تحليلات وآراء

دور تـــقنيات الحـــرب الالـــكترونـيـــة في تحديث قدرات حلف شمال الاطلسي

بقلم: الباحثة زينة مالك عريبي

مركز حمورابي للبحوث والدراسات الاستراتيجية

24أيلول 2025

تأسس مركز حمورابي للبحوث والدراسات الإستراتيجية عام 2008 بمدينة بابل (الحلة)، وحصل على شهادة التسجيل من دائرة المنظمات غير الحكومية المرقمة 1Z71874 بتاريخ 2012/12/25، بوصفه مركزا علميا بحثيا يهتم بدراسة الموضوعات السياسية والمجتمعية، فضلاً عن الاهتمام بالقضايا والظواهر الراهنة والمحتملة في الشأن المحلي والإقليمي والدولي، ويتعامل مع باحثين من مختلف التخصصات داخل العراق وخارجه، وتحتضن بغداد المقر الرئيسي للمركز.

للتواصل

العراق - بغداد - الكرادة

+964 7810234002

hcrsiraq@yahoo.com

www.hcrsiraq.net

مركز حمورابي للبحوث والدراسات الاستراتيجية

تعد الحرب الالكترونية جزءا من الحرب بشكلها الحديث، لانه لها تأثير عميق على الحرب السيبرانية والعكس صحيح، وذلك لأن الحرب الالكترونية هي الهجمات التي تشن في الطيف الكهرومغناطيسي الذي يستخدم في الانظمة الخاصة بالحرب السيبرانية خاصة، حيث يمكنها تعطيل الانظمة التحتية التي تشكل قدرات الحرب السيبرانية لخصومها دون توجيه ضربة مادية واحدة، وهذا الامر يمنح القوات المسلحة فرصة دحر التهديدات في البر والبحر والجو والفضاء قبل ان ترى بوقت طويل، تحاول هذه المقالة قراءة عملية.

اولا: الحرب الالكترونية اسلوب قتالي جديد

تطورت التهدديدات العسكرية بشكل سريع في الاونة الاخيرة، إذ أن الهجمات باتت تُشن بطرق غير مسبوقة وذلك بفضل نطاق ترددي واسع حيث اصبحت الحرب الالكترونية مصدر قلق بسبب ان تقنياتها المتقدمة تستخدم كجزء من العمليات العسكرية، كجزء مكمل للقوى التقليدية في ساحة المعركة حيث تستخدم ثلاثة **انواع من القدرات الالكترونية في العمليات العسكرية منها:**

1- الدعم الالكتروني: تعمل هذه القدرة على الكشف السريع عن مصادر الطاقة الكهرومغناطيسية واعتراضها وتحديدها وتتبعها للتعرف على التهديدات وهي تكون احدى مهام الاستخبارات والمراقبة والاستطلاع.

2- الحماية الالكترونية: تشمل هذه القدرة حماية افراد الدولة ومعداتها ومنشآتها من اثار الهجمات المعادية التي تعيق او تدمر القدرات القتالية .

3- الهجوم الالكتروني: يستخدم الهجوم الالكتروني الاستراتيجي للاسلحة الكهرومغناطيسية او اسلحة الطاقة الموجهة لمهاجمة البنية التحتية لالكترونية لقوات العدو بهدف اضعاف قراراتها القتالية او القضاء عليها.

ثانيا: انعكاسات الحرب الإلكترونية على تصميم القوة العسكرية لحلف الناتو

أصبحت الحرب الإلكترونية اليوم عاملاً مركزياً في إعادة تشكيل القوة العسكرية لحلف الناتو، إذ لم تعد مجرد أداة داعمة للعمليات التقليدية، بل مكوّناً رئيسياً يحدد مسار التفوق العسكري، هذا الواقع الجديد يفرض على الحلف تكثيف استثماراته في تطوير أنظمة متقدمة للحماية من التهديدات السيبرانية، وبناء قدرات هجومية قادرة على تعطيل أنظمة الخصوم وشل بنيتهم التحتية الحيوية، كما ينعكس ذلك على مستوى التدريب، اضطر حلف الناتو لاعداد الأفراد العسكريين على مواجهة سيناريوهات إلكترونية معقدة، وعمل على دمج هذه المهارات في مختلف برامج التأهيل والتمارين المشتركة، وإضافة إلى البعد التقني والبشري، يبرز البعد الاستراتيجي من خلال إدماج الحرب الإلكترونية في جميع مستويات التخطيط العسكري، بما يضمن للناتو مرونة عملياتية عالية ويحافظ على تفوقه التكنولوجي في مواجهة خصوم يمتلكون قدرات رقمية متنامية.

يمكن القول ان الحرب الإلكترونية ادت إلى تغييرات عميقة في العقيدة العسكرية للحلف من خلال:

1- إدماج القدرات السيبرانية والإلكترونية ضمن العمليات المشتركة بدل الاكتفاء بوحدات متخصصة.

2- إعادة توجيه الاستثمارات نحو البنية التحتية الرقمية والأنظمة المحصنة ضد التشويش.

