مقال رأي

لماذا يصر العراق على جيش تقليدي ويهمل جيشه السيبراني؟

أ.م. د حازم جري منيخر

مؤسسة إنكي للدراسات والبحوث
Enki Foundation for Studies and Research

المقدمة

لم يكن طرح إقرار قانون الخدمة الإلزامية في العراق مفاجئاً، بقدر ما كان كاشفاً عن خلل عميق في فهم طبيعة الدولة الحديثة. ففي الوقت الذي تتجه فيه القوى الكبرى إلى حروب غير مرئية تدار عبر الشيفرات والخوارزميات، ما زال النقاش المحلي يدور حول إعادة إنتاج نموذج عسكري تقليدي أثبت محدوديته في عالم لم يعد يعترف بالحدود الصلبة.

لقد سعيت منذ عام 2019، وبالتعاون مع نخبة من كبار الأساتذة والخبراء، إلى طرح مشروع متكامل لتأسيس مجلس أمن سيبراني أو ما يمكن تسميته بـ «الجيش السيبراني العراقي». لم يكن الطرح نظرياً أو إعلامياً، بل مدعوماً بدراسات مفصلة قدمت إلى مؤسسات الدولة، وعرضت في لقاءات رسمية مع جهات أمنية عليا، بل حتى داخل أروقة مجلس الوزراء في زمن حكومة مصطفى الكاظمي.

لم تحظى أطروحة مجلس الأمن السيبراني أو الجيش السيبراني بالأهمية المطلوبة وفقاً لطبيعة التطورات وحركة المتغيرات في هذا المجال على أقل تقدير في البيئة الإقليمية المجاورة للعراق، إذ يلاحظ غياب استجابة مؤسسية واضحة لدمج التحولات السيبرانية ضمن الاستراتيجية العامة للدولة؛

فبالرغم من تعدد الملفات والمسؤوليات التي تضطلع بها المؤسسات العراقية، لا يزال هناك فجوة ملموسة في حوكمة هذا الملف وإدارته. وقد أدى ذلك إلى بروز مواطن ضعف في قطاعات حيوية وحساسة، تأتي في مقدمتها المؤسسات الأمنية التي تواجه تحديات متزايدة في مواكبة هذا التطور

تفتيت الفكرة بدل تبنيها

أسهمت التحولات المتسارعة في المجال السيبراني إلى اهتمام دول المنطقة بتطوير قدراتها الرقمية والأمنية، ولا سيما في المملكة العربية السعودية والإمارات العربية المتحدة وإيران وتركيا، حيث بات الفضاء السيبراني يشكل ركيزة استراتيجية في منظومات الأمن الوطني. وقد تزايدت أهمية دمج التقنيات السيبرانية في دعم جهود مكافحة الجريمة المنظمة والتطرف العنيف، إلى جانب توظيفها في تحسين إدارة الموارد البشرية، وتعزيز كفاءة المؤسسات، ورفع مستويات الرصد والتحليل واتخاذ القرار، بما ينسجم مع متطلبات التحول الرقمي والتحديات الأمنية المعاصرة.

بات الفضاء السيبراني يشكل ركيزة استراتيجية في منظومات الأمن الوطني. وقد تزايدت أهمية دمج التقنيات السيبرانية في دعم جهود مكافحة الجريمة المنظمة والتطرف العنيف، إلى جانب توظيفها في تحسين إدارة الموارد البشرية، وتعزيز كفاءة المؤسسات

بدلاً من تبني مشروع وطني متكامل ينسجم مع هذه التحولات والاستراتيجيات في المحيط الإقليمي القريب، لجأت المؤسسات إلى تفتيت الفكرة. فأنشأت كل وزارة قسماً صغيراً تحت مسمى «الأمن السيبراني»، بلا رؤية موحدة، بلا هيكل استراتيجي، وبلا تأثير فعلي. هكذا تحولت الفكرة من مشروع سيادي إلى مجرد عناوين إدارية متفرقة، تستخدم للدعاية أكثر مما تستخدم للحماية. وبالرغم من محاولات تطوير الإجراءات عبر لجان وفريق وطني لصياغة استراتيجية

أمن سيبراني بقيت الإجراءات ضعيفة وغير قادرة على مواكبة التحولات المتسارعة في هذا المجال خاصةً بعد دمج الذكاء الاصطناعي في معالجة البيانات وحمايتها مما يجعل العراق في مراحل متأخرة بالمقارنة مع دول أخرى في المنطقة تواجه تهديدات ومخاطر أقل مستوى من العراق نفسه.

