مـــــــــركز المنبر
للدراسات والتنمية المستدامة
ALMANBAR CENTER FOR STUDIES
AND SUSTAINABLE DEVELOPMENT

الحرب الكهرومغناطيسية: نقطة عمياء لحلف الناتو قد تحدد الصراع القادم

الكاتب: كلارا لو غارغاسون وجيمس بلاك

المصدر: مؤسسة "رند" / نُشر بتاريخ 24 تشرين الثاني 2025

عن المركز

مركز المنبر للدراسات والتنمية المستدامة، مركز مستقلٌ، مقرّه الرئيس في بغداد. رؤيته الرئيسة تقديم وجهة نظر ذات مصداقية حول قضايا السياسات العامة والخارجية التي تخصّ العراق بنحو خاصٍ ومنطقة الشرق الأوسط بنحو عام – فضلاً عن قضايا أخرى – ويسعى المركز إلى إجراء تحليل مستقلّ، وإيجاد حلول عمليّة جليّة لقضايا تهمّ الشأن السياسي، الاقتصادي، الاجتماعي، والثقافي.

لا تعبر الآراء الواردة في المقال بالضرورة عن اتجاهات يتبناها المركز و إنما تعبر عن رأي كتابها

https://www.almanbar.org

info@almanbar.org

https://t.me/manbarcenter

07816776709

إخفاقات الغرور في غزو العراق تهدد بحدوث كارثة مماثلة في فنزويلا

الكاتب: كلارا لو غارغاسون و جيمس بلاك

المصدر: مؤسسة "رند" / نُشر بتاريخ 24 تشرين الثاني 2025[1].

كشفت الحرب في أوكرانيا عن جبهة جديدة كانت قد تجاهلتها القوات العسكرية الغربية لفترة طويلة: الحرب الكهرومغناطيسية. السيطرة على هذه الساحة القتالية غير المرئية، حيث يتم تعطيل الاتصالات، وتعطيل الطائرات المسيَّرة، وانحراف الأسلحة الدقيقة عن مسارها، بما يؤثر بشكل كبير على نتيجة الصراع.

لقد فهمت روسيا هذه المسألة بشكل أسرع من حلف الناتو، مستخدمةً الحرب الكهرومغناطيسية لعزل الوحدات الأوكرانية، وتعطيل شبكات القيادة، وتحييد الأنظمة الغربية.

على الرغم من أن أوكرانيا تكيّفت بذكاء، إلّا أنها تتعلم في ميدان المعركة ما كان يجب أن يتعلمه الناتو خلال التدريب. بعد عقود من التركيز على مكافحة التمرد، يواجه التحالف الآن خطر مواجهة أقوى خصم له دون أن يكون قد اتقن مجالات حاسمة في هذه الحرب الحديثة.

هذا لا يعني أن الحرب الإلكترونية ظاهرة جديدة. فقد كان الطيف الكهرومغناطيسي عنصراً أساسياً في الحروب منذ أوائل القرن العشرين، وتحديداً مع ظهور استخبارات الإشارات (SIGINT). فعلى سبيل المثال، ساعد اعتراض الإشارات اللاسلكية البحرية للإمبراطورية اليابانية على هزيمة روسيا القيصرية عام 1905.

مع مرور الوقت، بدأ استخدام الطيف الكهرومغناطيسي يتنوّع بطرق فعّالة، مثل الرادار، واعتراض وكسر شيفرة إنيغما[2]خلال الحرب العالمية الثانية، وتشويش البث الإذاعي في الحرب الباردة، وتعطيل أنظمة التوجيه في حرب يوم الغفران، وتشويش نظام تحديد المواقع العالمي (GPS) في حرب الخليج.

[1]Electromagnetic Warfare: NATO's Blind Spot Could Decide the Next Conflict.https://www.rand.org/pubs/commentary/2025/11/electromagnetic-warfare-natos-blind-spot-could-decide.html

[2]شيفرة إنيغما هي نظام تشفير استخدمته ألمانيا في الحرب العالمية الثانية لتأمين اتصالاتها العسكرية، وهي تتكون من آلة كهروميكانيكية معقدة تعمل على تشفير الرسائل وتغيير إعداداتها بشكل يومي، مما جعل فك شفرتها صعبًا للغاية في البداية .تمكن الحلفاء، بقيادة عالم الرياضيات آلان تورينغ وآخرين، من فك الشفرة بمساعدة البولنديين، مما ساهم في تقصير عمر الحرب وإنقاذ الكثير من الأرواح . المترجم

على الرغم من الاكتشافات المتكررة لأساليب جديدة في الحرب الإلكترونية، قللت الجيوش الغربية من أهمية هذه التقنيات خلال الحروب في أفغانستان والعراق. جاء ذلك في إطار تحوّل أوسع بعيداً عن الحروب التقليدية بين الدول نحو مكافحة التمرد.

