تحليلات وآراء

الأنظمة "السيبرانية- الفيزيائية" العسكرية وموجبات تطوير إستراتيجيات حفظ "الأمان السيبراني"

بقلم

د . ساعود جمال ساعود

جامعة دمشق

مركز حمورابي للبحوث والدراسات الاستراتيجية

2026

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

تبرز تمظهرات الأمان السيبراني إنطلاقاً من واقع فُرض تكنولوجياً تبعاً للتوظيف العسكري للفضاء الرقمي، وفق شاكلة زادتها خطورةً، اللجوء إلى دمج تقنيات الذكاء الاصطناعي بالأسلحة المبتكرة الحديثة والقديمة المحدّثة، وتتابعات تطوير أليات دفاعية وهجومية، مفاد هذا الواقع أن الأمان السيبراني لم يعد مجرد حماية للبيانات، بل أصبح يمثّل حماية للمكونات المادية التي يمكن أن تؤثر بشكل مباشر على ميزان القوى العسكرية، مما أقتضى قيام مراكز البحوث العلمية المعنية الأنظمة السيبرانية- الفيزيائية العسكرية، بتطوير أنظمة وقائية مضادة مساحات القوة التشابكية بين القوة المادية والتكنولوجية مثل أنظمة القيادة والتحكم وملحقاتها من مكونات البنية التحتية العسكرية والاستخباراتية لدى الدول التابعة تكنولوجيا في ظل ما فرضه التفاوت في المقدرات السيبرانية من تقسيمات نسقية للدولة على أساس معطيات قوتها وما تملكه من مراكز أبحاث بالمجال المذكور تعنى بالتخطيط والتطوير بما يتناسب مع العقيد العسكرية للدول، فمصر عبر مركز الدفاع السيبراني العسكري توظف مخرجاته للأغراض الدفاعية مثل حماية بنيتها التحتية، بينما تركيا تسخّر تقدّمها بالفضاء الرقمي لخدمة مشاريعها الجيوسياسية في عمقها الاستراتيجي، كما فعلت في سورية وتزويدها للفصائل المسلّحة بمقاتلات بيرقدار ونقل تكنولوجيا صناعة مسيرات الشاهين اللامحلية.

وبوتيرة متسارعة تحرص مجمعات صنع الأسلحة بتمظهراتها العصرية، على إتسام مخرجات التطورات العسكرية الحديثة بالتمدد والتداخل في مكوناتها وأبعادها، والهجينية سمة رئيسية ومنطلق لا يعرف له عنصر ولا شكل محدد ولا بعد واحد، حيث تبرز الحاجة لقياس مدى تعدد العناصر والمكونات المستخدمة في المنتج العسكري العصري للوقوف على حدود هجينتيه، إذ لم تعد تقتصر على الفضاء السيبراني أو الأجهزة المادية فقط، بل أصبحت تعتمد بشكل متزايد على الأنظمة السيبرانية- الفيزيائية ذات السمة الاندماجية بما تقوم عليه من **شبك المكونين: الرقمي والمادي.**

بعيداً عن تعقيدات المصطلحات ذات اللاجدوى، سوى لأغراض الطلسمة الاستخباراتية، التي تبعد مسافات سنين ضوئية عن الحقل الأكاديمي بطابعة النظري في الدراسات السياسية والاستراتيجية والمرتبطة برغبة الظهور والسيط الأكاديمي، وعدم الإلمام بحيثياته على غرار ما بحوزة مهندسي أمن المعلومات والحواسيب وضباط الغرف المظلمة في أجهزة الاستخبارات وما يملكون من خوارزميات استحلاب المعلومة الحقيقية لا المسيسة أو الخاضعة للتلاعب الأكاديمي والإعلامي، وباتباع أسلوب السهل الممتنع، فإن:

تعرّف الأنظمة السيبرانية- الفيزيائية في السياق العسكري بكونها منظومات متكاملة تدمج بين الفضاء الرقمي (البرمجيات- الشبكات- الخوارزميات) من جهة، والفضاء الفيزيائي (الأسلحة- المركبات- البنية التحتية- المجسّات) من جهة أخرى، بحيث يؤدّي أي تفاعل أو اختراق سيبراني فيها إلى أثر مادي مباشر على

أرض المعركة، والجدير بالتنويه أن الفضاء السيبراني لا يكون مجرد أداة دعم في هذه الأنظمة، بل عنصراً بنيوياً في عمل السلاح نفسه سواء القرار أو التوجيه أو الرصد، وحتى تنفيذ الضربة، ويتم ذلك عبر حلقة مغلقة تجمع أجهزة استشعار ونظم تحكم ومعالجة وشبكات اتصال ومنصات تنفيذ مادي (سلاح- مركبة- منشأة)، بالتالي فإنّ الحرب لم تعد فقط تدميراً مادّياً، بل إعادة برمجة للواقع الفيزيائي عبر الفضاء الرقمي.

