

الفضاء السيبراني نهوذج لتوسيع عقيدة الدفاع الإستراتيجي

الأستاذ الدكتور عامر مصباح،

كلية العلوم السياسية والعلاقات الدولية، الجزائر 03

الملخص

تتنافس الأمم من أجل رسم خريطة وطنها السيبراني بواسطة استغلال مصادر قوة متعددة: تجارية، اقتصادية، رمزية، ثقافية، استراتيجية، وكل العناصر التي يمكن أن تتمدد من مستوى الوطن الواقعي إلى البيئة السيبرانية. ليست هناك حدود ثابتة لخريطة الوطن السيبراني ولا خطوط دفاعية معلومة، كما لا توجد حصانة مضمونة ضد الأنشطة العدائية؛ إنما هي منافسة تدار على مسارح متعددة تشمل العقل والمشاعر والوعي وطرق التفكير، المتفوق فيها من يملك شروطها ويتقن فن إدارتها. تحافظ المنافسة السيبرانية على المعنى الاستراتيجي «للتغلب»، لكن بأدوات مغايرة وفريدة في خاصياتها وفواعلها. تتضمن هذه الدراسة مناقشة مثيرة للجدل وتعتبر في نفس الوقت حيوية لأبعاد الأمن القومي العميقة، إنها قضية الوطن السيبراني؛ من حيث امتيازاته، فرصه، وقابلياته للعطب.

الكلمات المفتاحية: الفضاء السيبراني، الأمن السيبراني، الوطن السيبراني، الدفاع السيبراني، الهوية السيبرانية، الثقافة السيبرانية.

Abstract

Nations compete in order to design their cybernation map throughout using multiple sources of powers: commercial, economic, symbolic, cultural, strategic, and all elements that can extend from real nation to cyber one. There are no fixed borders of cybernation map, no definite defensive lines, and no guaranteed immunity against aggressive activities; it is a competition managed on different theaters, encompassing mind, emotions, awareness, and ways of thinking; where the superior is the one who owns its conditions and has the art of conducting it. Cyber competition preserves the strategic meaning of « overcoming », but with different and unique instruments in its features and actors. This study includes an arguable discussion, and it's at the same time vital for deep national security dimensions. It is the issue of cybernation; through its advantages, opportunities, and vulnerabilities.

Keywords: Cyber-space, Cyber-security, Cyber-state, Cyber-defense, Cyber-identity, Cyber-culture.

المقدمة

تشكل القوة السيبرانية إحدى أدوات التأثير السحري غير المسبوقة المستخدمة من قبل الأمم لتعزيز القدرات الدفاعية الرمزية عن المعاني الوجودية للأمة، وفي نفس الوقت إحداث التأثير الاستراتيجي المطلوب في سلوك الآخرين والبيئة المحيطة بالدولة من أجل تحقيق عدد من الغايات السياسية، مثل المناخ المناسب لخدمة المصالح الوطنية، التباري الاستراتيجي الفعال، هزيمة استراتيجية العدو، بناء سمعة الدولة، تسويق المفاهيم الوطنية عبر العالم، تعديل أو تغيير الاتجاهات المضادة، دحض مضامين الحرب الدعائية والإشاعات، تعزيز الروابط السيكلوجية والروحية الوطنية بين الوطن والشتات، دعم الدبلوماسية، خلق الأصول التجارية والاقتصادية، تحسين نظم الإدارة والقيادة والسيطرة، وغيرها من مصفوفة الأهداف التي يمكن أن تساهم في الموقف الدفاعي الموسع والشامل للدولة.

بُنيت المفهمة التقليدية للدفاع على مذهب تطوير أو حيازة مكونات القوة العسكرية من أجل تحسين الموقف الدفاعي للدولة، لكن التطورات السريعة في حقل الشؤون الاستراتيجية والدفاعية الناتجة عن ظهور فضاءات جديدة للقوة العسكرية المادية وغير المادية، أدت إلى تبلور مفاهيم وعناصر جديدة بحاجة لأن تدمج ضمن الاستراتيجية الكلية للدفاع. إنها لا تتعلق بالتعديلات البسيطة الناتجة عن إبداع أسلحة جديدة، تستدعي إعادة هيكلة أو تستلزم تعديلات عملياتية وتكتيكية في إدارة حقل المعركة، كاستبدال مثلا السيف بالبندقية والدرع بالحصن والرمح بالبندقية والمدفع، وإنما القضية تتعلق بإدارة شؤون الدفاع بواسطة مقاربة جديدة ومغايرة لا تستلزم الأسلحة ولا الجنود المدربين على إطلاق النار، بقدر ما تتطلب إلى مهارة العقل الاستراتيجي والأدوات الرقمية ومناهج الحصول ومعالجة وتسويق المعلومات، ضمن فضاء جديد للتأثير الاستراتيجي وتحسين شروط الدفاع الوطني الموسع، يسمى «فضاء القوة السيبرانية»، التي انبثقت كنتيجة للتطور غير المسبوق في حقل أدوات الاتصال الرقمي والتفاعل السيبراني بين الأمم. عبر هذا الفضاء، تتمدد الأمم على حساب بعضها البعض، ليس بواسطة القوة العسكرية الصلبة كما كان شأن الإمبراطوريات الكبيرة، وإنما بواسطة اختراق المجتمعات كمنظومة سوسيو-ثقافية، قيمية، سياسية، تاريخية، بنية أمنية. الأخطر من ذلك، قلب المنافسة الاستراتيجية محددة في التفاعل فوق حقل معركة المعلومات، لربح معركة العقل والسيطرة الحضارية؛ تقاتل الأمم بعضها البعض عبر الفضاء السيبراني بطريقة صامتة من أجل ربح المعركة الرمزية، التي تؤمن السيطرة الاستراتيجية على عقول وطريقة تفكير الشعوب.

ضمن السياق العام للتأثير النوعي الممارس بواسطة القوة السيبرانية من قبل القوى المساهمة في تطوير أصولها أو تلك التي تستغلها، توضع المفاهيم التقليدية (مثل السيادة الوطنية، الدفاع الوطني، مفهوم البقاء القومي) للدولة تحت التساؤل والحوار الاستراتيجي، بسبب القابلية العالية للاختراق بواسطة القوى السيبرانية، وفي نفس الوقت

وجود فرص كثيرة للاستفادة وممارسة التأثير الاستراتيجي. إذا كانت فكرة كولن جراي بأن السجل الاستراتيجي يقضي بأن الخريطة الجغرافية للدول تُرسم بواسطة القوة العسكرية، ومناسبة في تفسير شؤون الدفاع التقليدية للدولة ككيان جغرافي مادي، فإنها غير مناسبة في رسم الخريطة السيبرانية للدولة. إن هذه الأخيرة ترسم بواسطة أدوات واستراتيجيات نوعية، قائمة على جيوش وقدرات من نوع خاص، لا يرتدون البزات العسكرية ولا يحملون الأسلحة النوعية، وإنما هم جيش من الكفاءات العلمية ذات مهارات فنية عالية وخبرة في صناعة المعلومات، التحكم في علم الحوسبة والرياضيات التطبيقية، وكل ما له علاقة ببرامج الحاسوب وفن الإقناع والتأثير؛ يتم تعزيز هذه المنظومة السيبرانية بجيش آخر من الكتاب والصحفيين والمفكرين والفنانين والمعلقين والمغردين الذين يحملون قضية الوطن السيبراني. تُشيد وتتمدد الخريطة السيبرانية للدولة بواسطة القدرة على صناعة المعلومات، بناء المواقع الشبكية، التغذية السيبرانية الوفيرة واليومية، تطوير تكنولوجيا الاتصالات الرقمية المتفوقة، وإبداع التطبيقات السيبرانية التي تستخدم كأدوات في تثبيت وتقوية خريطة الوطن السيبراني ودعم قدرات المنافسة مع الأمم السيبرانية الأخرى.

تتضمن الفرضية العامة فكرة أن رسم الخريطة السيبرانية المشكّلة لمفهوم الوطن السيبراني تُبنى بواسطة اتجاهين للقوة السيبرانية: قدرات تطوير البنية التحتية والمعلوماتية لتسويق مفاهيم الأمة في البيئة السيبرانية من أجل تحقيق التمدد الاستراتيجي لخصائص الشخصية الوطنية والأبعاد الحضارية؛ يتحدد الاتجاه الثاني في تشييد القدرة الدفاعية السيبرانية لحماية الأصول والمعلومات الحساسة للدولة. فإذا كان مفهوم "جوزيف ستالين" حول رسم الحدود الجغرافية للدولة معبر عنه بواسطة مقولته: "أي أحد يمكن أن يفرض نظامه بقدر ما يوصله جيشه لذلك، وليس هناك طريقة أخرى"⁽¹⁾؛ وإذا كانت مفهومة أنصار القوة البرية حول السيطرة الاستراتيجية ملخصة في فكرة وضع «الأحذية على الأرض»⁽²⁾ Boots on the Ground أو التغلب عند "ابن خلدون"⁽³⁾؛ فإن مفهومة القوة السيبرانية في رسم خريطة الوطن قائمة على فكرة أن حدود الدولة تمتد حيث تصل قوتها المعلوماتية والرمزية وقيمها الوطنية وحجم الحيز السيبراني الذي تشغله في تحميل وتدفع المعلومات نحو ومن محركات البحث ومواقع التواصل الاجتماعي والمواقع الشبكية وكل التطبيقات المتاحة. وفق هذا المنظور، تظهر الحاجة الحيوية لتطوير البنية التحتية السيبرانية عبر إنشاء المواقع ومحركات البحث والمنافسة في سوق البضائع السيبرانية.

بنية الإشكالية

ضمن سياق التأثيرات الاستثنائية، الإيجابية والسلبية المطروحة بواسطة القوة السيبرانية، التي تخترق بشكل متزايد عقولنا وطرق تفكيرنا قبل أن تؤثر في حياتنا الاجتماعية والاقتصادية والاتصالية، يمكن التساؤل عن طبيعة محتوى وإمكانيات القوة السيبرانية، هل

هي مجرد حقل فني لتوليد المنافع وصناعة الخدمات الفعالة لجعل الأنشطة الإنسانية أكثر سرعة وأقل كلفة من أجل تسهيل تطور الاقتصاديات الوطنية عبر العالم، أم هي ميدان للمنافسة الاستراتيجية حول المعلومات، القيم، الثقافة، الحضارة، أسلوب الحياة، الهيمنة والتحكم والسيطرة، الاستخبارات، وكل العمليات التي تحمل شروط التفوق على الآخرين؟ هل القوة السيبرانية موجهة للربح الاقتصادي والتجاري أو لربح معركة العقل، المشاعر، الاتجاهات، الإدراكات، والتصورات؟ هل القوة السيبرانية حقل لتفاعل مفاهيم الدولة في السيطرة وخدمة المصالح، أم هي ميدان لتمدد مفاهيم الأمة حول القيم، التاريخ، المعاني والأفكار الوطنية، العلاقات الاجتماعية، والرموز الثقافية والحضارية؟ هل القوة السيبرانية ميدان لتمدد مصالح الدولة فقط أم هي أيضا لتشكيل مفهوم الوطن السيبراني الذي يحمل العناصر المادية والرمزية للمجتمع؟ هل القوة السيبرانية مسرح للمنافسة الاستراتيجية المتعددة القطاعات أم هي لتواصل وتفاعل الجماعات والأفراد؟

يمكن الإجابة عن تساؤلات الإشكالية بواسطة مناقشة اتجاهين رئيسيين في تشكيل الخريطة الرمزية للوطن السيبراني: التمدد الاستراتيجي عبر السيبراني، مرتكزات تشييد الوطن السيبراني.

المحور الأول: التمدد الاستراتيجي عبر السيبراني

يعكس مفهوم التمدد الاستراتيجي القدرة على نقل التأثير بواسطة أشكال القوة المختلفة من المستوى الوطني إلى المستوى العالمي عبر انشاء واستغلال مكونات وفرض الفضاء السيبراني.

لماذا البحث عن الوطن السيبراني؟

يشق الوطن السيبراني قيمته الاستراتيجية من المنافسة بين الأمم حول فضاءات القوة الجديدة الناتجة عن تطوير أدوات السيطرة، الاكتشافات، الإبداعات التكنولوجية، الأفكار والافتراضات، وكل الأنشطة التي يمكن أن تساهم في تشكيل فضاءات جديدة لكسب وممارسة القوة العسكرية بدون الأسلحة من أجل الغايات السياسية. أدى إبداع الإنسان للقارب وركوب البحر إلى تنافس الأمم من أجل السيطرة على البحر والوصول إلى أبعد نقطة ممكن أن تصل إليها السفن، وبذلك استخدم البحر لغزو الأراضي البعيدة أو السيطرة على الدول الضعيفة، وتعتبر الحرب البولونيزية⁽⁴⁾ Peloponnesian War في تاريخ توسيديس أحد الأمثلة التي يمكن الاستشهاد بها في هذا الصدد؛ في العصر الحديث، يمكن الاستشهاد بالدور الذي لعبته السفن في المنافسة على الاكتشافات الجغرافية للعالم الجديد بين الإمبراطورية الإسبانية والبرتغالية. أدى اختراع المحرك البخاري إلى ظهور المنافسة بين الدول حول امتلاك عناصر ما سماها "كولن جراي" «بثورة الممكنة في الشؤون العسكرية»⁽⁵⁾

مثل سكك الحديد، المركبات الآلية، الدبابات، وكل الآلات التي ظهر استخدامها على نطاق واسع في الحرب العالمية الأولى؛ وهكذا بالنسبة لاختراع الطائرة في بداية القرن العشرين، الذي أدى إلى ظهور فضاء القوة الجوية وتطوره بسرعة؛ أنتجت التفجيرات النووية عام 1945 فضاء القوة النووية؛ أدى إرسال أول مركبة فضائية عام 1957 إلى ظهور القوة الفضائية؛ كما أن إرسال أول رسالة الكترونية في بداية سبعينيات القرن العشرين قد دشن عهد القوة السيبرانية التي تُمارس عبرها الأمم النفوذ بلا حدود جغرافية ولا قيود سياسية أو ثقافية أو دينية.

يؤكد السجل الاستراتيجي الطويل أن الأمم التي قادت المنافسة حول مجالات القوة الجديدة ونجحت في امتلاك مكوناتها هي التي استطاعت تحقيق فائز في عناصر القوة المتنوعة، التي مكنتها من توسيع نفوذها على حساب الأمم الأخرى، وتوفير أدوات السيطرة والتحكم فيما وراء حدودها الوطنية؛ ومن ثم، أهلها لأن تكون قوى عظمى تتحكم في النظام الدولي. المفارقة المثيرة للانتباه في هذا أن تمدد القوى المتحكمة في الفضاءات الاستراتيجية التقليدية والجديدة، لم يكن مجرد إسقاط القوة العسكرية الفجة لإخضاع الأمم الأخرى وفق المنظور الخلدوني⁽⁶⁾ فحسب، وإنما كان عملية نقل ونشر القيم السياسية، الثقافية، أسلوب الحياة، التنظيم، وكل المحتوى السياسي والرمزي للأمم المهيمنة؛ ومن ثم، كانت مهام السيطرة الاستراتيجية عبارة عن عملية تمديد للوطن القومي فيما وراء الحدود التقليدية، كمقاربة غير مادية للتحكم في سلوك وعقول الأمم الأخرى. هناك عدة شواهد جغرافية مازالت باقية للتدليل على إرادة الأمم في توسيع خريطة أوطانها إلى ما وراء حدودها، مثل الجزر التابعة للدول في وسط البحار والمحيطات التي تبعد عن الوطن الأم آلاف الأميال. في مثال القوة الفضائية، تتنافس الدول على توسيع خرائطها الجغرافية نحو الفضاء عبر الأدوات المساعدة على القيام بالحملات الاستكشافية نحو الكواكب البعيدة بحثاً عن الموارد والمعادن، كبدية لإعلان السيادة الوطنية عليها عندما تتحقق بوجود تلك الموارد، بواسطة تطوير الأسلحة الفضائية المناسبة لحمايتها.