على مدى السنوات الخمس الماضية، اكتسبت الحرب الإلكترونية أهمية متجددة كمجال قتالي، نظراً لدورها الحاسم في الصراعات الحديثة مثل حرب كاراباخ الثانية، وحرب أوكرانيا، وحرب غزة، والصراع في البحر الأحمر، وكذلك في إيران.

الحرب الإلكترونية الحديثة لا تقتصر على التشويش البسيط، بل تشمل أيضاً تعطيل القيادة والتحكم، وتعطيل أنظمة تحديد المواقع(GPS) ،وأنظمة الاستهداف، واعتراض الاتصالات والتلاعب بها. وهذا يوفر الحماية من الهجمات المماثلة.

يُعتبر إتقان أنظمة الطوارئ الإلكترونية أساسياً للجيوش الرقمية المعتمدة على أجهزة الاستشعار والأقمار الصناعية والأنظمة الشبكية، لتمكينها من العمل بفعالية حتى تحت النيران.

على عكس الغرب، لم تتردد روسيا في استخدام الحرب الإلكترونية بعد انهيار الاتحاد السوفيتي في التسعينيات والعقد الأول من القرن الحادي والعشرين. وقد طوّرت ولا تزال تطوّر بعضاً من أكثر قدرات الحرب الإلكترونية تقدماً في العالم.

تمتلك روسيا اليوم أكثر من 400 موقع رادار على أراضيها وفي أراضي حلفائها (حزيران، 2025)، بالإضافة إلى ما لا يقل عن 14 وحدة حرب إلكترونية عسكرية. تشمل معدات تكتيكية متنقلة مثل نظامي كراسوخا-4 وموسكفا-1، وأجهزة تشويش أرضية بمدى 300 كم مثل مورمانسك-بي إن، والتي يمكنها نظرياً الحد من الاتصالات اللاسلكية عالية التردد في معظم منطقة الصراع. كما تشمل قدراتها أيضاً أجهزة تشويش رادارات محمولة جواً مثل ديونوموري، وأجهزة تشويش رادارات الصواريخ أرض-جو مثل مروحية مي-8 إم تي بي آر-1. حيث تلعب الحرب الإلكترونية دوراً محورياً في التشكيلات والعقيدة العسكرية الروسية.

تتمثل الاستراتيجية المُفضّلة لروسيا في أوكرانيا في استخدام الحرب الإلكترونية لتحديد مواقع القوات الأوكرانية وعزلها قبل قصفها بالمدفعية. كما تستخدم روسيا الحرب الإلكترونية لتعطيل الاتصالات الأوكرانية، وتعطيل أنظمة تحديد المواقع (GPS)، والرادار، وأنظمة الطائرات بدون طيار الأوكرانية، بل وأحياناً لتعطيلها بالكامل.

منذ عام 2022، بدأت أوكرانيا في تطوير أساليب للدفاع عن نفسها ضد الحرب الإلكترونية الروسية، واستفادت من أنظمة الحرب الإلكترونية بفعالية. وقد شهدنا ابتكارات متسارعة من كلا الجانبيّن، سعياً لتحقيق التفوق في هذا المجال الحيوي.

تُشكّل ترسانة روسيا الضخمة والمتطوّرة من أسلحة الحرب الإلكترونية تناقضاً صارخاً مع قدرات حلف شمال الأطلسي (الناتو). بموجب سياسة الناتو للدفاع الجوي والصاروخي المتكامل، يُسمح للحلف بإجراء عمليات حرب إلكترونية حتى في أوقات السلم. ومع ذلك، يخضع هذا الاستخدام للقانون الدولي ويتطلب موافقة سياسية، مما يقيّد نشاط الناتو في هذا المجال.

