المركز العربي للأبحاث ودراسة السياسات
Arab Center for Research & Policy Studies

أوراق استراتيجية | 25 أيلول/ سبتمبر، 2023

الاستراتيجية الدفاعية من الحرب التقليدية إلى الحرب غير التقليدية

عمليات المعلومات في الحرب الروسية على أوكرانيا

ورقة استراتيجية رقم 9

حمد علي المهندي

وحدة الدراسات الإستراتيجية

الاستراتيجية الدفاعية من الحرب التقليدية إلى الحرب غير التقليدية

عمليات المعلومات في الحرب الروسية على أوكرانيا

سلسلة: أوراق استراتيجية

ورقة استراتيجية رقم 9

وحدة الدراسات الإستراتيجية

25 أيلول/ سبتمبر، 2023

حمد علي المهندي

باحث دكتوراه في الدراسات الدفاعية والأمنية بأكاديمية جوعان بن جاسم للدراسات الدفاعية، قطر. حاصل على ماجستير الدراسات الدفاعية من كلية "كينجز كوليج" في لندن، وماجستير العلوم السياسية والعلاقات الدولية من معهد الدوحة للدراسات العليا.

المركز العربيّ للأبحاث ودراسة السّياسات مؤسّسة بحثيّة عربيّة للعلوم الاجتماعيّة والعلوم الاجتماعيّة التطبيقيّة والتّاريخ الإقليميّ والقضايا الجيوستراتيجية. وإضافة إلى كونه مركز أبحاثٍ فهو يولي اهتمامًا لدراسة السّياسات ونقدها وتقديم البدائل، سواء كانت سياسات عربيّة أو سياسات دوليّة تجاه المنطقة العربيّة، وسواء كانت سياسات حكوميّة، أو سياسات مؤسّسات وأحزاب وهيئات.

يعالج المركز قضايا المجتمعات والدول العربيّة بأدوات العلوم الاجتماعيّة والاقتصاديّة والتاريخيّة، وبمقاربات ومنهجيّات تكامليّة عابرة للتّخصصات. وينطلق من افتراض وجود أمن قوميّ وإنسانيّ عربيّ، ومن وجود سماتٍ ومصالح مشتركة، وإمكانيّة تطوير اقتصاد عربيّ، ويعمل على صوغ هذه الخطط وتحقيقها، كما يطرحها كبرامجَ وخططٍ من خلال عمله البحثيّ ومجمل إنتاجه.

المركز العربيّ للأبحاث ودراسة السّياسات

شارع الطرفة، منطقة 70

وادي البنات

ص. ب: 10277

الظعاين، قطـر

هاتف: 40354111 974 +

www.dohainstitute.org

المحتويات

مقدمة

تعد حرب المعلومات أحد التهديدات الصاعدة التي استجدت في القرن الحادي والعشرين نظرًا إلى شيوع وانتشار البنى التحتية التقنية والتطور التكنولوجي وثورة المعلومات الرقمية. ومع ذلك، فهي قديمة قدم النزاع البشري، وتمت الإشارة إليها واستخدامها بأساليب مختلفة. تنبع أهمية هذا النوع من التهديدات من تحوّل الفاعلين من الدول وغير الدول إلى استخدام المعلومات بوصفها أحد أدوات الحرب والصراع على نحو متزايد؛ بهدف فرض إرادتها على خصومها بوسائل أقل عنفًا، والقدرة على التصعيد إلى ما قبل عتبة المواجهة المسلحة، إضافة إلى سهولة استخدامها وقلة تكاليفها. ويُعد التفوق في مجال المعلومات جزءًا أساسيًا من دعائم الأمن القومي، وخطوة مهمة في العمليات العسكرية؛ إذ إن البعد المعلوماتي هو البعد الخامس للحرب بعد الأبعاد البرية، والبحرية، والجوية، والفضائية. وما يميز هذا البعد أنه يتضمن مجموعة واسعة من الأدوات والأساليب مثل: الحرب النفسية، والحرب الإلكترونية، والحرب السيبرانية، وعمليات التأثير والتضليل والخداع العسكري.

منذ أكثر من عشرين عامًا، قبل بداية الغزو الروسي لأوكرانيا في شباط/ فبراير 2022، نشطت حرب معلومات إعلامية وعسكرية بين الأطراف المعنية بالأزمة؛ روسيا من جهة، وأوكرانيا والدول الغربية من جهة أخرى. لذلك فلا تعتبر هذه الحرب المعلوماتية جديدة بالنسبة إلى سلسلة الأزمات بين أوكرانيا وروسيا. ويمكن القول إن مظاهر التوتر والمواجهة بين البلدين كانت تشتد وتخبو منذ انهيار الاتحاد السوفياتي والمواجهات الروسية مع الغرب في مواقع الصراع والتنافس المختلفة في المحيط الروسي، والتي ازدادت حدةً في أعقاب الغزو الروسي لشبه جزيرة القرم الأوكرانية عام 2014، إلى أن وصلت إلى المواجهة المسلحة مع الغزو الروسي لأوكرانيا عام 2022.

تعد الأزمة الأوكرانية نموذجًا ملائمًا لدراسة عمليات المعلومات، وعمليات المعلومات المضادة، والحرب الهجينة. لهذا تركز هذه الورقة عليها بوصفها مثالًا تطبيقيًا لعمليات المعلومات واستخداماتها في هذا العصر، مسلطةً الضوء على إحدى الأدوات الرئيسة المستخدمة في الأزمة الأوكرانية والصراع الروسي الأوكراني - الغربي، سعيًا إلى عرض عمليات المعلومات الحديثة وشرح عناصرها وأدواتها، بصفتها أحد أساليب الحرب في القرن الحادي والعشرين، ثم توضيح كيفية استخدامها عمليًا.

تعتمدُ الورقة على النظرية الواقعية في تفسير الأزمة الروسية - الأوكرانية، التي ترتكز على الصراع ومدّ النفوذ بين الدول، ومحاولة كل دولة بسط سيطرتها ورؤيتها على الدول الأخرى، باستخدام كل أنواع القوة، بما فيها حرب المعلومات، وعمليات المعلومات المختلفة. ترى النظرية الواقعية أن الفوضى هي سمة النظام الدولي، وتؤثر في تصرفات الدولة، وتعمل الدول بدورها للحفاظ على توازن القوى[1]. ومن ثمّ، تدعم هذه النظرية فكرة أنه يمكن اتخاذ أي وسيلة ضرورية للحصول على السلطة والقوة، وأنه لا توجد أخلاق عندما يتعلق الأمر بالعلاقات الدولية، ومن ثمّ تقدم تفسيرًا لتبرير الاستخدام الروسي للوسائل غير التقليدية، جنبًا إلى جنب مع الوسائل التقليدية، للحصول على القوة. فقد تحولت المعلومات مع الثورة التكنولوجية إلى أحد أشكال القوة، وساهمت في التمهيد لبيئة أمنية ذات معايير جديدة، تلاشت فيها الفواصل بين ما هو مدني وعسكري.

يمكن القول إنه على الرغم من أن النظريات حول الأمن قديمة ومتعددة، فإن المرحلة الحالية قد تكون مختلفة شيئًا ما مع بروز حرب المعلومات ساحةً للتنافس والصراع والتفاعل العالمي؛ ما أبرز الحاجة إلى رؤى نظرية قادرة على نحو أكبر على تفسير طبيعة التغيرات التي ألحقتها الثورة المعلوماتية على العمليات العسكرية والحروب بشكل لا يتعارض مع المفاهيم التقليدية للأمن والقوة والفوضى، بل يضيف إليها أبعادًا وجوانب تواكب التغيرات في البيئة الاستراتيجية وطبيعة التهديدات الصاعدة.

1 William C. Wohlforth, "Realism and Foreign Policy," in: Steve Smith et al. (eds.), *Foreign Policy: Theories, Actors, Cases* (Oxford: Oxford University Press, 2008), p. 36.

تكمن إشكالية مفهوم حرب المعلومات في عدم وجود اتفاق حول تعريفها وخصائصها من الباحثين والخبراء المتخصصين، نظرًا إلى أن الثورة التكنولوجية جعلت من وسائل المعلومات في متناول الجميع وبمقدورهم استخدامها سلبيًا أو إيجابيًا مع انخفاض تكلفة تشغيلها. وبناءً عليه، تحاول الدراسة فك الارتباك والتشابك المفاهيمي والعقائدي حول مفهومي حرب المعلومات و»عمليات المعلومات». كما تطرح الورقة سؤالاً عن أهمية حرب المعلومات في الصراعات بين الدول، خاصةً فيما يتعلق بدورها في الحرب الدائرة حاليًا بين روسيا وأوكرانيا، وعن مدى نجاح روسيا في استخدام عمليات المعلومات خلالها. وتفترض أن الاستخدام المتفوق لعمليات المعلومات يساهم في تحقيق التفوق في العمل العسكري، وتؤثر نتائج المواجهة في بيئة المعلومات في تحقيق انتصارات على الأرض من خلال العمل العسكري التقليدي. كما تفترض وجود ضعف في إدارة روسيا لحرب المعلومات ولعمليات المعلومات ضد أوكرانيا.

تقعُ الدراسة في ثلاثة محاور رئيسة. يتناول الأول مفاهيم حرب المعلومات وتطورها واستخدامها، ويوضّح الآراء المختلفة حولها، مع توضيح المنظور الغربي لعمليات المعلومات وأبعادها وأدواتها والأساليب التي تستخدم فيها. أمّا الثاني فيتناول النهج الروسي في حرب وعمليات المعلومات، ويغطي التحول في الاستراتيجية الدفاعية الروسية الذي جعل من عمليات المعلومات أحد مجالات تركيز عملياتها العسكرية. في حين يتطرق الثالث إلى الأزمة الأوكرانية منذ عام 2022 وحرب المعلومات الروسية والحرب الغربية المضادة، ويُعنى بتقييم التطبيق الروسي لعمليات المعلومات في هذه الأزمة ومدى كفاءته.

أولًا: عمليات المعلومات: المفهوم والتطوّر والاستخدامات

1. المعلومات أداةً لقوة الدولة

يمكن تفسير الأنشطة المختلفة في بيئة المعلومات في إطار النظرية الواقعية، التي تفسر سلوك الدول تجاه محيطها. تقدم الواقعية الهجومية تفسيرًا للأحداث في الأزمة الأوكرانية - الروسية، حيث يجادل جون ميرشايمر بأن هيمنة الولايات المتحدة على حلف شمال الأطلسي «الناتو» والاتحاد الأوروبي جعل التركيز ينصب أساسًا على مواجهة الاتحاد السوفياتي خلال الحرب الباردة، فأدى هذا إلى تراكم انزعاج روسيا، خاصة مع تعدي الغرب على دول المحيط الروسي (أي الجمهوريات السوفياتية السابقة)[2]. وقدّر ميرشماير أن روسيا في عام 2004 كانت أضعف من أن تُبقي الجمهوريات السوفياتية السابقة خارج الناتو والاتحاد الأوروبي. لكنها اتخذت خطًا متشددًا عندما أعلن الناتو، في قمة بوخارست عام 2008، أن جورجيا وأوكرانيا ستصبحان في النهاية أعضاء في الحلف[3].

من جانب آخر، ترى مجموعة من المحللين الذين تنبؤوا بالصراع الروسي – الأوكراني منذ منتصف التسعينيات أن الوضع المثالي لأي دولة في السياسة الدولية هو أن تسيطر على منطقتها، وتتأكد من عدم سيطرة أي دولة أخرى على تلك المنطقة[4]. لم تكن روسيا قادرة بعد انهيار الاتحاد السوفياتي على الحفاظ على تلك الهيمنة الإقليمية، وثبت أن الحفاظ على الإمبراطورية والسيطرة على دول حلف وارسو (معاهدة الصداقة

2 The Tokyo Foundation for Policy Research, "John Mearsheimer on 'An Offensive Realist's View of China and Crimean Crisis'," YouTube, 25/12/2014, accessed on 3/7/2023, at: https://tinyurl.com/6vmmzkt9

3 يُنظر الفقرة 23 من إعلان قمة بوخارست:
North Atlantic Treaty Organization, "Bucharest Summit Declaration," 3/4/2008, accessed on 3/7/2023, at: https://tinyurl.com/25uaxtet

4 John Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton & Company, 2001), p. 100.

والتعاون والمعونة المشتركة) كان مكلفًا، لأسباب عديدة، منها السبب الاقتصادي[5]. لكن توقف روسيا عن السعي لتحقيق الهيمنة الإقليمية لا يعني عدم تمكنها من البدء من جديد؛ فالسعي نحو تحقيق الهيمنة في محيطها هو ما يخشاه الكثيرون في دول أوروبا الشرقية[6]. وكان تعزيز هذا الخوف متأصلًا في الخطاب الرسمي المستخدم في عمليات التأثير وكان أساسًا لعمليات المعلومات الروسية، مثل الإشارة إلى جيران روسيا على أنهم «الدول في الخارج القريب»[7].

استغلت روسيا تحول العالم إلى مشهد رقمي وسيبراني وبيئة معلوماتية متشابكة؛ للحصول على القوة والسيطرة على الدول الأضعف. ويمكن ملاحظة ذلك في الأجندة العسكرية والسياسية الروسية وتوظيفها القدرات التكنولوجية لكسب التفوق على خصومها. فقد حولت روسيا قدراتها السيبرانية والمعلوماتية إلى نوع من الأسلحة التي تمتد إلى ما هو أبعد من أغراض التجسس، فتهاجم على نحو مباشر المؤسسات الرئيسة لدول مختلفة؛ مثل الأنظمة الانتخابية في هذه الدول، حيث تسعى من خلال هذه الهجمات لتسهيل انتخاب قادة موالين لها في محيطها الإقليمي كجزء من استراتيجيتها الأمنية. ويندرج هذا في إطار المبدأ الواقعي للدول التي تسعى إلى اكتساب القوة والحفاظ عليها وتوسيعها، كما يتوافق مع الطبيعة غير الأخلاقية للنظام الدولي، حيث تذهب الدول إلى أبعد حدٍ من أجل تحقيق السيادة.

تدرك روسيا حجم قوتها في مجال الحرب السيبرانية والمعلوماتية، وتوظف هذه القدرات في السيطرة على محيطها. وتفسر الطبيعة الواقعية للسياسة الروسية استخدام البعد المعلوماتي كوسيلة للحرب وإرساء السيطرة؛ ما يؤكد بأن الدول بطبيعتها معادية بحسب المنظور الواقعي. من جانب آخر، ولمواجهة الهجوم السيبراني الروسي، اتخذ خصومها أساليب مضادة؛ مثل العقوبات، والعمل على تعزيز قدراتهم العسكرية السيبرانية والأمن السيبراني. وقامت أوكرانيا والدول الغربية بإنشاء مراكز وكيانات تتعامل مع عمليات المعلومات الروسية والحرب الهجينة على نحو مباشر؛ مثل المركز الإعلامي لأزمة أوكرانيا، الذي جرى تأسيسه كرد على الاحتلال الروسي لشبه جزيرة القرم، بهدف الدفاع عن سيادة أوكرانيا ومصالحها الوطنية في مجال المعلومات[8]، وهو متخصص في الرد على عمليات المعلومات الروسية من الجانب الإعلامي والتعامل معها.