الجيش التقليدي: استجابة عاطفية لا استراتيجية

في ظل عودة النقاش حول الخدمة الإلزامية، يبرز تساؤل جوهري يتعلق بطبيعة الدولة التي يراد بناؤها: هل تتجه نحو ترسيخ نموذج الدولة الحديثة القائم على الكفاءة والتخصص، أم نحو إعادة إنتاج أدوات تقليدية ارتبطت بظروف تاريخية مختلفة؟ إن هذا الجدل لا يقتصر على البعد العسكري فحسب، بل يمتد إلى فهم أوسع لوظيفة المؤسسة العسكرية ودورها ضمن منظومة الأمن الوطني المعاصر.

غالباً ما يستند الدفاع عن الخدمة الإلزامية إلى مبررات اجتماعية تتعلق بتعزيز الانضباط أو ترسيخ المسؤولية أو بناء الشخصية، وهي اعتبارات تحظى باحترام من الناحية المجتمعية، لكنها لا تكفي لتأسيس عقيدة أمن قومي أو صياغة سياسة دفاعية فعّالة. فالجيوش في السياقات الحديثة لم تعد مؤسسات للتنشئة الاجتماعية بقدر ما أصبحت أدوات سيادية متخصصة لحماية الدولة ومواجهة التهديدات المتغيرة. وإذا كانت هناك حاجة إلى معالجة اختلالات اجتماعية أو تربوية، فإن ذلك ينبغي أن يتم عبر إصلاح التعليم والتنمية وبناء الفرص، لا من خلال تحميل المؤسسة العسكرية أدواراً تتجاوز وظيفتها الاستراتيجية الأساسية.

القوة الحقيقية: جيش لا يُرى

في المقابل، يمثل الجيش السيبراني تحولاً نوعياً في مفهوم القوة الوطنية، إذ لم يعد معيار التفوق مرتبطاً بحجم القوات التقليدية أو عدد الأفراد بقدر ارتباطه بامتلاك قدرات تقنية متقدمة قادرة على العمل في الفضاء الرقمي. فالقوة السيبرانية الحديثة تعتمد على فرق محدودة العدد وعالية التخصص، تمتلك مهارات تقنية واستخبارية تتيح لها التعامل مع التهديدات غير التقليدية بكفاءة عالية وفي نطاقات تتجاوز الحدود الجغرافية.

ويمكن لجيش سيبراني يضم عدداً محدوداً من الخبراء أن يؤدي أدواراً استراتيجية تشمل حماية البنية التحتية الرقمية للدولة، والتصدي للهجمات الإلكترونية العابرة للحدود، وتنفيذ عمليات اختراق دفاعية أو هجومية عند الضرورة، فضلاً عن

التأثير في بيئات المعلومات والرأي العام عبر الفضاء الرقمي. كما أن كلفة تطوير هذه القدرات تبقى أقل بكثير مقارنة بالإنفاق المرتبط بالجيوش التقليدية واسعة النطاق، وهو ما تؤكده تجارب دول أعادت تعريف مفهوم القوة من منطق الكم العددي إلى معيار القدرة على التأثير والسيطرة في البيئات التكنولوجية الحديثة.