الخصوصية المميزة للفضاء السيبراني أن المنشأ الأصلي خاص بدولة الولايات المتحدة الأمريكية، التي تحتفظ بالملكية الحصرية للقاعدة المعلوماتية والأنظمة المعقدة في التخزين والتشغيل والتوزيع لكل الخدمات الموفرة بواسطة شركاتها السيبراني العملاقة؛ لكن قرارها بفتح هذا الفضاء للمساهمة العالمية وتحويله إلى فضاء مشترك بين الدول للاستخدام والتطوير، حوَّله إلى ميدان حيوي للمنافسة الاستراتيجية وليس مجرد فضاء لإنتاج الخدمات السريعة وتدفع الأرباح التجارية. المصادر الرئيسية في إدكاء المنافسة الاستراتيجية السيبرانية محددة في الاستخدامات المزدوجة لأجل الأغراض المدنية والعسكرية، توفير الخدمات بالترافق مع قابليات العطب، كسب القوة والحرمان منها، ميدان للحرب والسلام، حقل للهيمنة الثقافية وقمع أو تفكيك الهويات الضعيفة أو الهشة، مجال لعرض الشخصية

الوطنية للأمم أو استهداف التماسك السوسولوجي للمجتمعات؛ إنها تحمل شروط بقاء أو تفكك الدول.

وفق منطق النظرية الاستراتيجية التقليدية أو فرضيات أنصار النظرية الواقعية/ الواقعية الجديدة، فإن زيادة القوة السيبرانية لأحد الأطراف سوف تكون بالضرورة على حساب أمن الآخرين، وأن الأطراف الضعيفة أو التي لا تستطيع حماية نفسها أو تتهاون في تعزيز قدرات دفاعها يجب أن تدفع ثمن الاعتداء في شكل هجمات سيبرانية، قرصنة، تجسس، تخريب معلومات حساسة، وغيرها من الأنشطة العدائية التي تحدث عنها أنصار النظرية السيبرانية⁽⁷⁾. الجذر المعرفي الذي تقوم عليه القوة السيبرانية محدد في أطروحة "سان تزو" حول فكرتين أساسيتين: دور المعلومات في كسب الحرب، والثانية هزيمة استراتيجية العدو دون قتال. عبّر عن الأولى بقوله: "وكما قلنا ونعيده ثانية لأهميته... إذا عرفت عدوك وعرفت نفسك فليس هناك ما يدعو إلى أن تخاف نتيجته في مائة معركة، وإذا عرفت نفسك ولم تعرف عدوك فإنك تقاسي من هزيمة مقابل كل انتصار، وإذا لم تعرف نفسك ولم تعرف عدوك فإنك أحرق وسوف تواجه الهزيمة في كل معركة"⁽⁸⁾. يمكن استنتاج الثانية من قوله: "إن إخضاع العدو من دون قتال هو أرفع امتياز والعمل العسكري هو أقل الطرق جودة لإخضاع العدو، وتعلوها في المرتبة استراتيجية إفساد تحالف العدو وأفضل من كل هذا استخدام الاستراتيجية لهزيمة استراتيجية العدو، إن الأعظم بين القادة ليس المنتصر في مئة معركة بل ذلك الذي لا يحتاج إطلاقاً إلى القتال لينتصر"⁽⁹⁾.

تكمن أهمية الفضاء السيبراني في كونه أصبح مجالا حيويًا للتأثير الاستراتيجي في القوة الرمزية والمعنوية للدول، أو بتعبير "كريستوفر بول" (Christopher Paul) هو مجال حيوي لتفاعل مفهوم «عمليات المعلومات Operation Information»، التي تعني: «الاستخدام المندمج للقدرات الأساسية للقتال الإلكتروني، عمليات شبكة الحاسوب، العمليات النفسية، الخداع العسكري، وأمن العمليات، في تناغم مع الدعم الخاص والقدرات ذات العلاقة، للتأثير، تمزيق، إفساد، أو غصب عدائي للإنسان وصناعة القرار الآلي مع حماية الخصوصية»⁽¹⁰⁾؛ أو هي: «الاستخدام المندمج للقتال الإلكتروني، عمليات شبكة الحاسوب، والعمليات النفسية للتأثير، تمزيق، وإفساد معلومات الخصم وأنظمة المعلومات عند الدفاع عن الذات»⁽¹¹⁾. يشترك كلا التعريفين السابقين لعمليات المعلومات في أنها تستهدف مجالات متعددة للتفاعل القتالي تشمل العطب المادي لقدرات العدو، إحباط المعنويات، الخداع والتضليل المعلوماتي، تماسك القدرات النفسية والانفعالية، الإدراكات، وتمزيق بنى صناعة القرارات الحيوية في قيادة العدو؛ مما يعني بطريقة أخرى أن الحرب الحديثة لا تتفاعل فقط ضمن المجال المادي لحقل المعركة، وإنما تشمل المجالات الأخرى غير المادية التي يمكن أن تدار بطريقة فعالة، بواسطة استغلال القدرات المتاحة في الفضاء السيبراني.

إذا كانت الأطروحة الأصلية لسان تزو مركزة حول كسب الحرب بدون قتال عبر توظيف عناصر المعلومات، فإن عمليات المعلومات تركز على الكسب الحاسم للحرب عبر استغلال قدرات القتال المادية وغير المادية، ضمن الإطار العام المحدد في ربح حرب الأفكار؛ على افتراض أن السيطرة على العقول أهم من السيطرة على الأرض. إن نشر مفاهيم «تفوق القوة الأمريكية»، «أسلوب الحياة»، «المصلحة الوطنية»، «الردع الاستراتيجي»، «الرد الحاسم»، «التدخل السريع»، «الهيمنة السريعة»، وغيرها من المفاهيم التي يتم تسويقها عبر العالم بواسطة أدوات الدعاية المختلفة، هو مجرد بعض أشكال أو مظاهر إدارة حرب الأفكار؛ على اعتبار أن هناك الكثير من مجالات التفاعل الأخرى التي تشكل مستويات مصفوفة لإدارة حقل معركة الأفكار، المحددة من قبل كريستوف بول Christopher Paul في خمس مستويات هي: «العمليات النفسية، الخداع العسكري، العمليات الأمنية، القتال الإلكتروني، وعمليات شبكات الحاسوب»⁽¹²⁾. تعتبر هذه العناصر الخمسة مجالات التفاعل الأساسي لحرب الأفكار ضمن مفهوم عمليات المعلومات، مما يعني من الناحية المنهجية، إمكانية اعتبارها متغيرات مستقلة لتفسير حرب الأفكار كجزء من الحرب السيبرانية؛ بحيث لا يمكن فهم طبيعة وغايات هذه الحرب دون أخذ هذه العناصر الخمسة في الحسبان. صحيح أن حرب الأفكار هي من إنتاج الفكر الاستراتيجي الأمريكي، لكن تأثيرها المفاهيمي على الشؤون الاستراتيجية قد انتشر عبر العالم، وأخذت بها العديد من الدول وفي مقدمتها الصين، روسيا، الكيان الصهيوني وتركيا.

الفضاء السيبراني أصبح حقلاً لتباري القوة الرمزية بين الدول، عندئذ يجب أن يكون مسرحاً لعرض الشخصية الوطنية، الفكرة المقصود التأسيس لها من خلال هذه الأرضية المفاهيمية والنظرية، أنه طالما الفضاء للدولة كجزء من استراتيجية الدفاع من جهة، واشتقاق مصادر القوة الرمزية ومصادر الثروة والربح التجاري من جهة ثانية؛ لا يمكن أن تعرف هذه الأفكار طريقها نحو البيئة التطبيقية ما لم يتم اعتبار الفضاء السيبراني مجالاً لتمدد الجغرافية الرمزية غير المحدود للوطن السيبراني، الذي يتضمن عرض مفاهيم: الشخصية الوطنية، الأمة، التاريخ الاستراتيجي، الثوابت الوطنية، الثقافة الاستراتيجية، الأولويات الوطنية، القيم والتقاليد والأعراف، الانتماء الجغرافي والحضاري، الإنجازات والطموحات وكل العناصر والمعاني والمفاهيم التي تكوّن محتوى الوطن-الأمة.

تشكيل الوطن السيبراني ليس محكوماً بواسطة حجم الجغرافيا، الديمغرافيا أو القوة العسكرية، وإنما يتشكل ويتوسع بواسطة عناصر القوة السيبرانية: عدد المواقع، الشبكات، المحركات، المعلومات، المغردون، البنية التحتية للدفاع ضد الهجمات السيبرانية، القدرات الهجومية على الخصوم، المصممون للمواقع، المتابعون لما ينشر والرد على المحتوى السيبراني المعادي، القدرة على إنتاج التطبيقات المساعدة على إنتاج سرعة نشر المعلومات، الجمهور السيبراني الوطني الموالي، وكل ما يدخل ضمن تكوين البنية

السيبرانية الصلبة والبرمجيات والقدرات البشرية المحترفة. تقاس الأوطان السيبرانية بحجم المساهمة في المحتوى المعلوماتي المقسمة على الزمن، الذي يبدأ من الثانية، الدقيقة، والساعة، ونوعية المعلومات التي يمكن أن تجد لها مستهلكين من عدمه؛ بحيث أنه كلما كانت المعلومات ذات جودة ومفيدة وعلمية ومثيرة للاهتمام، وجدت لها جمهورا كبيرا عبر المجتمع السيبراني العالمي، والعكس صحيح. هناك عنصر آخر له دور في زيادة قوة الوطن السيبراني وهو اللغة، بحيث أنه كلما كتب المحتوى باللغات الأكثر استخداما عبر العالم (الإنجليزية، الروسية، الصينية، الإسبانية، وبالطبع العربية)، كانت فرص زيادة ثقل واتساع خريطة الوطن السيبراني كبيرة. يتطلب هذا الشرط عناصر متنوعة من الجيش السيبراني الذي لا يقوم فقط بإنتاج المعلومات وتخزينها وتوزيعها، وإنما أيضا ينجز ذلك بلغات عالمية متعددة؛ بالإضافة إلى عمليات التحديث للمعلومات وتعويض المتلف منها أو التي تعرضت للحذف أو التشويش أو التدليس أو غير ذلك من الأنشطة العدائية المقصودة، أو نتيجة للأضرار الجانبية الناتجة عن الهجمات السيبرانية. إن مهام جيش الوطن السيبراني ليست محددة في المسائل الدفاعية أو الهجومية فقط، وإنما أيضا القيام بزيادة الحضور السيبراني الوطني على مدار الساعة لأجل الوصول إلى أكبر دائرة ممكنة من المجتمع السيبراني، وفي نفس الوقت تعهّد الصورة الرمزية للشخصية الوطنية في المجال الذهني والإدراكي لكل الذين يتفاعلون مع البيئة السيبرانية يوميا.

ضمن نفس السياق، يقوم الوطن السيبراني على توفير قدرات وأدوات الاتصال والتدفق الفوري والمستمر للمعلومات الموجهة، التي تحمل الاتجاهات الفكرية، الفلسفة السياسية، والأولويات الاستراتيجية الموجهة نحو تعميق مشاعر الاعتزاز بالتفوق الوطني والإنجازات التاريخية أو الحالية، وغيرها من القيم السياسية والاجتماعية المشكّلة للشخصية الوطنية؛ على اعتبار أنه لا يمكن تصور وطن بدون شخصية رمزية تحمل المعاني الحضارية والقيمية. يعني الاتصال السيبراني تلك العمليات التفاعلية عبر البيئة السيبرانية التي تستهدف: النشر والإقناع بعناصر الشخصية الوطنية؛ تشييد وتشغيل عمليات الدفاع السيبراني عن الأصول الحساسة للأمن القومي؛ وفن إدارة استراتيجية هزيمة العدو بدون قتال. تشكل كل واحدة من هذه العمليات مجالا استراتيجيا قائما بذاته يستدعي طاقما بشريا فنيا وصفا من المخططين الدفاعيين وأدوات العمل الخاصة به. من هذا المنظور، يمكن الافتراض بأن عمليات الاتصال السيبراني هي المَعْلَمَات التي ترسم الخريطة الرمزية للوطن السيبراني، وتخلق شروط صموده كجبهة معززة لمفاهيم الدفاع التقليدي؛ وفي نفس الوقت، كقدرة تفاعلية على التمدد واستغراق كل مجالات الأنشطة الاتصالية للمجتمع السيبراني من أجل عرض المحتوى السوسيو-ثقافي-سياسي-اقتصادي، الذي يحمله مفهوم الأمة؛ بهذه الطريقة، يكون مفهوم الوطن السيبراني وعاءً يحمل عناصر الأمة إلى المجتمع السيبراني، وفي نفس الوقت مسرعا لإنتاج مصادر القوة وشروط الدفاع الاستراتيجي عن المصالح الحيوية.

الخطوة الأولى لتأمين نجاح أي جهد سيبراني في هذا الاتجاه محددة في وضوح صورة معاني وحدود وخاصيات عناصر الشخصية الوطنية في ذهن القيادة السياسية والعسكرية، وكذلك القائمين على تشغيل القوة السيبرانية؛ إحدى مؤشرات استقرار هذه الصورة في الذهن أن تكون هذه العناصر غير قابلة للتقسيم، عدم التنازل أو الاختلاف أو التغيير، وتكون موضوعاً للتنشئة الاستراتيجية، وعدم التردد أو التحفظ في الإيمان بها؛ على افتراض أن الأشياء التي لا يؤمن بها أصحابها أو غير مقتنعين بها، لا يستطيعون نقلها للآخرين، لا يستطيعون الدفاع عنها، كما لا يستطيعون تجسيدها في سلوكهم الاجتماعي. من ناحية المفهمة النظرية، لا تصنف العناصر الوطنية على مستوى واحد من الأهمية، وإنما هناك الجوهرية المستمرة في الزمن والمستجدة عبر التطور المستقبلي. تتضمن الفئة الأولى ما يصطلح عليه «بالثوابت الوطنية»، التي تشكل قواسم مشتركة بين عموم أفراد الشعب، وتحمل في مضمونها بذور الاستقرار واستمرار البقاء القومي للدولة وضمانات تلاحم معاني الأمة؛ الجهة المسؤولة عن صياغة وترتيب العناصر الوطنية هي القيادة السياسية، المخولة بتقدير الإجراءات والأدوات والفواعل الوطنية التي تختارها للاستشارة وتوسيع الفهم، ثم تقوم الجهات الفنية بصياغة استراتيجية تسويقها في الفضاء السيبراني.

