهب حرب المعلومات إلى إضافة بُعدٍ آخر يتعلَّق باستخدام هذه المعلومات أو البيانات للتأثير في صانع القرار وحاضنته الشعبية عبر عمليات التأثير والتلاعب والتضليل والأخبار الكاذبة.

وأخيرًا، يمكن أن تُعرَّف الحرب السيبرانية بأنها «الصراع الذي يستخدم تعاملات أو هجمات معادية وغير قانونية على أجهزة الكمبيوتر والشبكات في محاولة لتعطيل الاتصالات وأجزاء أخرى من البنية التحتية كآلية لإلحاق ضرر اقتصادي أو تعطيل الدفاعات»[6].

يرى بعض الخبراء -مثل توماس ريد- أن تسمية الحرب السيبرانية هي تسمية مجازية، من باب الحرب على الجوع والحرب على الغلاء؛ وذلك لأنها لا تستوفي الشروط الموضوعية للحرب التي حدَّدها كارل فون كلاوزفيتز في كتابه **«On War»**، وتتمحور حول الطبيعة العنفية، والطبيعة الأداتية، والطبيعة السياسية. فالحرب يجب أن تتضمَّن استخدام القوة لإحداث الضرر والأذى المادي، كما أنها وسيلةٌ لتحقيق غايةٍ تتمثَّل في إجبار الخصم على الانصياع لإرادة المعتدي، وأخيرًا يجب أن تتضمَّن هذه الأداة هدفًا سياسيًا، فالحرب لا تُشَنُّ لأجل الحرب، فهي لا تشكِّل فعلًا منعزلًا، بل هي فعلٌ يتم اللجوء إليه لتحقيق غاية سياسية، كالانصياع والتسليم والتبعية على سبيل المثال. وعلى حدِّ قول كلاوزفيتز، فإن «الحرب هي مجرَّد استمرار للسياسة بوسائل أخرى».

يرى أصحاب هذا الرأي أن هذه الشروط الثلاثة لا تنطبق على الحرب السيبرانية. ففي هذه الحرب تنعدم أدوات القوة المادية التي تؤدي إلى إيقاع الضرر والأذى الماديَّيْن من قتلى وجرحى وتدمير بُنى تحتية وإحداث فوضى الرُّكام. وبالرغم من كونها وسيلةً، فإنها لا تكفي لإجبار العدو على الانصياع. فالضرر الحاصل جراء الهجمات السيبرانية غالبًا ما يكون مؤقتًا، ويمكن معالجته بفترة زمنية محدودة، كتعطيل شبكة وإخراجها من الخدمة. وأخيرًا، قد لا تتضمَّن الهجمات السيبرانية بُعدًا سياسيًا، وذلك لمحدودية أهدافها التي تتمثَّل في التجسُّس وسرقة البيانات أو إتلافها، وهو ما يجعلها أقربَ إلى الجريمة الإلكترونية من الحرب الفعلية. هذا فضلًا عن أن الهجمات السيبرانية تفتقر -في الغالب- إلى عنصر الاعتراف. فواحدة من أبرز خصائصها هي المجهولية والخفاء. وطالما انتفى الاعتراف، انتفى الهدف السياسي. فأحد أهم شروط تحقيق الهدف السياسي هو أن يعترف المعتدي بتبنِّيه العمليات من أجل إجبار الخصم على تنفيذها تحت سوط التهديد والإيذاء[7]. ولذلك يخلص أصحاب هذا الرأي إلى أن الحرب السيبرانية -وَفْقَ هذه الشروط الثلاثة- لا يمكن حدوثها.

ويرى آخرون -من أمثال إريك جارتسكي- أن القوة السيبرانية بشكل عام أدنى من القوة المادية في أداء وظائف الإكراه والأذى ضد الخصم. ومن غير المرجَّح أن تثبت الهجمات السيبرانية فعاليتها بشكل خاص من الناحية الاستراتيجية الكبرى ما لم تتمكَّن من إلحاق ضررٍ كبيرٍ ودائمٍ بالخصم يجبره على تغيير سلوكه. وبناءً على ذلك، فإن الحرب السيبرانية لن تكون بمثابة الحكم النهائي للمنافسة في النظام الدولي[8].

هناك فريق آخر يخالف أصحاب الرأيين السابقين، ويجادل بأن الحرب السيبرانية نوع مختلف من الحروب يتمتَّع بمواصفاته الخاصة التي لا يمكن إخضاعها لمنطق الحروب التقليدية. بمعنى أنها لا تعمل «وَفْقَ منطق الداعم للقوة التكتيكية فحسب، بل وَفْقَ منطق الحرب الاستراتيجية المتكاملة التي تعمل كوسيلة لتحقيق الأهداف الاستراتيجية الكبرى في النظام العالمي المعاصر»[9]. ونقطة انطلاقتهم هي أن الحرب السيبرانية لا تمثِّل امتدادًا للحرب التقليدية، ولكنها صنفٌ آخر جديد يجري في فضاء آخر غير الفضاءات التقليدية للحرب: البرية والبحرية والجوية. إنه فضاء سيبراني يتألَّف من بنية رقمية افتراضية متكاملة. وبناءً على ذلك، اعتبر وليام لين أن الخصائص المميزة للفضاء السيبراني هي التي دفعت وزارة الدفاع الأمريكية إلى التعامل معه كفضاء جديد جنبًا إلى جنب الفضاءات المادية الأخرى[10]. ويذهب أصحاب هذا الرأي إلى أن الضرر والأذى الناجم من الحرب السيبرانية أبعدُ من معناها القريب.

فاستهداف شبكة الكهرباء في منطقة ما بهجوم سيبراني يخرجها من الخدمة قد يؤدي إلى وفاة العديد من الأشخاص الأكثر عرضةً للخطر، مثل أولئك الذين يعيشون على أجهزة التنفس الاصطناعي في غرف العناية المركزة. ويرى أصحاب هذا الرأي أن هذه الوفيات ليست أعراضًا جانبية للهجوم السيبراني، بل هي أهداف مباشرة. فالمهاجمون على دراية كاملة بأن مثل هذا الضرر يمكن وقوعه، وهنا تتأكَّد نيَّة إيقاع الإيذاء بالخصم.

ويجادل ستيفن والت بأن الحرب السيبرانية تتألَّف من أربع قضايا جوهرية: إضعاف القدرات العسكرية للعدو، واختراق الشبكات لإغلاق البنية التحتية المدنية، والأنشطة الإجرامية على شبكة الإنترنت، والتجسُّس الإلكتروني[11]. وهذا يمنح الحرب السيبرانية مرونةً في الانتقال ما بين الأهداف الاستراتيجية من خلال ضرب القدرات العسكرية والاقتصادية للخصم، والأهداف التكتيكية كالتجسُّس وسرقة البيانات. تتبنَّى هذه الورقة الرأي الثالث، وتجادل بأن الهجمات السيبرانية في الحرب الدائرة بين روسيا وأكرانيا كانت شاملةً من حيثُ مزاوجتها بين الوسائل الاستراتيجية من خلال المحاولات التي تمت لاستهداف مراكز السيطرة والتحكُّم والبنية المدنية الحيوية كشبكة الكهرباء، والوسائل التكتيكية من خلال التجسُّس وسرقة البيانات، مثل الهجمات التي استهدفت البريد الإلكتروني لأفراد الجيش الأوكراني. ليس هذا فحسب، بل ذهبت الحرب السيبرانية في سياق الحرب الروسية-الأوكرانية إلى تضمين تكتيكات حرب المعلومات من خلال اللجوء إلى تقنيات حروب الدعاية والتضليل والتأثير بما يشبه الحرب النفسيَّة. وبذلك تقف افتراضات الورقة على النقيض من تلك الآراء التي جادلت بأن الهجمات السيبرانية في الحرب الدائرة بين روسيا وأوكرانيا كانت هامشيةً أو غير ذات جدوى.

ونظرًا لطبيعة الحرب المتقلِّبة، فإن الورقة وضعت إطارًا زمنيًا في رصد الهجمات السيبرانية وتحليلها يبدأ من بداية الحرب في 24 فبراير/شباط حتى منتصف شهر إبريل/نيسان 2021. أي إن التحليل يغطي الشهرين الأوَّلين من عمر الحرب. كما ركَّزت الورقة على الهجمات السيبرانية بحدِّ ذاتها من خلال رصد طبيعتها وأنماطها وأهدافها، واضعةً الفاعل في المرتبة الثانية في دائرة الاهتمام؛ ولذلك قد يبرز أحد الفاعلين (روسيا) أكثر من غيره (أوكرانيا)، وذلك لأغراض التحليل وليس لغرض إبراز فاعلٍ على حساب فاعلٍ آخر، حيث إن كليهما لجأ -بدرجات متفاوتة- إلى استخدام تكتيكات الحرب السيبرانية.

ولتسهيل عملية التحليل، فقد قسمت الورقة إلى محورين: يعالج المحور الأول الهجمات السيبرانية عبر الشبكات الإلكترونية التي أسميتها بالقرصنة الخشنة، وتشمل هجمات من قبيل DDoS التي تصيب المواقع بالعطل وتخرجها من الخدمة، وهجمات التصيُّد Phishing التي تخترق الحسابات الإلكترونية بغرض التجسُّس أو استخدامها للولوج إلى الشبكات، والهجمات الماسحة التي تؤدي إلى إتلاف البيانات ومسحها من الشبكة، وهجمات البُنى التحتية سواء العسكرية منها أو المدنية بغرض إخراجها من الخدمة. ويعالج المحور الثاني القرصنة الناعمة، وهي استخدام الشبكات والمنصات الرقمية في تكتيكات الدعاية والتضليل وعمليات التأثير، وذلك عبر استخدام مجموعة من التكتيكات مثل: المتصيّد Troll، والروبوتات الاجتماعية Bots، والاختراق، والحميمية الإعلامية عبر إضفاء الطابع الشخصي، وفيديوهات التزييف العميق، وإسكات الأصوات المعارضة.

الجزء الثاني: القرصنة الخشنة.. حرب الشبكات السيبرانية

منذ بداية التصعيد الروسي ضد أوكرانيا في أوائل هذا العام، توجَّهت أنظار المراقبين جميعًا نحو الهجمات السيبرانية المحتملة التي يمكن أن تقوم بها روسيا ضد الأهداف المدنية والعسكرية في أوكرانيا. وقد كان هناك اعتقاد شائع بأن روسيا ربما ستستبق هجومها العسكري بهجمات سيبرانية موسَّعة ضد أوكرانيا؛ نظرًا للخبرات التي راكمتها عبر سنواتٍ في هذا المضمار.

وقد كانت أوكرانيا أحد أبرز الأهداف للهجمات السيبرانية في السنوات القليلة الماضية. ومن هذه الهجمات -على سبيل المثال- عمليات التدخل والتلاعب بالانتخابات الرئاسية الأوكرانية لعام 2014[12]، التي أضرَّت بالنظام الانتخابي المركزي، وشوَّهت نزاهة العملية الانتخابية؛ والهجوم الواسع الذي أصاب شبكة الكهرباء الأوكرانية عام 2015، مما أدى إلى انقطاع التيار الكهربائي في عموم البلاد[13]؛ وهجمات NotPetya التي عُدَّت واحدةً من أكثر الهجمات السيبرانية الضارة تكلفةً، حيث أصابت عام 2017 الشبكات الخدمية التابعة للقطاعات المصرفية والحكومية الأوكرانية وعطَّلت الوصول إليها، وتسرَّبت بعد ذلك لتصيب بعض الشبكات في كلٍّ من إيطاليا وبولندا وروسيا والمملكة المتحدة والولايات المتحدة وأستراليا[14]. وقد قُدِّرت تكلفة هذه الهجمات حينها بعشرة مليارات دولار. وبالمجمل، فقد أكَّدت وحدة الاستخبارات الأمنية المعروفة بـ SBU التابعة لوكالة المخابرات الأوكرانية أنها حيدت أكثر من 2200 هجوم سيبراني على أوكرانيا العام الماضي وحده[15].

لم تعترف روسيا على الصعيد الرسمي بارتكاب أيٍّ من هذه الهجمات، وهي بذلك تؤكِّد على واحدة من أبرز خصائص حروب الشبكات السيبرانية، وهي غياب الإسناد أو الاعتراف من جانب، والمجهولية من جانب آخر. وهي بذلك تعمل على جعل الانتقام من الطرف الآخر أكثر صعوبةً، فالرد والانتقام يحتاجان إلى معرفة الفاعل «على وجه التحديد»[16].

أما في الحرب الحالية التي بدأتها روسيا على أوكرانيا في 24 فبراير/شباط 2022، فقد لجأت روسيا إلى تفعيل الجبهة السيبرانية جنبًا إلى جنب الجبهة الميدانية للحرب، وَفْقَ مصادر رسمية أوكرانية وغربية، وذلك من خلال شنِّ مجموعة من الهجمات السيبرانية التي أصابت الشبكات الإلكترونية الأوكرانية، سواء الرسمية منها أو المدنية.

وقد جاءت هذه الهجمات واسعة ومركّزة، وهو ما ينفي فرضية تقاعس روسيا عن استخدام الاستراتيجية السيبرانية في حربها الدائرة مع أوكرانيا. أما تقييم نتائج هذه الهجمات فهو أمر آخر، حيث يرى العديد من المراقبين أن هذه الهجمات لم تُسفِر عن نتائج ملموسة من شأنها أن تُسهِم إمَّا في دعم العمليات العسكرية الروسية على الأرض، أو في إخراج الشبكات الإلكترونية الأوكرانية من الخدمة، ومن ثَمَّ إرباك الحكومة الأوكرانية وحرمانها من حرية التصرف والقيام بهجمات مضادة[17].

وقد يعود السبب في عدم فاعلية الهجمات الروسية على أوكرانيا التي شُنَّت في هذه الفترة التي يغطيها التقرير إلى عدَّة أسباب أبرزها:

أولًا: عدم رغبة روسيا في القيام بهجمات سيبرانية فتَّاكة تُحدث ضررًا كبيرًا بالشبكات الأوكرانية على أساس حسابات مُسبَقة لدى القيادة الروسية حول سهولة احتلال العاصمة كييف، ومن ثَمَّ تنصيب

حكومة موالية لموسكو ستكون بحاجة لهذه الشبكات للتحكُّم والسيطرة على البلاد بعد إسقاط حكومة الرئيس الأوكراني فولوديمير زيلينسكي.