2. مفاهيم عمليات المعلومات وتطورها واستخدامها

يمكن تقسيم عمليات المعلومات إلى ثلاثة مكونات عامة رئيسة، حيث يساهم الإلمام بها في تفسير سبب الارتباك المفاهيمي الذي يحيط بالمفهوم. الأول، هو البعد الإدراكي أو المعرفي Cognitive Dimension، وفيه تكون المعلومات هي الرسالة، ويدخل ضمن هذا الاستخدام العمليات النفسية، والخداع، وحشد الرأي والتأثير. والهدف في هذا البعد هو السيطرة على عقل الخصم وقراراته باستخدام المعلومات. الثاني، هو البعد الفيزيائي أو المادي؛ وفيه تكون المعلومات هي الأداة، وتدخل ضمن هذا المجال الحروب السيبرانية، والإلكترونية والتشويش التقني وغير ذلك. ويكون الهدف في هذا البعد هو استهداف أنظمة المعلومات وتدميرها. والثالث، هو استغلال المعلومات؛ وفيه تكون المعلومات هي

5 Richard Sakwa, "The Soviet Collapse: Contradictions and Neo-modernisation," *Journal of Eurasian Studies*, vol. 4, no. 1 (2013), p. 66.

6 Yury E. Fedorov, "Continuity and Change in Russia's Policy toward Central and Eastern Europe," *Communist and Post-Communist Studies*, vol. 46, no. 3 (2013), p. 324.

7 John Lepingwell, "The Russian Military and Security Policy in the 'Near Abroad'," *Survival*, vol. 36, no. 3 (1994), p. 70.

8 تأسس المركز الإعلامي للأزمة الأوكرانية في عام 2014، ويقدم رصدًا دائمًا لعمليات المعلومات الروسية والحرب الهجينة في أوكرانيا وبعض الدول المجاورة وتقارير ونشرات تتعلق بهذا المجال. يُنظر:
Ukraine Crisis Media Center, accessed on 3/7/2023, at: https://tinyurl.com/2fk4pujn

الغاية والهدف، مثل العمليات الاستخباراتية وجمع المعلومات والقيادة والسيطرة، والذي يجري فيها الاستفادة من المعلومات لتحقيق أهداف عسكرية[9].

تعتمد عمليات المعلومات على ما يطلق عليه «القدرات ذات العلاقة بالمعلومات» Information-Related Capabilities (IRC)، وهي الأدوات أو التقنيات أو الأنشطة المستخدمة في أحد أبعاد بيئة المعلومات التي يمكن استخدامها لإنشاء تأثيرات وظروف مرغوبة من الناحية العملياتية[10]. يعتمد تعريف عمليات المعلومات على نحو أساسي على هذه القدرات. لذلك، تصف وزارة الدفاع الأميركية عمليات المعلومات بأنها التوظيف المتكامل أثناء العمليات العسكرية للقدرات ذات العلاقة بالمعلومات، بالتنسيق مع خطوط العمليات الأخرى للتأثير في عملية صنع القرار لدى الخصوم والخصوم المحتملين[11].

ساهمت المؤسسة العسكرية الأميركية في صياغة مجموعة من التعريفات لحرب وعمليات المعلومات، وتطورت تدريجيًا مع تطور مجالها واستخداماتها. وتعود الإشارة الأولى لحرب المعلومات في مراجع وزارة الدفاع الأميركية إلى عام 1992، حيث جرى تعريفها بأنها: «المنافسة بين أنظمة المعلومات المعارضة لتشمل الاستغلال أو التعطيل أو تدمير أنظمة معلومات الخصم من خلال وسائل مثل استخبارات الإشارات وإجراءات القيادة والسيطرة المضادة مع حماية سلامة أنظمة المعلومات الخاصة بنا من مثل هذه الهجمات»[12]. وجرى استخدام هذا التعريف في العقيدة المشتركة للقيادة والسيطرة للجيش الأميركي[13].

وفي عام 1996، طور الجيش الأميركي تعريف حرب المعلومات ليصبح أكثر شمولاً وليتضمن التأثير، فقد عرفها بأنها «الأعمال التي تتخذ لتحقيق تفوق المعلومات عن طريق التأثير في المعلومات المعادية والعمليات المبنية على هذه المعلومات ونظم هذه المعلومات، وفي الوقت نفسه حماية معلوماتنا والعمليات المبنية عليها وحماية نظم معلوماتنا»[14].

حصل التحول الأكبر في المفهوم عند إصدار الجيش الأميركي مرجع العقيدة المشتركة لعمليات المعلومات في عام 2006[15]، إذ جرى استبدال مفهوم حرب المعلومات بمفهوم عمليات المعلومات، وتم إصدار عقيدة جديدة للجيش الأميركي مختصة بعمليات المعلومات حلت محل عقيدة القيادة والسيطرة. وأوضحت عقيدة عمليات المعلومات المرجعية بأن عمليات المعلومات أكثر اتساعًا وشمولاً من حرب المعلومات التي تحدث في الحرب فقط، في حين أن عمليات المعلومات «تُجرى أثناء وقت الأزمة أو النزاع (بما في ذلك الحرب) لتحقيق أو تعزيز أهداف محددة على خصم أو خصوم معينين»[16]. وهناك تحول لدى شريحة كبيره من الباحثين والمؤسسات الرسمية لاتباع النهج الأميركي في اعتماد مفهوم عمليات المعلومات بدلاً من حرب المعلومات.

---

9 James Adams, *The Next World War: The Warriors and Weapons of the New Battlefields in Cyberspace* (London: Hutchinson, 1998), p. 17.

10 Ibid., p. 1.

11 Joint Chiefs of Staff, Information Operations, Joint Publication (JP 3-13), Washington, DC: Department of Defense, 2014., p. GL-9.

12 Michael Warner, "Notes on Military Doctrine for Cyberspace Operations in the United States, 1992–2014," *The Cyber Defense Review*, 27/8/2015, accessed on 3/7/2023, at: https://tinyurl.com/y3ua4973

13 Joint Chiefs of Staff, "Joint Doctrine for Command and Control (C2W)," *Joint Publication*, no. 3 - 13.1, 7/2/1996, accessed on 3/7/2023, at: https://bit.ly/36DZuEn

14 Ibid.

15 "Joint Doctrine for Information Operations," Joint Chiefs of Staff, *Joint Publication*, no. 3-13, 13/2/2006, p. III, accessed on 3/7/2023, at: https://cutt.ly/XGuVU06

16 Ibid., p. GL-9.

3. الفرق بين حرب المعلومات وعمليات المعلومات

بعد التحول الأميركي في الوثائق المرجعية لوزارة الدفاع من استخدام مفهوم حرب المعلومات إلى مفهوم عمليات المعلومات، توسع الباحثون في استخدام المفهومين، وجادل عدد منهم مثل هيربرت لين ووليام رود أن هناك عدم وضوح في تعريف حرب المعلومات وعمليات المعلومات يمتد إلى داخل المؤسسات العسكرية نفسها، حيث يشير هيربرت لين في دراسته بعنوان «الارتباك العقائدي والخلل الثقافي في وزارة الدفاع»[17] إلى أن هناك التباسًا يؤدي إلى الفوضى في المواضيع ذات العلاقة بحروب المعلومات في داخل المؤسسة العسكرية الأميركية. في المقابل، يشير وليام رود إلى أنه على الرغم من اختلاف تعريف المؤسسة العسكرية الأميركية لعمليات المعلومات، فإن الأساس العام لمعظم التعريفات مبني على أن «حرب المعلومات هي «صراع تكون فيه المعلومات هي المورد والهدف والسلاح، كل ذلك في الوقت نفسه»[18]. وقامت كاثرين ثيوري في دراسة بعنوان «عمليات المعلومات» بالإشارة إلى أنه لا يوجد حاليًا تعريف رسمي من الحكومة الأميركية لحرب المعلومات، إلا أن المتخصصين يصورونها عادةً على أنها استراتيجية لاستخدام المعلومات وإدارتها لتحقيق ميزة تنافسية، بما في ذلك العمليات الهجومية والدفاعية. يمكن تحقيق هذه الاستراتيجية عن طريق عمليات المعلومات، وهي تمثل التقنيات والأدوات والإجراءات التي يجري اتخاذها لتحقيق أهداف حرب المعلومات؛ بمعنى أنه لا توجد حرب معلومات من دون عمليات معلومات، ولكن العكس صحيح[19]. يظهر هذا التداخل في العديد من الدوائر العسكرية والأمنية والأكاديمية التي تقدم تعاريف مختلفة لحرب المعلومات، فنجد جزءًا كبيرًا منها يعتمد على تعريف وزارة الدفاع الأميركية لعمليات المعلومات، ومن ثمّ يمكن القول إن المصطلحين فعليًا هما الشيء نفسه، ولكن الاختلاف يحدده السياق الذي يجري استخدامهما فيه.

من خلال استعراض أبرز التعريفات المرجعية لعمليات المعلومات ومتابعة تطورها، يمكن تمييز بعض الخصائص على نحو عام؛ منها أن عمليات المعلومات أو المتعلقة بالمعلومات تتصف بالديناميكية والتغير الذي غالبًا يكون مدفوعًا بالتقدم التقني؛ ما يؤثر في مجال عمليات المعلومات بشكل يجعله أكثر اتساعًا وشمولية. من جانب آخر، تستهدف عمليات المعلومات مجموعةً من القدرات المختلفة - تقنية أو نفسية أو إعلامية – والتي يطلق عليها القدرات المتعلقة بالمعلومات باختلافها. كما يكون استخدام المعلومات في عمليات المعلومات كرسالة، أو وسيلة، أو هدف، أو جميعها معًا مع مراعاة التزامن في أنشطة عمليات المعلومات. وكي توضع عمليات المعلومات في سياق أكثر دقة، تعرف هذه الورقة عمليات المعلومات بأنها: «الاستخدام المتزامن للقدرات المعلوماتية لتحقيق التأثير والتفوق في بيئة المعلومات بأبعادها الإدراكية والمادية والمعلوماتية، والتأثير في المعلومات المعادية والعمليات المبنية على هذه المعلومات وأنظمتها، وفي الوقت نفسه حماية المعلومات والعمليات المبنية عليها وأنظمتها في أوقات السلم والأزمات والحرب».

4. الثورة في الشؤون العسكرية وعمليات المعلومات

في القرنين العشرين والحادي والعشرين، تطورت طبيعة حرب وعمليات المعلومات على نحو أدى إلى إعلان البعض عن ثورة جديدة في الشؤون العسكرية (Revolution in Military Affairs RMA)[20]، لا سيما في المجالات

17 Herbert Lin, "Doctrinal Confusion and Cultural Dysfunction in DoD," *The Cyber Defense Review*, vol. 5, no. 2 (Summer 2020), p. 100.

18 William E. Rohde, "What is Info Warfare?" *US Naval Institute Proceedings*, vol. 122, no. 2 (1996), p. 34.

19 Catherine A. Theohary, "Defense Primer: Information Operations," *Congressional Research Service*, 9/12/2022, accessed on 3/7/2023, at: https://tinyurl.com/55c23wm7

20 Christopher Bellamy, "What is Information Warfare?" in: Ron Matthews & Jack Treddenick (eds.), *Managing the Revolution in Military Affairs* (London: Palgrave Macmillan, 2001), p. 2.

المعنية بالاتصالات الجماهيرية، وتكنولوجيا الاتصالات، وتطبيق تقنيات التسويق للتأثير في جماهير محددة وعامة. انعكس ذلك على الدراسات التي تناولت هذا المجال، حيث ركز بعضها على حرب المعلومات التي تتميز باستخدام تكنولوجيا المعلومات والاتصالات[21]. كما ركزت على عدد من القضايا التي تتراوح من الاستخدام العسكري للتكنولوجيات إلى تداعياتها السياسية والأخلاقية. وتتناول هذه الدراسات المفهوم بشكل متقارب في تعريفه واستخدامه ومجالاته، وترى بأن تهديد حرب المعلومات للأمن القومي يستمد تعقيده وتطور تهديداته من أنظمة الاتصالات والتكنولوجيا المتسارعة في النمو.

ذهبت دراسات أخرى إلى التركيز على مفهوم عمليات المعلومات بتركيز أكثر على الجوانب الفنية والتقنية والإجرائية[22]، واستخدام القدرات ذات العلاقة بالمعلومات في العمليات العسكرية أو الاستراتيجية. تناولت مجموعة أخرى من الدراسات موضوع حرب وعمليات المعلومات بشكل غير مباشر، وانقسمت إلى قسمين، الأول يضم الدراسات التي تناولت موضوع الحرب الهجينة[23]؛ فهناك إجماع لدى عدد كبير من الدراسات التي تناولت هذا الموضوع بأن عمليات المعلومات هي أحد محاور الحرب الهجينة. أما الثاني فيشمل الدراسات التي ركزت على مجال محدد من مجالات عمليات المعلومات[24]، حيث تناولت بتفصيل وعمق المجالات المتخصصة مثل الحرب السيبرانية أو عمليات التأثير والحرب النفسية وغيرها، إما بوصفها شكلًا من أشكال حرب المعلومات وإما عمليات المعلومات وإما بانتمائها إلى أحد محاور الحرب الهجينة.

5. الأسس النظرية لعمليات المعلومات

على الرغم من حداثة مصطلح عمليات المعلومات الذي تم استخدامه أول مرة في العقيدة العسكرية الأميركية في عام 2006، فإن عمليات المعلومات قديمة قدم الحرب نفسها. صحيح أن عمليات المعلومات اكتسبت أهميتها من الثورة الرقمية والتطور التكنولوجي، ولكن حتى قبل وجود تكنولوجيا المعلومات الحديثة أدرك منظرو الحرب أهمية الأساليب التي نسميها الآن حرب المعلومات أو عمليات المعلومات. بالتأكيد كانت أدوات حرب المعلومات مختلفة قبل التقدم التقني الحالي، لكن مفاهيمها موجودة منذ ظهور مفهوم الحرب.

وصف الاستراتيجي والفيلسوف الصيني صن تزو الحرب منذ أكثر من ألفي عام[25]، وفيها العديد من الجوانب التي ندرجها الآن في عمليات المعلومات. يرى صن تزو عمليات المعلومات كوسيلة لتحقيق التفوق في الحرب، وغالبًا ما تقتبس مقولته «القتال والانتصار في كل معاركك ليس تفوقًا كبيرًا؛ التميز الأسمى هو كسر مقاومة

---

21 للاطلاع على بعض هذه الدراسات، يُنظر:
Mariarosaria Taddeo, "Information Warfare: A Philosophical Perspective," *Philosophy & Technology*, vol. 25 (2012), pp. 105–120; Samuel Hamilton et al., "The Role of Game Theory in Information Warfare," in: *4th Information Survivability Workshop: ISW-2001/2002*, Vancouver, 2002; Jill I. Goldenziel & Manal Cheema, "The New Fighting Words? How US Law Hampers the Fight against Information Warfare," *Journal of Constitutional Law*, vol. 22, no. 1 (November 2019), pp. 81 - 170.