تم عملية تشييد خريطة الوطن السيبراني المتضمنة نشر وتسويق وترسيخ العناصر الوطنية، بواسطة إنشاء المواقع السيبرانية الناطقة باسم الأمة، التي تقوم الفواعل السيبرانية بالشرح والتعليق وذكر الأخبار، اليومية، القصص التاريخية، الدروس والعبر، التحقيقات والاستنتاجات، المعالجات والبحث في المسائل التاريخية المعقدة، طرح الموضوعات، توجيه تعليقات المغردين، والكثير من الأنشطة التي من شأنها جعل القضايا والعناصر الوطنية حاضرة على أجندة التفاعل السيبراني. يمكن أن تبدو في الظاهر هذه الأنشطة عملية سهلة وروتينية، لكن إذا أخذنا الأنشطة المعادية في الحسبان، فإنها تحتاج إلى جيش سيبراني متكامل؛ على اعتبار أن هناك منافسة سيبرانية نشطة على مدار الساعة بين الأمم حول توسيع خرائط أوطانها السيبرانية على حساب بعضها البعض، خاصة بالنسبة لتلك الدول المتنافسة في العالم المادي على مصالح حيوية، أو محكومة بواسطة ما اصطلح عليه باري بوزان و أوول ويفر «بمبدأ العداوة»⁽¹³⁾ التاريخية.

ليس هناك قائمة نهائية لمكونات البنية التحتية في دعم وتوسيع خريطة الوطن السيبراني المتضمنة عناصر الشخصية الوطنية، وإنما المواقع الشبكية هي مجرد مثال للتدليل على طبيعة وسائل الجيش السيبراني في رسم تلك الخريطة؛ إنها عبارة عن قائمة مفتوحة من الأدوات والمقاربات والتطبيقات القادرة على نقل المعلومات بسرعة الضوء إلى كل المتفاعلين والأعضاء الدائمين أو المؤقتين في المجتمع السيبراني. تشمل تلك الأنشطة البرامج الموجهة، المقالات الأكاديمية، التغريدات الرسمية وغير الرسمية، الكلمات والجمل الهزلية، الأفلام الترفيهية والتاريخية وحتى التجارية، المقاطع السينمائية، الاقتباسات التي لها

علاقة بموضوع الشخصية الوطنية، وتبقى القائمة مفتوحة؛ توجه مثل هذه الأنشطة إلى كل فئات المجتمع السيبراني بما فيها الأطفال. المهام المشتركة للجيش السيبراني ذات العلاقة بحقل التسويق السيبراني، محددة في التسويق، التهذيب، إعادة الصياغة، التنميق، الإثارة، وكل فنيات العرض السيبراني لمضامين المفاهيم والمعاني والأفكار المعبرة عن عناصر الشخصية الوطنية.

يمكن للقائمين على قيادة وتوجيه الجيش السيبراني الاستعانة بتجارب الأمم الأخرى حول استراتيجية رسم خريطة وطنهم السيبراني، خاصة فيما يتعلق بالفنيات والتكتيكات والتقنيات وحتى الإبداعات المتضمنة طرح وتجديد محتوى العناصر الوطنية. الاعتبار الاستراتيجي الموجه للعمل على هذا المستوى من التفاعل السيبراني محدد في افتراض أنه كلما كان فن النجاح في الوصول إلى عقل وقلب المجتمع السيبراني، توسعت وثبتت حدود خريطة الوطن السيبراني في بُعد عناصر الشخصية الوطنية؛ الأهم من ذلك، تكون هذه الخريطة قابلة للتمدد والتفاعل والسلاسة من أجل الوصول إلى أكبر دائرة من الجمهور السيبراني المتعدد الثقافات واللغات. يُشتق بدوره هذا الافتراض من التصور العام حول الاستراتيجية بأنها فن، المستمد أصلاً من فكر سان ترو والمعبر عنه صراحة من قبل "روبرت توماس" (Robert R. Tomes) الذي يرى أن الاستراتيجية هي: «فن وعملية مفهومة أشكال القوة العسكرية المطلوبة للأمن القومي»⁽¹⁴⁾؛ أو كما قال "لiddel هارت" (Liddel Hart) هي: «فن استخدام مختلف الوسائل العسكرية لتحقيق هدف السياسة»؛ أو تعريف الجنرال الفرنسي "أندري بيوفير" (André Beaufre)، الذي يقضي بأنها: «فن التنسيق بين جميع قوات دولة أو مجموعة دول، هدفها الحصول على النتيجة التي تحددها سياسة مشتركة واحدة»؛ أو مفهومة «هيئة أركان القوات المسلحة الأمريكية المشتركة»، التي اعتبرت: «فن وعلم استخدام القوات المسلحة للدولة بغرض تحقيق أهداف السياسة القومية عن طريق القوة أو التهديد باستخدامها»⁽¹⁵⁾. التأكيد على فكرة أن الاستراتيجية هي فن يعني أنها ليست علماً رياضياً دقيقاً (كما أكد على ذلك أيضاً "جين ماك كال" (Gene H. McCall) وزميله⁽¹⁶⁾)، وإنما هي اسقاط القدرة العقلية والمهارة الفنية والتجربة السابقة لغرض تحقيق التفوق العملي، إنجاز الأعمال الصعبة، وهزيمة استراتيجية العدو فوق كل مساح التباري الاستراتيجي، الفعلية والمحتملة؛ تلتقي كل هذه المهام وأخرى في الغاية المرجعية وهي تحقيق أهداف السياسة (المصالح الوطنية الحيوية للأمن القومي).

الوضع في البيئة السيبرانية مشابه وفي كثير من الأحيان أكثر تعقيداً من نظيره في البيئة الواقعية، بسبب أنه يتطلب نوعيات جد خاصة من الجنود الذين يتقنون علم الحوسبة والرقمنة وكل ما يتعلق بالمعادلات الرياضية والخوارزميات المستخدمة في إبداع التطبيقات المعقدة الخاصة بالقوة السيبرانية؛ ليس هذا فحسب، وإنما تشمل القائمة أيضاً علماء متخصصين في فروع المعرفة الاجتماعية المختلفة مثل علم الاجتماع، علم السياسة، الإعلام والاتصال، الأنثروبولوجية، علم النفس، علم الاستراتيجية، وكل علم يساعد على زيادة المعرفة

والاحتراف في توجيه عقل وسلوك الإنسان، يُحسّن مهارة الإقناع، التعلم السريع، صياغة الإدراك، السيطرة على التفكير، تسويق المعرفة والكلمات والرموز وكل الأشياء الموظفة في بناء الوطن السيبراني؛ بالإضافة إلى تطوير البنية التحتية والأصول الحيوية للقوة السيبرانية.

تقضي إحدى أفكار النظرية العامة في الإعلام والاتصال⁽¹⁷⁾ والتجربة العملية بأن الإقناع فن ومهارة يُنجزان بواسطة عقول متقدة الذكاء، تنتقي وتصوغ باحترافية المحتوى الرمزي وتتحكم في التطبيقات السيبرانية، بالطريقة التي تتمكن عبرها من التسلل بسهولة إلى عقول وقلوب الجمهور السيبراني العريض عبر العالم؛ وهكذا تكون هذه العقول هم الرسل السيبرانيون الذين يشيدون الوطن، تحت مناخ المنافسة الشديدة وصراع العقول الذكية والبيئة المتغيرة بمقياس زمن الثانية واللحظة. إذا كانت عملية تجنيد المقاتلين في الجيوش التقليدية تتم بواسطة الخدمة الوطنية أو إغراءات التوظيف، فإن التجنيد السيبراني عملية مركبة تبدأ من رصد مؤشرات العقول اللامعة في الصفوف الأولى من التعليم المدرسي إلى أن يتخصصوا في الجامعة؛ هناك طريق إضافي تقوم به الدول ذات الإمكانيات العالية في التعليم والموارد المالية، المتمثل في استقدام العقول اللامعة من المجتمعات الفقيرة، من أجل تعليمها وتدريبها واستغلال قدراتها المعرفية عبر دمجها في الجيش السيبراني.

في ظل الظروف الحالية، فإن المرحلة الأولى يجب أن تكون مركزة على العقول الوطنية الذكية والحد من النزيف الوطني في هذا المجال، بواسطة تعليمها، تكوينها (يشمل التكوين القضايا العلمية، الثقافة الاستراتيجية، وسياسة الدفاع الوطني)، وتدريبها لدمجها ضمن الجيش السيبراني. الفكرة المقصود التأكيد عليها في هذا الصدد، أن بناء والمحافظة على الوطن السيبراني لا يتطلبان فقط الموارد المالية، وإنما أيضا استراتيجية وطنية واضحة وطويلة الأمد خاصة بتجنيد الجنود السيبرانيين المنحدرين من التخصصات المعرفية المختلفة، ويقومون بممارسة وظيفة سفراء الأمة لدى المجتمع السيبراني العالمي.

فواعل الوطن السيبراني وعملية التشييد

يمكن النظر من ناحية المفهمة الإجرائية إلى فواعل الوطن السيبراني على أنهم أولئك الذين يساهمون بطريقة مباشرة أو غير مباشرة، رسمية أو غير رسمية في بناء الوطن السيبراني، من أجل تحقيق غاية سياسية ذات علاقة بالشخصية الوطنية للأمة، سواء كانوا جماعات أو أفرادا أو كان عملهم منظما أو تلقائيا. اشتقاقا من هذا التعريف، يمكن تحديد ثلاث فئات لهذه الفواعل: الجندي السيبراني، العامل السيبراني، والمواطن السيبراني.

الجندي السيبراني

يتمثل الجندي السيبراني في أولئك الذين يتم انتقاؤهم من بين النجباء في المؤسسات التعليمية المختلفة الذين يحملون الجنسية الوطنية، للعمل ضمن الدوائر المختلفة داخل

الجيش السيبراني بطريقة رسمية، سواء كانوا من العسكريين أو المدنيين، ينحدرون من تخصصات مختلفة يأتي على رأسها علم الحوسبة والرقمنة والبرمجيات؛ وذلك للقيام بالمهام المختلفة المطلوبة في تشييد والدفاع عن الوطن السيبراني. إذن، الشروط السياسية المطلوبة في هذا النوع من الفواعل السيبرانية، أن يكونوا من مواطني الدولة، يعملون وفق لوائح منظمة، ويلتزمون بالتعليمات والإجراءات الخاصة بعملهم؛ بالطبع هناك شروط أخرى خاصة بالوظيفة كالتخصص العلمي، التفوق في الأداء، والكفاءة العلمية والمهنية. تتعلق الشروط السياسية في المقام الأول بالجنسية الوطنية، الانتماء الوطني، وألا يكون متورطا في أعمال خيانة أو التآمر على الوطن؛ هذه الشروط مستمدة تقريبا من مواد الدستور.

العامل السيبراني

أما بالنسبة لفئة العامل السيبراني، فإنها تضم أولئك الذين ليسوا من مواطني الدولة، يتم استقدامهم كمستشارين، خبراء، مهندسين، فنيين، علماء، أساتذة، مرتزقة سيبرانيين، أو كطلبة ضمن برامج التعليم العالي للمهاجرين الذين يخضعون للتعليم على نفقة الدولة، ثم يتم دمجهم للعمل ضمن الجيش السيبراني للقيام بمهام فنية بحتة مطلوبة في عمل القوة السيبرانية. عادة يتم الاستعانة بالعاملين السيبرانيين لعدة أسباب، مثل قيادة المنافسة السيبرانية مع الخصوم، سد الفراغ في بعض المجالات الوظيفية، استخدامهم كطريقة لتوطين التكنولوجيا السيبرانية، الاستعانة بهم في تدريب وتأهيل الكوادر الوطنية، أو الاستفادة من قدراتهم العقلية المتميزة في تطوير أو تحديث البنية التحتية السيبرانية. الحقيقة أن كل الدول بحاجة إلى مثل هذه الكفاءات بسبب ندرتها في العالم، وأخرى تسعى إلى جذبها كطلبة وتشرف على تكوينهم وتوفير كل الشروط المغرية لبقائهم العمل داخل أراضيها بشكل دائم كما سبقت الإشارة إلى ذلك.

المواطن السيبراني

أخيرا، هناك فئة «المواطن السيبراني»، التي تشمل أولئك الذين يتفاعلون يوميا مع البيئة السيبرانية من مواطني الدولة، لغايات متعددة: تجارية، ترفيهية، اتصالية، سياسية، ثقافية، أو تعليمية؛ فهم قوة كامنة تساهم بطريقة تلقائية أو مقصودة في تشييد الوطن السيبراني. إذا استعنا مفاهيم النظرية الاستراتيجية التقليدية، يمكن أن يمثل هؤلاء الاحتياط الاستراتيجي الذي يمكن تعبئته في دعم القدرات الرسمية لغرض بناء والمحافظة أو حتى الدفاع عن الوطن السيبراني. عنصر قوة التأثير في هذا النوع من الفواعل يكمن في أنهم يتحدثون بمشاعر واتجاهات وعواطف الشعب العام، ويعبرون عن الحس الشعبي والاتجاهات السائدة والأيديولوجيات والعادات والأعراف الاجتماعية وكل ما يتعلق بتفاصيل الحياة الاجتماعية كما هي خام في المجتمع؛ ومن ثم، هم يمثلون الاتجاه الأعظم لشخصية الوطن

السيبراني. الأكثر من ذلك، إذا كانت الحروب يُنصب وقودها بواسطة احتياط الخدمة الوطنية أو ما يسميه "كارل فون كلاوزفيتز" «بالاحتياط الاستراتيجي»⁽¹⁸⁾ الذي يضم في معظمه المجندين من الشعب (جيش نابليون بونابرت مثلاً)، فإن أيضاً القاعدة العريضة لتشييد والمحافظة والدفاع عن الوطن السيبراني هي الفئة الثالثة من الفواعل السيبرانية. لا تكون هذه القاعدة العريضة فعالة في إحداث الفرق الاستراتيجي ما لم تكن مزودة بمجموعة من الخصائص الرمزية التي تجعلها قابلة لأن تكون جزءاً حياً من الأمة السيبرانية، مثل الوعي السيبراني، الثقافة السيبرانية، الانتماء السيبراني، والقدرة على التواصل السيبراني الإيجابي مع المعاني الحضارية والتاريخية لمفهوم الأمة.

تعمل العناصر السابقة وأخرى بشكل متلاحم في تكوين وتأسيس وتطوير الوطن السيبراني، على افتراض أن الأشياء تصنع كأفكار في العقل ثم تظهر مع عوامل الطبيعة، ثم تنتج السلوك الذي يشمل الانفعالات، الإنجازات، أنماط التفكير، وأسلوب الحياة؛ كذلك الأمر بالنسبة للوطن السيبراني يصنع بواسطة الوعي الوطني والثقافة السيبرانية المتضمنان الشروط الأولية، التي تشمل مصفوفة من الأنشطة والمتطلبات مثل الوعي بضرورة الوجود الرمزي للأمة في الفضاء السيبراني، الإجراءات المطلوبة في العمل، المعرفة الضرورية في تشغيل وتأمين النظم السيبرانية على المستوى المتدني والكبير، الوعي بقبليات العطب، وإدراك حقيقة وأهمية المنافسة مع الأمم الأخرى ضمن هذا الفضاء.