ثانيًا: عدم رغبة روسيا في توسيع دائرة الهجمات السيبرانية، خشيةً من حدوث هجمات مضادة من طرف حلف الناتو على الشبكات الروسية، خصوصًا تلك المتعلِّقة بالسيطرة والتحكُّم، والتي تُعَدُّ حيويةً في المجهود الحربي. وقد صرَّح مسؤول في حلف الناتو نهاية شهر فبراير/شباط، أي في الأيام الأولى للحرب، أن هجومًا سيبرانيًا على دولة عضو في حلف شمال الأطلسي قد «يؤدي إلى تفعيل المادة 5»[18]، أي بند الدفاع الجماعي، وذلك وسط مخاوف من قيادة الحلف من انتشار الفوضى في الفضاء الإلكتروني حول الغزو الروسي لأوكرانيا إلى مناطق أخرى تابعة للحلف.

ثالثًا: قد تكون أوكرانيا نجحت إلى حدٍّ كبيرٍ في تعزيز دفاعاتها السيبرانية، وهو ما انعكس إيجابًا على استراتيجية الردع السيبرانية، الأمر الذي حرم الهجمات الروسية من إمعان الضرر في شبكاتها الإلكترونية. وسوف تحظى استراتيجية الردع السيبرانية لأوكرانيا بمزيدٍ من تسليط الضوء لاحقًا.

أنواع الهجمات السيبرانية وطبيعتها

إن المتتبع للهجمات السيبرانية على أوكرانيا التي يُظَن على نطاق واسع أنها روسية المنشأ، يجد أنها تحمل بصماتٍ لهجمات سابقة من حيثُ الأسلوب والتكتيك. فقد حدثت عملياتٌ من نوع هجمات حجب الخدمة الموزعة Distributed Denial of Service (التي يشار إليها اختصارًا بـ DDoS) لتعطيل المواقع الإلكترونية الحساسة في أوكرانيا، وهجمات ضد البنية الحيوية المدنية، وأخرى ضد المواقع الإلكترونية العسكرية. وكان الهدف من هذه الهجمات هو تشتيت قدرات الخصم، والتجسُّس وسرقة البيانات، وضرب مراكز السيطرة والتحكُّم، وإحداث حالة من الذعر والفوضى بين المدنيين.

وقد صرَّح وزير التحول الرقمي الأوكراني، ميخايلو فيدوروف، أن بلاده قد تعرَّضت في الأيام الأولى من الحرب «لواحد من أكبر الهجمات السيبرانية في تاريخها، يحمل بصمات أجهزة مخابرات أجنبية»[19]. واستهدفت الهجمات مواقع وزارة الدفاع والجيش الأوكرانيَّين، ومواقع أكبر بنكَين في البلاد. وقد استخدم المهاجمون أسلوب DDoS في الهجوم، وذلك عبر إغراق خوادم هذه المواقع بكمٍّ هائلٍ من الحركات والإشارات، الأمر الذي أخرجها من الخدمة تمامًا. وقد أكَّد المسؤولون الأوكرانيون أن هذا الهجوم قد أُعِدَّ بشكل مسبق، وكلَّف على الأرجح ملايين من الدولارات، الأمر الذي يفوق بشكلٍ كبيرٍ قدرات القراصنة غير المحترفين، وهو ما يرجِّح رواية أن يكون وراء الهجوم جهات حكومية. من جانبها نفت روسيا على لسان الناطق باسم الكرملين ضلوع بلاده في أي هجمات DDoS على المواقع الأوكرانية، معبرًا عن دهشته من استمرار «أوكرانيا في إلقاء اللَّوم على روسيا في كل شيء»[20]. مجددًا، يدلُّ هذا الجدال على أنه طالما أن البرمجيات الخبيثة لا تحمل شارات عسكرية، فلا يمكن إسناد فعل القرصنة إلى فاعلٍ على وجه التحديد ما لم يعترف هذا الفاعل بقيامه بالهجوم.

وقد أدت هذه الهجمات إلى حرمان المواطنين الأوكرانيين من الوصول إلى حساباتهم لبعض الوقت؛ هذا فضلًا عن استخدام بطاقاتهم الائتمانية، بالرغم من تأكيد البنوك المستهدفة أن ودائع العملاء المالية لم تُمَسّ بأذى. وقد رجَّح المسؤولون الأوكرانيون أن يكون الهدف من هذا الهجوم هو «زعزعة الاستقرار،

وبثّ حالة من الرعب والفوضى»[21] بين الأوكرانيين. وقد دام تأثير هذا الهجوم لمدة 24 ساعة، حيث استطاع مسؤولو الأمن السيبراني الأوكرانيون الحدَّ بشكل كبير من مستوى حركة المرور الضارة، وَفْقَ تأكيدات أدلى بها فيكتور زورا، أحد مسؤولي مركز الاتصالات الاستراتيجية وأمن المعلومات، وهي وكالة حكومية أوكرانية أُنشئت لمواجهة التضليل الروسي[22]. وأكَّد فيكتور أن أحد أهداف الهجوم هو معرفة نقاط القوة والضعف في الشبكات الأوكرانية[23]. وهو ما يؤشر على أن الجهات المهاجمة ربما تبحث عن توسيع نقاط عملياتها لاحقًا من خلال البحث عن نقاط الضعف في الشبكات الأوكرانية وسرقة البيانات. فالهجمات السيبرانية لا تعمل وَفْقَ مبدأ إيقاع الضرر، بل أيضًا لأغراض التجسُّس والبحث عن نقاط الضعف من خلال زرع برمجياتٍ خاملةٍ في شبكات الخصم يتم تفعيلها عند الحاجة.

وما يدعم رواية أن الهجوم مصدره روسيا هو تأكيد رئيس قسم الأمن السيبراني بوكالة الاستخبارات الأوكرانية، إيليا فيتيوك، أنه يحمل أوجه تشابه مع هجوم حدث في وقت سابق، وتحديدًا في منتصف شهر كانون الثاني/يناير 2022، حيث عطَّل القراصنة عشرات المواقع التابعة للحكومة الأوكرانية، بما في ذلك وزارة الخارجية الأوكرانية، عبر هجوم يُعرف بـ WhisperGate[24]. حينذاك، نَشَر القراصنة رسالةً تحذيريةً على موقع وزارة الخارجية الأوكرانية مفادها: «أيها الأوكرانيون! لقد تمَّ تحميل جميع بياناتكم الشخصية على الإنترنت. يتم إتلاف البيانات الموجودة على حواسيبكم كافَّة. أصبحت جميع المعلومات المتعلِّقة بكم علنيَّة. خافوا! وتوقَّعوا الأسوأ»[25].

ومن اللافت للانتباه في هذا الصدد أن التصدي لهذه الهجمات لم يقتصر على السلطات الأوكرانية. فعلى بُعْد عشرات الآلاف من الأميال كان مركز استخبارات التهديدات التابع لشركة ميكروسوفت Microsoft's Threat Intelligence Center على موعدٍ مع رصد إحدى البرمجيات الضارة التي لم يسبق لها مثيل، وتنتمي لعائلة البرمجيات الماسحة، بمعنى أنها تقوم بإتلاف بيانات تلك الأجهزة والشبكات التي تتعرض للهجوم. وقد أطلقت ميكروسوفت على هذه البرمجية الضارة اسم «FoxBlade»، وأبلغت السلطات الأوكرانية فورًا بالمستجدات لديها[26]. وهو الأمر الذي أسهم إسهامًا كبيرًا في الحدِّ من تأثير الهجوم. ومن أجل احتواء أضراره الجانبية، فقد تمَّ مشاركة هذه البيانات مع دول الجوار لأوكرانيا، وذلك للتأهب في حال تسرّب الفيروس إلى شبكاتهم الإلكترونية. وقد كان لهذه التحذيرات المتقدمة دورٌ أيضًا في حماية أجهزة الحاسوب الشخصية التي تُستعمل في الإدارة والاستخدامات الفردية.

وفي وقت لاحق، أعلن مسؤولو الأمن السيبراني في أوكرانيا أن هجومًا إلكترونيًا مصدره بيلاروسيا استهدف البريد الإلكتروني الخاص بالأفراد العسكريين التابعين للجيش الأوكراني[27]. وقد أعلن فريق الاستجابة لطوارئ الكمبيوتر الأوكراني المعروف بـ CERT أن القراصنة يستخدمون رسائل بريد إلكتروني لسرقة كلمات المرور لحسابات الجنود الأوكرانيين، ومن ثَمَّ استخدام هذه الحسابات المخترقة لإرسال المزيد من الرسائل الضارة، وهو أسلوب يُعرف عادةً باسم Phishing Attack، والهدف منه عادةً هو سرقة البيانات والتحكُّم بالأجهزة المستهدفة[28]. وقد وُجِّهت أصابع الاتهام لمجموعة تُعرف باسم UNC1151، التي يُعتقد على نطاق واسع أنها وحدة الهجمات السيبرانية التابعة للجيش البيلاروسي. وهناك اتهامات بأن هذه الوحدة ذاتها قد شنَّت هجمات سابقًا على شبكات تابعة لحلف شمال الأطلسي بهدف تقويض الثقة بالمنظمة، وفقًا لبنيامين ريد، وهو مدير شركة الأمن السيبراني الأمريكية المعروفة بـ Mandiant[29]. وبالمجمل، فقد اتُّهِمَت روسيا بشنِّ أكثر من 200 هجوم إلكتروني على أوكرانيا منذ بدء غزوها في

24 فبراير/شباط حتى بداية شهر إبريل/نيسان، وفقًا لتحليل أجرته شركة Microsoft، واستهدفت الوكالات الحكومية والشركات الإعلامية بمحاولات قرصنة أو برامج ضارة مُدمِّرة مُصمَّمة لتعطيل الأنظمة والشبكات الإلكترونية[30].

ومن الجدير بالذكر أن روسيا قد أظهرت تنوعًا في وسائل الهجوم السيبراني تبعًا لظروف الحرب، وبعيدًا عن استخدام أسلوب «الصدمة والرعب» السيبراني، فقد اتبعت موسكو أسلوب كرة الثلج. فبَعيد هجمات البرمجيات الضارة الماسحة Wiper Malware، التفتت إلى استخدام برمجيات أخرى، مثل Industroyer2، موجَّهة لاستهداف الشبكات الحيوية الأوكرانية، مثل شبكات الكهرباء والطاقة.

فقد أعلن فريق الاستجابة لطوارئ الكمبيوتر الأوكراني CERT -بالتعاون مع باحثين من شركة ESET السلوفاكية للأمن السيبراني- عن اعتراض برنامج ضار يُعرف باسم Industroyer2، الغرض منه التسلُّل إلى أنظمة تشغيل شبكات الطاقة الكهربائية في أوكرانيا. ويعتقد المتخصِّصون الأوكرانيون في فريق الاستجابة لطوارئ الكمبيوتر الأوكراني CERT أن الجهة المسؤولة عن هذا الهجوم هي مجموعة تُدعى Sandworm، وترتبط بالأجهزة الأمنية الروسية. وقد نجح الخبراء الأوكرانيون -بمساعدة الشركات الأمنية الخاصة الحليفة- في احتواء الهجوم في الوقت المناسب، الأمر الذي أسهم في منع انقطاع التيار الكهربائي عن عموم البلاد. يُذكَر أن مجموعة Sandworm استخدمت النسخة الأولى من برنامج Industroyer في استهداف البنية الإلكترونية لشبكة الكهرباء الأوكرانية عام 2016[31].

ونظرًا لغياب أي تصريحاتٍ أو بياناتٍ رسمية من السلطات الروسية، فإن هذا التقييم يبقى في نطاق التكهُّن. فقد يكون تكتيك كرة الثلج خطَّة مُعدَّة مسبقًا، ومن ثَمَّ فاحتمالية تصاعد الهجمات تُعَدُّ أمرًا واردًا في المستقبل، وقد يكون تكتيكًا فَرَضته تطورات الحرب، خصوصًا تجاه فاعلية الردع السيبراني لأوكرانيا، الذي استطاع الحدَّ من هذه الهجمات وتحييدها. وهذا يعني أن إعادة تقييم روسيا لاستراتيجيتها السيبرانية واردة، وربما تعود وتلجأ إلى تكتيك «الصدمة والرعب» من خلال هجوم واسع النطاق يشلُّ شبكات البنية التحتية في أوكرانيا. فهذا الاحتمال يبقى واردًا، خصوصًا في ظل تصريحاتٍ من أعلى المستويات الأمريكية، كالرئيس جو بايدن[32]، والأوروبية، كجيريمي فليمنج، مدير وكالة التجسُّس البريطانية[33]، التي حذرت من هجمات سيبرانية واسعة قد تلجأ إليها روسيا في أي وقت لاحق.

الردع السيبراني والنموذج الأوكراني

تجلَّى في حرب الشبكات السيبرانية بين روسيا وأوكرانيا مفهومُ الردع السيبراني. وقد قام الردع الموجَّه ضد روسيا على أربع دعائم رئيسة. **أولًا:** تطوير أوكرانيا لبنيتها السيبرانية الأمنية. **وثانيًا:** التحالف السيبراني لمعسكر الغرب ومن ضمنهم أوكرانيا. **وثالثًا:** التعاون الوثيق بين القطاعَيْن الحكومي والخاص. **وأخيرًا:** الهجوم السيبراني المضاد.