22 من هذه المراجع إصدارات وزارة الدفاع الأميركية حول عمليات المعلومات والمنشورات المرجعية التي يطلق عليها (عقيدة عسكرية أو مفهوم العمليات أو إجراءات العمليات)، وهي إصدارات مختلفة تتدرج من المستويات الاستراتيجية إلى العملياتية والتكتيكية، وتشرح استخدامات عمليات المعلومات، وتصدر عن مراكز دراسات تابعة لوزارة الدفاع الأميركية.

23 يُنظر على سبيل المثال:
Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Santa Monica: RAND Corporation, 2017); Dean A Burbridge, *Employing US Information Operations against Hybrid Warfare Threats* (Carlisle: Army War College, 2013); Steven C. Williamson, *From Fourth Generation Warfare to Hybrid War* (Carlisle: Army War College, 2009).

24 يُنظر على سبيل المثال:
Michael Schwille et al., *Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities Between Intelligence and Information Professionals* (Santa Monica: RAND, 2020); William Marcellino, et al., *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations* (Santa Monica: RAND, 2017).

25 صن تزو، فيلسوف ومخطط عسكري استراتيجي صيني. اشتهر بكتاباته التي جُمعت في كتاب **فن الحرب**. من الصعب معرفة متى كُتب بالضبط، لكن يعتقد أنه بين عامي 475 و221 قبل الميلاد.

العدو بدون قتال»[26]. ووفقًا له، كل الحروب هي خداع في جوهرها، وغالبًا ما يجري تصوير «فن الحرب» الخاص به بإشارات إلى ما يمكننا تسميته فقط «حرب المعلومات»[27]. فقد طرح في كتابه خطط التلاعب بالعدو بواسطة المعلومات المقدمة إلى الجواسيس[28]. وقدّر القيم والمصالح والمقارنة العقلانية للسلطة، وأكد أنه على القادة تقييم ومقارنة وحدة الجبهة الداخلية ومعنويات الجيش مع معنويات العدو قبل الشروع في الحملة العسكرية، ويدخل في هذا التقييم فهم تداعيات الأعباء الاقتصادية الحتمية التي تلقيها الحرب على الناس[29].

أصبح المغول، بعد مرور 1500 عام على صن تزو، متفوقين في عمليات المعلومات، فقد استخدموا التجار والسفراء لجمع معلومات عن خصومهم، وقاموا بتوظيف هذه المعلومات في وضع استراتيجيات لا مثيل لها في الحجم حتى القرن العشرين. كما استخدموا الحرب النفسية لتثبيط المقاومة، وتمثل ذلك في استخدامهم الطرق الوحشية في القتل وتدمير المدن لبث الرعب في صفوف أعدائهم، وقد نجحوا إلى حد كبير في ذلك. ومن الأمثلة المبكرة على دور المعلومات في تخطيط مسرح العمليات وأهمية التفوق المعلوماتي في ساحة المعركة لقاء تيمورلنك مع ابن خلدون في دمشق في عام 1401م، عندما دعا ابن خلدون لتزويده بصورة استخبارية عن المغرب لجمع المعلومات اللازمة قبل الغزو، فطلب منه في لقائهما أن يكتب وصفًا تفصيليًا «بحيث إذا قرأه الفاتح بدا وكأنه يرى المنطقة»[30].

يمكن القول إن بدايات التنظير الناضج لعمليات المعلومات بدأت مع كارل فون كلاوزفيتز، فقد خالف منظري عصره الذين اتجهوا إلى دراسة التكنولوجيا العسكرية أو الحرب العلمية وتحليلهما. حاول العلماء، من بينهم عالم الفلك والفيزيائي جاليليو[31] وعالم الرياضيات والمهندس نيكولو تارتاليا[32]، تطوير معادلات من شأنها تحسين قوة المدفعية. وكان المنظر العسكري البارز في القرن السابع عشر سيباستيان لو بريستري دي فوبان Sébastien Le Prestre de Vauban مهندسًا، ولم ينتج هؤلاء كتابات نظرية عن طبيعة الحرب أو دمج الابتكارات التقنية الجديدة في الاستراتيجية، كونهم تقنيين، بل كان الاهتمام فقط بوضع الخطط والصيغ للهجوم الناجح على قلاع العدو وبناء التحصينات وتطوير الأسلحة القادرة على تحقيق النصر في الحرب انطلاقًا من خلفيتهم الهندسية. ولذلك أصبحت دراسة الحرب في عصر النهضة منفصلة عن الأسس النظرية[33]. واستمر التنظير العلمي حتى بلغ ذروته النظرية خلال الثورة الصناعية في كتابات أنطوان هنري دي جوميني. قام جوميني بتحليل حملات نابليون بحثًا عن مبادئ وممارسات الحرب التي لا تتغير. ورأى أن الحرب يمكن بالفعل تنظيمها من خلال قوانين ثابتة تشبه قوانين العلوم والمفاهيم شبه الرياضية تملي التنظيم الصحيح للتشكيلات العسكرية، واتجاه الهجوم وحجمه في «النقطة الحاسمة»[34].

اتجه كلاوزفيتز إلى مخالفة الاتجاه السائد في التنظير العسكري، والتحول بشكل أكبر نحو التركيز على الحرب كظاهرة إنسانية أبدية. ويمكن استنتاج ذلك عند مراجعة أطروحاته في كتابه **عن الحرب** ومقارنتها مع أطروحات

---

26 Sun Tzu, *The Art of War*, Samuel B. Griffith (trans.) (New York: Oxford University Press, 1971), p. 7.

27 Robert E. Neilson (ed.), *Sun Tzu and Information Warfare: A Collection of Winning Papers from the Sun Tzu Art of War in Information Warfare Competition* (Collingdale: Diane Publishing, 1997), p. 126.

28 Ibid., p.143.

29 Tzu, pp. 39-40, 63 - 71.

30 عز الدين عمر، "العالم والسفاح.. ابن خلدون في مواجهة تيمورلنك!"، **الجزيرة نت**، 2021/8/9، شوهد في 2022/3/23، في: https://bit.ly/3NhJngc

31 Jürgen Renn & Matteo Valleriani, "Galileo and the Challenge of the Arsenal," Max Planck Institute for the History of Science, 21/3/2001, accessed on 3/7/2023, at: https://tinyurl.com/4aykrzay

32 Serafina Cuomo, "Niccolò Tartaglia, Mathematics, Ballistics and the Power of Possession of Knowledge," *Endeavour*, vol. 22, no. 1 (1998), p. 32.

33 كارل فون كلاوزفيتز، **عن الحرب**، ترجمة سليم شاكر (بيروت: المؤسسة العربية للدراسات والنشر، 1997)، ص 173 - 174.

34 Antoine-Henri Jomini, George Henry Mendell & William Price Craighill, *The Art of War* (North Chelmsford: Courier Corporation, 2007).

جوميني الذي عاصره والتي قدمها في كتابه **فن الحرب**. يرى كلاوزفيتز أن الحرب ليست عقلانية، ولكنها متقلبة، وليست قابلة للاختزال، ولكنها معقدة؛ باختصار، هي نشاط بشري[35]. وكان مهتمًا على نحو أساسي بالأهداف النهائية للصراع. فقد أصر على الطبيعة السياسية للحرب، ووصف الحرب بأنها «عمل من أعمال القوة لإجبار عدونا على تنفيذ إرادتنا»[36]. من هذا المنطلق، يمكن القول إن الأسس النظرية لعمليات المعلومات باختلاف أداوتها وأساليبها مبنية على الفرضيات التي قدمها ونظمها كلاوزفيتز، وتحوله من دراسة كيفية تحقيق النصر في الصراع باستخدام الوسائل المادية إلى كيفية التحكم وإدارة الصراع بجوانبه المختلفة[37].

تقدم نظرية كلاوزفيتز للحرب رؤية ديناميكية لعمليات المعلومات داخل عالم متعدد المجالات للصراع السياسي وفهم أوضح للديناميكيات التي تملي الدور والتوظيف الظرفي الصحيح لعناصر القوة لتحقيق أهداف عمليات المعلومات، والذي هو فرض إرادتنا على العدو. وكان كتابه عبارة عن محاولة لتطوير نظرية حقيقية للحرب وصفت خصائص النزاع المسلح. أثناء تطوير نظريته، وصف كلاوزفيتز الحرب في سياق الصراع السياسي، الذي يهيمن عليه عاملان هما: العامل المادي، والعامل المعنوي أو النفسي، واللذان يعدان أحد الأركان الأساسية لعمليات المعلومات الحديثة[38]. العلاقة التي يشترك فيها هذان العاملان هي نفسها التي يسعى كُتاب العقيدة العسكرية الحديثة والمنظرون العسكريون والاستراتيجيون لوصفها بمصطلح العمليات العسكرية - باستخدام القوة والنيران - والعمليات المعلوماتية.

تستمد نظريه كلاوزفيتز في عمليات المعلومات قوتها من تحليل العلاقة بين الإرادة السياسية والقوة العسكرية المعبر عنها في العنف، حيث يشير إلى أن قيام الخصم بتنفيذ إرادتنا ليس مجرد عمل عسكري، بل هو أداة سياسية حقيقية، وهي استمرار للحوار السياسي، وتنفيذها بوسائل أخرى[39] ويقصد بالوسائل الأخرى العوامل المادية والمعنوية التي تهدف بالنهاية إلى تحقيق التأثير المطلوب في الخصم، وهي أيضًا أحد محاور عمليات المعلومات ويطلق عليها عمليات التأثير، والتي تعرفها مؤسسة راند بأنها: «التطبيق المنسق والمتكامل والمتزامن للقدرات الدبلوماسية والإعلامية والعسكرية والاقتصادية وغيرها من القدرات الوطنية في أوقات السلم والأزمات والصراع وما بعد الصراع للتأثير في المواقف أو السلوكيات أو القرارات من قبل العناصر أو الكيانات الأجنبية المستهدفة بهدف تعزيز مصالح الولايات المتحدة»[40].

في مستوى آخر، يعتبر كلاوزفيتز القوة العسكرية مزيجًا من جانبين، الأول، الجوانب المادية المتمثلة بالقوة الصلبة التي تشمل الأسلحة والقدرات والجنود الذي يقومون بممارسة العنف المادي. والثاني، الجوانب المعنوية أو النفسية أو الأخلاقية والتي تشمل المعلومات والأفكار والتحكم بها والتأثير فيها في الحرب. من ثمّ، ينشط في الجانب المعنوي الذي يقدمه كلاوزفيتز ما يطلق عليه اليوم عمليات المعلومات والتي تشمل العمليات النفسية والتجسس ومكافحة التجسس والتصدي لدعاية الخصوم وعمليات التأثير. وفقًا له، لا تكفي القوة المادية وحدها؛ لأن القوة المعنوية ضرورية أيضًا لتحقيق النصر. ويمكن كسب المعارك من دون قتال إذا رأى الخصم أن الجانب الآخر أقوى بكثير واستسلم نتيجة لذلك، وهو ما يمكن تحقيقه بواسطة التلاعب بفهم الخصم للموقف. وبحسب نظريته، يمكن تحقيق النصر من خلال التأثيرات النفسية، حيث إن العامل المعنوي أكثر مرونة وقادر على أن ينتشر بسهولة ليؤثر في كل شيء آخر.

---

35 كلاوزفيتز، ص 205. ورد أيضًا في:
Mikkel Vedby Rasmussen, *The Acme of Skill: Clausewitz, Sun Tzu and the Revolutions in Military Affairs* (Amaliegade: Dansk Udenrigspolitisk Institut, 2001), p. 50.

36 كلاوزفيتز، ص 103.

37 المرجع نفسه، ص 174.

38 المرجع نفسه، ص 129، 136.

39 المرجع نفسه، ص 121.

40 Eric V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (Santa Monica: RAND, 2009), p. 2.

6. أبعاد عمليات المعلومات ومجالاتها

ساهمت المؤسسة العسكرية بتطوير مفاهيم عمليات المعلومات، وانعكس ذلك على تطور خصائصها وممارستها. تعد عمليات التحكم في المعلومات قديمة قدم الحرب نفسها، حيث كان الغرض الرئيس من عمليات المعلومات هو تحقيق التأثير المطلوب بوسائل متنوعة غالبًا ما كانت تعتمد على الجوانب النفسية والمعنوية، واستخدام الخداع والتضليل للتأثير في عقل العدو كجزء أساسي من استراتيجيات الحرب لدى صن تزو وكلاوزفيتز. ومع ذلك، فقد كان يُنظر إلى استخدام المعلومات في الماضي على أنه قدرة داعمة، وليس مجالًا في الحرب في حد ذاتها[41]. ومع تطور الأدوات القادرة على تحقيق هذا التأثير، تنوعت مجالات عمليات المعلومات وأدواتها ليجري اعتمادها كإحدى المهمات الرئيسة للجيوش، وأصبحت عمليات المعلومات أكثر وضوحًا حيث تم تحديد الوسائل والأدوات التي يمكن اعتبارها عناصر أساسية في عمليات المعلومات للتحكم في بيئة المعلومات. ونظرًا إلى تطور التكنولوجيا وتطور مفهوم الحرب توسعت البيئة العملياتية لتتجاوز الحدود المادية إلى الحدود الافتراضية أو المعلوماتية، فتحولت المواجهة غير المباشرة أو العدو غير المرئي لتصبح أحد المواضيع التي تتعامل معها الجيوش في العمليات المعلوماتية[42].

وتعد بيئة المعلومات هي ساحة العمليات المعلوماتية، حيث تجري الأنشطة القائمة على المعلومات في الأبعاد المادية والمعلوماتية والإدراكية أو المعرفية. وتشمل عمليات المعلومات مجموعة متنوعة من القدرات ذات العلاقة بالمعلومات التي تعمل لتحقيق التأثير المطلوب في بيئة المعلومات، والتي تتألف من ثلاثة أبعاد رئيسة، وهي النطاق الذي تجري فيه عمليات المعلومات:

أ. البعد المادي

وهو بُعد العالم الحقيقي، حيث تحدث الأنشطة المادية ويتفاعل الأفراد والأمم والثقافات والمجتمعات[43]. ويشمل البعد المادي: البشر، ومرافق القيادة والسيطرة، ووسائط ورقية، وتقنيات المعلومات والاتصالات، مثل أجهزة الاتصالات، وأجهزة الكمبيوتر، والهواتف الذكية، والأجهزة اللوحية، وقدرات البنية التحتية للمعلومات، وقدرات معلومات الخصم، والأنظمة، والمعدات كأبراج الراديو وشبكات الألياف الضوئية وشبكات الهاتف[44]. في هذا البعد، يتم تحقيق أنشطة المعلومات العابرة للحدود واستخدام القدرات ذات العلاقة بالمعلومات لإحداث أضرار مادية معينة أو تعطيل قدرات لدى الخصم[45]، كالهجمات السيبرانية التي شنتها إسرائيل على المفاعل النووي الايراني[46].