مع وجود فرضية التباين حول مساهمة كل فئة في بناء الوطن السيبراني، إلا أنه من الناحية الوظيفية كل فئة متخصصة في ميدان معين؛ ومن ثم، يصبح وجودها مجتمعة ومتلاحمة قضية حاسمة في بناء وتطوير مفاهيم ومفردات عمل الوطن السيبراني، وتأسيس القواعد الفنية والتقنية لتشكيل البنية التحتية المسؤولة عن وجود وبقاء هذا الوطن متفاعلاً مع الأمم الأخرى ويطور نفسه بنفسه؛ تشكل هذه المعاني بطريقة غير مباشرة محتوى أهداف السياسة من وراء تشكيل الوطن السيبراني. مثل نظيره في العالم المادي، يحتاج الوطن السيبراني إلى جيش خاص من العاملين الدائمين وقوة الاحتياط السيبراني، بالإضافة إلى جلب المساعدة من الدول الأجنبية المتمثلة في أولئك الأشخاص الماهرين في استخدام أنظمة الحاسوب، تحميل التطبيقات الجديدة، تحديث البنية التحتية السيبرانية، وتدريب الأطقم الوطنية على كيفية تشغيل المعدات الجديدة المساعدة على تأطير وتوجيه المكونات الرمزية والاتصالية والتفاعلية للوطن السيبراني.

من ناحية أخرى، القواعد التي تحكم العلاقات بين الأوطان السيبرانية هي نفسها السائدة في العلاقات الدولية الواقعية، التي يزرعها بها تراث النظرية الاستراتيجية التقليدية (الواقعية/الواقعية الجديدة، نظرية فن الحرب، نظرية إدارة الحرب بالإضافة إلى النظريات الأخرى المصنفة في كتاب «نظريات علم الاستراتيجية»)، مثل المنافسة الاستراتيجية، الريبة، المساعدة الذاتية، الحرب، الفوضى، وغيرها من المفردات التي فصلنا شرحها في العديد من

الأعمال العلمية السابقة. إن القوة السيبرانية هي مجرد مجال اصطناعي جديد يشبه نظرائه الطبيعيين مثل فضاء البرية، البحرية، الجوية، والفضائية، تجد الدولة خلالها بحاجة لأن يكون لديها مستوى معين من السيطرة الاستراتيجية كمجال للدفاع الوطني أو إنشاء المصالح وحمايتها. المبرر الرئيسي لطرح فكرة الوطن السيبراني بدل الاكتفاء فقط ما يصطلح عليه المتخصصون في هذا المجال «بالفضاء السيبراني» أو «القوة السيبرانية»، محدد في أنه ميدان حيوي لتنافس وتواصل الأفكار والثقافات وعناصر الشخصية الوطنية للأمم، فضلا عن الفوائد التجارية والاقتصادية والعسكرية؛ ومن ثم، هو مجال لتمدد معاني الوطن ومصالح الدولة، التي تشكل بدورها مسرحا لتفاعل القوة الاستراتيجية.

إذا كان لابد من عقد التناظر الاستراتيجي، فإنه يمكن القول أن هناك تشابها طفيفا يجمع بين الفضاء السيبراني ونظرائه من القوة البحرية والجوية والفضائية، المحدد في امتداد يابسة الدولة تحت مياه البحر الذي يصطلح عليه «بالجرف القاري»، وسيادة الدولة على الأجواء فوق إقليمها. هناك نقاش حول سيادة الدول في الفضاء الخارجي عبر البنية التحتية التي تشيد في المدارات المختلفة وربما لاحقا فوق الكواكب، وكذلك الأمر بالنسبة لعناصر الشخصية الوطنية والمصالح الوطنية التي يجب أن تتمدد عبر الفضاء السيبراني؛ النقطة المشتركة بين كل هذه الفضاءات هي تمدد سيادة الدولة إلى خارج حدودها الترابية التقليدية. الجانب المميز في الوطن السيبراني أن التمدد يتعلق بالجوانب الرمزية، العناصر الحضارية الوطنية، الخبرات والمعاني المحمولة بواسطة التاريخ الاستراتيجي الوطني الطويل، وكل العناصر غير الملموسة التي تساهم في تشكيل معنى الوطن الافتراضي؛ تكون كل هذه العناصر والمعاني البنية التحتية الرمزية لترابط وتفاعل معنى المجتمع المتواصل مع بعضه البعض في العالم المادي والممتد نحو العالم السيبراني. بقدر توسع دائرة المنخرطين من الفئات السابقة في تشييد البنية التحتية والخريطة السيبرانية للوطن، يأخذ هذا الأخير في التماسك والاشتداد والتفاعل الاتصالي للوصول إلى معظم الشعوب المتفاعلة في العالم السيبراني، سواء للأغراض الاستراتيجية، التجارية، أو الاقتصادية.

القوة الضاربة في تشييد والدفاع عن الوطن السيبراني هي الفئة الأولى المكونة من الجنود السيبرانيين، وإذا كانت القوة البرية تشكل مركز الثقل الاستراتيجي للجيش التقليدي بالنسبة لكلاوزفيتز، والقوة الجوية بالنسبة لمنظريها، والقوة البحرية بالنسبة لأنصارها، فإن الثقل الاستراتيجي للوطن السيبراني محدد في أولئك الذين يعملون على تشغيل البنية التحتية السيبرانية من الطواقم الماهرة المنحدرة من مواطني الدولة؛ ومن ثم، تكون عملية استقطاب الكفاءات المتفوقة للعمل ضمن أطقم تشغيل القوة السيبرانية، هدفا استراتيجيا حيويا باتجاه بناء الوطن السيبراني. طالما أنها تمثل مركز الثقل الاستراتيجي، فإنه يجدر بفئة الجنود السيبرانيين أن يخضع أفرادها لشروط صارمة من أجل انتقاء أفضل العقول في المجتمع، لقيادة المهام السيبرانية في حالتي السلم والحرب.

يحتاج قلب قوة إدارة وتشغيل البنية التحتية للوطن السيبراني إلى دعم من قبل فئة العاملين لأغراض التدريب، التطوير، نقل التكنولوجيا والخبرات السيبرانية وأداء كل المهام ذات العلاقة بعقد الشراكة الموقع بين الحكومة وعناصر فئة العاملين. يجدر التذكير في هذا الصدد أن فئة العاملين يمكن أن تشمل شركات القطاع الخاص الوطني أو الأجنبي، فرق رسمية مبعوثة من قبل الدول الصديقة أو الحليفة، والأفراد الأجانب الذين يعملون لحسابهم الخاص كمرتزقة أو قراصنة سيبرانيين. تظهر الحاجة لهذا النوع من الفواعل السيبرانية عندما يواجه الوطن السيبراني تحدي قاسي مفروض بواسطة المنافسة السيبرانية، لا يستطيع تخطيه بواسطة قدراته المحلية. بالرغم من أهمية الفئة الأولى والثانية، فإن فئة المواطن السيبراني حاسمة في عمليات التشييد، التطوير، التمدد، التفاعل، ورسم الخريطة المطلوبة في تشكيل الحدود الرمزية للوطن السيبراني.

إذا كان "جيم أوبرغ" (Jim Oberg) قد حدد شروط بناء القوة الفضائية في: «الحجم الجغرافي والموقع، الرفاهية الوطنية، الكثافة والتعليم الجيد للسكان، وجود القوة الوطنية، الميل الشعبي للتكنولوجيا، والإرادة السياسية»⁽¹⁹⁾؛ فإن هناك متغيرات متعددة تتدخل في إضفاء خاصية الفعالية على عملية تشييد الوطن السيبراني، تتقدمها الطموحات السياسية، القيادة والتوجيه، الاستراتيجية، الموارد التكنولوجية والبشرية والمالية، الاعتبارات الحضارية والرمزية، وخصائص الشخصية الوطنية. عندما تتفاعل كل هذه العناصر أو المتغيرات المستقلة بشكل متلاحم، سوف تتدفق آثارها إلى المجالات الحيوية الأخرى فيما وراء الحدود الترابية التقليدية للدولة، لتشكّل المعنى الرمزي والخريطة المحتملة للمتغير التابع وهو الوطن السيبراني. الفكرة الأساسية المراد التأكيد عليها ضمن هذه الجزئية، مفادها أن فئة المواطن السيبراني تشتق أهميتها في التأثير الاستراتيجي من كونها المسرح الفعال في تفاعل كل المكونات الرمزية وخصائص وعناصر الشخصية الوطنية؛ إنها تعبّر عن حجم الوجود الوطني والحضاري النوعي داخل العالم السيبراني، في شكل علاقات اجتماعية، روابط قرابية وصدقات، التي تربط النسيج السوسيولوجي الممتد من البيئة الواقعية إلى نظيرتها السيبرانية.

من حيث المبدأ، فئة «العامل السيبراني» مهمة في تشييد الوطن السيبراني من خلال نقل الخبرة، تعميق المعارف، تحسين المستوى السيبراني، التغلب على التحديات التي تواجه الأمن السيبراني، بالإضافة إلى التدريب على تشغيل المعدات والبرمجيات الجديدة الخاصة بمشاريع تحديث وتشغيل البنية السيبرانية. لكن الأمة التي تبحث عن عمق استراتيجي لوطنها في العالم السيبراني، هي التي تعتمد على كفاءاتها الوطنية والاستثمار في المشاريع الوطنية حول انتقاء وتعهّد العقول الوطنية النابغة، التي تظهر عبر مستويات التعليم المختلفة؛ على اعتبار أنها تمثل جزءاً من الأصول الاستراتيجية الوطنية في الدفاع والأمن وتوليد عناصر القوة الوطنية. تمثل هذه الفئة من المجتمع المصدر الرئيسي لتغذية

صفوف الجندية السيبرانية المسؤولة عن رسم الخريطة الافتراضية للوطن السيبراني، وفي نفس الوقت تشكل القوة الأولية في دعم الخطوط الأمامية للدفاع عن الوطن السيبراني. مثل العالم الاستراتيجي التقليدي، لا يوجد أحد يدافع عن وطنك بالنيابة عنك، كما لا يتطوع أحد لحماية مصالحك السيبرانية؛ بالإضافة إلى أن مهمة صناعة والدفاع عن الوطن السيبراني عملية احترافية ليس بمقدور المواطن السيبراني القيام بها، فهي مهمة الجندي السيبراني المزود بالمهارات العقلية والمعرفية والخبرة والمهارة المكتسبة بواسطة الممارسة وبرامج التدريب، التي تساعد على القيام بالعمليات السيبرانية المعقدة.

الفكرة الأساسية المراد التأكيد عليها في هذا الصدد، أن الأمة التي تبحث عن وطن سيبراني لها، يجدر بها النظر إلى العقول النابغة والكفاءات اللامعة داخل مجتمعها كثروة عالية القيمة، تصنف تحت فئة المصالح الحيوية للدولة، التي يجب الاحتفاظ بها تحت كل الظروف، بواسطة خلق شروط المناخ المناسب الذي تستطيع -في ظله- هذه الفئة أن تبذل وتستثمر قدراتها العقلية والمعرفية لغرض إنتاج المعدات والتطبيقات والأفكار، القادرة على حمل الوطن السيبراني إلى مستوى الكفاءة المطلوبة في المنافسة الاستراتيجية مع الأمم السيبرانية الأخرى، وتمديد الخطوط التي تتدفق عبرها عناصر الشخصية الوطنية والمكونات الحضارية والرمزية للسوسيولوجية الوطنية نحو العالم السيبراني.

من الناحية التناظرية مرة أخرى، إذا كان ادعاء كولن جراي⁽²⁰⁾ صحيحاً حول فكرة أن الخرائط الجيو-سياسة للدول تُرسم بواسطة القوة العسكرية في العالم المادي، فإن خرائط الأمم السيبرانية ترسم بواسطة الجندي السيبراني الذي لا يحمل المعلومات والأفكار السيبرانية ذات المحتوى الفني والتقني فحسب، ولكنه يحمل أيضاً الثقافة والرموز والمعاني الوطنية والانتماء الحضاري؛ أو ما يمكن الاصطلاح عليه بثقافة الحضارة السيبرانية. نفس المنطق يُشتق من حقل الثقافة الاستراتيجية، فإذا كان أنصار نظرية الثقافة الاستراتيجية⁽²¹⁾ في العالم الواقعي يفترضون أن الثقافة ترحل مع الجنود إلى حقل المعركة، فإنه يمكن الافتراض بأن محتوى القيم الوطنية والجذور الحضارية للأمة ترافق الجنود السيبرانيين خلال كل عمليات رسم وتثبيت وتفاعل وتمديد حدود الخريطة الرمزية للوطن السيبراني.

المحور الثاني: مرتكزات تشييد الوطن السيبراني

تتضمن عملية تشييد الوطن السيبراني الاهتمام بتطوير القدرات حول ثلاث مجالات استراتيجية:

- (1) بناء القوة السيبرانية؛ (2) تطوير قدرات الدفاع السيبراني؛ (3) إدارة الحرب السيبرانية.

أولاً: بناء القوة السيبرانية

تعتبر مهمة بناء القوة السيبرانية عملية مركبة، شاقة، مستمرة، وطويلة الأمد، تبدأ من الأساسيات الأولى في التعليم وبحوث علم الحوسبة والبرمجيات، تشييد مكونات البنية التحتية في الاتصالات الرقمية والتفاعل السيبراني، إلى تطوير التطبيقات واستخدام التطبيقات الجديدة؛ في كل مرحلة، تتطلب عملية البناء انضمام أعداد كبيرة من العقول اللامعة والأدمغة النابغة من أبناء الوطن أو المستخدمين من المجتمعات الأخرى. الافتراض العام الذي تقوم عليه عملية بناء وتطوير القوة السيبرانية أن عامل الزمن حاسم في الفعالية والتفاعل عبر سيبراني الذي يحسب بالدقائق وليس بالساعات أو الأيام كما هو شأن الحياة العادية بسبب التطوير السريع الذي تشهده القوة السيبرانية عبر العالم، سواء كتطبيقات جديدة لتحسين قدرة تشغيل البنية التحتية، أو ظهور أشكال التهديد والهجمات السيبرانية التي تتفوق على البرمجيات العاملة وتحطم أو تعطل وظائفها التجارية والاتصالية بحساب سرعة الضوء. بصفة عامة، تشتمل القوة السيبرانية على ثلاثة مكونات رئيسية:

(1) **المكوّن المادي**، الذي يتضمن البنية التحتية المادية مثل المقرات والأبنية للإدارة والقيادة والتحكم، كابلات الاتصالات، أجهزة البث والنقل الاتصالي، منظومة الحواسيب، قدرات التخزين وتوزيع البيانات، شبكات التحكم والتوجيه وغيرها من العناصر المادية التي يمكن تصنيعها محلياً، بالشراكة مع الآخرين، أو اقتناؤها من الأسواق العالمية؛ بالطبع إذا تمت العملية بواسطة الخيار الأول، فإن الوطن السيبراني اكتسب أحد مؤشرات التفوق الاستراتيجي على الأمم السيبرانية الأخرى. في كل الأحوال، كلما اتسعت دائرة الاستقلالية الوطنية في تشييد البنية التحتية المادية للقوة السيبرانية، ازدادت حظوظ الأمة في رسم خريطة وطنها في العالم السيبراني ودعم قدراته على المنافسة والدفاع بنفسه عن نفسه.