شكَّلت الهجمات السيبرانية على شبكة الكهرباء الأوكرانية عام 2015، التي أدخلت ملايين الأوكرانيين في ظلامٍ دامس، جرسَ الإنذار الذي دقَّ في كل مفاصل الدولة الأوكرانية، الأمر الذي جعلها تسابق الزمن في وضع برامج واستراتيجيات عملية لخلق بنية دفاعية سيبرانية تجنِّب البلاد الوقوع

فريسةً سهلةً للهجمات السيبرانية الروسية، خصوصًا تلك التي قد تصيب بنيتها العسكرية والمدنية الحيوية. كانت البداية -وَفْقَ نائب وزير التحول الرقمي الأوكراني أليكس بورنياكوف- عبر تحرير قطاع الاتصالات الأوكراني من الهيمنة الروسية. فقد كانت روسيا إمَّا تملك كل الحصص في شركات الاتصالات الأوكرانية، أو تستحوذ على أغلبها قبل هذا التاريخ، من قبيل شركة Kyivstar[34].

جبنًا إلى جنب، بدأت أوكرانيا في إنشاء العديد من الوكالات السيبرانية المتخصِّصة، التي بدأت بدورها في نسج مجموعة من التحالفات مع نظيراتها في الدول الأوروبية والولايات المتحدة، وهو الأمر الذي زوَّد الجهات الأوكرانية بالعديد من الخبرات، فضلًا عن سهولة وسرعة التواصل في التعاطي مع التهديدات المباشرة. من هذه الوكالات كان فريق الاستجابة لطوارئ الكمبيوتر الأوكراني المعروف بـ CERT، الذي أسهمت شراكته مع الكيانات الدولية مثل ميكروسوفت في رصد فايروس Foxblade وإبطال مفعوله، وإدارة الأمن السيبراني بوكالة الاستخبارات الأوكرانية. ولكن الأهم هو إنشاء وزارة خاصة عام 2019، تُعنى بقضايا الإنترنت والحماية الرقمية، سُميت وزارة التحول الرقمي، التي يرأسها الوزير ميخايلو فيدوروف.

كان هدف الوزارة الرئيس هو تغطية جميع الأراضي الأوكرانية بإنترنت عريض النطاق وعالي السرعة، هذا فضلًا عن الاستثمار في رأس المال البشري من أجل خلق جيلٍ واعٍ ومتمكِّن رقميًّا. فخلال عام واحد (2021)، على سبيل المثال، تعاونت الحكومة الأوكرانية مع الوكالة الأمريكية للتنمية الدولية في برنامجٍ قام خلاله مدربون من جامعة فلوريدا الدولية وجامعة بوردو بتدريب أكثر من 125 من أعضاء هيئة التدريس في مجال الأمن السيبراني بالجامعة الأوكرانية، وأكثر من 700 طالب في مجال الأمن السيبراني[35]. وقد انعكس هذا الاستثمار في المعرفة السيبرانية على الاستراتيجيات والتكتيكات الوقائية التي اتخذتها الحكومة الأوكرانية للتخفيف من حدَّة الهجمات السيبرانية التي تتعرض لها، والحفاظ على بنيتها الرقمية فعالةً وأكثر مرونةً.

ومن هذه التكتيكات الوقائية قيامُ الجهات الأوكرانية المختصَّة بنقل المعدات الإلكترونية والنسخ الاحتياطية من قواعد البيانات إلى مناطق أكثر أمانًا في الأراضي الأوكرانية، بحيث لا يمكن للقوات الروسية الوصول إليها؛ وإنشاء نظام متعدِّد الطبقات للدفاع السيبراني للبنية التحتية الرقمية للدولة، وإنشاء خطٍّ ساخنٍ لخدمة الأمن في أوكرانيا، لتسهيل عمليات الاستجابة السريعة للتهديدات الإلكترونية على أنظمة تكنولوجيا المعلومات الخاصَّة بالبنية التحتية الحيوية؛ وأخيرًا، توقيع اتفاقية بين دائرة الأرشيف الحكومية في أوكرانيا والأرشيف الوطني للمملكة المتحدة بشأن النقل المؤقت لقاعدة البيانات السحابية والنسخ الاحتياطية للمواد الرقمية لمؤسسات الأرشفة الحكومية الأوكرانية في حالة فقدانها المحتمل جرَّاء هجمات إلكترونية عبر أسلوب الفيروسات الماسحة Wiper Malware[36].

وبالمحصلة، تدلُّنا التجربة الأوكرانية على أن الدفاع وحتى الردع في عصر المعلومات لا يقتصران على إنشاء أقوى الأنظمة، وإنما القدرة والمرونة على الاندماج في أنظمة أخرى. إن الاندماج ما بين الأنظمة هو ما يخلق شبكةً معقَّدةً يصعب اختراقها أو تعطيلها. وللتدليل على اندماج الأنظمة، فقد تمَّ نشر فريق الاستجابة السيبرانية السريع التابع للاتحاد الأوروبي، وترأسه ليتوانيا، للمساعدة في تعزيز الدفاعات الأوكرانية ضد الهجمات الإلكترونية[37]، كما وقَّع حلف شمال الأطلسي قبيل الغزو الروسي

اتفاقيةَ تعاون مشترك مع أوكرانيا تهدف إلى تعزيز قدراتها السيبرانية[38]. في حين أطلقت وكالة الأمن السيبراني الوطنية في رومانيا وشركة الأمن السيبرانية Bitdefender شراكةً بين القطاعَيْن العام والخاص لتقديم الدعم الفني والاستخباراتي المجاني للحكومة والشركات الخاصة في أوكرانيا[39].
لقد كان للتعاون والاندماج بين القطاعَيْن الخاص والعام أثرٌ واضحٌ في تعزيز المرونة السيبرانية. فمركز استخبارات التهديدات التابع لشركة ميكروسوفت كان على أهبة الاستعداد وعلى تواصلٍ دائمٍ مع المسؤولين في البيت الأبيض والمسؤولين الأوكرانيين، وأسهم في رصد فيروس Foxblade، وقبل ذلك فيروس WhisperGate. ومن جانبها، أسهمت شركة الأمن السيبراني ESET، ومقرها سلوفاكيا، في الكشف عن الشيفرة الضارة لفيروس HermeticWiper في الأيام الأولى للغزو الروسي[40]. أما شركة إيلون ماسك ومن خلال خدمة الإنترنت الفضائي Starlink، فقد استطاعت الإبقاء على أوكرانيا متصلةً بشبكة الإنترنت غالبية الوقت[41].

ولأن خير وسيلة للدفاع هو الهجوم، فإن السلطات الأوكرانية وبعض الشركات الخاصة لجأت إلى تكتيك تجنيد متطوعين من الهاكرز للمساعدة في شنِّ هجمات سيبرانية مضادة على الأهداف الروسية. لقد كانت هذه الفكرة نواةً لما سيُعرَف لاحقًا باسم جيش أوكرانيا السيبراني Ukrainian IT Army. وحسب نائب وزير التحول الرقمي الأوكراني، فإن إنشاء هذا الجيش في السياق الرقمي في أوكرانيا كان ممكنًا لعدَّة عوامل، أهمها: **أولًا**: البنية الرقمية الأوكرانية التي أبانت عن تطورات ملحوظة في الآونة الأخيرة من خلال الأنظمة الإلكترونية ورأس المال البشري المدرب. **وثانيًا**: عدالة القضية الأوكرانية، حيث عبَّر الآلف من المبرمجين والهاكرز والمتخصِّصين عن رغبتهم في التطوع لتقديم المساعدة لأوكرانيا في حربها مع روسيا[42].

كانت المبادرة بالمشاركة -حسب نائب الوزير- من قِبَل المتطوعين في المقام الأول. فقد كان العديد من طلبات المساعدة تصل إلى موقع وزارة التحول الرقمي الأوكرانية، وبسبب الانشغالات الكثيرة الملقاة عليها والوضع الأمني الصعب، وهو ما يُصعب من عملية متابعة هذه الطلبات كل على حدة، فقد اقترح وزير التحول الرقمي الأوكراني إنشاء قناة خاصَّة على تطبيق تلغرام لإدارة مجموعة المتطوعين ووضع الأهداف لمشاركتهم وتوجيهها[43]. وعلى إثر هذا المقترح أُنشئت المجموعة. ومع بداية شهر مارس/آذار 2022، ضمَّت المجموعة زهاء الـ 300 ألف عضو من أنحاء العالم كافَّة تتراوح أعمارهم ما دون الثلاثين. ووفق نائب وزير التحول الرقمي الأوكراني، فإن السلطات الأوكرانية تقوم فقط بالإسهام بتزويد المجموعة ببنكٍ من الأهداف الروسية لاستهدافها، مشددًا على خلو المجموعة من أي صيغة من التسلسل القيادي أو الإدارة الهرمية[44]. فالمجموعة تتبع الأسلوب الأفقي والمبادرات الذاتية، وتتكوَّن غالبًا من هاكرز أفرادًا ومجموعات. ويُسهم هذا الشكل من التنظيم في جعل المجموعة أكثر مرونةً وعصيةً على الاختراق، ففي ظل غياب قيادة واضحة، وفي ظل هذا الكم الكبير من الهاكرز المحترفين والهواة، يصبح من الصعب جدًّا على روسيا أو الجهات المرتبطة بها اختراق المجموعة، حسب ما أدلى به نائب الوزير[45].

وعن آلية العمل، يوجد داخل صفحة التلغرام الرئيسة للمجموعة باللغة الإنجليزية مستندٌ تمهيديٌّ مكوَّن من 14 صفحة يقدِّم تفاصيلَ حول كيفية مشاركة الأشخاص، بما في ذلك البرامج التي يجب تحميلها لإخفاء أماكن وجودهم وهويتهم[46]. وكل يوم، يتم إدراج أهداف جديدة، بما في ذلك المواقع الإلكترونية وشركات الاتصالات والبنوك والصرافات الآلية ATMs الروسية.

توزعت مهام الجيش الأوكراني السيبراني من المتطوعين على عمليات هجومية، كضرب أهداف حساسة عالية التأثير، مثل البنية التحتية والأنظمة اللوجستية المهمة للجيش الروسي، فضلًا عن مهام التجسُّس؛ وأخرى دفاعية تتمثَّل في المساعدة في حماية البنية التحتية الحيوية لأوكرانيا، فضلًا عن حملات الدعاية والتضليل. ومع بداية شهر آذار/مارس 2022، استطاع المتطوعون الهاكرز الوصول إلى أكثر من 50 مليون إنسان في روسيا جزئيًّا من خلال 100 ألف مكالمة هاتفية باستخدام تسجيل آلي، وَفْقَ تصريحات أدلى بها نائب وزير التحول الرقمي الأوكراني لوكالة رويترز[47].

وكان من بين أولى الأهداف التي أدرجتها مجموعة الهاكرز المتطوعين على صفحة التيلغرام مواقع 31 شركة ومؤسسة حكومية تابعة لروسيا، منها عملاق الطاقة غازبروم[48]، وثاني أكبر منتج للنفط الروسي Lukoil، وثلاثة بنوك، وعدد من المواقع الحكومية، منها موقع الكرملين Kremlin.ru، والموقع الرسمي لمكتب الرئيس الروسي فلاديمير بوتين، الذي خرج من الخدمة يوم السبت 26 فبراير/شباط، بسبب ما يرجَّح أنه هجوم رفض الخدمة DDoS[49]. وشهد الأسبوع الأول من مارس/آذار حزمةً من الهجمات على أهداف روسية، منها أكبر بورصة في البلاد، والبنك المركزي، ووزارة الخارجية الروسية[50].

وفي السابع من إبريل/نيسان، أعلن جيش أوكرانيا السيبراني أنه اخترق منصة Rossgram -وهي النسخة الروسية المشابهة لمنصة إنستغرام الأمريكية، التي أطلقتها موسكو بعد أن حظر الكرملين منصات التواصل الاجتماعي الأمريكية في روسيا- وتسريب بيانات المستخدمين فيها[51]. وفي موضعٍ آخر، أعرب المتطوعون من الهاكرز على مجموعة التلغرام عن رغبتهم في الذهاب أبعد من ذلك من خلال استهداف الشركات الخاصة وتعطيل الخدمات الحكومية. ففي تعليقٍ على المجموعة، عبَّر أحدهم بالقول: «كانت هناك طوابير طويلة أمام أجهزة الصراف الآلي في روسيا مؤخرًا. دعونا نجعلها أطول من خلال إغلاق الخدمات المصرفية عبر الإنترنت»[52].

ومن الجدير بالذكر أن جهود تجنيد المتطوعين الهاكرز لم تقتصر على المبادرات الحكومية، بل تعدَّت إلى القطاع الخاص، وهو الاتجاه الذي يعزِّز فكرة ضرورة التعاون والاندماج بين القطاعات العامة والخاصة في استراتيجيات الردع السيبرانية. في هذا السياق، أكَّد إيجور أوشيف، وهو المؤسس المشارك لشركة الأمن السيبراني الأوكرانية المسمَّاة Cyber Unit Technologies، أنه تلقى كمًّا كبيرًا من الرسائل بعد نشره على وسائل التواصل الاجتماعي دعوةً للمبرمجين حول العالم للمشاركة في اكتشاف أي عيوبٍ وثغراتٍ في الأنظمة الإلكترونية الروسية مقابل مكافأة مالية وصلت الـ 100 ألف دولار[53]. وأكَّد أن هناك أكثر من 1000 هاكرز متطوع يشاركون جهود شركته ويعملون في تعاونٍ وثيقٍ مع الحكومة الأوكرانية. وعلى المنوال نفسِه، نسجت شركة Hacken، وهي شركة للأمن السيبراني كانت العاصمة كييف مقرها سابقًا، وأعلنت عن برنامج مكافأة مالية لأولئك الهاكرز المتطوعين الذين يتمكَّنون من تحديد نقاط الضعف في الشبكات الأوكرانية لسدِّها، وفي الشبكات الروسية لاختراقها. وقد سجَّلت الشركة ما يقرب من 10 آلاف هاكرز متطوع من 150 دولة حول العالم[54].

لم يقتصر الأمر على الأوكرانيين، فالتوجُّه نحو تجنيد أو استقطاب المتطوعين أصبح تكتيكًا يصعب على أطراف مثل روسيا أن تفوته. فقد قامت جهات داخل روسيا -قد تكون تابعةً للكرملين- باتباع خطى فرقائهم الأوكرانيين في إنشاء جيش سيبراني من المتطوعين أسموه الجبهة السيبرانية Z

(بالإنجليزية Cyber Front Z) وأطلقوه في 11 مارس/آذار 2022، معتمدين أيضًا على تطبيق تلغرام أداةً في التواصل والتنظيم، ووصل عدد المتطوعين فيه إلى ما يقرب من 65 ألف شخص[55].