ب. البعد المعلوماتي لبيئة المعلومات

وهو مكان حدوث أنشطة المعلومات الإلكترونية، ويشمل الأنظمة والشبكات حيث يجري إنشاء المعلومات، ومعالجتها، ونقلها، ومشاركتها. في هذا البعد يجري جمع المعلومات ومعالجتها وتخزينها ونشرها وحمايتها. ووفقًا لعقيدة عمليات المعلومات الجديدة لحلف الناتو، يُطلق على هذا البعد اسم المجال الافتراضي. وقد تكون هذه الخصائص إلكترونية، أو من إنسان إلى آخر، أو مزيجًا من الاثنين معًا.

---

41 Robert Kozloski, "The Information Domain as an Element of National Power," *Strategic Insights*, vol. 8, no. 1 (2009), p. 9.

42 Ibid.

43 "Allied Joint Doctrine for Psychological Operations (AJP-3.10.1)," *NATO Standardization Office* (September 2014), pp. 1-2

44 Robert Cordray & Marc J. Romanych, "Mapping the Information Environment," *IO Sphere* (2005), p. 7.

45 Joint Chiefs of Staff, Information Operations, p. I-2.

46 Martin Chulov, "Israel Appears to Confirm it Carried out Cyberattack on Iran Nuclear Facility," *The Guardian*, 12/4/2021, accessed on 3/7/2023, at: https://bit.ly/3Mt5Tl5

ج. البعد المعرفي -أو- الإدراكي لبيئة المعلومات

يشمل هذا البعد الخصائص النفسية والثقافية والسلوكية والمعنوية وغيرها من السمات البشرية التي تؤثر في صنع القرار وتدفق المعلومات وتفسير المعلومات من الأفراد أو المجموعات على أي مستوى في دولة أو منظمة[47]. ويشمل هذا البعد، وفقًا لعقيدة الناتو المشتركة، النطاق النفسي وعقول الأفراد الذين ينقلون المعلومات ويستقبلونها ويستجيبون لها أو يتصرفون بناءً عليها. يتأثر هذا البعد بالمعتقدات الفردية والثقافية، والقيم، ونقاط الضعف، والدوافع، والعواطف، والخبرات، والأخلاق، والتعليم، والصحة العقلية، والهويات، والأيديولوجيات. ويعد تحديد هذه العوامل المؤثرة في بيئة معينة أمرًا بالغ الأهمية لفهم أفضل طريقة للتأثير في عقل الجماهير المستهدفة وخلق التأثير المطلوب. ووفقًا لعقيدة عمليات المعلومات المشتركة الأميركية، يعد هذا البعد العنصر الأكثر أهمية في عمليات المعلومات[48].

في هذه الأبعاد الثلاثة لبيئة المعلومات، تعمل القدرات ذات العلاقة بالمعلومات لتحقيق هدفها والتأثير المطلوب منها، سواء كان هذا الهدف للتأثير في الخصوم أو المجتمعات وتشكيل رأي عام يساعد العمل العسكري أو يفقد الخصم الرغبة أو القدرة على المقاومة، أو استهداف وسائل عمليات معلومات للخصم والتأثير فيها وفي عملها.

1. 7. وسائل وأدوات عمليات المعلومات

تعتمد عمليات المعلومات العسكرية على مجموعة من الأدوات التي تحقق أهداف عمليات المعلومات. إن هذه الأدوات قادرة على العمل على نحو منفرد لتحقيق تفوق عسكري، أو غالبًا ما يجري دمجها وتزامنها معًا لتحقيق التأثير المطلوب. وبشكل عام، تعمل هذه الأدوات في أبعاد بيئة المعلومات الثلاثة وترتبط على نحو مباشر بالعمليات العسكرية التقليدية أو العمليات العسكرية الحركية[49]، حيث إنها تسبق العمليات العسكرية كتمهيد سواء بالحصول على المعلومات أو إيصال معلومات معينة، والقيام بعمليات تأثير تجاه الخصم. يمكن تقسيم عمليات المعلومات العسكرية إلى ثلاثة مجالات رئيسة[50]:

أ. عمليات التأثير Influence Operations

يطلق عليها أيضًا مجال العمليات النفسية Psychological Operations، وهي تشمل مجموعة من العناصر والأنشطة غير الحركية Non-Kinetic والمتعلقة بالاتصالات والمعلومات، التي تهدف إلى التأثير في الخصائص المعرفية والنفسية والفكرية والأيديولوجية والأخلاقية للجمهور المستهدف. يجري استخدام «عمليات التأثير» كمصطلح شامل يتضمن مجموعة الأنشطة العسكرية مثل عمليات المعلومات، والدبلوماسية الدفاعية، والأنشطة الإعلامية العسكرية، وأنشطة الاستخبارات، والعمليات النفسية. وتعرف بأنها «التطبيق المنسق والمتكامل والمتزامن للقدرات الدبلوماسية والإعلامية والعسكرية والاقتصادية وغيرها من القدرات

---

47 Joint Chiefs of Staff, Information Operations, p I-3.

48 Ibid.; "Allied Joint Doctrine for Psychological Operations," p. I-2.

49 يقصد بالعمليات العسكرية الحركية العمل العسكري الذي يشمل الحرب النشطة بالقوة النارية التقليدية، بما في ذلك القوة المميتة. تستخدم العبارة للمقارنة بين القوة العسكرية التقليدية والقوة العسكرية الناعمة أو غير الحركية. وقد استخدم وزير الدفاع الأميركي دونالد رامسفيلد Donald Rumsfeld كلمتي "حركي" و"غير حركي" في كثير من الأحيان للتعبير عن الحرب التي تشن من دون معدات قتالية. أمّا الأنشطة غير الحركية Non-Kinetic Actions، فهو مصطلح عسكري غربي يقصد به أنشطة عسكرية تستهدف قوات العدو من دون استخدام القدرات القتالية النارية. هذه الأنشطة قد تكون نفسية، أو سلوكية، أو كهرومغناطيسية، أوسيبرانية، أو هجمات على شبكات الكمبيوتر أو أنظمة العدو. والمصطلح غير مستخدم في المراجع العربية العسكرية بشكل رصين، لكن في الأدبيات الغربية فهو مصطلح متفق عليه ويستخدم على نحو منتظم. للمزيد يُنظر:
Timothy Noah, "Birth of a Washington Word," *Slate*, 20/11/2002, accessed on 3/7/2023, at: https://bit.ly/3v7yma6

50 Larson, p. 2.

الوطنية في أوقات السلم والأزمات والصراع وما بعد الصراع لتعزيز المواقف أو السلوكيات أو القرارات من قبل الجماهير المستهدفة»[51].

ب. الحرب الإلكترونية والأنشطة الكهرومغناطيسية Electronic Warfare and Electromagnetic Activities

هي أنشطة عسكرية تتضمن استخدام الطاقة الكهرومغناطيسية والطاقة الموجهة للتحكم في الطيف الكهرومغناطيسي أو لمهاجمة الخصم[52]. تساهم الحرب الإلكترونية في نجاح عمليات المعلومات باستخدام التكتيكات والأساليب الهجومية والدفاعية في مجموعات متنوعة لتشكيل وتعطيل واستغلال الاستخدام العدائي للطيف الكهرومغناطيسي مع حماية التصرف في هذا الطيف. ويمنح الانتشار المتزايد للاتصالات اللاسلكية واستخدام الكمبيوتر فرصةً وتهديدًا من منظور الحرب الإلكترونية في عمليات المعلومات، ويمكن استغلال نقاط الضعف الإلكترونية للخصم وحماية المنظومات من التهديدات المحتملة، وفي الوقت نفسه حماية تعرض أنظمة الحرب الإلكترونية للاستهداف. ونظرًا إلى انتشار استخدام الطيف الكهرومغناطيسي في العمليات العسكرية، تشارك الحرب الإلكترونية في جميع جوانب عمليات المعلومات على نحو مباشر أو غير مباشر[53].

ج. العمليات السيبرانية Cyber Operations

تعتمد معظم جوانب العمليات المشتركة جزئيًا على الفضاء السيبراني ضمن بيئة المعلومات. ويتكون هذا الفضاء من شبكة مترابطة من البيانات والمعلومات والبنى التحتية لتكنولوجيا المعلومات، وتشمل الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم. ويقصد بعمليات الفضاء السيبراني توظيف قدراته لتحقيق الأهداف في -أو- من خلال هذا الفضاء نفسه[54]. وتخلق أنشطة الفضاء السيبراني وقدراته تأثيرات في بيئة المعلومات لدعم العمليات العسكرية. وتشمل هذه الأنشطة والقدرات، على سبيل المثال لا الحصر، جمع المعلومات، والاستفادة منها للتأثير في القرارات، ودعم عمليات المعلومات العسكرية، والخداع العسكري، وتغيير سلوك العدو. ويمكن القيام بها على نحو مستقل أو متزامن ومتكامل وغير متعارض مع الأنشطة والعمليات الأخرى[55].

ثانيًا: الاستراتيجية الروسية من الحرب التقليدية إلى الحرب غير التقليدية

أمضى الخبراء الروس خلال التسعينيات من القرن العشرين وقتًا وجهدًا في تطوير مفاهيم بديلة من الحرب التقليدية، بما في ذلك نظريات عمليات المعلومات. ومع ذلك، استمرت العقيدة الغربية، وبخاصة العقيدة العسكرية الأميركية، في تشكيل الاتجاه العام للفكر العسكري الروسي حول كيفية إجراء عمليات من دون عتبة النزاع المسلح التقليدي[56]. ومنذ منتصف التسعينيات وحتى أوائل العقد الأول من القرن الحادي والعشرين، ألهمت مبادئ عملية «عاصفة الصحراء» ودروسها[57]، والحملة الجوية لحلف الناتو في يوغوسلافيا، الاستراتيجيين

---

51 Ibid., pp. 2 - 3.

52 Joint Chiefs of Staff, "Cyberspace Operations," Joint Publication (JP 3-12), Washington, DC: Department of Defense, 2018, p. II-4, accessed on 28/8/2023, at: https://bit.ly/3L8AeF3

للمزيد حول الحرب الإلكترونية، يمكن الرجوع إلى عقيدة الجيش الأميركي المشتركة للحرب الإلكترونية، ينظر:
Joint Chiefs of Staff, "Joint Doctrine for Command and Control (C2W)."

53 Ibid.

54 Joint Chiefs of Staff, "Cyberspace Operations," p. I-1.

55 Ibid., p. I-7.

56 Jānis Bērziņš, "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria," *The Journal of Slavic Military Studies*, vol. 33, no. 3 (2020), p. 380.

57 عاصفة الصحراء هي اسم العملية العسكرية في المرحلة الثانية من حرب الخليج الثانية (تحرير الكويت)، في الفترة 17 كانون الثاني/ يناير - 28 شباط/ فبراير 1991.

العسكريين الروس؛ ما ساعد اللواء فلاديمير سليبشينكو Vladimir Slipchenko في تقديم نظريته عن حرب الجيل السادس أو «الحرب غير المتصلة»[58]، وهي مفاهيم حديثة تهدف إلى تحقيق تفوق عسكري من خلال الوسائل غير التقليدية. يمكن اعتبار هذا السلوك الروسي تغييرًا في الأسلوب العسكري، وطريقة روسيا لإدارة الصراع، ونهجًا جديدًا في الاستراتيجية الدفاعية الروسية التي بدأت تنظيريًا بعد انهيار الاتحاد السوفياتي، وعمليًا مع أزمة شبه جزيرة القرم في عام 2014.

1. الأسلوب الروسي في عمليات المعلومات

في العقد الأول من القرن الحادي والعشرين، ألهمت عقيدة الجيش الأميركي عن حروب الشبكات[59] تطورات مماثلة في الفكر العسكري الروسي. وابتداءً من عام 2008، قام الخبراء العسكريون الروس، وعلى الأخص سيرجي تشيكينوف Sergey Chekinov وسيرجي بوجدانوف Sergey Bogdanov[60]، بدمج هذه المفاهيم في نهج واحد: حرب الجيل الجديد New Generation Warfare. يمكن وصف حرب الجيل الجديد كمفهوم بأنه سلسلة متصلة من التأثيرات بكثافة متفاوتة ومراكز ثقل[61] متغيرة. في هذا المفهوم، يجري تنفيذ أنشطة مستمرة لإضعاف استقرار المجتمعات المستهدفة وعزلها وزعزعتها، يليها المزيد من الأعمال العسكرية التقليدية إذا لزم الأمر. اعتمدت العمليات الروسية في شبه جزيرة القرم وشرق أوكرانيا على نحو أساسي على هذه الأطروحات والمبادئ الأساسية لحرب الجيل الجديد.

من خلال مراجعة عقيدة أمن المعلومات الروسية لعام 2000[62]، واستراتيجية الحرب الإلكترونية لعام 2011[63]، والعقيدة العسكرية للجيش الروسي لعام 2014[64]، يمكن التعرف إلى جوانب أهداف عمليات المعلومات الروسية وأهميتها وطبيعتها وخصائصها، وكيف يمكنها أن تتناسب مع التفكير الاستراتيجي الروسي الشامل. جرى تلخيص أهداف العمليات المعلوماتية الروسية على أنها تشويش القدرات العسكرية والصناعية والإدارية الرئيسة في الدول المستهدفة أو تعطيلها، فضلاً عن ممارسة الضغط النفسي والإعلامي للتأثير في خصومهم من خلال استخدام تقنيات المعلومات، بما في ذلك برامج الكمبيوتر المتطورة والتكنولوجيا[65] وروبوتات وسائل التواصل الاجتماعي[66]. ويشير ستيفن بلانك إلى أن الأدوات الروسية والغربية لعمليات المعلومات متشابهة، إلا أن هناك اختلافًا كبيرًا في طريقة توظيفهم هذه الأدوات[67].

---

58 B□rzi□š, p. 380.

59 "The Implementation of Network-Centric Warfare," Office of Force Transformation, Transformation Report, 5/1/2005, accessed on 3/7/2023, at: https://tinyurl.com/2j5ardkn

60 Yuriy Danyk, Tamara Maliarchuk & Chad Briggs, "Hybrid War: High-Tech, Information and Cyber Conflicts," *Connections*, vol. 16, no. 2 (2017), pp. 5 - 24.

61 مركز الثقل هو مفهوم عسكري طوره كارل فون كلاوزفيتز، وهو بحسب تعريف الجيش الأميركي "مصدر قوة الخصم الذي يوفر القوة المعنوية أو المادية، أو القدرة على العمل العسكري بحرية، أو الإرادة للعمل". ومن ثمّ، يُنظر إلى مركز الثقل عادةً على أنه "مصدر قوة الخصم" الذي عند حرمانه منه يفقد القدرة على مواصلة العمل العسكري.
Joint Chiefs of Staff, "Dictionary of Military and Associated Terms," Joint Publication, no. 1-02, 15/2/2010, p. 29, accessed on 3/7/2023, at: https://bit.ly/38hcb8j

62 "Information Security Doctrine of the Russian Federation," United Nations International Telecommunications Union Archive (2000), accessed on 28/8/2023, at: https://tinyurl.com/44duj852

63 Marius Kristiansen & Njaal Home, "Small Players in a Limitless Domain: Cyber Deterrence as Small State Strategy," *Comparative Strategy*, vol. 41, no. 1 (2022), p. 25.