(2) **مكون البرمجيات**، الذي يصطلح عليه أيضاً بالقوة اللينة، التي تشكل كل ما يتعلق بأنظمة الحاسوب والتطبيقات السيبرانية وبرامج التشغيل ونظم التخزين والتوزيع للبيانات ومستوى سرعة معالجة تدفق المعلومات؛ بالإضافة إلى برمجيات الحماية والمراقبة وقوة توفير الخدمات السيبرانية لأكبر عدد ممكن من المستخدمين في الدقيقة الواحدة. الأمم الأكثر منافسة حول تطوير أفضل البرمجيات الفعالة، والنوعية في توفير الخدمات السريعة للعملاء هي الولايات المتحدة والصين، تبحث الأولى عن استمرار هيمنتها على الفضاء السيبراني، في حين تبحث الثانية عن الاستغلال الأمثل لهذا الفضاء من أجل توليد الحجم الأكبر من الخدمات النوعية والسريعة عبر العالم.

(3) يتضمن المكون الثالث **الجيش السيبراني** الذي يتولى عملية تشغيل البنية التحتية السيبرانية في صورتها المادية واللينة، من أجل تحقيق مهام متغيرة تشمل عملية توليد الخدمات المربحة، عمليات الدفاع عن الوطن السيبراني، وعمليات الهجوم على الأصول

الحساسة للخصوم كجزء من المنافسة والسيطرة الاستراتيجية في البيئة السيبرانية. تتحكم معايير الجودة، النوعية، الكفاءة، المهارة، النبوغ العقلي، والتجربة في الطريقة التي يتم بواسطتها انتقاء الأشخاص الذين يشكلون الجيش السيبراني؛ في مقابل ذلك، يعتبر الحجم أو أعداد القائمين على تشغيل البنية السيبرانية مؤشرا مهما على قوة الوطن السيبراني، على اعتبار أنه كلما زاد عدد الجيش السيبراني بالمعايير السابقة الذكر، اتسعت خريطة الوطن السيبراني وتصادت فعالية الاتصال والتفاعل وحتى التأثير في الأوطان السيبرانية الأخرى. نفس الملاحظة المسجلة في المكون الأول يمكن تكرارها، وهي أنه كلما اتسعت دائرة العاملين في الوطن السيبراني من المواطنين، ازدادت رقعة نفوذ الوطن السيبراني وقوته في نقل عناصر الشخصية الوطنية، زيادة مصادر الدخل الوطني، تحسين الخدمات ذات الجودة العالية، والتأثير في أساليب التفكير وسلوك الآخرين. يقضي الافتراض العام الذي تتشاطرهُ المكونات الثلاثة، أن القوة الحقيقية القادرة على إحداث ما يسميه بعض المنظرين بالفرق الاستراتيجي، منبثقة من قلب الأمة وليس بمساعدة أو استئجار الآخرين، حتى ولو أن الاستعانة بالآخرين ليست مهمة أو مستثناة من عملية تشييد الوطن السيبراني.

الفكرة العامة المراد التأكيد عليها في هذا الصدد، أن عملية صياغة العقيدة السيبرانية يجب تضع في الحسبان الاهتمام المركّز حول تطوير وتعهّد المكونات الثلاثة للقوة السيبرانية، كمقاربة عملية في رسم خريطة الوطن السيبراني وتعزيز قدراته على المنافسة مع الآخرين، الدفاع عن نفسه بنفسه، وتقويض استراتيجية الخصوم أو الأعداء الفعليين والمحتملين على حد سواء. مثل العالم المادي، قوة الأمم منبثقة من ذاتها وإرادتها في البقاء، التمدد، والتأثير في الآخرين حولها أو البعيدين عنها؛ نفس المنطق ينسحب على القوة السيبرانية التي تنبثق من القدرات الذاتية للوطن السيبراني، الذي يصنع بها نفسه، يفرض بواسطتها نفسه على الخريطة السيبرانية، يدافع بها عن نفسه، وفي نفس الوقت ينتج عناصر القوة الوطنية الأخرى مثل الخدمات التجارية، الاتصالات، الترفيه، التفاعل الاجتماعي، وغيرها من المصادر المدّرة للأرباح المالية والاقتصادية.

من ناحية التحديد الاصطلاحي، يرى "جوزيف ناي" أن القوة السيبرانية هي التي تعتمد على: «الموارد التي تميز مجال الفضاء السيبراني»⁽²²⁾. عرّف كل من "براندون فالريانو" (Brandon (Valeriano و"راي مانيس" (Ryan C. Maness) القوة السيبرانية على أنها: «القدرة على السيطرة واستعمال الأشكال النمطية من السيطرة والتحكم في الفضاء السيبراني. فالخاصية الفريدة للفضاء السيبراني هي قدرة الدول الصغيرة على منافسة القوى الكبيرة في نفس الميدان»⁽²³⁾. يشير مفهوم القوة السيبرانية من الناحية الاستراتيجية إلى الدور المتزايد -وفي بعض الأحيان المهيمن- لنظم الحاسوب والشبكات في صياغة وتشكيل نمط العلاقات الإنسانية، وفي مقدمتها علاقات الحرب والنزاع. في المفهوم العام للقوة عندما يركب بمتغير آخر، فإنه لا يكون معتبرا إلا إذا أدى إلى إنتاج النفوذ السياسي والتأثير

الاستراتيجي للدولة على سلوك الآخرين في مجالات القضية المختلفة، إذ لا معنى للقوة الاقتصادية، العسكرية، الفضائية ما لم تنتج عناصر التأثير على سلوك الآخرين؛ وهذا ما ينطبق أيضا على القوة السيبرانية، التي تكون معتبرة في التحليل الاستراتيجي عندما تنتج تلك الآثار التي تجعل مواقف وسلوكيات الأطراف الأخرى تتغير بناء على تأثير مكونات محتوياتها.

تعني القوة السيبرانية مصفوفة نظم الحاسوب والشبكات التي تتدخل بشكل ملحوظ في تنظيم الحياة الاجتماعية، تحسين أداء الاقتصاد، تأسيس الشركات السيبرانية، زيادة الأرباح المالية والتجارية، ظهور نمط الإنتاج السيبراني، تعزيز القوة العسكرية، تحسين أدوات الحرب، تغيير طريقة القتال، وغيرها من الآثار المحتملة التي تصب كل مخرجاتها في زيادة النفوذ السياسي والتأثير الاستراتيجي للوطن السيبراني على سلوك الأمم السيبرانية الأخرى. يأخذ تمظهر القوة السيبرانية عدة صورة مركزة حول القدرة على إبداع المعدات والتطبيقات الجديدة بالإضافة إلى انضمام مهارات بشرية جديدة من فترة زمنية لأخرى، بحيث تكون أكثر قدرة على المنافسة الخارجية وليس مجرد سوق استهلاك لما ينتجه الآخرون. تحتاج هذه الخاصية إلى دافع سياسي محدد في الإيمان الراسخ بالقدرة على استقطار الكفاءة البشرية في إدارة شؤون الوطن السيبراني من أبناء الوطن، الذين يكونون جسرا مناسباً للعبور إلى كل المجتمعات الأخرى للاستفادة منها أو التأثير في سلوكها وفق الأولويات الوطنية.

الافتراض العام المقترح في هذا الصدد، أن عملية تشييد والمحافظة على الوطن السيبراني ليست مجرد أمني أو تفكير رغبوي، وإنما هي جهود جماعية منسقة ومتلاحمة وموجهة بواسطة استراتيجية جيدة وواضحة نحو الغايات السياسية للأمة؛ ومن ثم، القوة السيبرانية المعتبرة كجسر عملي نحو تشييد الوطن السيبراني هي الأكثر قدرة على إنتاج أجيال بضائع البرمجيات ونظم الحاسوب بقدرات وطنية، واستغلال الظروف المتاحة لتسويقها في الأسواق العالمية، وليس مجرد استهلاك لتلك البضائع القادمة من المجتمعات الأخرى. إذا كانت عملية انتاج البضائع السيبرانية وتحسين البنية التحتية شرطان ماديان لقيام الوطن السيبراني، فإنهما في نفس الوقت يساهمان في خلق التقدير السياسي والأخلاقي من قبل الأمم الأخرى، الذي يعتبر أحد الشروط الفلسفية في رسم خريطة الوطن السيبراني. الأكثر من ذلك، كلما تراكم حجم الإنتاج السيبراني للخدمات التجارية وتحسين الكفاءة الاقتصادية وتسويق المحتوى الرمزي لعناصر الشخصية الوطنية للأمة، ازداد الثقل الاستراتيجي للوطن السيبراني في التأثير على سلوك الآخرين وخلق الانطباعات الجيدة، السمعة، والتقدير الحضاري. إن القوة السيبرانية تعمل باتجاه دعم الوطن السيبراني في جانبه المادي والرمزي بشكل متزامن، من خلال خلق عناصر جديدة للثروة، تحسين الأداء الاقتصادي، فعالية التنظيم ونوعية الخدمات في المجالات المختلفة؛ جنبا إلى جنب في

دعم العناصر الرمزية المتعلقة بالثقافة، الرموز الحضارية، التاريخ الاستراتيجي، المعرفة العلمية، العادات والتقاليد والأعراف الاجتماعية وكل ما يتعلق بتمدد المحتوى الرمزي للأمة في العالم السيبراني.

من الخطأ الجسيم اختزال القوة السيبرانية في مواقع التواصل الاجتماعي أو الاتصالات الرقمية، حتى ولو أنها تشكل مكوناً رئيسياً في بناء الوطن السيبراني، عوضاً عن ذلك، تتعلق بقوة الحوسبة وما يتعلق بها من قدرات الإبداع المتدائب للتطبيقات المختلفة وتحسين أداء الخوادم؛ يمكن قياس هذا النوع من القوة بواسطة مجموعة من المؤشرات الإمبريقية مثل: عدد المشغلين، عدد المهندسين، عدد الباحثين، عدد المبدعين، براءات الاختراع، عدد مراكز البحث، عدد الطلبة في الجامعات والمعاهد المتخصصة، عدد المجالات، عدد البحوث المنجزة سنوياً، حجم الميزانية المخصصة للبحث الأكاديمي، عدد مراكز التحكم والتوجيه، نوعية المعدات وجنسياتها، الحصة الوطنية في إنتاج هذه المعدات، عدد برامج التدريب والتأهيل، حجم المستهلكين للبضائع السيبرانية، حجم الخدمات السيبرانية، أنواع الخدمات، العوائد المالية السنوية؛ يمكن إضافة مؤشرات أخرى حسب ما تدعو إليه الحاجة العلمية كنتيجة لتطور التخصصات الوظيفية للقوة السيبرانية في القطاعات العسكرية والمدنية على حد سواء.

من ناحية أخرى، يمكن النظر إلى المؤشرات السابقة على أنها حقول لتطوير القوة السيبرانية المساهمة في تشكيل المعاني الاستراتيجية، التي يمكن أن تنبثق عن أي توظيف لها في الشؤون الدفاعية والأمنية؛ وبالطبع خلق الوضعية المثلى لتثبيت أسس تشييد الوطن السيبراني. ليس هذا فحسب، وإنما الحديث عن بناء هذا النوع من الأوطان ليس شعاراً سياسياً ولا حملة دعائية، ولكن يتطلب الكثير من الشروط الموضوعية المطلوب توفيرها كمقدمات للحديث عن العقيدة السيبرانية للدولة بصفة عامة. إن القوة السيبرانية هي منظومة مركبة من العناصر المادية والرقمية والقدرات العقلية الفذة، المنتجة لقوة التأثير الاستراتيجي المرغوب على مستوى مجتمع الدولة الواقعي بشقيه المدني والعسكري، والعالم الافتراضي؛ وسواء اتخذ صورة إنتاج مصادر جديدة للثروة أو تسويق المحتوى الرمزي لعناصر الشخصية الوطنية الخاصة بالأمة.

السيادة السيبرانية: الفرص والقيود

الحصة الكبيرة من العالم السيبراني مشيدة في مواقع التخزين والتوزيع العملاقة للمعلومات في الولايات المتحدة الأمريكية، ومن ثم تبقى الأصول المطوّرة في هذا الصدد تحت السيطرة الأمريكية بطريقة ما، لكن هناك الكثير من الدول تسعى لتطوير قوة سيبرانية مستقلة خاصة بها متحررة من الهيمنة السيبرانية الأمريكية إلا في حدود قواعد الاتصال الدولي، مثل ما يحدث في الاتصالات الهاتفية؛ عندئذ، يمكن الادعاء بأن العالم

يتجه نحو ما يمكن الاصطلاح عليه «بالسيادة السيبرانية الوطنية» أو «الاستقلال السيبراني الوطني». الدول المرشحة حالياً لتحقيق هذا النوع من السيادة في المستقبل القريب هي: الصين، روسيا، تركيا، وإيران؛ وذلك لأسباب سياسية محددة في الدوافع الوطنية الملحوظة لدى هذه الدول في التحرر من كل قيود الهيمنة والسيطرة والانكشاف الاستخباري أمام الولايات المتحدة الأمريكية أو دول أخرى. إلى أن يحدث ذلك، يمكن القول أن هناك نوعاً من السيادة السيبرانية الوطنية المقيدة أو المحدودة، المجسدة بواسطة تطوير الدول للتطبيقات الدفاعية وإجراءات الحظر والحرمان من الخدمة التي تعيق أي محاولات للوصول إلى المعلومات الحساسة الخاصة بأمنها القومي أو استهداف بنيتها التحتية، كما سنناقشه لاحقاً؛ لكن السيادة الكاملة تتحقق بواسطة تشييد فضاء سيبراني وطني خالص. الفكرة الأساسية المراد التأكيد عليها في هذا الصدد، تقضي بأن المستوى الأعلى في تطور القوة السيبرانية محدد ضمن تحقيق الاستقلال السيبراني الوطني بواسطة تشييد فضاء سيبراني قائم على بنية تحتية مؤسسة فوق أرض الوطن، ومتدفقة نحو الأمم السيبرانية الأخرى، متحررة من الأصول التحتية للهيمنة الأمريكية على شبكة الإنترنت، وتأمين بنيتها التحتية والمعلومات الحساسة المصنفة تحت فئة مصالح الأمن القومي للدولة.

بالطبع الوصول إلى المستوى الأعلى في تشييد القوة السيبرانية لا يعني بأي حال من الأحوال الاستغناء عن العوالم السيبرانية للآخرين من أجل استغلالها في عمليات التفاعل الاستراتيجي، التمدد الوطني الرمزي، توليد مصادر الثروة الجديدة، وتموضع الخطوط الدفاعية المتقدمة لحماية الأصول الوطنية الحساسة؛ بالإضافة إلى إمكانية أن تكون مسرحاً محتملاً للقتال السيبراني في حالة وقوع النزاعات الكبرى، وعند اشتداد المنافسة الاستراتيجية. كما يجب التأكيد على أن التحديات الأمنية، التهديدات القاسية، المنافسة الاستراتيجية، والمخاوف الأمنية سوف لا تختفي تحت خيمة الاستقلال السيبراني، طالما أن هناك متغيران ثابتان في عمل البيئة السيبرانية وهما: التواصل التفاعلي على المستوى الوطني، والحاجة للتمدد نحو العوالم السيبرانية الأخرى.