ولكن من الملاحظ أن عمليات جيش Z السيبراني التابع لروسيا قد أولت حملات التضليل ونشر الدعاية الروسية جُلَّ اهتمامها على حساب شنّ هجمات سيبرانية على الشبكات الأوكرانية. وبما أننا سوف نتحدَّث عن حروب الدعاية بين الجانبَيْن بالتفصيل لاحقًا، فإنه يكفي الإشارة هنا إلى أن السبب وراء تجنُّب جيش Z الروسي الهجمات السيبرانية والاكتفاء بحملات التضليل ربما يعود إلى طبيعة النموذج الروسي في حروب الشبكات الإلكترونية في تفضيل البناء المركزي الخاضع لتراتبية القيادة وسلاسل الأوامر والتوجيه على البناء الشبكي اللامركزي، وهو النموذج الذي اعتمدته أوكرانيا في التعاطي مع ظاهرة المتطوعين السيبرانيين.

إن ظاهرة التطوع السيبرانية امتدَّت لتشمل أطرافًا ثالثة، هي بالأساس جماعات سيبرانية شبه منظَّمة، مثل مجموعة Anonymous collective، التي أعلنت الحرب السيبرانية على روسيا عبر حسابها على تويتر يوم 25 فبراير/شباط 2022[56]. وقد نشطت المجموعة سابقًا في العديد من حملات الاختراق السيبرانية ضد أهداف من قبيل وكالة المخابرات المركزية الأمريكية CIA، وتنظيم داعش الإرهابي. وبالرغم من أن السلطات الأمريكية قد نجحت إلى حدٍّ كبيرٍ في التضييق عليهم، فإنهم عادوا للنشاط بشكلٍ ملحوظٍ بُعيد حادثة مقتل المواطن الأمريكي من أصول إفريقية جورج فلويد على يد رجل شرطة أبيض.

ومنذ الأيام الأولى لإعلانها الحرب على روسيا تبنَّت المجموعة العديد من الهجمات السيبرانية عبر أسلوب هجمات رفض الخدمة DDoS على بعض المواقع الروسية، مثل موقع روسيا اليوم RT، ونشرت عليه أغاني وصورًا مؤيدة لأوكرانيا وضد ما أسمته «الغزو الروسي». واخترقت أيضًا الموقع الرسمي للكرملين ووزارة الدفاع. وفي وقت لاحق، اخترقت المجموعة خدمات البث الروسي Wink و Ivi (وهي منصة شبيهة بشبكة نيتفليكس) وقناة موسكو 24، حيث بثَّت لقطات من الحرب في أوكرانيا أثناء نشرات الأخبار الرسمية، كان في آخرها رسالة تدَّعي أن «عامَّة الروس يعارضون الحرب»، وتدعو إلى إنهاء الغزو الروسي العنيف لأوكرانيا[57]. وقد عزت قناة «روسيا اليوم» بشكل علني مشاكلها الإلكترونية إلى مجموعة Anonymous، وادعت أن الهجمات جاءت من الولايات المتحدة بعد أن نشرت المجموعة إعلان الحرب ضد روسيا على حسابها الخاص على تويتر، وقال المتحدث باسم القناة: «بعد بيان Anonymous، تعرض موقع RT لهجمات DDoS ضخمة من حوالي 100 مليون جهاز إلكتروني، معظمها يقع في الولايات المتحدة»[58].

مثله مثل باقي العمليات التي تجري في الجبهة السيبرانية، فإن إسهام المتطوعين السيبرانيين وتأثيرهم الفعلي والمدى الذي وصلوا إليه يبقى صعبًا تجاه عمليات التحقُّق والتثبُّت. ففي العمليات السيبرانية يحاول كلُّ طرف التحفُّظ على نشر التفاصيل، وفي حال اضطر لفعل لذلك فهو يجري على نطاقٍ محدودٍ من باب ممارسة الحرب النفسية للتأثير في تصورات الخصم وقناعاته وثقته بنفسه. ولذلك يمكن وضع عمليات المتطوعين السيبرانيين في إطار العمليات النفسية والتلاعب بالعقول. فبناءً على ما تمَّ تسريبه من عمليات سيبرانية حتى الآن ضد الشبكات الإلكترونية في كلٍّ من روسيا وأوكرانيا، يظهر

مدى محدودية هذا النوع من العمليات، وهي محدودية يصعب معها التنبؤ بأن يكون لهذه العمليات تأثير جوهريٌّ في مجريات الحرب على الأرض.

لقد أصبح من المعلوم بالضرورة أن الهجمات السيبرانية المدمِّرة تحتاج إلى تضافر إمكانات مادية وتقنية ولوجستية كبيرة جدًّا ومُكلِّفة في الوقت ذاته، يقوم بها هاكرز متخصِّصون ينتمون إلى جهات حكومية؛ ولذلك من الصعب تخيُّل أن تقوم مجموعات المتطوعين السيبرانيين بشنِّ هجمات مُدمِّرة كتلك التي قامت بها روسيا على أكثر من 50 شركة ووكالة فيديرالية أمريكية عام 2021 فيما سُمي بهجمات SolarWind، أو هجمات Stuxnet التي قامت بها كلٌّ من الولايات المتحدة وإسرائيل عام 2010 ضد المنشآت النووية الإيرانية، التي كلفت عشرات الملايين من الدولارات.

إن ظاهرة التطوع السيبرانية سيكون له انعكاسان مباشران. **أولًا**: لا يخضع مجمّع القراصنة المتطوعين إلى أي آليات تتعلَّق بالسيطرة وتراتبية القيادة؛ ولذلك فإن الهجمات التي يقومون بها قد تعرّضهم أو تعرّض الدول التي يوجدون بها وينطلقون منها في شن هذه الهجمات لحسابات غير دقيقة لدى الطرف الآخر، الأمر الذي من شأنه أن يقود إلى ردود فعلٍ قد تعمل على تصعيد مستوى الصراع، خصوصًا في ظل غياب القدرة على التحقُّق من الهوية أو إسناد الفعل للجهات المهاجمة. ولقد لحظنا ذلك عندما قامت بعض الجهات الروسية بتحميل الولايات المتحدة المسؤولية عن بعض الهجمات الإلكترونية على قاعدة أن هذه الهجمات انطلقت من أراضيها. **ثانيًا**: قد تحفز هذه الظاهرة في ظل غياب الحدود الواضحة للفعل القراصنةَ ذوي القبعات السوداء لتنفيذ العمليات السيبرانية التي يظهر منها دعمهم لفريق ضد فريقٍ آخر في الحرب، ولكنها في باطنها إجرامية، الغرض منها الحصول على منافع مادية، مثل عمليات الفدية التي تكثر في مثل هذه الحالات.

الجزء الثالث: القرصنة الناعمة.. الدعاية والتضليل والتلاعب

في موازاة العمليات السيبرانية الخشنة التي استهدفت الشبكات الإلكترونية عبر عمليات التعطيل والاختراق وضرب البيانات، جرت عملياتٌ من نوعٍ آخر أسميتها القرصنة الناعمة، وهي التي تتعلَّق بحروب الدعاية والتأثير في معنويات الخصم عبر هجمات التضليل والتلاعب وبثِّ الأخبار الكاذبة Fake news. والهدف من هذه العمليات هو محاولة تحطيم «مراكز الثقل» لدى الخصم[59]. ففي عصر الإنترنت، لا يكفي السيطرة والتقدُّم في العمليات العسكرية الأرضية فحسب، بل يجب أن تتوازى معها عمليات أخرى تتعلَّق بكسب سرديَّة والتأثير في تصورات الناس، والحفاظ على الحاضنة الداخلية أو ضربها. على الجانب الروسي، كان هناك هدفان رئيسان لعمليات القرصنة الناعمة؛ **أولًا**: كسب رواية الحرب على الصعيد الداخلي من خلال تعزيز حالة التأييد الشعبي لما أسمتها بـ«العمليات العسكرية الخاصة» في أوكرانيا، وإسكات الأصوات المعارضة أو طمسها. **وثانيًا**: ضرب الروح المعنوية للخصم من خلال تصويره على أنه ضعيف ومهزوم ويبحث عن الاستسلام أو تشويهه من خلال نعته بالنازية الجديدة والتطرف. أما على الصعيد الأوكراني، فكان هدف القرصنة الناعمة السعي -**أولًا**- إلى ضرب الرواية الروسية عن الحرب وتصويرها بعيدًا عن مجرَّد كونها عمليات عسكرية خاصة، بل على أنها حرب طاحنة تستهدف المدنيين والأبرياء العزل. **وثانيًا**: رفع الروح المعنوية للشعب الأوكراني من خلال التركيز على بسالة القوات الأوكرانية، مثل الطيار الذي ذاع صيتُه وسُمي بـ«شبح كييف»، وقرب القيادة الأوكرانية من الشعب، الذي جسَّده الرئيس الأوكراني من خلال فيديوهات البث المباشر التي كان يخرج بها على

شعبه بين الفينة والأخرى من شوارع العاصمة الأوكرانية كيف عبر تطبيق Tik Tok وإنستغرام. وقد رصدت الورقة ستة تكتيكات رئيسة في عمليات القرصنة الناعمة: عمليات المتصيد الـ Troll، والروبوتات السياسية Political bots، والحسابات المخترقة، والتزييف العميق Deep-fake، وإضفاء الطابع الحميمي، وإسكات الأصوات المعارضة.

أولًا: عمليات المتصيد الـ Troll

يُعَدُّ اللجوء إلى تكتيك الـ Trolls واحدًا من الأساليب التقليدية في حروب الدعاية الإلكترونية. ويُعرّف الـ Trolls أو المتصيد (بصيغة اسم الفاعل) في لغة الإنترنت العامية، وَفْقَ وقع Wikipidia، بأنه «الشخص الذي ينشر رسائلَ تحريضية أو غير صادقة أو استطرادية تُعَدُّ خارجة أو بعيدة عن الموضوع في مجتمع ما عبر الإنترنت، ويقصد منها استفزاز القرَّاء لإظهار ردود أفعال عاطفية أو التلاعب بتصورات الآخرين»[60].

لقد وظفت العديد من القوى الفاعلة، سواء أكانت حكومة أو غير حكومية، تقنية الـ Trolling في حروب الدعاية (البروباغندا) والتحريض. ومن خلال التعريف السابق، يمكن الحديث عن ثلاثة أهداف لهذه التقنية. **أولًا**: جعل الناس يصدقون أمرًا هو بالأساس كذب. **ثانيًا**: إثارة الشكوك وعدم الثقة في مصادر المعلومات التي يُنظَر إليها عادةً على أنها شرعية. **ثالثًا**: خلق شعور بالإجماع على فكرة هي بالأساس محلُّ جدال من أجل لفت الانتباه أو التشويش.

في الحرب على أوكرانيا، لجأت روسيا إلى استخدام هذه التقنية بشكل لافت. فالجبهة السيبرانية Z هي بالأساس فكرة متطورة عن مزرعة Trolling، ومُحدثة عن نماذج سابقة استخدمتها روسيا، وتتمركز حول وكالة أبحاث الإنترنت Internet Research Agency، وموقعها مدينة سانت بطرسبرغ. فمن خلال مقرها الرئيس في مدينة سانت بطرسبرغ أيضًا، أعلن مؤسس الجبهة Z المقرب من الكرملين، ألكسندر كابيتانوف، أن هذه الجبهة هي «حركة شعبية» ذات خلفيات وطنية تسعى إلى صدِّ الحملات الدعائية ضد روسيا وحملتها العسكرية على أوكرانيا، التي تصفها بـ«العمليات الخاصة»[61].

وقد اتخذت المجموعة من منصة تلغرام موطنًا لتنسيق جهودها. وفي الوقت الذي تحاول فيه الظهور بمظهر الجماعة المتطوعة، فإن تقريرًا نشرته صحيفة Fontanka الروسية يشير إلى أن هذه المجموعة هي ذراع تابعة للكرملين تقوم بوظيفة الـ Trolling من خلال توظيف مجموعة من المدوّنين براتب شهري يصل إلى ما يقرب من 500 دولار أمريكي[62]. ويتم إعطاء المنتسبين حق الوصول إلى حسابات وهميَّة أنشئت سابقًا، ويتم الطلب منهم كتابة تعليقات تصل إلى 200 تعليق خلال فترة عملهم، ويتم بث هذه التعليقات على منشورات تتبع شخصيات ومجموعات مؤثرة، خصوصًا تلك الناطقة باللغة الروسية، وذلك لإعطاء انطباع بأن العملية العسكرية الروسية على أوكرانيا تحظى بإجماع شعبي[63].

ومن خلال تتبُّع مسار هذه العمليات، يمكن تحديد بعض الأنماط التي انتهجتها الجبهة Z.

أولًا: تم إنشاء مجموعة عامَّة ومفتوحة على تطبيق تلغرام تتضمَّن العديد من التعليقات الوطنية المؤيدة للحرب، وهو ما يضمن نشوء انطباع ذي وجهَيْن: أن المشاركين هم مجموعة من الوطنيين

الروس الحريصين على دعم رواية بلادهم، وأن المجموعة تحظى بالأصالة التي تمنحها المصداقية في أفعالها ومنشوراتها. وبالرغم من أن تقرير صحيفة Fontanka، الذي أعدَّته الصحافية الاستقصائية كسينيا كلوشكوفا، التي عملت متخفيةً في المجموعة، يدعم فكرة أن العاملين في الجبهة Z عبارة عن Trolls تمَّ توظيفهم، فهذا لا ينفي أن يكون جزء من المشاركين من الوطنيين حقًّا، الذين تولَّدت لديهم الرغبة في دعم رواية بلادهم عن الحرب، خصوصًا أن المجموعة وصل تعدادها حتى نهاية مارس/آذار إلى ما يقرب من 65 ألف مشارك.