عملياً، يتركز هذا النشاط على التدريبات والمحاكاة والاختبارات، مما يقلل من خبرة قوات الناتو في الحرب الإلكترونية. في المقابل، تُجري روسيا اختبارات على تكتيكات وتقنيات مختلفة في ساحة معركة نشطة، مما يمكنها من تحسين قدراتها واكتساب فهم أعمق للمجالات التي يمكن أن تثمر فيها المزيد من الاستثمارات عن ابتكارات مفيدة.

يزيد اعتماد الناتو على الولايات المتحدة من تفاقم المشكلة. حيث توفِّر الولايات المتحدة قدرات إلكترونية حيوية، مثل جمع المعلومات الاستخباراتية الإلكترونية (ELINT)عبر الأصول الجوية والفضائية، وإدارة البيانات المركزية لمكتبة التهديدات، وقمع الدفاعات الجوية المعادية إلكترونياً(SEAD)، إضافة إلى تشويش الإشارات.

مع تركيز إدارة ترامب الثانية على الحرب ضد المخدرات ومنطقة المحيط الهندي الهاديء، أصبح هذا الاعتماد نقطة ضعف استراتيجية. كما يرسل اعتماد الناتو على الولايات المتحدة رسالة إلى روسيا عن ضعف الناتو الأوروبي النسبي في هذا البعد المتزايد الأهمية من الحرب، مما يُقوّض الردع ويزيد من خطر مهاجمة الكرملين لدفاعات أوروبا واختبار عزمها في المستقبل.

هناك دلائل على أن بعض أعضاء الناتو بدأوا يدركون هذه الفجوة في القدرات. في نيسان الماضي، أنشأ الناتو وأوكرانيا تحالفاً جديداً للحرب الإلكترونية لإضفاء الطابع الرسمي على تبادل المعدات والتدريب والمباديء بين الدول الثلاث عشرة الموّقعة حالياً. سيساهم هذا التحالف إلى حد ما في سد الفجوة المعرفية التي يعاني منها الناتو في مجال الحرب الإلكترونية، وسيساعد الحلفاء على فهم أفضل لأنواع الأنظمة

التقنية التي يحتاجون إلى اقتنائها. ومع ذلك، سيستغرق تطوير قدرات الحرب الإلكترونية العميقة وقتاً طويلاً، خاصةً مع نقص المهارات والخبرات المتخصصة اللازمة لاستخدام هذه المعدات بشكل صحيح.

يجب على حلف الناتو أن يُثبت جاهزيته وقدرته على مواجهة روسيا في مجال الحرب الإلكترونية، سواء بالمعدات والخبرات الأمريكية أو بدونها. لتحقيق هذا الهدف، ينبغي على الدول الأوروبية الأعضاء في الناتو الاستثمار في الخبرات والمعدات والبنية التحتية في مجال الحرب الإلكترونية لضمان قدرتها على الصمود في حال تراجع الولايات المتحدة أو تشتتها في مسارح عمليات أخرى.

يعني هذا إعطاء الأولوية لطموحات أكبر في مجال الحرب الإلكترونية ضمن خطط الناتو وأهدافه المتعلقة بالقدرات، والبناء على الهدف الجديد المتمثل في تخصيص 5% من الناتج المحلي الإجمالي للإنفاق الدفاعي. كما يتضمن ذلك تشجيع المزيد من الدول على الانضمام إلى تحالف الحرب الإلكترونية مع أوكرانيا، وفرض التكامل المنهجي لبُعد الحرب في نظام إدارة الطوارئ (EMS)، ضمن مناورات الناتو والمناورات الوطنية.

من خلال التجارب، يجب على القوات أن تتكيّف مع العمل في ظروف ضعف الاتصالات أو أجهزة الاستشعار أو نظام تحديد المواقع العالمي (GPS). كما يتطلب الأمر تعزيز سلاسل التوريد الأوروبية لمكونات الحرب الإلكترونية لتقليل الاعتماد على الخارج.

بغض النظر عن الطريقة التي سيتعامل بها حلف الناتو مع هذه القضية، يجب أن يكون رده سريعاً وواضحاً. فخطر الصراع المباشر مع روسيا لا يتضاءل، ولا يمكن لأوروبا أن تتخلف عن الركب في المجال الكهرومغناطيسي. يحتاج التحالف إلى إثبات أنه، في جميع المجالات بما في ذلك نظام إدارة الطوارىء، جاهز وقادر على القتال والانتصار.

***