في المستوى دون الاستقلال السيبراني الوطني، تجري عمليات استغلال العالم السيبراني القائم على اغتنام الفرص، وتوليد المناخ المناسب لغرض تمديد عناصر القوة الوطنية المادية والرمزية في صورة خريطة للوطن السيبراني، حتى ولو جرى ذلك تحت هيمنة الأمم العظمى الأخرى؛ على افتراض أن العنصر الحيوي في عمل القوة السيبرانية هو التفاعل الاتصالي بواسطة خاصيات التفوق الاستراتيجي المحددة في: الفورية، الكثافة، النوعية، الاتاحة الدائمة، والاثارة وشد الانتباه؛ تمثل كل هذه العناصر متغيرات مستقلة حاسمة في تثبيت أركان الوطن السيبراني المزود بقبابليات المنافسة، الاستمرارية، وتوليد المنافسة غير المحدودة. من ناحية أخرى، يجب أن يضع المصممون لخريطة ومحتوى الوطن السيبراني في الحسبان أن ليس فقط العناصر السياسية والثقافية والسوسولوجية والرمزية بصفة عامة هي التي يجب أن تحظى

بالأولوية العالية، وإنما أيضا تدفق المنافع الاقتصادية، الأرباح التجارية، والقابلية العالية لتوليد مصادر الثروة بالنسبة للفواعل الوطنية أو الأجانب الذين يرغبون في الانخراط ضمن عمليات التواصل السيبراني؛ بهذه الطريقة يتحول الوطن السيبراني إلى بيئة جاذبة للأمم الأخرى بدوافع الانتفاع الربحي أو الاطلاع وإشباع الفضول المعرفي والثقافي.

الثقل الاستراتيجي السيبراني

إذا أراد الوطن السيبراني كسب الثقل الاستراتيجي لابد أن يتحول إلى بيئة جذب قوي للمستهلكين على المستوى الوطني في المقام الأول، والأجانب من العوالم السيبرانية الأخرى، طالما أن منطق المنافسة الاستراتيجية هو الذي يحكم عالم الأشياء المادية والرمزية على حد سواء. بالتوازي مع ذلك، يمكن أن يتمدد الوطن السيبراني تحت سيادة الآخرين نسبيا بهدف إنجاز التأثير الاستراتيجي المرغوب كجزء من سياسة الدفاع الوطني، بطريقة تحاكي استغلال أراضي الدول الأخرى لأغراض الربح التجاري، الحصول على مواد الخام، ممارسة الأنشطة الثقافية للتعريف بالقيم الوطنية والحضارية وسط الأمم الأخرى وهكذا؛ فهي ضرورة تستدعيها حاجة الدولة للآخرين، ليس للبقاء رهينة للآخرين وإنما من أجل دعم عناصر القوة الوطنية وتحقيق الثقل الاستراتيجي للبقاء كوحدة متحدة وامتددة عبر العوالم المختلفة بواسطة الربط المحوسب، بحيث تصبح عملية التأثير والتفاعل السيبراني في الاتجاهات المختلفة عالية الاحتمال؛ إنها تتعلق باستغلال الفرص الاتصالية لتسويق المعاني الوطنية، السياسات، رموز التاريخ الاستراتيجي، زيادة حجم المواطنين السيبرانيين، فضلا عن الربح المادي.

الحقيقة أنه ليس هناك قائمة أهداف محددة يجب أن تسعى وراءها الأمة من وراء تشييد الوطن السيبراني، وإنما هناك أجندة متنامية عبر الزمن بقدر ما تتطلبه شروط تطوير عناصر القوة الشاملة للأمة، على أن تكون الخاصيات الحضارية والرمزية الأكثر حيوية ويجب أن تحظى بالأولوية في ترتيب أجندة سياسة الدفاع الوطني. الافتراض العام المقترح في هذا السياق التحليلي، أن القوة السيبرانية وكل ما ينبثق عنها هي مجرد إحدى روافد التمكين الاستراتيجي للدولة، مثل مجالات القوة الاستراتيجية الأخرى: البرية، البحرية، الجوية، الفضائية، وقوة الروبوت أو الذكاء الاصطناعي. من حيث الجوهر، كل مجالات القوة المشار إليها سابقا تحتكرها فقط القوى العظمى التي هي معدودة في النظام الدولي، أما الباقي فإنه يعتمد على الأسواق العالمية بشكل متغير من دولة لأخرى، في الحصول على حاجاته من التجهيزات والمعدات والأسلحة لغرض تحديث وتعهد قواته المسلحة؛ نفس المنطق الاستراتيجي ينطبق على القوة السيبرانية، لكن هذا لا يعني عدم وجود سعي حثيث من قبل الدول الكبيرة والصغيرة وراء تحقيق الاستقلال الوطني السيبراني من أجل تقليص قابلية عطبها الدفاعي، في حالة وقوع نزاع كبير مع الدولة أو مجموع الدول المهيمنة على الفضاء السيبراني.

خلال فترات السلم، كل الأطراف متفقة ضمناً أو بواسطة معاهدات على أن يبقى الفضاء السيبراني مفتوحاً وأمناً أمام المجتمع العالمي لتفاعل الأفكار، المعلومات، الاتصالات، الثقافات، تدفق الخدمات التجارية والاقتصادية والملاحية، وحتى بناء الصداقات؛ لكن في نفس الوقت هناك منافسة شديدة بين الدول والفواعل تحت الدولة حول تطوير البنية التحتية السيبرانية، التطبيقات الجديدة، وقدرات استغلال فرص الربح الاقتصادي والتجاري، بنفس درجة الاهتمام بتقويض قدرات الآخرين في التماسك السوسولوجي، التناغم الثقافي، السمعة السياسية، وتسويق عناصر الشخصية الوطنية؛ كمكونات أساسية في تشكيل الوطن السيبراني. بطريقة أخرى، ليس هناك مجال مفتوح لتأسيس الأمم أوطانها السيبرانية بسهولة، وإنما عقبات التخريب، الإعاقة، الحرمان، تغذية قابليات العطب، تمزيق الخريطة السيبرانية هي ديدن العلاقات السيبرانية الدولية؛ ومن ثم، تظهر مسألة عامة أن الدول التي تسعى وراء تشييد أوطانها السيبرانية يجب أن تهتم بمقاربات البناء والمحافظة بشكل متزامن، على افتراض أن المنطق الاستراتيجي الذي يحكم العلاقات الدولية المفسر بواسطة النظرية التقليدية هو نفسه المهيمن على العلاقات السيبرانية بين الأمم.

إن التناظر بين العالمين مبرر بواسطة محتوى إدراك الدول للقوة السيبرانية على أنها جزء من عناصر القوة الوطنية الشاملة، التي تضيف درجة من الفعالية والتفوق الامتيازي على مجالات القوة الأخرى؛ إنها تساهم في زيادة ثروة الدولة، تقوية الاقتصاد، تنويع الموارد، وتطوير الأدوات الجديدة ذات الاستخدامات العسكرية والمدنية (أرباح الشركات السيبرانية في الولايات المتحدة الأمريكية مثلاً تفوق بكثير الدخل الوطني السنوي لعشرات الدول من العالم مجتمعة). ضمن هذا السياق، يمكن الاستنتاج أنه إذا كانت ظاهرة الثورات في الشؤون العسكرية خاصة فقط بإبداع طرق جديدة في القتال وفق اعتقاد كولن جراي⁽²⁴⁾، فإنه يمكن الحكم بأن القوة السيبرانية قد أحدثت ثورة في الشؤون المدنية والعسكرية، المادية والرمزية على حد سواء. بالطبع فرضت الثورة السيبرانية في الشؤون العسكرية والمدنية منطقاً جديداً في التفكير، إحدى مظاهره أن للأوطان وجود مادي وآخر سيبراني يشكل مسرحاً متعدد الأغراض، يتضمن الربح الاقتصادي والتجاري، التمدد والتفاعل الحضاري نحو ومع الأمم الأخرى، إدارة العمليات الاستراتيجية والاستخباراتية المختلفة (التأثير في اتجاهات الرأي العام، مقاومة الحملات السيبرانية، وتسويق السياسات مثلاً)، وغيرها من الأنشطة التي تشكل جزءاً من قوة الدولة ومهامها الدفاعية بدون نيران الأسلحة.

المصدر الرئيسي لتوليد الدافعية السياسية نحو تشييد الوطن السيبراني محدد في إضفاء النزعة الاستراتيجية على علم الحوسبة والرقمنة وكل ما يتعلق بمكونات البنية التحتية المشكّلة للقوة السيبرانية، كنتيجة ملحوظة لتمدد خاصيات النظام الدولي التقليدي (المحددة من قبل أنصار النظرية الواقعية/الواقعية الجديدة في الريبة، الفوضى، المنافسة الأمنية، المساعدة الذاتية، سباق التسلح وغيرها) نحو هذا المجال الجديد من القوة، وظهور

ربما يحتاج البعض بأن الأسس الأولى التي بنيت عليها القوة السيبرانية هي عسكرية وليست مدنية باعتبارها كانت شبكة الاتصال للجيش الأمريكي، ثم تم فتحها للأنشطة المدنية الوطنية والعالمية؛ هذه الحاجة صحيحة جزئياً، لكنها لا تحمل كل الحقيقة. الجذر الأصلي للقوة السيبرانية هو الاتصالات الهاتفية ثم القوة الإلكترونية المستخدمة لطاقة الذبذبات في نقل المحادثة وإرسال الرسائل عبر الأسلاك وموجات البث الإذاعي بدون أسلاك في بداية القرن العشرين، ثم استخدمت هذه التكنولوجيا للأغراض العسكرية على نطاق واسع في الحرب العالمية الثانية، من أجل تسريع نقل المعلومات مباشرة بطريقة فورية، اعتراض المعلومات المضادة الخاصة بالعدو، التشويش على خطوط وصول المعلومات إلى العدو، وغيرها من الاستخدامات العسكرية التي كانت حاسمة في ربح الحلفاء الحرب على ألمانيا بواسطة فك شيفرة الاتصالات الألمانية بواسطة نظام المعلومات الذي أبدعته المخابرات البريطانية آنذاك، وحمل اسم «ENIGMA انيغما»⁽²⁶⁾. مازالت لحد الآن البنية التحتية لتفاعل القوة السيبرانية هي خطوط الاتصالات الهاتفية، بالرغم من وجود في الظاهر علاقة الاعتماد المتبادل بين القوة الإلكترونية والقوة السيبرانية.

للوطن السيبراني أبعاد اقتصادية وتجارية حيوية تدعم بشكل ملحوظ الأصول الوطنية في العالم المادي، بحيث أصبحت تساهم في الدخل الفردي والجماعي، لفواعل الدول وغير الدول على حد سواء؛ في كثير من الأحيان تفوق تدفقات الثروة السيبرانية الكثير من المصادر الاقتصادية التقليدية بما فيها النفط والمعادن النفيسة. تمثل الأصول السيبرانية مصالح حيوية للدولة تساهم بطرق مباشرة في زيادة ثقلها الاستراتيجي وتأمين حاجاتها المختلفة، وتوفر لها مداخل إضافية لدعم ميزانيتها الوطنية العامة؛ تتمتع الأصول السيبرانية حصة كبيرة من قوى العمل، تحسن الوجود الاجتماعي للمواطنين؛ كذلك تطوّر الكفاءة والمهارة الفردية والجماعية في تشغيل البنية التحتية، إبداع التطبيقات الجديدة، وتحسين موقف الوطن السيبراني في المنافسة الاستراتيجية وأسواق البضائع والخدمات التجارية والاتصالات. يقود هذا التحليل إلى أن الوطن السيبراني ليس مجرد ميدان لتفاعل العناصر الرمزية، وإنما هو أيضاً تنمية اقتصادية وتطوير للعلاقات التجارية والخدماتية، أو ما يسمى «باقتصاد المعلومات»؛ الذي يشكل مكوناً أساسياً في الاقتصاديات الحديثة.

يوجد حجم كبير من الأنشطة الاقتصادية والتجارية تمارس في العالم السيبراني وتدرّ أرباحاً كبيرة على الاقتصاديات الوطنية، وأنها في تمدد كبير بسبب جذب أعداد كبيرة من الناس لممارسة هذا النوع من التجارة بدون التنقل إلى مكان العمل أو ضرورة الحضور الفيزيقي في عقد الصفقات وممارسة التبادل التجاري. المستوى المتقدم في تطور الاقتصاد السيبراني هو إبداع العملة السيبرانية التي اعتمدتها بعض الدول كوسيط في المبادلات التجارية وتحقيق مكاسب جيدة على حساب العملات التقليدية للدول.

ضمن هذا السياق، أظهر وباء كوفيد- 19 أهمية الأسواق، التجارة، والاقتصاد في العالم السيبراني؛ ففي الوقت الذي كانت الشركات التي تعمل بالطريقة التقليدية تخسر أسواقها وتراجع أرباحها بفعل إجراءات الحجر الصحي وغلق حدود الدول، فإن نظيرتها السيبرانية كانت تحقق أرباحاً بآلاف المليارات من الدولارات. لا شك في أن إحدى الدروس المتعلمة من وباء كورونا عام 2020 هي اندفاع الدول والفواعل غير الدول نحو تطوير استراتيجياتها السيبرانية حول التجارة، الإنتاج الاقتصادي، وكل معاملاتها المالية من أجل خفض التكاليف وزيادة الأرباح بدون الحاجة لتنقل العمال أو المتعاملين إلى مواقع العمل. ليس هذا فحسب، وإنما الاقتصاديات الكبيرة والناشئة في العالم سوف تأخذ قضية الاستقلال السيبراني الوطني على محمل الجد، وتسرع وتيرة تطوير بنية تحتية وطنية خاصة بالوطن السيبراني، تكون مستقلة في جذورها الشبكية عن منشأ الإنترنت في الولايات المتحدة الأمريكية؛ وذلك من أجل تفادي الهيمنة الأمريكية على التجارة السيبرانية العالمية، وتفادي إمكانية وضع قيود أو القيام بعمليات الحرمان أو تقويض أوطانها السيبرانية. إذا فضلنا التخمين حول الدول التي تحمل نيات جدية في تحقيق الاستقلال السيبراني الوطني، فإنه يمكن ترتيبها وفق القائمة التالية: الصين، روسيا، تركيا، إيران، ويمكن أن تظهر قوى أخرى في المستقبل. الحالة العامة المميزة للاقتصاد العالمي هي اعتماد باقي الدول على العالم السيبراني الحالي في زيادة دخلها الاقتصادي، توسيع سوقها الوطني، ومساعدة مواطنيها على زيادة أرباحهم الشخصية من التجارة السيبرانية. إذا أخذنا الحالة العربية، فإننا نجد بعض الدول العربية انخرطت في التجارة السيبرانية بشكل نشط مثل دول الخليج ومصر والمغرب.