ثانيًا: سعت المجموعة إلى عدم نشر تعليقات مسيئة للغاية، وذلك من أجل تعزيز المصداقية من جانب، وتجنُّب الحظر من قِبَل منصات التواصل الاجتماعي من جانب آخر.

ثالثًا: البحث عن حسابات شرعية لمستخدمين يتمتعون بالشهرة (مثل رئيس الوزراء البريطاني بوريس جونسون، والمستشار الألماني أولاف شولتز، ومنسق السياسة الخارجية في الاتحاد الأوروبي جوزيب بوريل)، أو تعليقات تحظى بالمصداقية والقيام بالرد عليها، وهذا من شأنه أن يزيد من الانتشار؛ نظرًا لكثرة المتابعين لمثل هذه الحسابات، وتحقيق المصداقية والأصالة. فعلى سبيل المثال، في العام الماضي ادعى الكاتب والمخرج السينمائي جون بيلجر أن «الولايات المتحدة هي المسؤول عن الإطاحة بالحكومة المنتخبة في أوكرانيا عام 2014، مما سمح لحلف الناتو بالتمدُّد نحو الحدود الغربية لروسيا»[64]، وهذا بلا شكٍّ يتماشى مع الرواية الروسية بأن ثورة عام 2014 في أوكرانيا ما هي إلَّا مجرَّد انقلاب قادته الولايات المتحدة. وفي موضع آخر، يذهب النائب العمَّالي السابق كريس ويليامسون إلى أبعد من ذلك حينما وصف الحكومة الأوكرانية بأنها «نظام فاسد مدعوم من النازيين الجدد في فترة ما بعد انقلاب 2014»[65]، وهذا أيضًا يتماشى مع رواية الكرملين الذي استخدم وصف «الحكومة الفاشية» أو «الحكومة النازية» في أوكرانيا لتبرير الحرب.

رابعًا: القيام بدسِّ التعليقات السياسية ضمن الحسابات والتعليقات المحايدة التي توجد عادةً في الموضوعات الاجتماعية، كالحسابات المهتمَّة بالحيوانات الأليفة، أو الطبخ أو السفر وما شابهها.
وأخيرًا، كان للمؤثرين الروس على منصات التواصل الاجتماعي دورهم أيضًا في هذا المضمار. فقد أظهرت إحدى الدراسات، التي نشرتها Media Matters for America في 11 مارس/آذار، كيف شارك أكثر من 180 مؤثر روسي على منصة Tik tok في حملة دعائية منسَّقة لتعزيز الدعم عبر الإنترنت للحرب الروسية، حيث شاركوا مئات المنشورات تحت هاشتاغ #RussianLivesMatter[66]. ولم نعتبر هذه النقطة نقطةً خامسةً في التصنيف السابق لسببٍ جوهريٍّ يتعلَّق بصعوبة التحقُّق إذا ما كانت هذه الحملة هي إحدى حملات الـ Trolling الروسية، أم أنها بدافع وتنسيق ذاتي من هؤلاء المؤثرين، فكلا الاحتمالين وارد، وتصعب المفاضلة بينهما من غير التحقُّق بدليل استقصائي.

ثانيًا: الروبوتات السياسية The Political Bots

في القسم السابق تمَّ التركيز على العنصر الاجتماعي من حروب الدعاية عبر إظهار العامل البشري المتمثِّل في كتائب المتصيدين الـ Trolls، التي يتم تجنيدها للقيام بنشر وتضخيم رواية طرفٍ على حساب الطرف الآخر أو تشويه روايته وتكذيبها. ولكي تكون البروباغندا الإلكترونية فعالةً في تحقيق أهدافها، لا بدَّ من تضافر العنصرين معًا، أي التقني مع الاجتماعي. ويلجأ الخصوم إلى هذه التقنية

دائمًا من أجل دعم روايتهم وقمع رواية الخصم أو التشويش عليها. ولا يمكن أن نتصور أيَّ تنافس في هذ الأيام، سواء أكان سلميًا كالعملية الانتخابية أو عنفيًا كالحرب، إلَّا وتكون البروباغندا الإلكترونية أو روبوتات الدعاية جزءًا أصيلًا منه.

وعند الحديث عن العنصر التقني من هذه العملية، تظهر تكنولوجيا الروبوتات أو ما تُعرف بالـ Bots، وهي «برامج آلية مُصمَّمة لتقليد المستخدمين الحقيقيين». وتنقسم هذه الروبوتات إلى قسمَيْن: روبوتات حميدة، وهي التي تقوم بتنفيذ غالبية العمليات على الإنترنت. فمعظم برامج الرد الآلي -على سبيل المثال- تتم من خلال هذه الروبوتات، كما أن غالبية الروابط الداخلية التي تسمح لنا بالتنقل في موقع ويكيبيديا يتمُّ إنشاؤها وصيانتها بواسطة برامج الروبوت هذه[67].

أما النوع الآخر فهو الروبوتات الخبيثة، التي يتم استخدامها لتنفيذ الأعمال المُسيئة من إرسال رسائل ضارة والتشويش وبث الأخبار الكاذبة وافتعال المضايقات. وعند تناول البروباغندا الإلكترونية، فإن هذا النوع من الروبوتات يتصدَّر المناقشات. ويميل بعض الباحثين إلى تسمية هذا النوع بـ«الروبوتات السياسية»، لسهولة التمييز بينها وبين روبوتات المحادثة والروبوتات الاجتماعية التي تتبع النوع الأول الحميد في العموم[68]. وهنا يورد هؤلاء الباحثون تعريفًا أكثر تحديدًا للروبوتات السياسية على أنها «برامج (أو وكلاء إلكترونيون) يتم إنشاؤهم لأداء مهام بسيطة ومتكررة وقائمة على النصوص عادةً، وذلك لقيادة الدعاية عبر الإنترنت وحملات الكراهية، وقد يقوم شخص واحد أو مجموعة صغيرة من الأشخاص -بسهولة إلى حد ما- بإنشاء وتنسيق جيش من الروبوتات السياسية على منصات مثل تويتر ويوتيوب وإنستغرام، وذلك لخلق نوعٍ من الوهم بوجود إجماعٍ على نطاق واسع أو اهتمام بقضية معينة»[69]. وبشكل عام، تُستخدم هذه الروبوتات لتحسين قدرة البشر على إنجاز الأعمال عبر الإنترنت، من حيثُ الحجم والسرعة. إن قدرة هذه الروبوتات على التفاعل مع المستخدمين الحقيقيين يعطيها ميزةً استثنائيةً. فهي قادرة على نشر الرسائل بسرعة، والتفاعل مع محتوى المستخدمين الآخرين، والتأثير في الخوارزميات الشائعة أو معالجتها، كل ذلك يحدث مع خلال إعطائهم انطباعًا بأنهم مستخدمون بشريون[70].

منذ انطلاق الأعمال العسكرية الروسية على أوكرانيا، رصدت منصات التواصل الاجتماعي والخبراء المعنيون بالكشف عن حملات التضليل والأخبار الكاذبة زيادةً كبيرةً في استخدام الروبوتات السياسية لأغراض البروباغندا. وقد صرحت منصة تويتر، وهي الأكثر عرضةً لمثل هذا النوع من الروبوتات نظرًا لتركيبتها التقنية المفتوحة API، بأنها منذ بداية الحرب على أوكرانيا (وحتى نهاية شهر آذار/مارس) قد حيدت أكثر من 75 ألف حساب لمخالفتها سياسة المنصة المتعلِّقة بالتلاعب والبريد العشوائي Spam[71]. وبالرغم من جهود هذه المنصات في مكافحة وتحييد روبوتات التلاعب، فإن العديد من الخبراء، مثل تيم غراهام، يرون أن هذه الجهود ليست كافيةً. فعلى سبيل المثال، صرحت شركة تويتر بأنها حظرت أكثر من مائة حساب كانت تدعم هاشتاغ #IStandWithPutin. يرى غراهام من جانبه أن هذه العدد يُعَدُّ ضئيلًا جدًّا، حيث رصد شبكتَيْن كبيرتَيْن من آلاف حسابات الروبوت المشتبه بها لا تزال تغرد تحت الهاشتاغ ذاته[72].

وقد استخدمت الجهات المحسوبة على روسيا بعض التكتيكات التي من شأنها الالتفات على الإجراءات الاحترازية التي تتخذها هذه المنصات ضد الحسابات المدعومة من روبوتات التلاعب. فعلى سبيل المثال، عكفت شركة تويتر من أجل التحذير من احتمالية التلاعب على إدراج رسائل تنبيه من قبيل:

«ابـق علـى اطـلاع: هـذه التغريـدة مرتبطـة بموقـع إعلامـي تابـع للدولـة فـي روسـيا» مـع التغريـدات التـي تصـدر عـن الحسـابات المحسـوبة علـى مواقـع روسـية. ولكـن هـذا الإجـراء لا ينطبـق علـى الحسـابات الحكوميـة الرسـمية، مثـل حسـابات السـفارات الروسـية التـي نشـطت مؤخـرًا بشـكل ملحـوظ[73].

وفـي دراسـة تتبعـت هـذه الحسـابات فـي الفتـرة الممتـدَّة مـا بيـن 15 مـارس/آذار و15 إبريل/نيسـان، أظهـرت النتائـج أن 9 بالمائـة مـن هـذه الحسـابات عبـارة عـن حسـابات روبـوت، و21 بالمائـة لديهـا احتماليـة عاليـة لتكـون روبوتًـا، وأن 29 بالمائـة فقـط مـن الحسـابات لهـا خصائـص بشـرية كاملـة، و41 بالمائـة لديهـا سـلوكيات غامضـة، ربمـا تُعـزى إلـى إنسـان، ولكـن لا تـزال هنـاك درجـة معيَّنـة مـن عـدم اليقيـن بشـأنها. ومـن الملاحـظ -وَفْـقَ الدراسـة- أن مـا يقـرب مـن 73 بالمائـة مـن هـذه الحسـابات قامـت بالتغريـد لأول مـرة بعـد 24 فبرايـر/شـباط، وهـو اليـوم الـذي بـدأت فيـه الحـرب، وهـذا يعنـي أن هنـاك ترابطًـا بيـن واقعـة الحـرب وبيـن الزيـادة الكبيـرة فـي عـدد هـذه الحسـابات التـي تدعـم الروايـة الروسـية[74].

وبطبيعـة الحـال، إن هـذه الظاهـرة غيـر مقتصـرة علـى منصـة تويتـر فحسـب. فشـركة Alphabet المشـغلة لمنصـة يوتيـوب صرحـت بأنهـا أوقفـت العديـد مـن القنـوات علـى المنصـة، التـي تضـم أقـلَّ مـن90 مشـترك، كجـزء مـن تحقيقاتهـا فـي عمليـات تلاعـب منسَّـقة مرتبطـة بروسـيا[75]. كمـا قامـت الجهـات الأمنيـة الأوكرانيـة فـي منتصـف شـهر مـارس/آذار بإحبـاط شـبكة تقـوم بإرسـال آلاف الرسـائل القصيـرة SMS إلـى الأفـراد العامليـن فـي الدوائـر الرسـمية الأوكرانيـة، أو إجـراء آلاف المكالمـات المسـجَّلة معهـم، تحثُّهـم علـى الاستسـلام والانصيـاع لإدارة روسـيا[76].

ثالثًا: الحسابات المخترقة

يُعَـدُّ اللجـوء إلـى اختـراق الحسـابات وبـثِّ الدعايـة مـن خلالهـا واحـدًا مـن الأسـاليب التقليديـة فـي حـروب البروباغنـدا. وقـد أصبحـت حادثـة اختـراق البريـد الإلكترونـي لمديـر حملـة المرشـحة الرئاسـية هيـلاري كلينتـون عـام 2016 مثـالًا واضحًـا للتدليـل علـى هـذه السياسـة.

عـادةً مـا يتـم اسـتهداف القنـوات الرسـمية الأكثـر مشـاهدة، وحسـابات الشـخصيات العامـة والمشـاهير مـن عمليـات الاختـراق هـذه. وتُعَـدُّ هـذه العمليـات مـن ضمـن القرصنـة الإلكترونيـة، وهـي عمليـات لا تتطلـب تقنيـات أو خبـرات كبيـرة ومعقَّـدة فـي مجـال الاختـراق والتسـلُّل الإلكترونـي. حيـث تهـدف هـذه العمليـات إلـى انتـزاع الثقـة مـن الخصـم عبـر الإيهـام بضعـف دفاعاتـه الإلكترونيـة، وبـثِّ رسـائل سـريعة لشـريحة واسـعة مـن المتابعيـن لتعزيـز الشـائعة، ومـن ثَـمَّ تضخيمهـا عبـر وسـائل أخـرى، كاسـتخدام روبوتـات الداعيـة أو الـ Trolls.

ومـن الأمثلـة علـى ذلـك مـا أقـدم عليـه قراصنـة محسـوبون علـى الجانـب الروسـي حينمـا اخترقـوا شـركة الإذاعـة العامـة الأوكرانيـة Suspilne وبثـوا رسـالة مُضلّلـة مفادهـا أن الرئيـس الأوكرانـي أعلـن اسـتسـلامه، ويدعـو الأوكرانييـن لوقـف القتـال[77]. وفـي السـياق ذاتـه أيضًـا يأتـي الاختـراق الـذي تـمَّ ضـد حسـابات لقـادة سياسـيين وعسـكريين أوكرانييـن رفيعـي المسـتوى ونشـر رسـائل كاذبـة مـن خلالهـا حـول اسـتسـلام أوكرانيـا، وقـد ضمَّـن المتسـللون تلـك الرسـائل مقاطـع فيديـو لجنـود يلوحـون بعلـم أبيـض إشـارة إلـى اسـتسـلامهم. وبعـد التحقُّـق مـن خـلال طـرف ثالـث متخصِّـص، تبيَّـن لاحقًـا أن هـذه المقاطـع لا تعـود لجنـود أوكرانييـن[78].