وبين تعديل المضمون وانتفاء الطراز والأثر، تجثم الأسلحة التقليدية بأهميتها الغير بالغة إلا برياً في الدول ذات الترتيب العسكري المتدني من حيث المقدرة، والفاعل المؤثر هنا للدول التي عكفت على توظيف التكنولوجيا وتطويعها لأغراض الردع والتوسع واللعب بالنار في مساحات الخفاء والتأثير بالقوة الناعمة التي تحوّر معناها من كلام فارغ "ثقافة ودبلوماسية وغيرها" إلى جميع أنماط وأصناف القوة المحدثة للأثر والتغيير المادي بأساليب غير صلبة وغير مادية، فالهجوم السيبراني الذي يدمر بنية تحتية عسكرية عبر "جماعات هاكتيفية" مجهولة الهوية في عالم اليوم يتفوق بفوارق غير قابلة للحصر على صاروخ صلب تقليدي مجرد من التقنيات الحديثة، قدرته التدميرية مقيدة بحفرة مساحة محدودة وعمق ضئيل. لذا هنا وأمام ضرورة غير بالغة الأهمية، ولكن لتجنب الهوة المعرفية، يضطر المنظر كما الأكاديمي بتوضيح الفارق بين الأنظمة السيبرانية- الفيزيائية في السياق العسكري والأسلحة التقليدية، وهو توضيح لاستكمال بناء الصورة المعرفية وليس بضرورة بالغة كونه يحوي قدراً من البديهية التي تدخر الجهد والوقت أمام الأثر العملي في ميزان المقارنات والمفارقات.....

فيما يتعلّق بالفرق الجوهري بين الأسلحة التقليدية والأنظمة الفيزيائية العسكرية يكمن في منطق العمل فالأسلحة التقليدية تعمل بشكل مستقل نسبياً عن الشبكات، وتعتمد على الإنسان في القرار والتنفيذ، وتأثيرها خطي ومباشر (قذيفة← انفجار← تدمير)، بينما تعتمد الأنظمة السيبرانية- الفيزيائية على الاتصال المستمر والبيانات الحية، والقرار قد يكون آلياً أو شبه آلي، والتأثير غير خطي حيث اختراق صغير قد يؤدي إلى شلل واسع، كما أن تعطل النظام في السلاح التقليدي، يعني توقفه، أما الأنظمة السيبرانية- الفيزيائية، فإنّ السيطرة عليه من العدو تعني تحوّله إلى سلاح ضده أو ضد الحليف.

وعند دراسة المخرجات المصنعة عملياً بمعزل عن تطبيقاتها وأثارها، فنحن أمام أصناف من الأسلحة متشعبة التهجين، وللمشرّح أن يقول في توصيفاته: "سلاح ثلاثي التهجين واخر رباعي التهجين.. الخ"، والتي ستزداد مستقبلاً كلما دقّت التكنولوجيا وتضاعف أثرها، إشارة ودلالة على كم وعدد العناصر الداخلة في تكوين السلاح وطابعها، **ومن أمثلة الأنظمة السيبرانية- الفيزيائية العسكرية:**

أولاً: الطائرات المسيّرة المسلحة (UAVs): هي ليست مجرد طائرات بل أنظمة CPS كاملة تعتمد على نظم ملاحة رقمية (GPS)، تتلقى أوامر عبر شبكات اتصال، وتستخدم خوارزميات تعرّف بصري وتوجيه آلي، وأي اختراق سيبراني قد يؤدي إلى تغيير الهدف وإسقاط الطائرة واستخدامها لجمع معلومات مضادة.

ثانياً: أنظمة الدفاع الجوي الذكية: مثل أنظمة الاعتراض الصاروخي التي تدمج الرادار والتحليل الخوارزمي والقرار الآلي والتنفيذ الفوري، مع التنويه أن الزمن بين الاكتشاف والرد يقاس بالثواني، وفي هذه الحالة فإن الهجوم السيبراني لا يستهدف الصاروخ، بل بيانات الرصد وخوارزمية التقييم وأولوية الأهداف.

ثالثاً: المركبات العسكرية ذاتية القيادة: تشمل دبابات غير مأهولة وعربات إمداد ذاتية وزوارق أو غواصات آلية، تعتمد هذه الأنظمة على الذكاء الاصطناعي وشبكات استشعار كثيفة وقرارات تكتيكية آنية، وأي خلل سيبراني حسب الخبراء المختصين قد يحولها من أداة دعم إلى عبء أو تهديد مباشر.