الفكرة الأساسية المطروحة في هذا الصدد محددة في أن جهود بناء الوطن السيبراني يجب أن تشمل الجوانب الاقتصادية والتجارية والخدمات الأخرى المربحة بهدف خلق مصادر جديدة للدخل القومي، التي تستخدم -إلى جانب تحسين رفاهية المجتمع- في دعم الشؤون الدفاعية والاستراتيجية؛ على افتراض أن الدولة إذا أهملت هذه الاعتبارات من حساباتها، فإن خصومها أو أعداءها سوف لا يفعلون ذلك، كجزء من الخصائص المتحركة في العلاقات الاستراتيجية الدولية وفق تقدير "جون ميرشمر"⁽²⁷⁾، سوف ينسحب هذا المنطق الاستراتيجي على العلاقات السيبرانية بين الأمم. مثل العالم الواقعي، كل شيء يجب أن يحسب ويفسر بعيون استراتيجية حتى ولو بدا في الظاهر أنه ذو طابع مدني بحت، كالأرباح التي تجنى من وراء الخدمات السيبرانية. بالطبع النموذج الأمثل في هذا الصدد هو الولايات المتحدة الأمريكية التي شيدت وطنها السيبراني المتكامل الأبعاد وحولته إلى بيئة متدفقة بالأرباح التجارية والاقتصادية، التي ولدت بدورها إمبراطوريات تجارية عالمية كبيرة (مثل فيسبوك، تويتر، يوتيوب وأخرى كثيرة) تدر مداخيل هائلة على الاقتصاد الأمريكي، كجزء من الهيمنة الأمريكية على الاقتصاد العالمي؛ تلحق بها الصين والاتحاد الأوروبي ودول أخرى عبر

تأسيس الشركات السيبرانية العملاقة. ليس هذا فحسب، وإنما أصبحت القوة السيبرانية إحدى المحركات القوية للاقتصاديات الوطنية عبر تصعيد فعالية الإنتاج ورفع حجم الأرباح التجارية ومضاعفة المداخل الوطنية الكلية للدول. لقد أصبحت القوة السيبرانية تستخدم على نطاق واسع كنظام للتحكم وتشغيل الأنظمة الشبكية المعقدة لغرض تصعيد الفعالية وتقليل التكاليف وزيادة الأرباح، إنها تشغل شبكات إمدادات الطاقة، توزيع المياه، إدارة البنوك، أسواق المال، وغيرها من مجالات الأنشطة التي تمثل القوة العصبية للدولة؛ تشكل كل هذه العناصر امتيازات تطور الاقتصاديات السيبرانية.

ثانياً: تطوير قدرات الدفاع السيبراني انعكاس للسيادة الوطنية

الفرضية التي يبنى عليها هذا الفصل أن لا بقاء لوطن بدون دفاع، ولا أحد يسمح برسم خريطة إلا إذا أُجبر على ذلك، كما أن منطق الدفاع ييسر الكثير من العقبات أمام الأمم في تشييد أوطانها؛ في الوضعية التقليدية، لا يمكن تحريك أي حجر داخل التراب الوطني للدولة أو خارجه بإرادة مستقلة ما لم تكن وراءها قوة عسكرية كافية تحميها؛ نفس المنطق يمكن إسقاطه على الوطن السيبراني بطرق مختلفة تبعا لخصوصية البيئة ومتطلبات عملها. إذا نظرنا فيما وراء الإجراءات والاستراتيجيات الشكلية، فإنه يمكن الادعاء بأن جوهر نظرية الدفاع السيبراني متأصلة في القدرة الإبداعية والمهارة الفنية التي تتمتع بها جماعة كبيرة من العلماء والفنيين والمهندسين المتخصصين في علم الحوسبة والرقمنة من مواطني الدولة، الذين يستطيعون توفير القدرات الحوسبية المختلفة لحماية الأصول الوطنية الحساسة، المعلومات السرية، البنية التحتية، المصالح السيبرانية لمواطني الدولة، وغيرها من الأشياء القابلة للعطب الشديد بواسطة العمليات السيبرانية الخبيثة مثل التجسس، التطفل، القرصنة، السرقة، الحرمان من الخدمة، وغيرها من الأنشطة العدائية التي يمكن أن تهدد المصالح الخاصة للمواطنين، الشركات، والمؤسسات الحكومية.

هناك أصول سيبرانية بحاجة للحماية متعلقة بأنظمة الإدارة والتحكم والتوجيه السيبراني لتوليد فعالية عالية في تشغيل شبكات أنظمة توزيع الكهرباء، المياه، الطاقة، النقل العام، الملاحة الجوية والبحرية، وغيرها من القطاعات المختلفة المتحركة في العمل اليومي للدولة والمجتمع. وهناك مستوى آخر للقوة السيبرانية أكثر حساسية متعلق بقدرات التفوق على الأمم الأخرى والاحتفاظ بإمكانات المنافسة الاستراتيجية حول المجالات المختلفة للقضية، مثل تكنولوجية الذكاء الصناعي، تصاميم الأسلحة المتطورة، الأسلحة النووية، مدخرات المؤسسات والأفراد والدولة، وغيرها من المكونات الحساسة التي تؤدي عملية السيطرة عليها من قبل العدو إلى إنهاء التفوق أو التسبب في أضرار بليغة في جسم الأمن القومي للدولة.

تقضي مفهمة كارل فون كلاوزفيتز للدفاع بأنه انتظار العدو، أو كما قال: "تعني المعركة الدفاعية إن كنا [نحن] من ينتظر الهجوم -ونعني بذلك، انتظار ظهور العدو أمام خطوطنا وضمن المدى. والحملة الدفاعية [هي] إذا انتظرنا اجتياح العدو لمسرح عملياتنا"⁽²⁸⁾. لقد لخصت نظرية إدارة الحرب لكلاوزفيتز جوهر مفهوم الدفاع في انتظار العدو وتفادي الهجوم، يعني ذلك اتخاذ كل الإجراءات المطلوبة في التحضير لساعة قدوم العدو المهاجم والاشتباك معه، ومن ثم استراتيجية المدافع محددة في الدفاع عن المنطقة أو الحدود التي يتموضع فيها، وليس هناك مهمة للمدافع إلا «انتظار المهاجم ليأتيه في بلاده، والمدافع عن مسرح الحرب ينتظر المهاجم على ذلك المسرح، والمدافع عن الموضع ينتظر المهاجم عند ذلك الموضع. وحال بدء الهجوم، فأية أنشطة وأية تحركات تعرضية تقريبا يقوم بها المدافع وقتها لن تلغي مفهوم الدفاع، فقد تم إرساء ميزته الهامة وفائدته الأساسية [في] الانتظار»⁽²⁹⁾. بهذا المعنى، يتألف مفهوم الدفاع من عنصرين أساسيين: الانتظار والأعمال القتالية عند قدوم المهاجم، يتضمن مفهوم «الانتظار» رسم الاستراتيجية، التخطيط الدفاعي، تحضير جاهزية القوات المسلحة ومعداتها للاشتباك مع العدو حين وقوع الاعتداء، تطوير نظم الاستخبارات والاستطلاع والمراقبة، وتحضير مسرح القتال؛ أما الأعمال القتالية، فإنها تشمل كل الأنشطة التي يتم مباشرتها أثناء الاشتباك.

هناك تشابه كبير في منطق التفكير الاستراتيجي حول الدفاع التقليدي ونظيره السيبراني، خصوصا فيما يتعلق بفكرة «انتظار العدو»، التي تعني في الفضاء السيبراني نشر كل الأنظمة والتطبيقات الدفاعية المضادة حول المواقع الشبكية لحمايتها من الهجمات الفيروسية المقصودة والعرضية، العمليات التخريبية، القرصنة، السرقة، وغيرها من الأنشطة العدائية؛ إذا قدمت تلك التهديدات، يجدر بالتطبيقات المضادة أن تكون في انتظارها لإحباطها تماما أو على الأقل تقليص أضرارها الهجومية إلى الحدود الدنيا، بشكل لا يؤدي إلى انهيار كلي للخطوط الدفاعية أو التسبب في تدمير مميت للبنية التحتية السيبرانية أو سرقة المعلومات الحساسة الخاصة بالأمن القومي.

اتساقا مع منظور كلاوزفيتزي، فإن جوهر الدفاع مركّز حول جميع القدرات العقلية والمهارات الفنية حول توليد أو ابداع التطبيقات المتفوقة على الهجمات السيبرانية، ومن ثم فإن المسرح الدفاعي الرئيسي مركّز حول الذكاء المتفوق الذي يقوم بوظيفة الدرع والسيف لغرض الدفاع والتفاعل الاستراتيجي. الوضعية الدفاعية السيبرانية الجيدة غير موجودة، بسبب أن الذكاء العقلي السيبراني موزع بين المهاجم والمدافع، وأن خبرة الأنظمة السيبرانية مع الهجمات الفيروسية أثبتت أن الاختراقات مستمرة حتى ولو لم تكن مميتة. يمكن إرجاع العيوب الدفاعية إلى الأنظمة السيبرانية نفسها التي تحمل معها بذور القابلية للعطب التي تستغل من قبل المهاجمين، ليس هذا فحسب، وإنما أيضا حيوية الأصول المحمية بواسطة الأنظمة الدفاعية التي تتخطى حدود المنافع المادية إلى المصالح الاستراتيجية المرتبطة

بالبقاء القومي للدولة (حالة ادعاء الولايات المتحدة الأمريكية عام 2021 أن الصين قرصنت المعلومات حول تصاميم طائرة F-35). خلقت ظاهرة استفحال القابلية السيبرانية للعطب قلقاً متزايداً لدى صناع القرار عبر العالم حول الخوف من وصول الخصوم إلى مصادر التفوق الاستراتيجي للقوة الوطنية السيبرانية، لعل هذا هو الذي جعل الرئيس الأمريكي "جو بايدن" يطلق تهديداً هادئاً في أوت 2021 بأن استمرار الهجمات السيبرانية ضد المنشآت الأمريكية الحيوية سوف يؤدي بنا إلى نشوب الحرب مع قوة عظمى؛ يعكس هذا التحذير حجم التحدي الجدي الذي يواجهه الدفاع السيبراني لأقوى دولة في العالم ومنشأ القوة السيبرانية.

الجانب الأكثر تعقيداً في الدفاع السيبراني أن مسألة التفوق الاستراتيجي غير محسومة بناءً على اعتبارات القوة المادية أو الوفرة الكبيرة في الموارد البشرية والمالية، وإنما محكومة بواسطة العقول اللامعة والأدمغة النابغة التي ليس بالضرورة أن تكون إلى جانب الطرف المتفوق عسكرياً؛ تعتبر هذه النقطة إحدى محاور مسرح المنافسة الدفاعية وكذلك تشكل ثغرة كبيرة في الخطوط الدفاعية في نفس الوقت. ومن ثم، يصبح الدفاع السيبراني مركزاً على البحث الحثيث عن تلك العقول النوعية عبر المجتمع الوطني والمجتمعات الأخرى، بالتزامن مع تصعيد عمليات التعبئة الدفاعية لانتظار قدوم الهجمات السيبرانية. لا تنتهي متاعب الدفاع السيبراني عند حدود هذا التحدي العصي، وإنما تتمدد لتشمل احتمال أن يكون العدو قادماً من الوطن نفسه أو من العاملين داخل المؤسسات الدفاعية.

إحدى الخصائص المميزة وفي نفس الوقت معضلة عملياتية للدفاع السيبراني محددة في أن قدوم العدو يكون في سرعة الضوء، ومن كل أنحاء العالم، ولا يحتاج لأعداد كبيرة من البشر، والخسائر تكون جسيمة في مصالح الطرف المستهدف متنوعة بالأضرار الجانبية التي تضرب الأطراف غير المقصودة؛ مما يستدعي في مقابل ذلك، أن تكون البنية التحتية لأنظمة الدفاع المكثفة لانتظار قدوم العدو، تعمل على مدار الساعة وجاهزة للتعامل مع مصفوفة الهجمات على المستوى الكبير أو الصغير، تشتبك مع الفيروسات وتقاوم محاولات الاختراق وكل الأنشطة العدائية الموجهة ضد الوطن السيبراني باعتباره منطقة حساسة، تحتوي مصالح حيوية مرتبطة مباشرة بالبقاء القومي للدولة؛ كتلك المواقع الشبكية المتحكممة في إدارة الأسلحة النووية، توزيع الطاقة الكهربائية والغاز والمياه، تنظيم حركة المرور في الشوارع، شبكة النقل وقطارات الأنفاق، تنظيم حركة الملاحة، والاتصالات والقيادة والسيطرة والتحكم؛ إذا استعربنا بعض مفهومة كلاوزفيتز حول نظرية إدارة الحرب، فإنه يمكن النظر لكل العناصر السابقة الذكر على أنها تمثل «مراكز الثقل» الاستراتيجي لبقاء الدولة، إذا تمت السيطرة عليها أو تخريبها بواسطة الهجمات السيبرانية، سوف يؤدي ذلك إلى تحقيق مبدأ الشل الاستراتيجي المقترح من قبل أنصار نظرية القوة الجوية⁽³⁰⁾.

التأكيد على حيوية الدفاع السيبراني يعني وجود عناصر ذات قيمة حيوية خاصة بالدولة، تسعى لحمايتها من الانتهاكات غير الشرعية أو الأنشطة العدائية من قبل الآخرين (الدول وغير الدول)، كما تستلزم أيضا منع الآخرين باستغلالها بدون ترخيص أو إذن منها؛ وهذا مما يؤثر على وجود الملكية الوطنية الحصرية للأصول السيبرانية (سواء ملكا للدولة أو لمواطنيها) التي يجب على الدولة توفير شروط حمايتها، وهذا تجسيد لمعنى السيادة الوطنية على الحقوق الشرعية للدولة في هذا الفضاء الجديد، كأحد تمظهرات الوطن السيبراني، مثل الحقوق الوطنية الأخرى في المياه الإقليمية، الجرف القاري، الإقليم البري، والأجواء فوق الدولة التي هي مقررة كحقوق للدولة الوطنية بموجب قواعد القانون الدولي. تشتق السيادة السيبرانية للدولة على أصولها الوطنية أيضا من حقوق الملكية الفكرية في تشييد المواقع الشبكية، المحتويات الفكرية والعلمية السيبرانية، المعلومات المخزنة وغيرها من الأصول الوطنية العامة أو الخاصة، التي ليس للآخرين الوصول إليها أو استغلالها إلا بترخيص سيبراني من الدولة المعنية. الأكثر من ذلك، الدفاع عن الشيء يستلزم الحق بملكه، والدفاع الوطني يستلزم بالضرورة السيطرة الحصرية للدولة على كل الأشياء المادية والرمزية التابعة لها كتجسيد لمعاني السيادة الوطنية؛ ينسحب هذا المنطق الدفاعي على البنية السيبرانية المشيدة من أجل حماية المعلومات، الأصول الوطنية، براءات الاختراع، وحتى الخصوصية الشخصية للمواطنين من الانتهاكات أو التطفل أو القرصنة من قبل الآخرين.

ضمن سياق الدفاع السيبراني، فإن السيادة الوطنية ليست ادعاءً لحقوق غير شرعية ولا مبهمة، وإنما هي مصالح حيوية عالية الحساسية للأمن القومي محاطة بأنظمة متعددة للحماية ومنع اختراقها، وصول الآخرين إليها، السيطرة عليها، أو استغلالها بطريقة غير شرعية. مثل العالم الواقعي، تتحدد مهام الدفاع السيبراني في عمل الدول على تعزيز وتحسين قدراتها الدفاعية وإجراءات الحماية لجعل الآخرين بعيدين عن حدود وطنها السيبراني، احتواء الهجمات السيبرانية، الاحتفاظ بالملكية الحصرية لحقوقها في الإنجازات الوطنية المختلفة؛ الأكثر أهمية من كل ذلك، الاحتفاظ بالتفوق العملي على الآخرين بواسطة منعهم من الوصول إلى البيانات الحساسة حول التكنولوجيا المتقدمة، الأسلحة النووية، استراتيجية الدفاع، فك شيفرات الدخول، وغيرها من المهام المقترحة من قبل أنصار النظرية السيبرانية في الدفاع والأمن. تنظر الدول إلى الهجمات السيبرانية والأنشطة العدائية الأخرى على أنها انتهاكات أمنية متفاوتة الخطورة، تبدأ من القرصنة أو التجسس على هواتف المواطنين أو حواسيبهم الخاصة إلى أعلاها خطورة، التي تستهدف معلومات حساسة أو اختراق المواقع الشبكية للمؤسسات الحيوية في الدولة مثل وزارة الدفاع والخارجية والمنظمات الأمنية والاستخباراتية والشركات الكبرى مثل تلك المتخصصة في تطوير تكنولوجيا الذكاء الاصطناعي، الأسلحة النووية، الأقمار الصناعية، الطائرات المقاتلة والصواريخ الباليستية.