دخلت على الخط أيضًا مجموعة Ghostwriter، التي يُعتقَد على نطاق واسع أنها ذراع سيبرانية تتبع القوات الأمنية في روسيا البيضاء الحليفة لروسيا، وتعمل على اختراق حسابات منصات التواصل الاجتماعي والبريد الإلكتروني، ومن ثَمَّ استخدامها لبثّ الرسائل التي تريد إيصالها للجمهور. ووفق شركة Meta، فقد حاولت المجموعة التسلُّل إلى حسابات على منصة فيسبوك واستخدامها في نشر مقاطع فيديو تصور القوات الأوكرانية على أنها ضعيفة ومهلهلة. وقد أكَّدت الشركة أنها استطاعت رصد هذا التسلُّل سريعًا، ومن ثَمَّ النجاح في منع المجموعة من بثّ رسائلها المضللة[79].

رابعًا: الحميمية الإعلامية عبر إضفاء الطابع الشخصي

في الحرب لا يكفي الحفاظ على سلامة القيادة أو مراكز السيطرة والتحكُّم للانتصار وتحقيق الفوز. هناك شرط آخر يتمثَّل في الحفاظ على الحاضنة الداخلية. فالالتفاف الشعبي حول القيادة يُعَدُّ واحدًا من أبرز العوامل التي تُسهِم في الانتصار أو تقوية إرادة المقاومة وتجنُّب الاستسلام. ومن الملاحظ أن هذه الشروط متداخلة فيما بينها؛ بمعنى أن الحفاظ على الحاضنة الشعبية يعتمد على صمود القيادة، والعكس بالعكس. ومن هنا، فإن الحفاظ على التواصل بينهما وضبط آليات الخطاب وطبيعته يُعَدُّ شرطًا جوهريًّا في عمليات البناء والتماسك ما بين القيادة والحاضنة الشعبية. فالدعاية كما يُقصَد منها تحطيم إرادة الخصم والحدّ من عزيمته، فإنه يُقصَد منها أيضًا على الطرف الآخر شحذ هذه العزيمة وبثّ روح الصمود والمقاومة والاستبسال. وقد أولَى مُنظّرو الحرب منذ زمن كلاوزفيتز أهميةً خاصةً للروح المعنوية. حيث إن الطرف الذي يحافظ على روح معنوية عالية طيلة فترة الحرب، يكون النصر حليفه، وكما قيل: «اكتشف كيفية تحطيم الروح المعنوية للخصم، وقد تربح الحرب بينما تتجنَّب ملاقاة جيش العدو تمامًا»[80].

وقد أضفت شبكة الإنترنت -وتحديدًا منصات التواصل الاجتماعي- بُعدًا جوهريًّا في عملية بناء الروح المعنوية وتحطيمها، وذلك يعود إلى أسباب تتعلَّق ببنيتها الرقمية وطبيعتها الشبكية. فمنصات التواصل الاجتماعي تُعَدُّ بين المتخصِّصين على نطاق واسع منصات «شخصنة» للأفراد يعرضون عليها المحتوى الذي يفضِّلونه ويختارونه، وتعكس تصوراتهم وأفكارهم وتفاصيل حياتهم. وهو الأمر الذي يعزِّز الثقة لدرجة كبيرة، ويُسهِم في شحذ الروح المعنوية. وبناءً على ذلك، فقد كان القادة السياسيون من أبرز الفاعلين الذين استعانوا بمنصات التواصل الاجتماعي للتواصل مع القاعدة الانتخابية بعيدًا عن التغطيات التقليدية، وذلك من أجل زيادة نسبة الودّ والتفاعل المباشر والحميمية بينهم، لِما لذلك من نجاحٍ في وصولهم إلى المناصب المرجوَّة. ويريد القادة السياسيون من هذا التكتيك عبر منصات التواصل الاجتماعي الانسلاخَ من الصورة النمطية للقائد السياسي الجاف والقابع خلف كرسي المسؤولية، والظهور بمظهر الإنسان الطبيعي والمواطن العادي الذي يتعايش مع هموم المواطنين والناس العاديين، ويملك القدرة على تفهمهم والتفاهم معهم.

إن إبراز الجانب الشخصي والحميمي في الحرب الدائرة في أوكرانيا لرفع الروح المعنوية كان أمرًا لافتًا للعيان. حيث تصدَّر هذه العملية الرئيس الأوكراني فولوديمير زيلينسكي من خلال مقاطع الفيديو التي قام بنشرها مباشرةً من عدَّة أماكن عامَّة في العاصمة الأوكرانية كييف في بداية الحرب. وقد تمتَّعت مقاطع الفيديو هذه بالطابع الشخصي والحميمي بشكل لافت. فقد حرص الرئيس على الظهور العفوي بعيدًا عن الحراسات المشدَّدة من حوله، وذلك لطمأنة شعبه بأنه رغم الحرب والمخاطر التي تكتنفها

ما زال قادرًا على السَّيْر في الطرقات برفقة عناصر حماية قلائل. كما أنه ظهر بملابس عادية، بعيدًا عن أي محسنات أو مجملات للجسد، مصحوبًا بالعديد من وزرائه، متحدثًا بشكل مباشر، وبلغةٍ بعيدةٍ عن المصطلحات والصياغات الرسمية، وهو الأمر الذي يُسهِم في جعل هذه الرسائل شخصيةً وحميميةً، بحيث يشعر كلُّ من يستمع إليها ويشاهدها كأن الرئيس يتحدَّث معه وإليه شخصيًّا.

لا يقتصر الأمر -والأوضاع كذلك- على القادة وحدهم. فالشعب في ظل حروب كهذه يبتكر من الأساليب ما يمكِّنه من تعزيز روح الصمود من ناحية، وتدعيم الرواية المحلية عن الحرب مقابل رواية الخصم، من ناحية أخرى. ولا شكَّ أن الإنترنت وتكنولوجيا الهواتف المحمولة ومنصات التواصل الاجتماعي قد منحت الفرد العادي من الأدوات التي تمكِّنه من نقل الأحداث مباشرة بعيدًا عن سلطة قنوات الإعلام التقليدية. وهنا تجدر الإشارة إلى أن التكنولوجيات الرقمية جعلت من «الصحافي المواطن» ظاهرةً تفرض نفسها على الأحداث بقوة. وتكثر الأمثلة على ذلك، ولكن كان من أبرزها المدونون العراقيون من أمثال Salam Pax، الذين استطاعوا من خلال مدوناتهم الإلكترونية دحض الرواية الأمريكية حول الحرب على العراق عام 2003. فمن خلال مدوناتهم، أبرز هؤلاء المدونون الجانب المدني من الحياة العراقية التي حاولت الرواية الأمريكية تصويرها على أنها مجرَّد أهداف عسكرية لشعبٍ مطبوعٍ على التخلُّف والعدوان والدونية.

وفي السياق الأوكراني، انتشرت الكثير من الفيديوهات القصيرة على منصات السوشيال ميديا، مثل تيك توك وإنستغرام، تعكس حالة الصمود الشعبي، وتحاول مجابهة الحرب من خلال إشاعة حسِّ الفكاهة، فضلًا عن دحض الرواية الروسية التي سعت إلى تصوير الشعب الأوكراني على أنه شعب منهزم. فمع بداية الحرب وتحديدًا في 24 فبراير/شباط نشرت مستخدمة تُدعى whereislizzyy مقطعَيْن من مقاطع الفيديو الشخصية المرحة في بيتها المؤثث تأثيثًا فاخرًا، وفي الخلفية الصوتية أغنية Who's That Chick، وقد أدرجت تعليقًا مفاده «عندما يهاجمنا الروس، سنغادر الساعة 8 صباحًا». كان الأثاث الفاخر الذي ظهر في الفيديو يتقاطع مع صورة في الخلفية لما يبدو أنه وجبة فطور متواضعة. وقد حمل المقطع الفيديو الذي حصد 2.7 مليون مشاهدة على تيك توك إشارةً واضحةً إلى أن الشعب الأوكراني شعبٌ متحضِّر، يحبُّ الحياة والموسيقى والجمال، وأنه ليس كما تحاول الآلة الإعلامية الروسية تصويره عبر وصف «النازيون الجدد».

وهناك مستخدمة أوكرانية أخرى على منصة تيك توك تُدعى valerisssh ويتابعها 1.1 مليون، نشرت مقطع فيديو مع بداية الحرب يتبع صيحة نموذجية معروفة على تيك توك، حيث يشير الحاضرون إلى أجزاء من منازلهم في أثناء تشغيل أغنية إيطالية مرحة، ويقومون بإيماءة يد متطابقة. وقد تضمَّن مقطع الفيديو المرافقَ التي توجد في الملجأ الذي آووا إليه بسبب الحرب. وفي مقطع فيديو لاحق، تشرح المستخدمة فيه كيفية عمل القهوة في الملجأ عندما لا تتوفر الإمكانيات العادية، وغيرها من الفيديوهات التي تعكس حجم الدمار الذي أصاب المرافق المدنية في أوكرانيا، وبذلك تبعث برسالة واضحة أن الحرب أو «العمليات الخاصة العسكرية» -وفق الرواية الروسية- لا تقتصر على الأهداف العسكرية كما أشاعت ذلك روسيا في بداية الحرب، بل تستهدف المواطنين المدنيين ومرافقهم الحيوية. وفي هذا إشارة إلى أن هذه الإعمال تندرج ضمن خانة جرائم الحرب. ففي أحد الفيديوهات مع مُسِنّ أوكراني تجاوز السبعين من عمره، يشرح فيه كيف أن صاروخًا روسيًّا قد أودى بحياة عائلة

بعد أن أهال عليهم بناية تعرضت للقصف، ويعبّر عن فرحته عندما استطاع التأكُّد من أن طفلًا من العائلة ما زال على قيد الحياة.

خامسًا: فيديوهات التزييف العميق Deepfake Videos

يُعرف التزييف العميق بأنه فيديوهات يتم إنتاجها عبر الذكاء الاصطناعي وتكنولوجيا التعليم الآلي Machine-learning، وذلك بقصّ وتركيب ودمج العديد من الوسائط الرقمية والصوتية لإنتاج فيديو مزيف يبدو كأنه أصلي. والغرض من هذه الفيديوهات هو طمس الحدود الفاصلة بين الفيديو الأصلي والفيديو المزيَّف[81].

وقد تم استخدام هذه التقنية بشكل واسع النطاق في مجال الأفلام الإباحية، إلَّا أن استخداماته في عمليات التضليل والتلاعب بدأت تتزايد في الآونة الأخيرة. فقد استخدمته القناة الرابعة البريطانية لنشر فيديو مزيف يظهر الملكة إليزابيث الثانية وهي تلقي كلمة عيد الميلاد عام 2020 في ظل جائحة كورونا. وقد يبلغ الفيديو المزيف من الإتقان والاحترافية ما يصعب على المشاهدين معه تمييزه عن فيديو أصلي كما حدث مع شبكة التلفزيون لكوريا الجنوبية MBN، التي أعلنت أنها استخدمت تقنية التزييف العميق لمحاكاة مقدمة النشرات الإخبارية المعروفة Kim Joo Ha[82]. وقد يكون إخراج الفيديو المزيف متواضعًا، وهو ما يجعل رصده ومن ثَمَّ دحضه أمرًا سهلًا، مثلما جرى مع الفيديو الذي سُرّب في أواسط شهر مارس/آذار الماضي ويحاكي الرئيس الأوكراني وهو يدعو مواطنيه للاستسلام ووضع السلاح.

وقد أثار الفيديو المزيف السخرية، حيث ظهر بشكل رديء ولم يعبّر عن حقيقية ظهور الرئيس الأوكراني ولا عن مظهره. ومن الملاحظات التي أبداها المشاهدون والخبراء على الفيديو المزيف أن لون بشرة زيلينسكي بدت مختلفة، وتحدَّث بلهجة غير مألوفة، كما تمَّ رصد أن جودة الفيديو لم تكن عاليةً خصوصًا حول رأسه ووجهه[83]. وقد أدان الرئيس الأوكراني هذا العمل، وخرج على شعبه عبر قناته الرسمية في تلغرام لرفض مزاعم الفيديو حول الاستسلام قائلًا: «نحن ندافع عن أرضنا وأطفالنا وعائلاتنا»، «لذلك نحن لا نخطط لإلقاء أي سلاح حتى نصرنا»، كما أصدرت وزارة الدفاع الأوكرانية لاحقًا مقطع فيديو للرئيس الأوكراني يصف فيه هذه الخطوة بأنها «عمل صبياني»[84].

وبغض النظر عمَّا إذا كان العمل صبيانيًّا أم لا، فإن حادثة الفيديو المزيف حول الرئيس الأوكراني تكشف عن أمرين مهمين يجب أخذهما بعين الاعتبار؛ **أولًا**: طريقة تسريب الفيديو. ففي عمليات الدعاية والتضليل، يحرص الفاعلون على تحقيق أقصى درجات الإقناع لدى الجمهور من خلال الاقتراب من الأصالة والمصداقية قدر الإمكان. وهنا في حادثة الفيديو المزيف للرئيس الأوكراني حدث الأمر ذاته. فلم يتم تسريب الفيديو عبر منصات التواصل الاجتماعي أو من خلال حسابات مشبوهة أو غير أصلية، بل قامت الجهات الفاعلة باختراق حساب Ukrayina 24 وبث الفيديو من خلالها لإيهام المشاهدين بأنه إصدار رسمي. وبعد ذلك انتشر الفيديو انتشارًا كبيرًا على الحسابات الناطقة باللغة الروسية على منصة تلغرام ومنصةVK الشبيهة بتطبيق فيسبوك. ومن هناك انتقل الفيديو إلى منصات أخرى، مثل إنستغرام وتويتر ويوتيوب وفيسبوك. تُحقِّق مثل هذه الطرق في النشر هدفَين جوهريَّين يتعلقان بالمصداقية وسعة الانتشار. وهنا فإن المشاهد الذي من المحتمل أن يشكّك في جودة الفيديو، سيجد في مصدره

مـا يصـرف عنـه هـذا التشـكيك ويجعلـه يصـدِّق أصالتـه، وهنـا تكْمُـن أهميـة طريقـة النشـر جنبًـا إلـى جنـب جـودة العمـل وأصالـة المحتـوى.