3- تزايد الاعتماد على الذكاء الاصطناعي في رصد الأنماط غير المرئية للهجمات والتصدي لها بسرعة.

4- تطوير آليات هجومية إلكترونية لضمان مبدأ الردع، إذ لا يقتصر الأمر على الدفاع.

هذا التحول يعني أن تصميم القوة العسكرية للناتو لم يعد محصورًا في العتاد التقليدي، بل أصبح يشمل قدرات غير ملموسة تُحدد مسار المعارك المقبلة.

ثالثا: كيف تؤثر الحرب الإلكترونية على تصميم القوة العسكرية لحلف الناتو؟

1- تطوير التقنيات والمعدات

أصبح تطوير التقنيات المتقدمة حجر الأساس في مواجهة تحديات الحرب الإلكترونية، حيث يدرك الناتو أن الحفاظ على التفوق التكنولوجي يتطلب استثمارات واسعة في البنى التحتية الرقمية والمعدات المتطورة.

- **الحماية الإلكترونية (EP):**

تسعى دول الحلف إلى تعزيز قدراتها الدفاعية عبر أنظمة حماية متخصصة قادرة على صد محاولات التشويش والتشويش المعاكس، والكشف المبكر عن محاولات الاختراق الإلكتروني، يشمل ذلك تطوير أجهزة استشعار عالية، وبرمجيات تشفير واتصالات مؤمنة، إضافة إلى أنظمة إنذار مبكر للتعامل الفوري مع الهجمات المحتملة. هذه الإجراءات لا تقتصر على المستوى التكتيكي، بل تمتد لتشمل حماية شبكات القيادة والسيطرة الاستراتيجية التي تعد العمود الفقري للعمليات المشتركة.

- **الهجوم الإلكتروني (EA):**

يدرك الناتو أن التفوق لا يتحقق عبر الدفاع فقط، بل من خلال امتلاك قدرات هجومية متقدمة تتيح تعطيل أو تحييد أنظمة الخصوم الإلكترونية، تشمل هذه القدرات استهداف الرادارات لتعطيل عملها، واختراق أنظمة الاتصالات لتضليلها أو شلها، بالإضافة إلى التشويش على أنظمة الملاحة وتوجيه النيران، هذا يفرض على الحلف تطوير أسلحة إلكترونية هجومية تتسم بالدقة والفعالية، وقادرة على إحداث تأثير مباشر في بنية الخصم العملياتية.

2- إعادة هيكلة التدريب والجاهزية

لا يقتصر تأثير الحرب الإلكترونية على التكنولوجيا فحسب، بل يمتد إلى العنصر البشري، إذ أصبح تدريب الجنود والقادة على التعامل مع بيئة عملياتية "ملوثة إلكترونياً" أمراً لا غنى عنه، لذا، يعمد الناتو إلى إدماج سيناريوهات إلكترونية معقدة في مناوراته العسكرية الدورية، مع التركيز على التنسيق بين القوات الجوية والبرية والبحرية في ظروف تتعرض فيها الاتصالات والتوجيه للتشويش أو التعطيل، كما يتم تطوير عقائد جديدة تدمج بين المهارات القتالية التقليدية والقدرات الرقمية، بما يضمن مرونة وفعالية أعلى في أرض المعركة.

3- الدمج في مستويات التخطيط العسكري

تتجلى أهمية الحرب الإلكترونية أيضاً في بعدها الاستراتيجي، حيث أصبحت جزءاً لا يتجزأ من جميع مستويات التخطيط العسكري، بدءاً من وضع العقيدة الدفاعية العامة وصولاً إلى تنفيذ العمليات التكتيكية. فالناتو لم يعد ينظر إليها كأداة مساندة، بل كركيزة أساسية في أي عملية عسكرية مشتركة. إن دمج القدرات الإلكترونية في هيكل القوة يضمن للناتو القدرة على العمل في بيئات عالية التهديد، ويحافظ على توازنه أمام خصوم يمتلكون أدوات متقدمة للحرب الرقمية.

رابعاً: التحديات المستقبلية للحرب الإلكترونية على حلف الناتو

يواجه حلف الناتو في المرحلة المقبلة مجموعة من التحديات البنيوية والاستراتيجية التي تُهدد قدرته على الحفاظ على تفوقه العسكري والتكنولوجي، هذه التحديات يمكن تصنيفها ضمن أربعة أبعاد مترابطة: تكنولوجية وابتكارية، تشغيلية ومؤسسية، مفاهيمية واستراتيجية، وأخيرًا اجتماعية ومجتمعية.

1- التحديات التكنولوجية والابتكارية

- **التطورالسريع للتقنيات الهجومية:**

خصوم الناتو- ولاسيما روسيا والصين – يواصل ونتطوير قدرات متقدمة فيمجالات الحرب السيبرانية، والتشويش الكهرومغناطيسي، والطائرات المسيّرة المدعومة بالذكاء الاصطناعي. هذا التطور المتسارع يفرض على الحلف استثمارات مستمرة في البحث والتطوير لمواكبة المنافسة وعدم فقدان ميزة التفوق.