64 "The Military Doctrine of the Russian Federation," *President of the Russian Federation* (December 2014), accessed on 28/8/2023, at: https://tinyurl.com/36fsjcuw

65 Salahudin Ali, "Coming to a Battlefield Near You: Quantum Computing, Artificial Intelligence, & Machine Learning's Impact on Proportionality," *Santa Clara Journal of International Law*, vol. 18 (2020), p. 1.

66 Bazylev Dylevsky, S.A. Komov & A.N. Petrunin, "The Russian Armed Forces in the Information Environment: Principles, Rules, and Confidence-Building Measures," *Military Thought*, vol. 21, no. 2 (2012), p. 10.

67 Stephen Blank, "Cyber War and Information War a La Russe," in: George Perkovich & Ariel E. Levite (eds.), *Understanding Cyber Conflict: 14 Analogies* (Washington, DC: Georgetown University Press, 2017), p. 82.

ينبع الاهتمام الروسي بعمليات المعلومات من منطلق علاقتها بالحرب الهجينة الذي تبنته روسيا ضمن نهج حرب الجيل الجديد. وساهم رئيس هيئة الأركان العامة للقوات المسلحة الروسية فاليري جيراسيموف Valery Gerasimov، الذي عُيّن في تشرين الثاني/ نوفمبر 2012، في تبنّي الجيش الروسي مفاهيم الحرب الهجينة وعمليات المعلومات الروسية وأدواتها، التي يعتقد البعض أنها طُبقت أول مرة في أوكرانيا في عام 2014[68]. وقد اشتمل المنهج الروسي في عمليات المعلومات على أدوات وأساليب مثل الإجراءات الفعالة[69]، والتحكم الانعكاسي[70]، التي تندرج ضمن عمليات التأثير في عمليات المعلومات وفق أسلوب روسيا في الجيل الجديد من الحروب.

2. استراتيجية التحكم الانعكاسي في حروب الجيل الجديد الروسية

تبنت روسيا نهجها في حروب الجيل الجديد على نحو واضح ضد أوكرانيا، والذي يعتمد على مفهوم روسيا لعمليات المعلومات. ولا تعد عمليات المعلومات الروسية حرب معلومات كما تعتقد الولايات المتحدة، بل هي جزء من أسلوب روسيا في الحرب الهجينة، الذي يتكون من حملة تضليل متعمّدة مدعومة بإجراءات من أجهزة المخابرات ومصممة لإرباك العدو وتحقيق ميزة استراتيجية بأقل تكلفة. تجعل طبيعة العمليات الهجينة من الصعب جدًا اكتشافها أو حتى تحديد بدايتها، نظرًا إلى أن إرباك العدو هو أحد مكوناتها الأساسية. ومع ذلك، فقد أصبح من الواضح أن روسيا تستخدم تقنيات عمليات المعلومات لدعم جهود الحرب الهجينة لتحقيق أهدافها الحالية، والمتمثلة في تنازل كييف عن الوضع القانوني الخاص للمناطق التي يسيطر عليها الانفصاليون في شرق أوكرانيا. ولتحقيق التأثير المطلوب في عمليات معلوماتها، لجأت روسيا إلى تطبيق أدوات التحكم الانعكاسي في مناطق الصراع كأداة رئيسة من أدوات عمليات التأثير في حرب الجيل الجديد التي تنتهجها.

مفاهيم وأدوات التحكم الانعكاسي في عمليات التأثير الروسية Reflexive Control in Influence Operations، هي نفسها التي استخدمها الاتحاد السوفياتي، ولكن مع السياق الجيوسياسي المعاصر. يُعرَّف تيموثي توماس «التحكم الانعكاسي» بأنه وسيلة لنقل معلومات معدة خصيصًا لشريك أو خصم لحثه على اتخاذ القرار المحدد مسبقًا بشكل طوعي»[71]. بعبارة أخرى، هي طريقة يمكن من خلالها للطرف المسيطر أن يؤثر في الخصم لاتخاذ قرارات سيئة عن غير قصد من خلال التدخل في تصوراته[72]. ويشير توماس إلى أنه في سياق الحرب، يكون لدى اللاعب الأكثر قدرة على التنبؤ ومحاكاة منطق خصمه وأفعاله احتمالية أعلى للنجاح[73]. وكتب فلاديمير لوفيفر Vladimir Lefebvre، أحد العلماء السوفيات البارزين في مجال التحكم الانعكاسي، «أنه

---

68 Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," In Moscow's Shadows, 6/7/2014, accessed on 4/7/2023, at: https://bit.ly/3OsFkOC

69 كان مصطلح "الإجراءات الفعالة" يشير إلى العمليات الخادعة التي أجريت لدعم السياسة الخارجية السوفياتية. والهدف من "التدابير الفعالة" هو التأثير في آراء الأفراد والحكومات والمجتمعات وأفعالها. والخداع هو جوهر "الإجراءات الفعالة". وفي الاتحاد السوفياتي، كان تنفيذ "التدابير الفعالة" من مسؤولية جهاز المخابرات الروسي، "كي جي بي" KGB، وكان جميع الوكالات والممثلين السوفيات في الخارج متاحين لدعم هذه الحملات أو المشاركة فيها. وتضمنت الأساليب التضليل والتزوير (محاولات متعمدة لخداع الرأي العام أو الحكومة من خلال تزوير الحقائق أو الوثائق). إضافة إلى ذلك، تم دمج الكنيسة الأرثوذكسية الروسية ماليًا وهيكليًا في جهاز الدعاية الخارجية السوفياتي لدعم تنفيذ "الإجراءات الفعالة". للمزيد حول هذه الإجراءات، ينظر:
Fletcher Schoen & Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," *Strategic Perspectives*, no. 11 (2012).

70 لتحليل الحملة الإعلامية الروسية ضد أوكرانيا، يتعين الرجوع إلى مفهوم التحكم الانعكاسي، وهو موضوع تمت دراسته في الاتحاد السوفياتي وروسيا نحو 50 عامًا. والمفهوم قريب من حيث المعنى إلى مفهوم التأثير النفسي. ويمكن القول إن الحملة الإعلامية الروسية ضد أوكرانيا، والتي تتماشى جيدًا مع الإجراءات على الأرض، كانت مظهرًا من مظاهر السيطرة الانعكاسية. وخلال حملة أوكرانيا، مارست روسيا سيطرة ناجحة على وسائل الإعلام واستخدمت ضعف الحكومة في كييف وعدم قدرتها على الوصول إلى سكان شبه جزيرة القرم والمناطق الشرقية. استكمل هذا الجهد الروسي لتشويه سمعة الحكومة الأوكرانية كجزء من خطة السيطرة الانعكاسية. للمزيد ينظر:
Thomas Timothy, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies*, vol. 17, no. 2 (2004), pp. 237 - 265.

71 Ibid., p. 237.

72 Thomas Timothy, "Russian Views on Information-Based Warfare," *Airpower Journal Special Edition* (1996), p. 32.

73 Timothy, "Russia's Reflexive Control Theory and The Military."

يجري استخدام المعلومات حول منطقة الصراع، وعن قدرات القوات المقاتلة، وكفاءتها القتالية، وما إلى ذلك، من أجل اتخاذ القرارات في المعركة. وسيجعل التأثيرُ في هذه المعلومات وإرسال الرسائل والتحكم أو التلاعب في تدفق المعلومات الخصمَ يتخذ قرارات مرسومة له مسبقًا»[74].

3. الاختلاف بين المنظور الغربي والروسي في عمليات المعلومات

يكمن الاختلاف الرئيس بين المفاهيم النظرية الغربية لعمليات المعلومات وعمليات المعلومات الروسية في طريقة استخدامها لإدارة الصراع. فكما تمت الإشارة سابقًا، إن الغرض الرئيس لعمليات المعلومات وفق المنظور الغربي هو التأثير في الخصم لحسم الصراع أو احتوائه في مراحله الأولى، في حين أن عمليات المعلومات الروسية تهدف إلى إطالة أمد النزاع من خلال دعم أحد الأطراف المتحاربين بطريقة تمنح روسيا القدرة على التأثير في النزاع على نحو أكثر حسمًا في الوقت الذي تختاره، وربما السعي لتغيير النظام[75].

يقدم مارك جالوتي تحليلًا لمفهوم روسيا للحرب الهجينة، والذي يلقي نظرة على التصور الروسي لمفهوم عمليات المعلومات[76]؛ إذ يشير إلى أن روسيا مدركة لتفوق الولايات المتحدة، وحتى الصين، عسكريًا. ومن ثمّ تتجنب روسيا المواجهة العسكرية المباشرة[77]. وعلى الرغم من الاستعداد الروسي، وفي ظل قيود الموارد الحالية، يدرك الجيش الروسي أنه سيخسر أي مواجهة أو حرب عالمية بقدراته الحالية وفي وضع الحرب التقليدية. ومن ثم، فإن الجيش الروسي يعوض ضعفه النسبي باستراتيجيات غير مباشرة ودقيقة تهدف إلى إرباك العدو، فتركز روسيا بشدة على عمليات المعلومات. وعندما نقارن القوات الخاصة الروسية مع القوات الأميركية، والاختلاف الشاسع في القدرات والخبرة بينهما، نجد زيادة في التركيز والاعتماد على العمليات المعلوماتية في العقيدة العسكرية الروسية[78].

كما يعتقد جالوتي بأن أنماط الحرب غير الحركية ستؤدي دورًا رئيسًا في تحقيق الأهداف السياسية والاستراتيجية لروسيا بكفاءة أكثر من الأسلحة العسكرية، وأن أي عمل عسكري مباشر سيكون مدعومًا بالاستخدام الفعال للمعلومات المضللة وقوات العمليات الخاصة. وعلى حد تعبير بيدريتسكي، «لن تشكل العمليات العسكرية سوى جزء صغير وليس أهم جزء من العمليات المعلوماتية»[79] من أجل تحقيق النجاح النهائي في الصراع. وقد استخدمت روسيا هذا التكتيك في ضم شبه جزيرة القرم في عام 2014 عندما أنكرت عمليات مجموعة الرجال الخضر الصغار[80]، وهي قوات خاصة روسية، جرى الكشف عنها بعد أن تم ضم شبة جزيرة القرم فعليًا[81].

في كتابه عن التضليل السوفياتي، أشار ضابط المخابرات السوفياتي السابق أيون ميهاي إلى أن حملة جهاز المخابرات الروسي النموذجية تتضمن دائمًا إنكار تورطها المباشر. كما يشير إلى أن حملة التضليل الثلاثية

---

74 Clifford Reid, "Reflexive Control in Soviet Military Planning," in: Brian Dailey & Patrick Parker (eds.), *Soviet Strategic Deception* (Pennsylvania: Lexington Books, 1987), p. 294.

75 V.I. Yevdakov, "Characteristic Features and Peculiarities of Wars at the Start 21st Century," *Journal of the Academy of Military Sciences*, no. 3 (2008), p. 24.

76 Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War."

77 Ibid.

78 Aarne Ermus & Karl Salum, "Changing Concepts of War: Russia's New Military Doctrine and the Concept of Hybrid Warfare," *The Estonian Military Academy*, no. 7 (2017), p. 63.

79 A.V. Bedritsky, "Information War: Concepts and their Realization in the USA," *RISI* (2008), p. 187.

80 إشارةً إلى الجنود الملثمين من الاتحاد الروسي الذين ظهروا خلال الحرب الروسية - الأوكرانية في 2014، وكانوا يرتدون الزي العسكري الأخضر غير المميز ويحملون أسلحة ومعدات عسكرية روسية حديثة. وظهر المصطلح أول مرة خلال ضم الاتحاد الروسي لشبه جزيرة القرم، من نهاية شباط/ فبراير إلى آذار/ مارس 2014.

81 Kathy Lally, "Putin's Remarks Raise Fears of Future Moves against Ukraine," *The Washington Post*, 17/4/2014, accessed on 4/7/2023, at: https://cutt.ly/kGuMs4H

الأبعاد في عمليات المعلومات الروسية تتبع بدقة «قواعد كي جي بي الثلاثة لتخفيف حدة الأزمة السياسية التي قد تتعرض لها روسيا، وهذه القواعد هي: رفض الربط الذي يثبت التورط المباشر في الأزمة، وتقليل الضرر، وعندما تظهر الحقيقة، يصر على أن العدو كان مخطئًا»[82].

ثالثًا: عمليات المعلومات الروسية في الأزمة الروسية – الأوكرانية 2022

تعد الأزمة الأوكرانية – الروسية أزمةَ عمليات معلومات بامتياز؛ فمن جهة تقوم روسيا بحملة منظمة منذ عام 2014 تجاه أوكرانيا والدول التي قد تقع تحت تأثير دول الناتو من جمهوريات الاتحاد السوفياتي السابقة. ومن جهة أخرى، تقود أوكرانيا والولايات المتحدة والدول الغربية حملة عمليات معلومات مضادة أدت في عدة حالات إلى تقييد التحركات العسكرية الروسية على الحدود الأوكرانية من خلال تسريبات استخباراتية مقصودة لوضع روسيا تحت ضغط دولي. وقد ساهمت عمليات المعلومات على نحو مباشر في التأثير في العمل العسكري الميداني، وقدمت هذه الأزمة مؤشرات لتقييم نتائج تصادم النموذجين الغربي والروسي واختبارهما في تطبيق المفاهيم النظرية لعمليات المعلومات ومدى كفاءتها لتحقيق التفوق في العمليات العسكرية.

1. خلفية الأزمة الأوكرانية

منذ انهيار الاتحاد السوفياتي في عام 1990، سعت روسيا لإعادة تموضع نفسها في محيطها الإقليمي واستعادة مكانتها ضمن القوى العظمى العالمية. وتسعى الإدارة الروسية الحالية وفق مجموعة من السياسات التي تهدف إلى إعادة تموضع روسيا ضمن القوى العظمى واستعادة إرث الاتحاد السوفياتي. ولتحقيق هذا الهدف، كانت تتحدى الأحادية الأميركية، وتحاول إنشاء مناطق نفوذ، وخلق عمق استراتيجي، وتغيير أطر الأمن والدفاع العالمية الحالية من خلال تطبيق الأدوات السياسية والاقتصادية والثقافية والنفسية وغيرها من الأدوات غير الحركية. وظهرت هذه التوترات الأكثر عدوانية في السياسة الروسية لأول مرة علانية في شباط/ فبراير 2007، عندما ألقى الرئيس الروسي فلاديمير بوتين خطابه الشهير في ميونيخ[83]. في هذا الخطاب، أكد أن روسيا لن تقبل بعد الآن النموذج أحادي القطبية الذي تقوده الولايات المتحدة للعلاقات الدولية، وأن روسيا ستنفذ سياستها الخارجية المستقلة لتحقيق مصالحها الجيوسياسية، وظهر ذلك بوضوح في الحرب الروسية - الجورجية في عام 2008، وفي تدخلات روسيا في سورية وأوكرانيا.