رابعاً: أنظمة القيادة والسيطرة (C4ISR): وهي العمود الفقري للجيوش الحديثة وتشمل كلا من القيادة والتحكم والاتصالات والاستخبارات والاستطلاع، واختراق هذا النظام لا يدمر سلاحاً واحداً، بل يشلّ الجيش بأكمله عبر تعطيل التنسيق.

كما تجدر الإشارة أن عقيدة "السرب الذكي" في جوهرها تطبيق لهذه الأنظمة ولا تدرس في سياق منعزل عن الإطار العام الجامع لها إلا كجزئية تفصيلية.

نقاط الضعف الاستراتيجية الجديدة لهذه الأنظمة، تتمثل بكونها تخلق أنواعاً جديدة من الهجمات التي لم تكن ممكنة في السابق منها الهجمات على سلسلة التوريد، حيثيمكن للخصم أن يدخل شيفرات خبيثة أو عيوباً في المكونات الإلكترونية أو البرامج خلال عملية التصنيع، هذه الهجمات صعبة الاكتشاف ويمكن أن تسبب أضراراً جسيمة بعد سنوات من نشر السلاح، إضافة إلى الخلل في المكونات المادية مثلاً الهجوم السيبراني لا يقتصر على سرقة البيانات، بل يمكنه أن يؤثر على الأداء المادي للنظام، إذ يمكن لبرنامج خبيث أن يتسبب في إرسال أوامر خاطئة **لمحركات الطائرة المسيرة، مما يؤدي إلى سقوطها أو انحرافها عن مسارها، إضافة إلى تهديدات أخرى مثل:**

أولاً: الهجوم السيبراني ذو الأثر المادي المباشر ويتمثل باختراق رقمي يؤدّي إلى تعطيل محركات وفتح صمامات وتغيير مسارات وتفجير أو تصادم ذاتي.

ثانياً: الهجمات الصامتة وهي هجمات لا تُحدث انفجاراً بل تُبطئ الاستجابة وتُشوّه البيانات وتُربك القرار وهي أخطر لأنها قد لا تُكتشف إلا بعد وقوع الكارثة.

ثالثاً: الهجوم عبر التلاعب بالبيانات عبر تغيير البيانات الداخلة للخوارزمية والتي تؤدي إلى قرارات خاطئة واستهداف غير صحيح وفشل تكتيكي دون أي عطل تقني ظاهر.

رابعاً: الهجوم على الحلقة البشرية- الآلية من خلال استهداف واجهة التفاعل بين الإنسان والنظام، عبر التضليل والإجهاد المعلوماتي وخلق ثقة زائفة بالنظام.

وحول التحديات الأمنية في بيئة الأنظمة السيبرانية - الفيزيائية:

تتعدّد التحديات الأمنية التي في بيئة الأنظمة السيبرانية- الفيزيائية والتي تهدد أدائها وفعالية تأثيرها واستدامة دورها **ومن هذه التحديات:**

أولاً: تعقيد الأنظمة: كلما زاد التعقيد زادت نقاط الضعف وصعوبة الاختبار الكامل واحتمالات الخطأ غير المتوقع

ثانياً: الاعتماد على الاتصال الدائم: أنظمة CPS تفترض اتصالاً مستقراً وزمن استجابة منخفض، لذا إن أي تشويش أو قطع اتصال قد يؤدّي إلى فشل النظام كليًا.

ثالثاً: غموض مصدر الهجوم: في الهجمات السيبرانية يصعب تحديد الفاعل وتتداخل الدول مع الجماعات غير النظامية وتتآكل قواعد الردع التقليدية

رابعاً: التداخل المدني- العسكري: كثير من مكونات CPS العسكرية تعتمد على بنى مدنية (أقمار، شبكات) ما يخلق مخاطر تصعيد غير مقصود.

خامساً: انعدام الفصل بين الأمان السيبراني والأمان المادي: كانت الأنظمة العسكرية المادية في الماضي معزولة عن التهديدات الرقمية، وبالوقت الراهن أصبحت الأجهزة المتصلة ببعضها البعض نقطة ضعف. أي هجوم سيبراني ناجح قد يكون له عواقب مادية وخسائر في الأرواح.

سادساً: التهديدات غير المتماثلة: لا تحتاج الدول إلى امتلاك قوة عسكرية تقليدية لمواجهة خصومها، يمكن لدولة أصغر أن تستثمر في القدرات السيبرانية لاستهداف الأنظمة السيبرانية- الفيزيائية لخصمها الأقوى، مما يعطل أصوله العسكرية باهظة الثمن بتكلفة منخفضة نسبياً. وهنا نذكر التحوّل في المشهد الناجم عن الفواعل الثانوية من منظور مقدرات بعضها من الناحية التكنولوجية، وإحداث أضرار بالغة في الدولة التي تنشط بها...