الخلاصة: قرار بين الماضي والمستقبل

في المحصلة، لا يتعلق النقاش بالاختيار بين وجود الجيش أو غيابه، بل بكيفية إعادة صياغة دوره بما يتوافق مع طبيعة التهديدات والتحولات التي يشهدها العالم. إن الإصرار على إعادة إنتاج نموذج الجيش التقليدي بمعزل عن بناء قدرات سيبرانية متقدمة قد يعكس قراءة محدودة لمتطلبات الأمن المعاصر، ويؤدي إلى فجوة بين طبيعة المخاطر الحديثة والأدوات المستخدمة لمواجهتها.

يمكن لجيش سيبراني يضم عدداً محدوداً من الخبراء أن يؤدي أدواراً استراتيجية تشمل حماية البنية التحتية الرقمية للدولة، والتصدي للهجمات الإلكترونية العابرة للحدود، وتنفيذ عمليات اختراق دفاعية أو هجومية عند الضرورة

إن الحاجة اليوم لا تتمثل في إلغاء المؤسسة العسكرية أو التقليل من أهميتها، بل في إعادة تعريفها ضمن إطار استراتيجي أكثر شمولاً ومرونة. فالجيوش الحديثة مطالبة بالجمع بين القدرات التقليدية والرقمية، وبناء منظومات دفاعية قادرة على حماية الدولة في المجالات البرية والبحرية والجوية، إلى جانب الفضاء السيبراني الذي أصبح ساحة مركزية للصراع والتأثير في القرن الحادي والعشرين.

التوصيات:

1. تأسيس مجلس وطني مستقل للأمن السيبراني من خلال إنشاء هيئة وطنية مستقلة تتولى وضع الاستراتيجيات السيبرانية، وتنسيق السياسات الأمنية الرقمية، وإدارة الاستجابة الوطنية للتهديدات الإلكترونية، بما يضمن وجود مرجعية موحدة لصنع القرار في هذا المجال الحيوي.
2. بناء جيش سيبراني محترف ومتخصص وتطوير قوة سيبرانية تعتمد على الكفاءات التقنية والخبرات المتقدمة في مجالات الأمن الرقمي، والتحليل الاستخباري، وحماية البنية التحتية الرقمية، بما يعزز قدرة الدولة على الردع والدفاع في الفضاء السيبراني.
3. توحيد الجهود المؤسسية ضمن إطار وطني متكامل والحد من تشتت المسؤوليات بين الوزارات والمؤسسات المختلفة عبر إنشاء منظومة تنسيق مركزية، تضمن تكامل الأدوار وتبادل المعلومات ورفع كفاءة إدارة المخاطر السيبرانية على المستوى الوطني.
4. الاستثمار في المعرفة والتأهيل التقني والانتقال من التركيز على النماذج التقليدية في بناء القوة إلى الاستثمار في التعليم التقني والبحث العلمي وتطوير المهارات الرقمية، بما يسهم في إعداد كوادر قادرة على التعامل مع التحديات الأمنية المستقبلية.
5. إعادة تعريف مفهوم الأمن الوطني وتبني رؤية أمنية حديثة تدمج بين القدرات العسكرية التقليدية والقدرات الرقمية، بحيث يصبح الأمن السيبراني جزءاً أساسياً من منظومة الدفاع الوطني والاستراتيجية الشاملة للدولة.

6. تطوير بنية تشريعية وتنظيمية للأمن السيبراني وسن قوانين وسياسات واضحة تنظم الأمن الرقمي، وتحمي البيانات والبنى التحتية الحيوية، وتحدد مسؤوليات المؤسسات الحكومية والقطاع الخاص في مواجهة التهديدات الإلكترونية.
7. تعزيز الشراكات الدولية والإقليمية وتوسيع التعاون مع الدول والمنظمات المتخصصة في الأمن السيبراني لتبادل الخبرات والمعلومات، والاستفادة من التجارب الناجحة في بناء القدرات الدفاعية الرقمية.
8. اعتماد مقاربة مستقبلية في إدارة الدولة وتحديث آليات التخطيط الأمني والاستراتيجي بما ينسجم مع طبيعة التحولات التكنولوجية، لتجنب إدارة تحديات القرن الحادي والعشرين بأدوات ومفاهيم تعود إلى سياقات القرن العشرين.