منذ استعادة استقلالها عن الاتحاد السوفياتي في عام 1990، تعرضت أوكرانيا لضغوط روسية مستمرة[84]. وتتمثل إحدى الطرق التي تجلت فيها هذه الضغوط في التهديد العسكري التقليدي، الذي تخللته مناورات عسكرية واسعة النطاق على طول حدودها وإنشاء القواعد العسكرية [85]، ودعم أقاليم تسعى للانفصال في شرق أوكرانيا، والتصرف العام للقوات العسكرية الروسية في المنطقة العسكرية الحدودية بين البلدين[86].

---

82 Ion Mihai Pacepa & Ronald J. Rychlak, *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism* (Chicago: WND Books, 2013), p. 329.

83 Ted Galen Carpenter, "Did Putin's 2007 Munich Speech Predict the Ukraine Crisis?" Cato Institute, 24/1/2022, accessed on 4/7/2023, at: https://bit.ly/3OvoheG

84 "Lithuania Rejects Soviet Demand to Renounce its Independence," *History*, accessed on 4/7/2023, at: https://bit.ly/3k08u9X

85 Sandrine Amiel, "Russia's Military Build-up near Ukraine is Different this Time, Say Experts," *Euro News*, 6/12/2021, accessed on 4/7/2023, at: https://bit.ly/37wlRw1

86 "EU Foreign Affairs Chief: 100,000 Russian Troops at Ukraine Border," *Euro News*, 20/4/2021, accessed on 4/7/2023, at: https://bit.ly/3LlwKiw

بدأت الأزمة الأوكرانية - الروسية كعمليات معلومات عسكرية قبل أن تتحول لمواجهة عسكرية، ويمكن القول إن تعامل أوكرانيا مع عمليات المعلومات الروسية منذ احتلال القرم ساهم في تقييد الحملة الروسية في عام 2022، حيث أنشأت أوكرانيا مركزًا متكاملاً للتعامل مع عمليات المعلومات الروسية، كما أشرنا سابقًا. يقوم المركز بمتابعة الحملة المعلوماتية الروسية ودحضها أو تفنيدها بأسلوب يحاكي تعقيدات عمليات المعلومات الحديثة ويؤثر في أهداف الحملة المعلوماتية الروسية بدرجة كبيرة.

في سياق الأزمة الأوكرانية، نفت روسيا مرارًا وجود عمليات عسكرية روسية في أوكرانيا منذ بداية الصراع. ويمكن الإشارة إلى أسلوب روسيا في التضليل على أنه نسق مستمر ضمن أسلوبها في عمليات المعلومات، حيث رد وزير الخارجية الروسي سيرجي لافروف في كانون الثاني/ يناير 2015 بعدم وجود أدلة وحقائق تؤيد اتهام القوات الروسية بأنها كانت في أوكرانيا[87]. وفي الوقت نفسه، تُظهر تسريبات وتقارير تؤكد التدخل العسكري الروسي[88].

من الصعوبة فهم استراتيجية روسيا في أوكرانيا، حيث كان الغزو الروسي لأوكرانيا في البداية يهدف إلى إسقاط نظام الرئيس، فولوديمير زيلينسكي، ونزع سلاح أوكرانيا، وإجبارها على الاعتراف بضم روسيا لشبه جزيرة القرم واستقلال منطقتي دونيتسك ولوهانسك، من أجل إنشاء «حزام» جنوبي شرقي يربط شبه جزيرة القرم وترانسنيستريا. وقد دعا بوتين القيادات العسكرية في أوكرانيا إلى القيام بانقلاب وتسلم السلطة في إشارة إلى أن الهدف الروسي هو تغيير النظام السياسي. بمعنى، أن هدف موسكو هو تدمير القدرات العسكرية الأوكرانية، والسيطرة على جنوب أوكرانيا، والمدن الكبرى شرق نهر الدنيبر، والعاصمة كييف، من خلال «عملية عسكرية سريعة»، ومن ثمّ انهيار الإرادة السياسية للقيادة الأوكرانية والموافقة على توقيع اتفاق استسلام مع موسكو وفق الشروط الروسية؛ دون تدخل من القوى الغربية أو المجتمع الدولي. ويؤكد هذا ما أشار إليه وليام بيرنز William Burns، رئيس وكالة الاستخبارات المركزية «سي آي آيه» CIA، من أن الخطة الروسية للحرب في شباط/ فبراير 2022 كانت تستهدف السيطرة على كييف خلال يومين من بدء الغزو[89].

تشمل أهداف روسيا منع انضمام أوكرانيا إلى الناتو والاتحاد الأوروبي، إلى جانب تأمين درجة معينة من السيطرة على صنع السياسة الأوكرانية[90]. وتحاول تحقيق هذا من خلال المطالبة بفدرالية لأوكرانيا، أو منح المناطق التي يسيطر عليها الانفصاليون في دونيتسك ولوهانسك وضعًا خاصًا. لا يمثل هذا الفهم للأهداف الروسية في أوكرانيا سوى تقييم؛ لأن روسيا تحاول عمدًا إخفاء أهدافها لتظل مرنة، وتحافظ على الخيارات، وتشوش خصومها. ولكن مع وضع هذا الفهم في الاعتبار، يمكن تقسيم تطبيق روسيا لهذه الأهداف إلى مقاربتين دبلوماسية وعسكرية.

2. الاختلاف بين الأسلوبين الروسي والغربي في عمليات المعلومات

تعد روسيا من أكثر الدول استخدامًا لقدرات المعلومات في تحقيق أهدافها الاستراتيجية، والتي بدت واضحة في الأزمة الروسية - الأوكرانية. في المقابل، تتعامل أوكرانيا، وبدعم من القوى الغربية، مع عمليات المعلومات

87 Gabriela Baczynska, "Russia Says No Proof it Sent Troops, Arms to East Ukraine," *Reuters*, 21/1/2015, accessed on 4/7/2023, at: https://cutt.ly/UGuMXmn

88 Maksymilian Czuperski et al., "Hiding in Plain Sight: Putin's War in Ukraine," Atlantic Council, 14/9/2015, accessed on 4/7/2023, at: https://bit.ly/3ELUEBt

89 "الحرب الأوكرانية في شهرها الثاني: تبعات ثقيلة ومتغيرات مديدة"، مركز الجزيرة للدراسات، 2022/3/27، شوهد في 2023/7/4، في: https://bit.ly/3K2xXdb

90 "حسابات واشنطن في أوكرانيا ومحاولات احتواء روسيا"، **تقدير موقف**، المركز العربي للأبحاث ودراسة السياسات، 2022/3/3، شوهد في 2023/7/4، في: https://tinyurl.com/yau7y7tm

الروسية على نحو مكثف منذ احتلال روسيا لشبة جزيرة القرم في عام 2014. ومن ثمّ، نشأ نموذجان في تطبيق عمليات المعلومات يمكن تسميتهما بعمليات المعلومات الهجومية (الروسية)، وعمليات المعلومات المضادة أو الدفاعية من أوكرانيا وحلفائها. وقد أدّى هذا الصدام إلى ظهور اختلاف في تطبيق الأسس النظرية لعمليات المعلومات في العمليات العسكرية بين روسيا من جانب، وأوكرانيا وحلفائها من جانب آخر.

تناولت العديد من الدراسات النشاط الروسي في أوكرانيا ودول البلطيق، وغطت جوانب الحرب الباردة والثورات الملونة، والحرب الروسية - الجورجية في آب/ أغسطس 2008، والغزو الروسي لجزيرة القرم في عام 2014. وقدمت بعض هذه الدراسات تفسيرات حول الأسلوب الروسي في فرض النفوذ والتأثير، واستعادة إرث الاتحاد السوفياتي. ويمكن رصد مواجهة بين جميع الأطراف في بيئة المعلومات، سواء بالتصريحات أو التصريحات المضادة أو التسريبات الاستخباراتية لوسائل الإعلام أو محاولة شيطنة الخصم أو شرعنه العمل العسكري.

يميز أسلوب عمليات المعلومات الروسية التداخل بين المجالين السياسي والعسكري؛ فالحكومة الروسية تستخدم مفاهيم عمليات المعلومات ومبادئها في الحملة السياسية والإعلامية المصاحبة لعملياتها العسكرية في أوكرانيا، والتي تعتمد على الإنكار المستمر بالتركيز على العمليات النفسية وعمليات التأثير؛ لتسهيل أنشطة قواتها في أوكرانيا ولفرض مزيدٍ من التعقيد على صناع القرار في أوكرانيا وحلفائها. على سبيل المثال، تسلَّمت إدارة الرئيس الأميركي جو بايدن معلومات تتعلق بمخطط للحشد الروسي حول أوكرانيا منذ أيلول/ سبتمبر 2021، قبل انتشار التقارير التي أكدت وجود تلك الحشود[91]. وكان الرد الروسي أن هذا الحشد العسكري يقوم بإجراء تمارين عسكرية روتينية[92]. وشهدت الفترة من أيلول/ سبتمبر 2021 حتى شباط/ فبراير 2022 تغطية إعلامية مدعومة بتقارير استخباراتية أو من شخصيات سياسية شكلت مواجهة معلوماتية بين أطراف الصراع، ما منح ميزة لروسيا في عدم معرفة أهدافها الحقيقية وفق استراتيجيتها في التضليل، حيث يجري وضع الخصم في موقف غير يقيني أو حاسم. اعتمدت استراتيجية عمليات المعلومات الروسية في البداية على الإنكار المستمر للوجود العسكري الروسي من أجل الحصول على مساحة أكبر لإدارة الأزمة[93]. وفي الوقت نفسه، هدفت إلى تقويض الحماس الغربي للمشاركة المباشرة في الأزمة الأوكرانية[94]. ومن المرجح أن التذكير بقدراتها النووية سواء من قبل سياسيين أو وسائل إعلامية روسية، يخدم الغرض نفسه؛ وهو تصوير تصرفات الحكومة على أنها غير متوقعة، واستخدام القوة المعلوماتية لردع العدو عن تصعيد الصراع[95].

على المستوى العسكري، تسمح عمليات المعلومات لروسيا بتحقيق عنصر المفاجأة في وقت أو أسلوب العمل العسكري. وبذلك تكسب روسيا الوقت والكفاءة ضد جيش الخصم، نظرًا إلى أن الحرب في أوكرانيا، بحسب الرواية الروسية، هي «عمليات خاصة» وليست حربًا[96]. توفر عمليات المعلومات الغطاء المطلوب للحصول على المزيد من المرونة والكفاءة للجيش، وتحسن سرعة المناورة وسرعة الاستجابات في ساحة المعركة. ويمكن أن نورد مثالاً على ذلك بالرواية الروسية بشأن وجود قواتها على الحدود الأوكرانية لإجراء

---

91 "نهاية حقبة ما بعد الحرب الباردة: مغامرة روسيا في أوكرانيا تعيد تشكيل النظام العالمي برمته"، مركز الجزيرة للدراسات، 2022/2/28، شوهد في 2023/7/4، في: https://tinyurl.com/2uyeywc9

92 "موسكو تعلن انتهاء المناورات بالقرب من أوكرانيا وفي جنوب البلاد"، **فرانس 24**، 2021/12/25، شوهد في 2023/7/4، في: https://f24.my/8Fkj

93 Leonid Bershidsky, "Why Putin is Lying about Ukraine," *Bloomberg*, 9/2/2015, accessed on 4/7/2023, at: https://bit.ly/3vACDSx

94 Mark Galeotti, "'Hybrid War' and 'Little Green Men': How it Works, and How it Doesn't," in: Agnieszka Pikulicka-Wilczewska & Richard Sakwa (eds.), *Ukraine and Russia: People, Politics, Propaganda and Perspectives* (Bristol: E-International Relations Publishing, 2015), pp. 156 - 164.

95 "Putin Puts Russia's Nuclear Deterrent Forces on Alert, *Aljazeera*, 27/2/2022, accessed on 4/7/2023, at: https://bit.ly/3k42cpH

96 "Russian Federation Announces 'Special Military Operation' in Ukraine as Security Council Meets in Eleventh-Hour Effort to Avoid Full-Scale Conflict," UN Security Council, SC/14803, 8974th Meeting, 23/2/2022, accessed on 4/7/2023, at: https://bit.ly/3K7vI8C; "Do not Call Ukraine Invasion a 'war', Russia tells Media, Schools" *Aljazeera*, 2/3/2022, accessed on 4/7/2023, at: https://bit.ly/3xLr51k

تمارين عسكرية في كانون الثاني/ يناير 2022 والإنكار الأولي من قبل كبار القادة الروس حول نوايا العمل العسكري؛ ما أتاح لروسيا كسب الوقت لتولي مواقع استراتيجية على الحدود الأوكرانية، وإنهاء تحضيرات الغزو. فاستخدام روسيا للمعلومات المربكة هو جزء من عمليات التأثير في عمليات المعلومات التي تشنها على أوكرانيا. وساهمت هذه المناورة المعلوماتية في إرباك الموقف الدولي من خلال متابعة تضارب الروايتين، ومن ثمّ لم يظهر موقف دولي حاسم ضد روسيا إلا بعد أن تم دخول القوات الروسية إلى أوكرانيا. وكان الرد على شكل عقوبات اقتصادية وأسلحة ومعدات عسكرية تم تقديمها للجيش الأوكراني[97].

كما يمكن استنباط أن عمليات التأثير هي أساس عمليات المعلومات الروسية، وبخاصة في دول الجوار الروسي التي تتشارك مع روسيا مجموعة من العوامل، والتي ترى روسيا بأنه من الممكن توظيفها في عمليات التأثير؛ مثل اللغة والعرق والانتماء والإرث السوفياتي السابق والمرجعية المسيحية الأرثوذكسية. وغالبًا ما تكون هذه العوامل الهوياتية الأساس الذي تبني عليه روسيا استراتيجيتها في عمليات المعلومات وممارسة التحكم الانعكاسي. كما أنها تستثمر أيضًا في أدوات قوتها الناعمة، مثل سياسة الغاز والطاقة والإعلام وجماعات الضغط للتأثير في النخب السياسية وصناعة موالين لها.

نجحت بعض عمليات التأثير الروسية إلى حد ما في بعض المناطق التي تتألف من أغلبية روسية أو موالية لروسيا. وقد تمركزت هذه الفئات غالبًا في شرق أوكرانيا وكانت محط تركيز خطة عمليات المعلومات الروسية ونقطة اختراق أوكرانيا بواسطة استراتيجية التحكم الانعكاسي. بالنظر إلى هذا التوجه الروسي في عمليات المعلومات، يلاحظ أن استراتيجية عمليات التأثير تهدف إلى صناعة التأثير المطلوب وتحقيق الأهداف الاستراتيجية الروسية أو التمهيد لتحقيقها بأقل تدخل ملحوظ وبأقل تكلفة على روسيا. ونجد أنه حتى الولايات المتحدة، القوة الأكبر في العالم، اتهمت روسيا بتدخلها للتأثير في الانتخابات الرئاسية الأميركية بواسطة أدوات عمليات المعلومات[98]. ومن خلال مراجعة خطاب الرئيس بوتين في بداية الغزو الروسي لأوكرانيا وتحليله، يمكن ملاحظة استخدامه أدوات التأثير من خلال تذكيره بالتاريخ السوفياتي والتشكيك في سيادة أوكرانيا، ولاحقًا بالتلويح بالقدرات النووية.