ومن الأمثلة الواقعية على مديات الأنظمة السيبرانية الفيزيائية ذات الطابع العسكري وأبعاد تأثيرها وحدوده، ما حصل للبرامج النووية الإيرانية ضمن هجوم "ستوكسنت (Stuxnet)" على برنامج تخصيب اليورانيوم الإيراني كونه مثال بارز على هذا النوع من الهجمات، حيث أثرت شفرة خبيثة على أجهزة الطرد المركزي المادية. كما تمتد سيناريوهات تخمين الأثر إلى إمكانية حدوث هجمات مستقبلية تستهدف السيطرة على أسراب طائرات مسيّرة ذاتية، وأنظمة القيادة والتحكم أو الأقمار الصناعية العسكرية أو حتى شبكات الكهرباء والبنية التحتية الحيوية التي تعتمد عليها القوات المسلحة.

استراتيجيات حفظ الأمان السيبراني للأنظمة العسكرية: CP

أصل وضع الاستراتيجيات متمثل في جهد بشري متعدد المنظورات غرضه ابتكار وتطوير أليات وأدوات التعامل مع الأوضاع المستجدة لدرئ مخاطرها أو التقليل من أثارها، بما يضمن ملاحقة الحدث وتجنّب

البينية اللاتمثلية، وتلافي فخ تفاوت المقدرة، وتحييد عامل التضليل في وجهة التوظيف وحصر أبعاد وعنصر المكون، كما في حالة التحديات الأمنية المنبثقة من تطّور الأنظمة (السيبرانية- الفيزيائية) العسكرية في البيئة الدولية، الناتجة عن استحالة الفصل بين الأمان السيبراني والأمان المادي، حيث الاندماجية سمة السلاح العصري (دمج مكونات)، والهجينية سمة الاستخدام العسكري من حيث التخطيط التكتيكي والاستراتيجي والمراحل التنفيذية والأدوات المؤثرة، ووفقاً لهذا كمنظور ومنطلق في الأدراك الاستراتيجي في الدول المتنافسة وتلك الحريصة على بلوغ عتبة الردع في البيئة الدولية" الفوضوية حيث لغة القوة والحكم للأقوى والنبرة التنافسية رائجة خفية وعلانية خاصّة "فواعل النسق الأعلى"، التي تلجأ إلى إدارة الصراع عند معاناة قادتها من "عقدة النكوص"، لذا فإنّ مراكز التخطيط العسكري والاستخباراتي والبحث العلمي، ومجمعات صنع الأسلحة وتطويرها، تطور الأدوات والتقنيات، ولكن بالمقابل تقوم هذه المراكز بالترادف مع مراكز صنع القرار السياسي بتطوير الاستراتيجيات للتعامل مع التهديدات التي تواكب التطوير اللامتناهي لأنظمة الأسلحة السيبرانية- الفيزيائية العسكرية ومنها **على سبيل المثال:**

1. **استراتيجية التصميم الآمن:** إدماج الأمن فيالبرمجياتوواجهات التحكم منذ بدايات مرحلة التصنيع والتجهيز لا إضافته لاحقاً كطبقة ثانوية.
2. **استراتيجية الفصل الوظيفي:** عزل الأنظمة الحرجة وقنوات التحكم والبيانات الحساسة لتقليل أثر الاختراق.
3. **الاعتماد على الإنسان كصمام أمان:** يجب إبقاء القرار النهائي في حالات حرجة بيد الإنسان رغم الأتمتة، ومنع الاستقلال الكامل في الاستخدام القتالي.

تطوير عقيدة ردع سيبراني بما يشمل تحديد خطوط حمراء ووضوح قواعد الرد ودمج الرد السيبراني بالرد العسكري التقليدي.

بالنتيجة العامة: لم تغيّر الأنظمة السيبرانية- الفيزيائية فقط وسائل الحرب بل غيّرت طبيعة القوة نفسها، فالقوة لم تعد تتمثل بامتلاك السلاح فقط، بل في القدرة على التحكم بخوارزميته وحمايته ومنع العدو من إعادة توجيهه، وكتخمين مستقبلي أقرب إلى الجزم فإن ماكندر وسبيكمان العصور القادمة سيؤكدون، من نصيب من يسيطر على الكود ينتصر في الحروب المقبلة لا من يمتلك أكبر عدد من الصواريخ.