ثانيًـا: ردَّة الفعـل علـى الفيديـو المزيـف. فرغـم أن الفيديـو أثـار سـخرية المشـاهدين، وتـمَّ رصـده سـريعًا علـى منصـات التواصـل الاجتماعـي ومـن ثَـمَّ حذفـه تمامًـا، فـإن ردة الفعـل المباشـرة مـن الجهـات الرسـمية الأوكرانيـة عبَّـرت عـن خطـورة مثـل هـذه الهجمـات الدعائيـة وتأثيراتهـا الكبيـرة المحتملـة فـي معنويـات المواطنيـن، خصوصًـا فـي ظـل الحـالات الحرجـة كالحـرب علـى سـبيل المثـال أو العمليـات الانتخابيـة. ونظـرًا للفجـوة بيـن عجلـة تطـور مثـل هـذه التقنيـات الاحترافيـة وبيـن الأميـة الرقميـة لـدى عمـوم النـاس، فـإن هـذه التقنيـة يمكـن أن تكـون أكثـر إقناعًـا فـي المسـتقبل، وهـو الأمـر الـذي ينبـئ بتحـولات كبيـرة فـي قطـاع حمـلات التضليـل والدعايـة والتلاعـب.

فهـذه التقنيـة لا تتعلَّـق بتزييـف حسـابٍ علـى منصـات التواصـل الاجتماعـي فحسـب كمـا يجـري فـي تقنيـة الروبوتـات السياسـية Bots، بـل بتزييـف متكامـل يتضمَّـن طبقـات الصـوت والصـورة والحـركات والإيمـاءات، مـا يجعـل مـن الصعوبـة بمـكانٍ التحقُّـق منـه أو تمييـزه. فالأمـر لا يتعلَّـق فقـط بمجـرَّد القيـام بأعمـال تثيـر السـخرية، مثـل الفيديـو المزيـف الـذي ظهـر فيـه الرئيـس الروسـي فلاديميـر بوتيـن وهـو يعلـن فيـه عـن توصلهم إلـى اتفـاق سـلام مـع الأوكرانييـن وأن شـبه جزيـرة القـرم سـوف تصبـح جمهوريـة فيديراليـة تحـت سـيادة أوكرانيـا، بـل يتعلَّـق بأعمـال قـد تغيّـر قواعـد اللعبـة فـي العديـد مـن الميادين، وأهمهـا الميادين الاسـتراتيجية: الاسـتخباراتية منهـا والعسـكرية. وهنـا يمكـن النظـر إلـى المثـال الآخـر الـذي وقـع بعـد ذلـك وتحديـدًا فـي شـهر يونيو/حزيـران عندمـا تـمَّ خـداع رؤسـاء بلديـات العديـد مـن العواصـم الأوروبيـة باتصـال فيديـو مـع نظيرهـم الأوكرانـي فـي كييـف، فيتالـي كليتشـكو، والـذي تبيَّـن بعـد ربـع سـاعة مـن الاتصـال أنـه مجـرَّد محـاكاة للشـخصية الحقيقيـة عبـر تقنيـة التزييـف العميـق. وقـد تـمَّ اكتشـاف الخـداع عندمـا بـدأ كليتشـكو المزيـف يتحـدَّث عـن خـداع الأوكرانييـن المهاجريـن للسـلطات الألمانيـة واسـتغلالهم كـرم الضيافـة، وضـرورة عودتهـم إلـى أوكرانيـا مـن أجـل تلبيـة نـداء التجنيـد فـي صفـوف القـوات الأوكرانيـة، وهـو الأمـر الـذي أثـار شـكوك رؤسـاء البلديـات الذيـن كانـوا معـه فـي الاتصـال[85].

سادسًا: إسكات الأصوات المُعارضة

تناولـت الورقـة فـي السـابق حمـلات الدعايـة والتضليـل التـي تهـدف إلـى إعـادة توجيـه قناعـات الجمهـور، وتشـتيت الآراء المعارضـة. وفـي الحقيقـة، إن الأمـر لا يتوقـف عنـد هذيـن الهدفَيْـن المركزيَّيـن، بـل يتعداهمـا إلـى هـدف ثالـث يتضمَّـن هـذه المـرة إسـكات الأصـوات المُعارضـة وقمعهـا باسـتخدام إجـراءات زجريـة، وأبـرز هـذه الإجـراءات كان التشـريع الـذي سـنَّته السـلطات الروسـية، والـذي تفـرض بموجبـه غرامـة تُقـدَّر بالسـجن لمـدة 15 عامًـا علـى أي كيـانٍ يثبـت أنـه نشـر معلومـاتٍ تعـارض الروايـة الروسـية الرسـمية عـن الحـرب. وردًّا علـى هـذه الإجـراءات، قامـت العديـد مـن وسـائل الإعـلام المعارضـة بإيقـاف عملياتهـا أو تـمَّ حظرهـا مـن قِبَـل الجهـات الأمنيـة الروسـية، مثـل TV Dozhd، والصحيفـة الاسـتقصائية Mediazona، وأخيـرًا وليـس آخـرًا مجلـة Snob[86].

كمـا قامـت السـلطات الروسـية بتقييـد الوصـول إلـى كلٍّ مـن منصـة فيسـبوك وتويتـر، وذلـك بنـاءً علـى رفـض هـذه المنصـات طلبـات الحكومـة الروسـية بضـرورة وقـف عمليـات تدقيـق الحقائـق المسـتقل التـي تقـوم بهـا

ضد محتوى وسائل الإعلام الحكومية الرسمية الروسية. كما فرضت الحكومة الروسية شروطًا أخرى تتعلَّق برخص التسجيل لهذه الشركات. فحسب القانون الجديد، يجب على كل شركة من شركات التكنولوجيا الأجنبية التي لديها أكثر من 500 ألف متابع إقامة مكتب تمثيل رسمي لها داخل الأراضي الروسية، الأمر الذي من شأنه أن يُخضع محتوى هذه الشركات لاحقًا لرقابة السلطات الروسية، ويسهل عليها حذف المحتوى المخالف لروايتها. ومن بين الشركات التي التزمت بهذا التشريع كانت Apple وSpotify وViber فقط[87].

كانت الرقابة التي فُرضت على المحتوى دقيقة، حيث حظرت السلطات الروسية -على سبيل المثال- استخدام كلمتي «غزو» و «اعتداء» لوصف هجومها على أوكرانيا، الذي تَعُدُّه مجرَّد «عمليات عسكرية خاصة». كما أن محرك البحث الروسي الشهير Yandex قام بإرسال تحذيراتٍ لمستخدميه الروس الذين يبحثون عن أخبار أوكرانيا بشأن المعلومات غير الموثوقة على الإنترنت التي تتعلَّق بالعمليات العسكرية، وضرورة توخي الحذر في نقل أيٍّ من هذه المعلومات المخالفة للرواية الروسية الرسمية[88].

الخاتمة

ذهب العديد من المنظرين إلى أن الحرب السيبرانية ليست إلَّا عمليات تكتيكية مُلحَقة بالحرب الأرضية؛ ولذلك لا يمكن اعتبار الحرب السيبرانية -من وجهة نظرهم- ضمن تصنيف الحروب إلَّا إذا كانت تخدم غايةً من غايات العمليات العسكرية التي تجري على الأرض؛ كإبطال الشبكات الإلكترونية التابعة لمراكز السيطرة والتحكُّم، على سبيل المثال. غير أن العمليات السيبرانية التي وقعت (وربما ستقع) في الحرب الدائرة بين روسيا وأوكرانيا تثبت أن العمليات السيبرانية لا يمكن حصرها في البُعْد التكتيكي. فهي غير مقيَّدة في طيف واحد من العمليات، بل جرت على طول الطيف الرقمي، من تلك العمليات التي استهدفت الشبكات الحيوية، سواء المدنية أو العسكرية، ببرمجيات خبيثة، إلى تلك التي جرت عبر الشبكات الرقمية من أجل التضليل والتلاعب والتأثير في معنويات الخصم. وإذا كان الهدف المركزي لكل حربٍ هو شلّ قدرات الخصم على الرد من خلال ضرب مراكز الثقل لديه، فإن الحرب السيبرانية قادرة على الإسهام في ذلك من تلقاء نفسها دون وجود مرادف لها من العمليات العسكرية. ولا ينفي هذا -بطبيعة الحال- أن العمليات المشتركة بين الهجمات السيبرانية والهجمات الأرضية يكمل بعضها بعضًا ويدعم بعضها بعضًا. ولكن من المهم النظر إلى العمليات السيبرانية من زاوية أنها تُعبّر عن شكلٍ جديدٍ من أشكال الحرب يضاف إلى الأشكال الأخرى. ولذلك ذهبت العديد من الدول مثل الولايات المتحدة إلى اعتبار الفضاء السيبراني، وهو الفضاء الذي تحدث فيه ومن خلاله العمليات السيبرانية، فضاءً جديدًا لعملياتها العسكرية يُضاف إلى الفضاءات التقليدية: البحرية والبرية والجوية.

قامت كلٌّ من روسيا وأوكرانيا بعمليات سيبرانية، وإن كانت كفَّة الهجوم في هذه العمليات تميل إلى الجانب الروسي في حين مالت كفَّة الدفاع والردع إلى الجانب الأوكراني. ومن الجدير بالذكر هنا أن العمليات السيبرانية تحدث في الخفاء ولا تتمتَّع بصفة الإسناد، بل تحافظ على مجهوليتها. ومن هنا، فإن الأطراف الفاعلة لا تعلن عن عملياتها أو تتبنَّاها بشكل صريح. وعند الحديث عن الهجمات الروسية، فالمعنى هنا يكون الهجمات المسندة إلى روسيا. فروسيا على الجانب الرسمي لم تتبنَّ أيًّا من الهجمات السيبرانية التي قيل إنها شنَّتها على أهداف أوكرانية أو غير أوكرانية.

وقد انتشرت العمليات السيبرانية في الحرب الدائرة بين روسيا وأوكرانيا على كامل الطيف الرقمي، من هجمات الاختراق (القرصنة الخشنة)، إلى هجمات التلاعب (القرصنة الناعمة). فقد كانت هناك هجمات على الشبكات الحيوية لأوكرانيا، سواء العسكرية منها أو المدنية، عبر العديد من التكتيكات السيبرانية، مثل هجمات تعطيل الخدمة DDoS، وهجمات البرمجيات الماسحة، وبرمجيات التصيّد Phishing، وغيرها. وقد رأى العديد من الخبراء أن هذه الهجمات لم تكن في المستوى المتوقَّع، كما أنها لم تحقِّق نتائجَ مدمرةً كما حدث سابقًا عندما استهدف هجوم نُسِبَ إلى روسيا شبكة الكهرباء الأوكرانية وأخرجها من الخدمة لساعات طويلة عام 2015.

ومن أهم أسباب عدم فاعلية الهجمات الروسية هو أن الردع الأوكراني السيبراني كان فعالًا هذه المرة مقارنةً بالمرات السابقة. وقد قام الردع الأوكراني على المزاوجة بين تكتيكات الدفاع من خلال تقوية البنية الرقمية الداخلية، وتكتيكات التحالف الذي نسجته أوكرانيا على مدار أعوام مع حلفائها الغربيين على الصعيد السيبراني، وأخيرًا تكتيكات الهجوم، حيث كانت أوكرانيا رائدةً في إنشاء الجيش الأوكراني السيبراني التطوعي IT Army، الذي ضمَّ على صفحته في تطبيق تلغرام أكثر من 300 ألف متطوع يعملون في مجال القرصنة من أماكن مختلفة حول العالم، وتبنَّى العديد من الهجمات السيبرانية على أهداف روسية.

وكان الطيف الآخر المتعلِّق بالقرصنة الناعمة، وهي العمليات السيبرانية التي تختصُّ بهجمات التلاعب والتضليل والتأثير (البروباغندا)، حاضرًا بقوة. فبجانب العمليات العسكرية بالسلاح الحيِّ للسيطرة على الأرض، والعمليات السيبرانية لإخضاع الشبكات الإلكترونية، كانت هناك عملياتٌ موازية من أجل السيطرة على رواية الحرب تحدث في فضاء منصات التواصل الاجتماعي على وجه التحديد من خلال استخدام تكتيكات الـ Trolling، والروبوتات Bots، والتزييف العميق، والاختراق، وإسكات الأصوات المعارضة. وكانت روسيا تريد أن تُظهر حجم الدعم الداخلي لعملياتها العسكرية وطمس الأصوات المُعارِضة، في الوقت الذي تحاول فيه خارجيًّا إظهار الخصم كأنه في حالة انهيار واستسلام. وفي المقابل، حاولت أوكرانيا الدفاع عن روايتها من خلال إظهار حجم الدمار في أثناء الحرب، ورفع الروح المعنوية، ودحض الرواية الروسية التي تصبغ السلطات الأوكرانية بالصبغة النازية.

تشكِّل الحرب الروسية-الأوكرانية مختبرًا عمليًّا لقياس العديد من الافتراضات المتعلِّقة بالعمليات السيبرانية. وقد رصدت الورقة العديد من هذه العمليات. ولكن نظرًا لطبيعة العمليات العسكرية التي تتصف بسرعة التطور والتأقلم، فإن استمرار الحرب على الأرض ربما يُسفر عن مزيدٍ من أوجه العمليات السيبرانية. وفي الوقت الذي لم نشهد فيه حتى الآن هجماتٍ واسعة النطاق على أهداف البنية الحيوية، فهذا لا يعني عدم وقوعها في المستقبل. فما زال احتمال حدوثها قائمًا، حيث تخضع العمليات السيبرانية -مثلها مثل أي عمليات عسكرية- لمنطق التقييم المتواصل والتأقلم مع مجريات الأحداث على الأرض.

المراجع

1- Melzer, Nils. "Cyberwarfare and international law." (2011). P. 4.

2- Shane M, Coughlan. "Is there a common understanding of what constitutes cyber warfare?," *The University of Birmingham School of Politics and International Studies*, 30 September 2003, p. 2.

3- المصدر السابق.

4- المصدر السابق.