توظف روسيا جميع وسائل عمليات المعلومات وأدواتها؛ من عمليات تأثير، وحرب إلكترونية، وعمليات سيبرانية في إنجاح عملياتها العسكرية على نحو منسق ومتزامن. وسعت في بداية الأزمة إلى ثني الأوكرانيين عن المقاومة، وحثهم على الاستسلام من خلال عمليات حرب نفسية مكثفة. فقامت على سبيل المثال بإرسال رسائل نصية إلى المواطنين الأوكرانيين تهدف إلى إضعاف مقاومة الأوكرانيين من خلال اتهام النخب السياسية وتشويه سمعتها[99] وتحريض الجيش الأوكراني ضد قياداته[100]. كذلك نشرت في وسائل إعلامها والمنصات التابعة لها معلومات مضللة تظهر انتصارات ميدانية وهزائم في صفوف الأوكرانيين هدفها مهاجمة الجانب المعنوي لدى الجيش والقيادة الأوكرانية[101]. كما استخدمت تقنيات الذكاء الاصطناعي في تزييف مقاطع مرئية للرئيس الأوكراني أعلن فيها هزيمة أوكرانيا، وطالب الجيش بالاستسلام[102]، وذلك في المراحل الأولى من بدء العمليات العسكرية.

---

97 "واشنطن في أوكرانيا ومحاولات احتواء روسيا".

98 Eric Manpearl, "Securing US Election Systems: Designating US Election Systems as Critical Infrastructure and Instituting Election Security Reforms," *Boston University Journal of Science and Technology Law*, vol. 24 (2018), p. 168.

99 Raphael Satter, "'You're Just Meat' - Ukrainian Soldiers Get Chilling Texts," *Associated Press*, 11/5/201, accessed on 4/7/2023, at: https://bit.ly/37Hebqx

100 Julie Coleman, "Russian Operatives Sent 5,000 Text Messages in a Failed Attempt to Incite Ukrainians to Attack their Own Capitol," *Business Insider*, 1/4/202, accessed on 4/7/2023, at: https://bit.ly/3K9OQTg

101 Lorenzo Franceschi-Bicchierai, "Ukraine Accuses Russia of Using WhatsApp Bot Farm to Ask Military to Surrender," *Vice*, 1/4/202, accessed on 4/7/2023, at: https://bit.ly/3LbBIOP

102 Jane Wakefield, "Deepfake Presidents Used in Russia-Ukraine War," *BBC*, 18/3/202, accessed on 4/7/2023, at: https://bbc.in/3rHmlGg

في مجال الحرب الإلكترونية، أمر الجنرال فاليري جيراسيموف، رئيس الأركان العامة للقوات المسلحة الروسية، بدعم وحداته القتالية من كتائب وألوية متخصصة في الحرب الإلكترونية. ولتحقيق التفوق الكامل على القوات الأوكرانية، تشمل مهمات هذه الوحدات التشويش، وتحييد، وعرقلة إرسال الجيش الأوكراني للاتصالات واستخدامه للترددات HF وVHF وUHF. وتبحث وحدات الحرب الإلكترونية الروسية عن إشارات تنبعث من الرادارات الأوكرانية لمنعها من العمل بشكل صحيح. ومن خلال إضعاف أو تعمية أو تزوير الترددات الرادارية واللاسلكية فوق الأراضي الأوكرانية وأنظمة تحديد المواقع وصور الأقمار الصناعية يصبح من الصعب مراقبة مسار الصواريخ قصيرة ومتوسطة المدى التي يطلقها الروس على أوكرانيا[103].

على الرغم من ذلك، يرى عدد من المراقبين أن روسيا لم تحقق تفوقًا ملحوظًا في مجال الحرب الإلكترونية في الحرب الأوكرانية[104]، وظهرت تقارير تشير إلى خلل في أنظمة الاتصالات الروسية[105]. يعود ذلك إلى حد ما إلى الدعم الغربي لأوكرانيا في إمدادها بأسلحة ذات تقنية حديثة في مقابل تقادم الأسلحة الروسية وأنظمة اتصالاتها[106]. ومن منظور آخر، قد يكون لعملية تحول الجيش الروسي إلى استراتيجية حرب الجيل الجديد وتبني أسلوب الحرب الهجينة التي تمت الإشارة إليها دورٌ في عدم كفاءة القوات الروسية في شن عمليات عسكرية على مستوى واسع، والتي تتطلب جهدًا في التخطيط والدعم اللوجستي والاتصالات. وقد يكون هذا الأمر ساهم في عدم تحقيق الحسم العسكري خلال مدة قصيرة من بداية الاجتياح العسكري لأوكرانيا في شباط/ فبراير 2022. كما أن استمرار حملة عمليات المعلومات الروسية ضد أوكرانيا منذ عام 2014 ساهم إلى حد ما في قدرة أوكرانيا على التكيف والتعامل مع عمليات التأثير الروسية بشكل أكثر كفاءة[107].

في المجال السيبراني، تنظر روسيا إلى قدراتها كجزء من استخدام الأساليب غير المتكافئة أو غير المباشرة لتحقيق الهيمنة والتفوق في عملياتها العسكرية. وتعد الأزمة في أوكرانيا منذ عام 2022 أكبر ساحة معركة للحرب السيبرانية منذ الهجمات السيبرانية الروسية على إستونيا في عام 2007[108]. وقد شنت روسيا سلسلة من الهجمات ضد المواقع الأوكرانية في أوائل شباط/ فبراير 2022 عن طريق وكالة المخابرات العسكرية الروسية GRU. واستهدفت الهجمات المواقع المصرفية والدفاعية الأوكرانية[109] في 25 شباط/ فبراير. واتهم فريق الاستجابة لطوارئ الكمبيوتر في أوكرانيا مجموعة القرصنة البيلاروسية UNC1151، التي ترعاها الدولة، بمحاولة اختراق حسابات البريد الإلكتروني لأفرادها العسكريين. وفور اختراق المتسللين حسابات العسكريين، استفادوا من العناوين المخترقة لإرسال المزيد من رسائل البريد الإلكتروني الضارة[110].

في المقابل، اتبعت أوكرانيا استراتيجية مختلفة في الفضاء السيبراني، تمثلت في محاولة لتعبئة المشاعر الدولية وإنشاء جيش من المتخصصين في الأمن السيبراني لمهاجمة أهداف البنية التحتية العسكرية والحرجة

103 Juan Pons, "The Unseen and Unknown Electronic War in Ukraine," *Atalayar*, 14/3/2022, accessed on 4/7/2023, at: https://bit.ly/3MlobVe

104 Andrew Eversden & Jaspreet Gill, "Why hasn't Russia Used its 'Full Scope' of Electronic Warfare?" *Breaking Defense*, 28/3/2022, accessed on 4/7/2023, at: https://bit.ly/3MtMm3X

105 Jack Detsch & Amy Mackinnon, "'The Ukrainians are Listening': Russia's Military Radios are Getting Owned, Foreign Policy," 22/3/2022, accessed on 4/7/2023, at: https://bit.ly/3MtMtwp; Sergei Dobrynin & Mark Krutov, "Communication Breakdown: How Russia's Invasion of Ukraine Bogged Down," *Radio Free Europe/Radio Liberty*, 19/3/2022, accessed on 4/7/2023, at: https://bit.ly/3OwvsTR

106 Pons.

107 Stephanie Carvin, "How to Explain the Failure of Russia's Information Operations in Ukraine?" Centre for International Governance Innovation, 25/3/2022, accessed on 4/7/2023, at: https://cutt.ly/bGuZab6

108 "The Ukrainian Crisis – A Cyber Warfare Battlefield," *Defense Update*, 5/4/2014, accessed on 4/7/2023, at: https://cutt.ly/EGuZg6f; Matthew Bell, "Russian Cyber Attacks on Ukraine: The Georgia Template," *Channel 4*, 3/5/2014, accessed on 4/7/2023, at: https://cutt.ly/VGuZlva

109 "UK Assesses Russian Involvement in Cyber Attacks on Ukraine," UK Government, *Government Response*, 18/2/2022, accessed on 4/7/2023, at: https://cutt.ly/BGuZxPm

110 Catalin Cimpanu, "Ukraine says Belarusian Hackers are Targeting its Military Personnel," *The Record*, 25/2/2022, accessed on 4/7/2023, at: https://cutt.ly/NGuZvXs

في روسيا. فقد أعلنت مجموعة Anonymous، وهي مجموعة عالمية من نشطاء القرصنة الإلكترونية، «الحرب» على روسيا في الأول من آذار/ مارس 2022[111]، وادعت أنها عطلت المواقع التي تديرها وسائل الإعلام الروسية المملوكة للدولة، وقامت باختراق العديد من محطات البث الروسية الكبرى، بما في ذلك القنوات التلفزيونية التي تديرها الدولة؛ مثل روسيا 24، والقناة 1، وموسكو 24. وقامت المجموعة بتسريب أكثر من 360 ألف ملف، بما في ذلك إرشادات حول كيفية الإشارة إلى غزو أوكرانيا[112].

في مجال عمليات التأثير والحرب النفسية، أظهرت الممارسات الروسية لعمليات المعلومات في أوكرانيا، كما أوضحت هذه الدراسة، بأن الجمع بين رسائل وسائل الإعلام التقليدية والهجمات السيبرانية وحملات وسائل التواصل الاجتماعي قد يمهد الطريق للتأثير في السكان والتحكم في الخيارات. في الواقع، يؤدي نقل السرد حول الموضوعات الاجتماعية والسياسية المثيرة للجدل إلى زيادة الفجوة بين المجموعات المختلفة ويضع العلاقة بين السكان والحكومة تحت الضغط. وتنزلق هذه الاستراتيجية إلى ما دون عتبة المواجهة المفتوحة، بما في ذلك العسكرية، ويمكن تصنيفها على أنها حرب معلومات[113]. وقد نجحت روسيا في ذلك إلى حد ما في شرق أوكرانيا، أي في المناطق التي توجد فيها غالبية من الأصول الروسية، رغم الدعاية الأوكرانية المضادة بأن هذه الأرض أوكرانية، وأن مواطنيها أوكرانيون بغض النظر عن أصولهم ودياناتهم. ورغم نجاحها في المناطق الشرقية لأوكرانيا، فإن الدعاية الروسية لم تحقق التأثير المرغوب في الداخل الأوكراني. بل على العكس من ذلك، أشارت تقارير إلى نتائج عكسية لعمليات المعلومات الروسية، حيث وحدت الصف الأوكراني، وأدت إلى دعم دولي مباشر وغير مباشر لأوكرانيا، وأتاحت القدرة على عزل روسيا سياسيًا واقتصاديًا[114].

خاتمة

تعتبر عمليات المعلومات من أخطر أساليب المواجهة بين الدول في العصر الحالي، فقد تطورت خلال السنين الماضية لتصبح اليوم الأساس الذي يقوم عليه الصراع بين الدول المتنافسة، سلمًا أو حربًا. وأدى التطور المتسارع في تكنولوجيا الاتصالات والمواصلات ووسائل التواصل الاجتماعي إلى أن تؤدي عمليات المعلومات دورًا حاسمًا في النصر أو الخسارة. وتزايد الاعتماد عليها في القيام بمهمات مسانده للعمليات العسكرية، إلا أن دورها الأساسي هو في قدرتها على التأثير لتجنب المواجهة، كما أشار إلى ذلك كلاوزفيتز وصن تزو.

وقد فرّقت الدراسة بين مصطلح الحرب المعلوماتية ومصطلح عمليات المعلومات، على أساس أن كلمة حرب تستخدم فقط عند وقوع الحرب بشكل رسمي، بينما تشن عمليات المعلومات في كل وقت، سواء في الحرب أو السلم. وبيّنت أن ثمة معنًى شاملًا لعمليات المعلومات؛ أي استخدام المعلومات في عمليات التأثير والدعاية، وعمليات الجمع الاستخباري، وعمليات التعامل مع المعدات المعلوماتية. وهكذا تصبح حرب المعلومات، وفقًا لهذا التعريف، جزءًا فقط من ضمن عمليات المعلومات الواسعة.

---

111 Chris Morris, "Hacker collective Anonymous Declares War on Russia," *Fortune*, 1/3/2022, accessed on 4/7/2023, at: https://cutt.ly/NGuZEMm

112 Lorax B. Horne & Emma Best: Release, "Roskomnadzor (820 GB)," Distributed Email of Secrets, 10/3/2022, accessed on 28/8/2023, at: https://tinyurl.com/2mk4pxf9

113 L.B. Monov & M.L. Karev, "Information Warfare Conceptual Framework," *International Journal of Recent Scientific Research Research*, vol. 9, no. 5 (2018), pp. 26859 - 26866.

114 Haley Ott, "Information Warfare Expert Says the U.S. is Finally Countering Russia at its Own Game," *CBS News*, 17/2/202, accessed on 4/7/2023, at: https://cutt.ly/5GuZDaa

تعتبر روسيا الاتحادية من أكثر الدول استخدامًا لعمليات المعلومات في عملياتها العسكرية، وحتى في فرض الهيمنة وتحقيق المصالح السياسية؛ فقد سعت لتحقيق ذلك في بداية حربها مع أوكرانيا في عام 2022، ولكنها لم تنجح بالشكل المطلوب بسبب الخلل في أنظمة الاتصالات الروسية الذي ظهر أثناء المعارك، والدعم الغربي لأوكرانيا من ناحية العتاد العسكري والمعلوماتي، من مخابرات ودعاية معلوماتية مضادة، وكذلك بسبب طول المدة التي شنت فيها روسيا عمليات المعلومات على أكرانيا منذ عام 2007، ما أدّى إلى تمكين أوكرانيا من التكيف والتعامل مع عمليات التأثير الروسية على نحو فعّال. ويؤكد هذا أن عمليات المعلومات متشابهة في المفاهيم والأدوات، ولكن التطبيق والسياق الذي تجري فيه يختلف، كما اتضح في الحالة الأوكرانية.

وعلى الرغم من أن روسيا انتهجت مبكرًا أسلوب الاعتماد على العمليات المعلوماتية وفق استراتيجية تطوير الجيش الروسي في أعقاب الحرب الجورجية في عام 2008 ولتحقيق التفوق على خصومها عن طريق القدرات غير التقليدية، تميزت العمليات المعلوماتية الروسية من ناحية الكثافة والتأثير، ولكن تطبيق عمليات المعلومات بالغ في تقدير قدرة هذه العمليات على النجاح في الحالة الأوكرانية، عندما اعتقدت روسيا بأنه يمكن تحقيق النصر خلال أشهر قليلة، ما دفعها إلى التوغل عميقًا في الأراضي الأوكرانية منذ بداية المعركة سعيًا لمحاصرة كييف. لقد بدأت روسيا المعركة من دون معلومات دقيقة عن الوضع في الداخل الأوكراني، معتمدة على تفوقها العسكري والعناصر الموالية لها في شرق أوكرانيا؛ أي إنّها راهنت على كسب المعركة في إطار معادلة جيش روسي قوّي يُصنّف الثاني عالميًا، مقابل جيش أوكراني يصنّف في المرتبة الثانية والعشرين عالميًا. وقدرَّت دوائر صنع القرار في موسكو أنّ التفوق العسكري والإرث التاريخي سيقود إلى نصر محقق، لكنّ ذلك لم يتجسّد على أرض الواقع.