- **التقنيات الناشئة والمزعزعة للاستقرار:**

ظهور أدوات جديدة مثل الأنظمة المستقلة (Autonomous Systems) والذكاء الاصطناعي التوليدي (Generative AI) يغيّر طبيعة الصراع جذريًا. هذه التقنيات لا تقتصر على تعزيز قدرات الناتو، بل تمنح الخصوم فرصًا لإحداث اختراقات استراتيجية يصعب التنبؤ بها، مما يخلق حالة من عدم الاستقرار التكنولوجي.

2- التحديات التشغيلية والمؤسسية

- **بطء الاستجابة المؤسسية:**

يعتمد الناتو فيصنع قراراته على مبدأ الإجماع، مايؤدي إلى بطء في اتخاذ القرارات الحاسمة عند وقوع أزمات مفاجئة. هذا القيد المؤسسي يضعف من سرعة رد الحلف على الهجمات الإلكترونية التي تتسم غالبًا بالمباغتة والمرونة.

- **غياب المعايير الموحدة:**

لا تزال هناك فجوة كبيرة في وضع معايير موحدة للعمليات الإلكترونية المشتركة بين الدول الأعضاء. هذا الغياب يخلق صعوبات في تنفيذ عمليات منسقة ويزيد من التكاليف والازدواجية، فضلًا عن احتمالية وقوع

أخطاء عملياتية تؤثر على الفعالية القتالية.

- **تطوير القدرات والتنسيق:**

الحاجة قائمة لتعزيز مستوى التنسيق بين الدول الأعضاء من خلال برامج مشتركة للتدريب، والبحث، وتبادل المعلومات الاستخبارية. فالتباين في القدرات الوطنية يُضعف الجاهزية الشاملة للحلف أمام التهديدات الإلكترونية المعقدة.

3- التحديات المفاهيمية والاستراتيجية

- **الحرب المعرفية (Cognitive Warfare):**

يشكل استهداف الوعي البشري، سواء عبر المعلومات المضللة أو الهجمات السيبرانية النفسية، بعدًا جديدًا في ساحة الصراع. هذه "الحرب على الإدراك" تتجاوز الأنظمة التقنية إلى العقول البشرية نفسها، مما يفرض على الناتو تطوير مفاهيم واستراتيجيات تتعامل مع الأبعاد النفسية والمعرفية للصراع.

- **التهديدات الهجينة:**

يستخدم خصوم الناتو بشكل متزايد أدوات هجينة تجمع بين الهجمات الإلكترونية، والضغوط الاقتصادية، والتدخلات الإعلامية، وأحيانًا التهديدات العسكرية المباشرة. هذا النمط الهجين يجعل من الصعب التمييز بين حالات الحرب والسلم، ويستدعي من الناتو اعتماد مقاربة شاملة تتكامل فيها القدرات العسكرية والسياسية والاقتصادية.

4- التحديات الاجتماعية والمرونة المجتمعية

- **زيادة المرونة المجتمعية:**

إن الهجمات الإلكترونية لا تستهدف الأنظمة العسكرية وحدها، بل تمتد إلى البنى التحتية المدنية مثل شبكات الطاقة والاتصالات والنقل.

كما يعمل الحلف على تعزيز المناعة المجتمعية في مواجهة تهديدات الحرب الالكترونية حيث ان المناعة المجتمعية تمثل خط الدفاع الأول ضد آثار الحرب الإلكترونية، وتعمل على التقليل من قدرة خصوم الناتو على شلّ إرادة المجتمعات.

الخاتمة

تشير التطورات المتسارعة في ميدان الحرب الإلكترونية إلى تحوّلها من مجرد وسيلة مساندة للعمليات التقليدية إلى ركيزة استراتيجية قائمة بذاتها، تُعيد صياغة قواعد الاشتباك وتوازنات الردع داخل حلف شمال الأطلسي. فالتحديات الجديدة التي يفرضها خصوم الحلف من خلال القدرات التقنية المتقدمة، والاعتماد المتزايد على الهجمات الهجينة والمعرفية، تجعل الناتو أمام استحقاق حتمي يتمثل في إعادة تقييم بنيته المؤسسية ومراجعة منظومته العقائدية بما يتلاءم مع طبيعة البيئة الرقمية المعاصرة.

غير أن امتلاك التكنولوجيا المتطورة لا يكفي بحد ذاته لضمان التفوق، فالعنصر الحاسم يكمن في القدرة على تحقيق الانسجام بين القرار السياسي والبعد العملياتي، إلى جانب بناء قدرة مجتمعية تستطيع امتصاص الصدمات الإلكترونية وتقليل تداعياتها على الأمن المدني والعسكري. ومن ثم، يمكن القول إن مستقبل الحلف الأطلسي لن يُقاس بمدى ما يمتلكه من أدوات تقنية فحسب، بل بقدرته على التكيف مع بيئة أمنية سريعة التحول ومعقّدة الملامح، حيث غدت الحرب الإلكترونية عاملا حاسما في الحفاظ على وحدة الحلف وفاعليته الاستراتيجية.