5- The Congressional Research Service (CRS), IF10537, Updated December 1, 2021. https://sgp.fas.org/crs/natsec/IF10537.pdf (Internet Access on August 1, 2022)

6- Kevin Coleman. "The Cyber Arms Race Has Begun". *CSO Online*, 28 January 2008. https://www.csoonline.com/article/2122353/coleman--the-cyber-arms-race-has-begun.html/.

7- Rid, Thomas. "Cyber war will not take place." In Strategic Studies, pp. 418-438. Routledge, 2014. P. 1-10.

8- Gartzke, Erik. "The myth of cyberwar: bringing war in cyberspace back down to earth." *International security* 38, no. 2 (2013): 41-73.

9- Sharma, Amit. "Cyber wars: A paradigm shift from means to ends." *Strategic Analysis* 34, no. 1 (2010): 62-73.

10- Lynn III, William J. "The Pentagon's Cyberstrategy, One Year Later." Foreign Affairs (2011).

11- Walt M, Stephen. "Is the Cyber Threat Overblown?". *Foreign Policy* .(2010)

12- Ukraine Election Task Force. "Foreign interference in Ukraine's election". *Atlantic Council* (May 15, 2019). https://www.atlanticcouncil.org/in-depth-research-reports/report/foreign-interference-in-ukraine-s-election/

13- Jakub Przetacznik and Simona Tarpova, Russia's war on Ukraine: Timeline of cyber-attacks", *European Parliamentary Research Service* (June 2022). https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

14- المصدر السابق.

15- Hopkins, Valerie. "A hack of the Defense Ministry, army and state banks was the largest of its kind in Ukraine's history". *The New York Times* (Feb. 15, 2022). https://www.nytimes.com/2022/02/15/world/europe/ukraine-cyberattack.html?action=click&module=RelatedLinks&pgtype=Article

16- David D. Clark and Susan Landau, Untangling Attribution,"Harvard National Security Journal, Vol. 2, No. 2 (March, 2011), pp. 25-40. Internet Access on July 29, 2022. https://harvardnsj.org/2011/03/untangling-attribution-2/

17- Sanger E. David, Barnes E. Julian and Conger, Kate. "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War". *The New Yok Times* (Feb. 28, 2022). https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html?action=click&module=RelatedLinks&pgtype=Article

18- Pearson, James and Landay, Jonathan, "Cyberattack on NATO could trigger collective defence clause – official". *Reuters* (October 21, 2021). https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/

19- Hopkins, Valerie. A hack of the Defense Ministry, army and state banks was the largest of its kind in Ukraine's history", *The New York Times* (Feb. 15, 2022) https://www.nytimes.com/2022/02/15/world/europe/ukraine-cyberattack.html?action=click&module=RelatedLinks&pgtype=Article

20- المصدر السابق.

21- المصدر السابق.

22- المصدر السابق.

23- المصدر السابق.

24- المصدر السابق.

25- Hakmeh, Joyce and Naylor, Esher. "How the tech community has rallied to Ukraine's cyber-defence". *The guardian* (Mon 7 Mar 2022) https://www.theguardian.com/commentisfree/2022/mar/07/tech-community-rallied-ukraine-cyber-defence-eu-nato

26- Sanger E. David, Barnes E. Julian and Conger, Kate. "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War". *The New Yok Times* (Feb. 28, 2022). https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html?action=click&module=RelatedLinks&pgtype=Article

27- Satter, Raphael. "Ukraine says its military is being targeted by Belarusian hackers". *Reuters* (February 25, 2022). https://www.reuters.com/world/europe/ukraine-says-its-military-is-being-targeted-by-belarusian-hackers-2022-02-25/
28- المصدر السابق.
29- المصدر السابق.
30- Burt, Tom. "The hybrid war in Ukraine". *Microsoft* (April 27, 2022). https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
31- Coker, James. "Ukrainian Energy Supplier Targeted by New Industroyer Malware". *Infosecurity Magazine* (April, 2022). https://www.infosecurity-magazine.com/news/ukrainian-energy-industroyer/
32- Statement by President Biden on our Nation's Cybersecurity, the White House (March 21, 2022). https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/
33- Sabbagh, Dan. "Russian hackers targeting opponents of Ukraine invasion, warns GCHQ chief". *The guardian* (10 May 2022). https://www.theguardian.com/technology/2022/may/10/russian-hackers-targeting-opponents-of-ukraine-invasion-warns-gchq-chief
34- Labott, Eise. "We Are the First in the World to Introduce This New Warfare': Ukraine's Digital Battle Against Russia". *Politico Magazine* (March 8, 2022). https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber-social-media-00014880

35- Peacock, Robert, "How Ukraine has defended itself against cyberattacks – lessons for the US". *The conversation* (April 5, 2022). https://theconversation.com/how-ukraine-has-defended-itself-against-cyberattacks-lessons-for-the-us-180085
36- The Ukrainian Digital Resistance: cyber resilience and digital diplomacy at work. webinar at CEPS (18 May 2022). https://www.ceps.eu/ceps-events/the-ukrainian-digital-resistance-cyber-resilience-and-digital-diplomacy-at-work/
37- Hakmeh, Joyce and Naylor Esther. "How the tech community has rallied to Ukraine's cyber-defence". *The guardian* (Mon 7 Mar 2022) https://www.theguardian.com/commentisfree/2022/mar/07/tech-community-rallied-ukraine-cyber-defence-eu-nato
38- المصدر السابق.
39- المصدر السابق.
40- المصدر السابق.
41- Lerman, Rachel and Zakrzewski, Cat. 'Elon Musk's Starlink is keeping Ukrainians online when traditional Internet fails". *Washington post* (March 19, 2022) https://www.washingtonpost.com/technology/2022/03/19/elon-musk-ukraine-starlink/
42- Labott, Elise. "We Are the First in the World to Introduce This New Warfare': Ukraine's Digital Battle Against Russia". *Politico Magazine* (March 8, 2022). https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber-social-media-00014880
43- المصدر السابق.
44- المصدر السابق.
45- المصدر السابق.
46- Conger, Kate and Satariano, Adam. "Volunteer Hackers Converge on Ukraine Conflict With No One in Charge". *New York Times* (March 4, 2022). https://www.nytimes.com/2022/03/04/technology/ukraine-russia-hackers.html
47- Dave, Paresh and Dastin, Jeffrey. "Ukraine's tech diaspora races to mobilize Silicon Valley in war with Russia". *Reuters* (March 3, 2022).
48- Pearson, James. "Ukraine launches 'IT army,' takes aim at Russian cyberspace". *Reuters* (February 27, 2022). https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/
49- المصدر السابق.

50- Conger, Kate and Satariano, Adam. "Volunteer Hackers Converge on Ukraine Conflict With No One in Charge". *New York Times* (March 4, 2022). https://www.nytimes.com/2022/03/04/technology/ukraine-russia-hackers.html
51- Braw, Elisabeth. "Ukraine's Digital Fight Goes Global: The Risks of a Self-Directed, Volunteer Army of Hackers". *Foreign Affairs* (May 2, 2022). https://www.foreignaffairs.com/articles/ukraine/2022-05-02/ukraines-digital-fight-goes-global
52- المصدر السابق.
53- Dave, Paresh. "Exclusive: Google blocks RT, Sputnik from Play app store in Europe". *Reuters* (March 2, 2022). https://www.reuters.com/technology/exclusive-google-blocks-rt-sputnik-play-app-store-europe-2022-03-02/
54- Thornhill, Johb. "Ukraine is winning the information war against Russia". *Financial Times* (March 3 2022) https://www.ft.com/content/2a11a507-80a3-4da5-9eee-4dafa4a7ee6e
55- المصدر السابق.
56- @YourAnonOne: https://twitter.com/YourAnonOne/status/1496965766435926039?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1496965766435926039%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.theguardian.com%2Fworld%2F2022%2Ffeb%2F27%2Fanonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

57- Tangermann,Victor. "ANONYMOUS SAYS IT'S HACKING ENTIRE RUSSIAN TELEVISION CHANNELS NOW". *The Byte* (March 7, 2022). https://futurism.com/the-byte/anonymous-hacking-russian-television?utm_campaign=trueanthem_manual&utm_medium=social&utm_source=facebook&fbclid=IwAROz4YofehvV1WktCj-L1Fdoi_iy3GtZgsE2UkljRzK5pMGkjqfUkpK1WCe8
58- Milmo, Dan. "Anonymous: the hacker collective that has declared cyberwar on Russia". *The guardian* (Sun 27 Feb 2022). https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

59- Singer, P.W. and Brooking, E.T., 2018. LikeWar: The weaponization of social media. Eamon Dolan Books. P.17-23.
60- Internet troll. Wikipedia. https://en.wikipedia.org/wiki/Internet_troll
61- Gilbert, David, "Inside Cyber Front Z, the 'People's Movement' Spreading Russian Propaganda". The Vice (April 4, 2022). https://www.vice.com/en/article/7kbjny/russia-cyber-front-z-telegram
62- "You don't believe these are real reviews, do you?" How Fontanka looked at the front line of information fronts Z". f*ontanka* (March 21, 2022). https://www.fontanka.ru/2022/03/21/70522490/
63- Gilbert, David, "Inside Cyber Front Z, the 'People's Movement' Spreading Russian Propaganda". The Vice (April 4, 2022). https://www.vice.com/en/article/7kbjny/russia-cyber-front-z-telegram

64- Monbiot, George. "We must confront Russian propaganda – even when it comes from those we respect". *The guardian* (March 2, 2022). https://www.theguardian.com/commentisfree/2022/mar/02/russian-propaganda-anti-imperialist-left-vladimir-putin
65- المصدر السابق
66- Kaplan, Alex. "YouTube is making money off a false Ukraine-biolabs conspiracy theory that is tied to Russian disinformation and QAnon". *Media Matters For America* (March 8, 2022) https://www.mediamatters.org/google/youtube-making-money-false-ukraine-biolabs-conspiracy-theory-tied-russian-disinformation-and
67- المصدر السابق، ص٣-١٥.
68- المصدر السابق، ص٣-١٥.
69- المصدر السابق، ص٣-١٥.
70- المصدر السابق، ص٣-١٥.

71- Purtil, -James. “Twitter bot network amplifying Russian disinformation about Ukraine war, researcher says”. *ABC Net* (March 29, 2022). https://www.abc.net.au/news/science/2022-03-30/ukraine-war-twitter-bot-network-amplifies-russian-disinformation/100944970
72- المصدر السابق.
73- المصدر السابق.
74- Di Blasi, Fransesco. “A pro-Russian bot network in the EU amplifies disinformation about the war in Ukraine”. *European Digital Media Observatory* (April 28, 2022). https://edmo.eu/2022/04/28/a-pro-russian-bot-network-in-the-eu-amplifies-disinformation-about-the-war-in-ukraine/
75- Culliford, Elizabeth. “Facebook-owner Meta says Ukraine’s military, politicians targeted in hacking campaign”. *Reuters* (February 28, 2022). https://www.reuters.com/technology/facebook-owner-meta-says-ukraines-military-politicians-targeted-hacking-campaign-2022-02-28/
76- المصدر السابق.
77- Conger, Kate. “Hackers’ Fake Claims of Ukrainian Surrender Aren’t Fooling Anyone. So What’s Their Goal?”. *New York Time* (April 5, 2022). https://www.nytimes.com/2022/04/05/us/politics/ukraine-russia-hackers.html
78- المصدر السابق.
79- المصدر السابق.
80- Singer, P.W. and Brooking, E.T., 2018. LikeWar: The weaponization of social media. Eamon Dolan Books. P.18.
81- Marie-Helen, Maras, and Alexandrou Alex. “Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos.” The International Journal of Evidence & Proof 23, no. 3 (2019): 255-262.
82- Debusmann, Brend Jr. “‘Deepfake is the future of content creation”. *BBC* (March 8, 2021). https://www.bbc.com/news/business-56278411
83- Nixon, Geoff. “Zelensky, Putin videos provide glimpse of evolving deepfake threat, experts say”. *CBC* (March 20, 2022). https://www.cbc.ca/news/world/zelensky-putin-ukraine-war-deepfake-video-1.6391033
84- »A falsified video of Ukrainian President Zelensky showed how deepfakes can be disarmed«. The Washington Post (March 23, 2022). https://www.washingtonpost.com/opinions/2022/03/23/zelensky-geopolitical-deepfake-reaction-disarmed/

85- Klitschko, Vitali. “European politicians duped into deepfake video calls with mayor of Kyiv”. *The guardian* (June 25, 2022). https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko
86- Myers, Steven Lee and Thompson A. Thompson. “Truth Is Another Front in Putin’s War: The Kremlin has used a barrage of increasingly outlandish falsehoods to prop up its overarching claim that the invasion of Ukraine is justified.”. *New York Times* (March 20, 2022). https://www.nytimes.com/2022/03/20/world/asia/russia-putin-propaganda-media.html?campaign_id=51&emc=edit_mbe_20220321&instance_id=56269&nl=-morning-briefing%3A-europe-edition&regi_id=80012506&segment_id=86081&te=1&user_id=be6138bede-8a70452f3addc7d93ec316
87- Culliford, Elisabeth. “Analysis: Moscow battles big tech to control the narrative”. *Reuters* (February 28, 2022). https://www.reuters.com/technology/russia-invades-ukraine-moscow-battles-big-tech-control-narrative-2022-02-28/
88- المصدر السابق.

الشرق للأبحاث الاستراتيجية

AL SHARQ
STRATEGIC
RESEARCH

عن الشرق للأبحاث الاستراتيجية

هو مركز يقوم بأبحاث محايدة ودقيقة، هدفها تعزيز قيم المشاركة الديمقراطية، والمواطنة المستنيرة، والحوار المتبادل، والعدالة الاجتماعية.

Address: Istanbul Vizyon Park A1 Plaza
Floor:6 No:68 Postal Code: 34197
Bahçelievler/ Istanbul / Turkey
Telephone: +902126031815
Fax: +902126031665
Email: info@sharqforum.org

عن المؤلف

متخصّص في علم الاجتماع الرقمي والسياسة السيبرانية