في المقابل، استثمرت أوكرانيا طوال السنوات الماضية في خلق نقاط عمياء في الإدراك والقراءة الروسيين للعمق الاستراتيجي لأوكرانيا عبر أربعة مداخل رئيسة؛ المدخل الأول هو تحويل دوائر صناعة القرار الأوكرانية إلى علب سوداء بالنسبة إلى روسيا عبر إعادة تشكيل النخب ذات المناصب الحساسة في الدولة وفق مبدأ مدى القرب من الاتحاد الأوروبي والناتو. والمدخل الثاني، كسر الهدوء الروسي الذي سبق ضمّ شبه جزيرة القرم، حيث عملت أوكرانيا على سحب روسيا إلى منطقة تصريحات إعلامية وتراشق اعلامي عالمي، ما أعطى للعالم فرصة لتوجيه انتباهه إلى حركة الصراع وتوجهاته والترويج لسردية مظلومية أوكرانيا أمام العدوان الروسي. المدخل الثالث، تبنّي عقيدة غربية، وفهم عميق للقدرات الروسية، ومن ثمّ امتلاك القدرة على التنبؤ بخطواتها ومواجهتها. وأخيرًا، الانتباه المبكر للقدرات المعلوماتية الروسية، وتحذير القوات العسكرية والمواطنين منها، والتحضير لمواجهتها؛ ما خلخل الاستراتيجية الروسية المبنية على عمليات المعلومات والحرب الهجينة.

واستشعرت أوكرانيا التفوق الروسي في عمليات المعلومات في مراحل مبكرة، ونجحت في عمليات المعلومات المضادة أو الدفاعية التي أدت إلى وحدة الصف الأوكراني ضد الغزو الروسي والمقاومة، وهو ما لم يكن متوقعًا لدى روسيا وحتى الدول الغربية. فقد كانت أوكرانيا مدركة تمامًا لأبعاد عمليات المعلومات الروسية وتعمل في المقابل وفق سياسة ونهج مضادين للتعامل معها وتحييد تأثيرها؛ ما دفع الجيش الروسي إلى التخبط في الداخل الأوكراني وتغيير أهدافه وفق المعطيات على الأرض[115].

لذلك ساهم التعامل الأوكراني والقوى الغربية مع عمليات المعلومات الروسية على نحو مباشر في تعطيل أهداف الحملة الروسية أو جعلها أكثر تكلفة وصعوبة مع اصطفاف المجتمع الدولي إلى جانب أوكرانيا، على

115 Ibid.

الرغم من أن عمليات المعلومات جزء من استراتيجية الجيش الروسي الحديث. لم تحقق روسيا أهدافها العسكرية على الأرض، وانسحبت قواتها العسكرية من محيط العاصمة كييف، ونتيجة لذلك ركزت على أهداف أقل طموحًا من أهدافها في بداية الأزمة في شباط/ فبراير 2022.

يؤكد هذا صحة فرضية الدراسة التي تقول إن لعمليات المعلومات دور حاسم في العمل العسكري. فنتائج المواجهة في بيئة المعلومات بين روسيا وأوكرانيا أثرت على نحو مباشر في العمل العسكري التقليدي؛ إذ عجزت روسيا عن إسقاط دوائر صنع القرار الأوكرانية، واصطدمت بواقع وحدة الصف الأوكراني تجاه الغزو. كما لم تقم بأي عملية معلوماتية نوعية تؤدي إلى إسقاط العاصمة كييف، على الأقل من ناحية التأثير والتخويف وفرض الأمر الواقع على الحكومة والسكان في أوكرانيا كما حصل عند احتلالها شبه جزيرة القرم عام 2014. وعلى الرغم من أن عمليات المعلومات جزء من استراتيجية الجيش الروسي الحديث، فإن التحول في الاستراتيجية الدفاعية الروسية وتركيز المفاهيم العسكرية على العمليات الخاصة والحرب الهجينة وعمليات المعلومات، وتكيّف أوكرانيا مع حملة المعلومات الروسية، أدى إلى عدم كفاءة العمليات العسكرية التقليدية التي شنتها روسيا تجاه أوكرانيا مع عدم تقديرها الصحيح لمقاومة عمليات المعلومات والإجراءات الوقائية التي اتخذتها أوكرانيا وجعلتها قادرة على مقاومة عمليات التأثير الروسية، مثلما حدث سابقًا مع جورجيا وإستونيا. فقد قامت جورجيا نتيجة الغزو الروسي في عام 2008 بتحديث قواتها المسلحة، وقامت إستونيا في أعقاب الهجمات السيبرانية الروسية عليها في عام 2007 بالاستثمار في القدرات السيبرانية لتصبح من الدول الرائدة في هذا المجال. كذلك تعاملت أوكرانيا مع عمليات المعلومات الروسية بعد احتلال القرم؛ ما جعلها على مستوى من الجاهزية المعلوماتية للتعامل مع تلك العمليات أثناء غزو روسيا لأوكرانيا في عام 2022.

المراجع

1. **العربية**

«الحرب الأوكرانية في شهرها الثاني: تبعات ثقيلة ومتغيرات مديدة». مركز الجزيرة للدراسات. 2022/3/27. في: https://bit.ly/3K2xXdb

«حسابات واشنطن في أوكرانيا ومحاولات احتواء روسيا». **تقدير موقف.** المركز العربي للأبحاث ودراسة السياسات. 2022/3/3. في: https://tinyurl.com/yau7y7tm

«نهاية حقبة ما بعد الحرب الباردة: مغامرة روسيا في أوكرانيا تعيد تشكيل النظام العالمي برمته». مركز الجزيرة للدراسات. 2022/2/28. في: https://tinyurl.com/2uyeywc9

كلاوزفيتز، كارل فون. **عن الحرب**. ترجمة سليم شاكر. بيروت: المؤسسة العربية للدراسات والنشر، 1997.

2. **الأجنبية**

4th Information Survivability Workshop: ISW-2001/2002. Vancouver, 2002.

Adams, Agnieszka & Richard Sakwa (eds.). *Ukraine and Russia: People, Politics, Propaganda and Perspectives.* Bristol: E-International Relations Publishing, 2015.

Adams, James. *The Next World War: The Warriors and Weapons of the New Battlefields in Cyberspace.* London: Hutchinson, 1998.

"Allied Joint Doctrine for Psychological Operations (AJP-3.10.1)." *NATO Standardization Office* (September 2014).

Ali, Salahudin. "Coming to a Battlefield Near You: Quantum Computing, Artificial Intelligence & Machine Learning›s Impact on Proportionality." *Santa Clara Journal of International Law*. vol. 18 (2020).

Bedritsky, A.V. "Information War: Concepts and their Realization in the USA." *RISI* (2008).

Bērziņš, Jānis. "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria." *The Journal of Slavic Military Studies*. vol. 33, no. 3 (2020).

Burbridge, Dean A. *Employing US Information Operations against Hybrid Warfare Threats.* Carlisle: Army War College, 2013.

Carvin, Stephanie. "How to Explain the Failure of Russia's Information Operations in Ukraine?" Centre for International Governance Innovation. 25/3/2022. at: https://cutt.ly/bGuZab6

Cordray, Robert & Marc J. Romanych. "Mapping the Information Environment." *IO Sphere* (2005).

Cuomo, Serafina. "Niccolò Tartaglia, Mathematics, Ballistics and the Power of Possession of Knowledge." *Endeavour*. vol. 22, no. 1 (1998).

"Cyberspace Operations." Joint Chiefs of Staff, Joint Publication (JP 3-12). Washington, DC: Department of Defense, 2018.

Danyk, Yuriy, Tamara Maliarchuk & Chad Briggs. "Hybrid War: High-Tech, Information and Cyber Conflicts." *Connections*. vol. 16, no. 2 (2017).

Dailey, Brian & Patrick Parker (eds.). *Soviet Strategic Deception.* Pennsylvania: Lexington Books, 1987.

"Dictionary of Military and Associated Terms." Joint Chiefs of Staff, Joint Publication. no. 1-02, 15/2/2010. at: https://bit.ly/38hcb8j

Dylevsky, Bazylev, S.A. Komov & A.N. Petrunin. "The Russian Armed Forces in the Information Environment: Principles, Rules, and Confidence-Building Measures." *Military Thought*. vol. 21, no. 2 (2012).

Ermus, Aarne & Karl Salum. "Changing Concepts of War: Russia's New Military Doctrine and the Concept of Hybrid Warfare." *The Estonian Military Academy*. no. 7 (2017).

Fedorov, Yury E. "Continuity and Change in Russia's Policy toward Central and Eastern Europe." *Communist and Post-Communist Studies*. vol. 46, no. 3 (2013).

Fletcher & Christopher J. Lamb. "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference." *Strategic Perspectives*. no. 11 (2012).

Galeotti, Mark. "The 'Gerasimov Doctrine' and Russian Non-Linear War." In Moscow's Shadows. 6/7/2014. accessed on 4/7/2023. at: https://bit.ly/3OsFkOC

Goldenziel, Jill I. & Manal Cheema. "The New Fighting Words? How US Law Hampers the Fight against Information Warfare." *Journal of Constitutional Law*. vol. 22, no. 1 (November 2019).

Horne, Lorax B. & Emma Best. "Release: Roskomnadzor (820 GB)," Distributed Email of Secrets. 10/3/2022. at: https://tinyurl.com/2mk4pxf9

Information Operations. Joint Chiefs of Staff, Joint Publication (JP 3-13), Washington, DC: Department of Defense, 2014.

"Information Security Doctrine of the Russian Federation." United Nations International Telecommunications Union Archive (2000). at: https://tinyurl.com/44duj852

Ion Mihai & Ronald J. Rychlak. *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism.* Chicago: WND Books, 2013.

"Joint Doctrine for Command and Control (C2W)." Joint Chiefs of Staff, *Joint Publication*. no. 3 - 13.1. 7/2/1996. at: https://bit.ly/36DZuEn

"Joint Doctrine for Information Operations." Joint Chiefs of Staff, *Joint Publication*. no. 3 - 13. 13/2/2006. at: https://cutt.ly/XGuVU06

Jomini, Antoine-Henri, George Henry Mendell & William Price Craighill. *The Art of War.* North Chelmsford: Courier Corporation, 2007.

Kozloski, Robert. "The Information Domain as an Element of National Power." *Strategic Insights*. vol. 8, no. 1 (2009).

Kristiansen, Marius & Njaal Home. "Small Players in a Limitless Domain: Cyber Deterrence as Small State Strategy." *Comparative Strategy*. vol. 41, no. 1 (2022).

L.B. Monov & M.L. Karev. "Information Warfare Conceptual Framework." *International Journal of Recent Scientific Research Research*. vol. 9, no. 5 (2018).

Larson, Eric V. et al. *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities.* Santa Monica: RAND, 2009.

Lepingwell, John. "The Russian Military and Security Policy in the 'Near Abroad'." *Survival*. vol. 36, no. 3 (1994).

Lin, Herbert. "Doctrinal Confusion and Cultural Dysfunction in DoD." *The Cyber Defense Review*. vol. 5, no. 2 (Summer 2020).

Marcellino, William et al. *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations.* Santa Monica: RAND, 2017.

Mearsheimer, John. *The Tragedy of Great Power Politics.* New York: W.W. Norton & Company, 2001.

Manpearl, Eric. "Securing US Election Systems: Designating US Election Systems as Critical Infrastructure and Instituting Election Security Reforms." *Boston University Journal of Science and Technology Law*. vol. 24 (2018).

Matthews, Ron & Jack Treddenick (eds.). *Managing the Revolution in Military Affairs.* London: Palgrave Macmillan, 2001.

Neilson, Robert E. (ed.). *Sun Tzu and Information Warfare: A Collection of Winning Papers from the Sun Tzu Art of War in Information Warfare Competition.* Collingdale: Diane Publishing, 1997.

Pacepa, Perkovich, George & Ariel E. Levite (eds.). *Understanding Cyber Conflict: 14 Analogies.* Washington, DC: Georgetown University Press, 2017.

Radin, Andrew. *Hybrid Warfare in the Baltics: Threats and Potential Responses.* Santa Monica: RAND Corporation, 2017.

Rasmussen, Mikkel Vedby. *The Acme of Skill: Clausewitz, Sun Tzu and the Revolutions in Military Affairs.* Amaliegade: Dansk Udenrigspolitisk Institut, 2001.

"Russian Federation Announces 'Special Military Operation' in Ukraine as Security Council Meets in Eleventh-Hour Effort to Avoid Full-Scale Conflict." UN Security Council. SC/14803. 8974th Meeting. 23/2/2022. at: https://bit.ly/3K7vI8C

Renn, Jürgen & Matteo Valleriani. “Galileo and the Challenge of the Arsenal.” Max Planck Institute for the History of Science. 21/3/2001. at: https://tinyurl.com/4aykrzay

Rohde, William E. “What is Info Warfare?” *US Naval Institute Proceedings*. vol. 122, no. 2 (1996).

Sakwa, Richard. “The Soviet Collapse: Contradictions and Neo-modernisation.” *Journal of Eurasian Studies*. vol. 4, no. 1 (2013).

Schwille, Michael et al. *Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities Between Intelligence and Information Professionals.* Santa Monica: RAND, 2020.

Smith, Steve et al. (eds.). *Foreign Policy: Theories, Actors, Cases.* Oxford: Oxford University Press, 2008.

Taddeo, Mariarosaria. “Information Warfare: A Philosophical Perspective.” *Philosophy & Technology.* vol. 25 (2012).

Taddeo, Thomas. “Russian Views on Information-Based Warfare.” *Airpower Journal Special Edition* (1996).

“The Implementation of Network-Centric Warfare.” Office of Force Transformation, Transformation Report. 5/1/2005. at: https://tinyurl.com/2j5ardkn

“The Military Doctrine of the Russian Federation.” *President of the Russian Federation* (December 2014). at: https://tinyurl.com/36fsjcuw

Theohary, Catherine A. “Defense Primer: Information Operations.” *Congressional Research Service*. 9/12/2022. at: https://tinyurl.com/55c23wm7

Timothy, Thomas. “Russia’s Reflexive Control Theory and the Military.” *Journal of Slavic Military Studies*. vol. 17, no. 2 (2004).

Tzu, Sun. *The Art of War*. Samuel B. Griffith (trans.). New York: Oxford University Press, 1971.

Williamson, Steven C. *From Fourth Generation Warfare to Hybrid War.* Carlisle: Army War College, 2009.

Yevdakov, V.I. “Characteristic Features and Peculiarities of Wars at the Start 21st Century.” *Journal of the Academy of Military Sciences*. no. 3 (2008).