المذهب السيبراني

السيادة السيبرانية الوطنية لا تعني الاستخدام الحصري للفضاء السيبراني وحرمان الآخرين، وإنما تعني الوفرة الكافية في القدرات والأنظمة المساعدة على التحكم والسيطرة في التفاعلات السيبرانية، بشكل يجعل الدولة أو المؤسسات تمنح ترخيص استغلال الخدمات والمعلومات بإرادتها وحرمانه على المتطفلين، كما تكون لها القدرة على حماية أصولها السيبرانية والبيانات الحساسة ذات العلاقة بالأمن القومي أو المصالح الحيوية؛ بمعنى آخر، القدرة على منع الانكشاف السيبراني أمام الاختراقات والتهديدات المقوضة لعناصر أمنها القومي وسلامة مواطنيها.

يستلزم هذا المنظور، بلورة المذهب السيبراني في سياسة الدفاع الوطني الذي يتضمن بالضرورة تحديد الأصول أو مراكز الثقل الحيوية الجديرة بالحماية، استراتيجية الدفاع، الأنظمة وأدوات الحماية، حجم المشغلين للبنية السيبرانية الدفاعية، المحللين وهيئة المستشارين المتخصصين، مفهمة طبيعة ومسرح الحرب السيبرانية، وطبيعة العلاقة التي تحكم تفاعل الوطن السيبراني بالأمم السيبرانية الأخرى. يشق المذهب السيبراني مفهمته النظرية والوظيفية من نظيره التقليدي، الذي عرّفه "نفيل براون" (Neville Brown) «المذهب Doctrine» بأنه: «مجموعة الاعتقادات العملية، القيم، والتأكيدات التي توجّه بطريقة مهمة السلوك الرسمي [للدولة] نحو [أجندة] البحث الاستراتيجي والتطوير، خيار الأسلحة، القوات، الخطط العملية، مراقبة الأسلحة، إلخ»⁽³¹⁾. اشتقاقاً من هذا التعريف، المذهب العسكري هو عبارة عن مصفوفة من الاعتقادات والتصورات والقيم الاستراتيجية والعملية التي تشكل الإطار العام لفلسفة الدفاع الوطني، والمثبتة ضمن الثقافة الاستراتيجية كسياسة عامة للدولة، ليس لها الخيار في التنازل عنها. جمع من جهته "كا بو نج" (Ka Po Ng) مجموعة من التعاريف للمذهب العسكري، استهلها بالتعريف الخاص به الذي يتضمن معنى وجود «الإطار المركزي للاعتقادات حول إدارة الحرب، الذي يوفر توجيه القوة في العمل، البنية، المنظمة، والتطوير.

الأكثر من ذلك، يمثل المذهب التعبير الأعلى في التأسيس الفكري للقوة الدفاعية». عرّف «القاموس العسكري والمصطلحات ذات العلاقة لوزارة الدفاع الأمريكية Dictionary of Military and Associated Terms of the United States Department of Defense»، المذهب العسكري بأنه: «المبادئ الأساسية التي توجه القوات العسكرية أو العناصر لأعمالها في دعم الأهداف الوطنية. إن [هذه المبادئ] سلطوية لكن تتطلب التكيف في التطبيق». عرّف كتيب «العمليات FM 100-5 Operations» للجيش الأمريكي في طبعة 1993، المذهب العسكري بأنه: «بيان كيف يدير الجيش الأمريكي كفريق مشترك الحرب والعمليات الأخرى غير الحربية... إنه يلخص المقاربة الأساسية للجيش في القتال، كيفية إحداث التأثير في عمليات أخرى غير الحرب، وتحديد الأفعال

المضرة بالمصالح الوطنية». عرّف «كتيب القوة الجوية The Air Power Manual» للجيش الأسترالي المذهب العسكري (وهو تعريف مطابق تقريبا لما جاء في القاموس العسكري الأمريكي المشار إليه سابقا) بأنه: «المبادئ الأساسية التي توجه أفعال القوات العسكرية في دعم الأهداف الوطنية. إنها سلطوية لكنها تتطلب الحكم في تطبيقها»؛ أو هو: «الإطار المركزي للمعرفة، الذي يؤثر على طريقة كل أعضاء القوة الجوية في التفكير والعمل لإشباع حاجات الأفراد [من أجل القيام] بالمسؤوليات الجماعية، لأجل دعم الأمن الأسترالي عبر القوة الجوية»⁽³²⁾.

مرة أخرى من الناحية النظرية والوظيفية، لا تبتعد المفهمة السيبرانية للمذهب عن نظيرتها التقليدية، المطلوب صياغتها لأغراض تحديد مهام الدفاع عن الوطن السيبراني؛ يتعلق المذهب السيبراني بالمصالح الحيوية أو الأصول الوطنية الحساسة التي يجب حمايتها والأدوات والموارد المسخرة الموظفة من أجل القيام بمهام الدفاع. لا يعني هذا أن عناصر القوة الرمزية غير مدرجة تحت خيمة اهتمامات المذهب، مثل الاهتمام بالتماسك السوسيولوجي، الهوية، عناصر الشخصية الوطنية للأمة، التاريخ الاستراتيجي، والثوابت الوطنية التي تشكل الأصول الوطنية غير المادية الجديدة بمهام الدفاع السيبراني. الحقيقة أن معظم دول العالم تواجه تحديات التهديدات السيبرانية لعناصر قوتها الرمزية والمعنوية بنفس حجم التهديد الموجه ضد مصالحها المادية الحيوية، الفرق الوحيد البارز بين نوعي التهديد هو أن تهديدات الفئة الأولى صامتة، لا تثير الانتباه، ومستمرة بدون انقطاع؛ في حين أن الفئة الثانية تحدث جلبة وتحدث عنها وسائل الإعلام وتستفز صناعات القرار للتنديد بها، بالإضافة إلى إطلاق أنظمة الإنذار بوقوع هجمات سيبرانية وذكر الآثار الأمنية والأضرار المادية التي خلفتها وراءها.

الجانب الحيوي في التهديدات السيبرانية غير المادية محددة في قدرتها على إحداث التأثير المجتمعي العميق، الذي يأخذ عدة مظاهر مثل تصاعد الانقسامات المجتمعية، الكراهية ضد الأجانب، تنامي نفوذ الجماعات المتطرفة، إذكاء الصراعات العرقية والدينية، إضعاف الروح المعنوية لمؤسسات الدولة، تشجيع الكراهية بين الشعوب، تشويه سمعة الدول، وغيرها من التهديدات التي تقوض التماسك الوطني للدولة؛ تستوي في ذلك الدول الكبيرة والصغيرة. إحدى المظاهر العملية لهذا النوع من التهديدات، تصاعد جماعات اليمين المتطرف الذي أصبح يهدد التماسك السوسيولوجي للمجتمعات الديمقراطية في الغرب (اقتحام جماعات العرق الأبيض لمبنى الكونغرس في جانفي 2020)، وتنامي نفوذ الجماعات المتطرفة في الشرق الأوسط.

الوظيفة العملية للمذهب السيبراني مركزة حول صياغة التصور العام للكيفية التي يجب أن تنجز بواسطتها مهام الدفاع، الموجهة نحو احتواء نوعي التهديدات

(المادية والرمزية) التي تتحدى أركان الأمن القومي للدولة. فهي مسألة معقدة، تشتق عناصر تركيبها من طبيعة الوطن الذي يشيد في البيئة السيبرانية، المحددة في التفاعل الاتصالي المفتوح بلا حدود يمتد حيث تصل شبكات الربط المحوسب ومستويات عملية تخزين البيانات الهائلة بشكل لحظي، ومن ثم، ليست هناك قواعد ثابتة ولا خطوط دفاعية محددة؛ بالإضافة إلى خاصية التطوير المتسارع للتطبيقات والقدرات السيبرانية التي يمكن أن تقوض أي حواجز دفاعية في زمن لحظة. وفق هذا الفهم، تصبح عملية الدفاع السيبراني تفاعلية تتطور بشكل يومي، وتستلزم تحديث الأنظمة الدفاعية ما بين فترات زمنية متقاربة من أجل تفادي أي اختراقات محتملة؛ أكثر الانتهاكات خطورة تلك التي تكون هادئة تتحايل على أنظمة الإنذار المبكر ولا تتجاوز معها نظم الحماية. يتم تضمين كل هذه الاعتبارات ضمن المحتوى الاستراتيجي للمذهب السيبراني، كطريقة لرسم صورة واضحة في أذهان المخططين الدفاعيين والمشغلين وحتى المصممين لنظم الحماية حول طبيعة العالم الذي يواجهونه خلال القيام بمهام الدفاع عن الوطن السيبراني. لا يختلف المذهب السيبراني عن نظيره التقليدي من حيث المهام، وإنما الاختلاف محدد في طبيعة ونوعية العالم الذي يتعامل معه كل واحد منهما.

يتعامل المذهب السيبراني مع بيئة مفتوحة مكونة من أعداء وخصوم: الدول وغير الدول، حقيقيين ومحتملين، تقليديين ومتجددين، غير واضحين ومحددين الهوية والمواقع التي يهاجمون منها، بالإضافة إلى أنهم لا يستخدمون نيران الأسلحة ولا مفردات الحرب التقليدية؛ لكن الغايات السياسية جد متشابهة محددة في المعاني المقترحة من قبل المنظرين في حقل علم الاستراتيجية، مثل المنافسة الأمنية، تقويض الأمن القومي، سباق التسلح، الهيمنة الاستراتيجية، وغيرها من الأهداف المرتبطة بالمصالح الحيوية للدولة. الأكثر من ذلك، أن حقل المعركة السيبرانية شامل لكل خطوط القتال، عطب قوات العدو، شل قدرته على القتال، إعاقة تطوير نفسه، تخريب مجتمعه، تدمير قدراته الرمزية والفكرية، تفكيك تماسكه السوسيو-الثقافي؛ كل هذه الاعتبارات يجب أن تدرج ضمن اهتمامات وحسابات المذهب السيبراني. تؤخذ هذه المعاني في حسابات المذهب الهجومية والدفاعية بشكل متزامن، خدمة لغاية تحقيق هزيمة استراتيجية العدو. عادة القوة السيبرانية الدفاعية موجهة نحو تمديد خريطة الوطن السيبراني وتوفير شروط حماية عمليات التقدم في تثبيت أركانه وزيادة هيمنته؛ في حين توجه القوة السيبرانية الهجومية في التخلص من كل العقبات التي تعترض سبيل بناء الوطن السيبراني وفتح الطريق أمام عناصر الشخصية الوطنية للتفاعل بحرية داخل الأوطان السيبرانية الأخرى، وفي حالات أخرى، يمكن توسيع قائمة المهام الهجومية لتشمل تعطيل أو حرمان العدو من الوصول إلى امتيازات التفوق السيبراني أو كسب مزيد من القوة المساعدة على توسيع نفوذه الاستراتيجي في العالم السيبراني.

نماذج الدفاع السيبراني

لا توجد لحد الآن بيانات كافية ولا أفكار ناضجة حول مفاهيم الدفاع السيبراني عدا تلك الإجراءات الأمنية المضادة للهجمات السيبرانية، وكذلك الاحتياطات المحوسبة ضد وقوع هجمات أو حدوث اختراقات مأساوية لنظم الحاسوب أو المواقع الشبكية؛ الأكثر من ذلك، أن إحدى الأفكار المتماسكة نوعاً ما المقترحة من قبل بعض المنظرين الاستراتيجيين، تقضي بأن يكون الرد على الهجمات السيبرانية القاسية بواسطة استخدام القوة العسكرية أو ما يسمى بالقوة الحركية المادية؛ مما يعني بطريقة أخرى، أن مفهوم الدفاع السيبراني في النهاية يعتمد بشكل حاسم على المفاهيم التقليدية في الرد العسكري المادي (هذا ما تبين من تهديد جو بايدن عام 2021 بأن الهجمات السيبرانية يمكن أن تؤدي إلى نشوب حرب مع قوة عظمى). لكن في مقابل ذلك، يبقى هذا الوضع مؤقتاً إلى حين أن تقوم الدول بالكشف عن قدراتها الدفاعية أو تطوير الجديد منها، مع الإقرار بأن حالة الانكشاف الاستراتيجي والقبالية الأمنية للعطب الشديد مازالت هي الخاصة المسيطرة على الفضاء السيبراني. تحت هذه الوضعية السيبرانية المسيطرة، يعمل المصممون السيبرانيون على تطوير الإجراءات الأمنية الوقائية من أجل تفادي الآثار المأساوية للهجمات على نظم المعلومات، والحد من الأنشطة الخبيثة التي تستهدف المعلومات السرية الحساسة للمؤسسات الحكومية والشركات. يتلزم مع التطوير الفني والتكنولوجي للإجراءات الوقائية والحماية الأمنية، حوار استراتيجي حول تطوير المقاربات الدفاعية المتناسبة مع طبيعة الفضاء السيبراني، وفي نفس الوقت قائمة على الأرضيات النظرية المطورة في الفكر الاستراتيجي التقليدي كأفكار سان تزو، «المعركة العميقة»⁽³³⁾، وفكرة «الدفاع في العمق»⁽³⁴⁾.

ضمن هذا السياق، يندرج الحديث عن نماذج الدفاع السيبراني المقترحة لمواجهة مصفوفة التهديدات الفعلية والمحتملة، لكن تجدر الإشارة إلى أن ما يأتي في القائمة التالية ليس نهائياً، وإنما هي مجرد أمثلة للاستدلال النظري، لأن هناك الكثير من النماذج التي سوف يتم تطويرها في المستقبل تناغماً مع التطوير المتسارع للبنية التحتية السيبرانية، ظهور التطبيقات الجديدة، وكذلك تنامي الأشكال الجديدة من الهجمات السيبرانية.

1) نموذج الاتجاه العام

يقوم «نموذج الاتجاه العام Mainstream Paradigm» على مجموعة من المعايير النمطية الأولية المشكّلة لغالبيت دفاع سيبراني يُشغل في تحديد المخاطر، تحليلها، وتقييمها من أجل تحديد «قوائم الفحص Checklists» المطلوبة لتحديد طبيعة الهجمات السيبرانية واعتراضها أو منعها من التسبب في إحداث أضرار جسيمة للبيانات؛ فهذا النموذج عبارة عن مستودع من البرمجيات التي توظف في تشخيص الخطر ومكافحته أو اعتراض الهجمات على نظام الحاسوب، يقوم بانتقاء المعالجة السيبرانية المخزنة في المستودع بناءً على نتائج

التشخيص والتقييم. أنماط المعالجة المخزنة في البرنامج تسمى «بقوائم الفحص»، التي تحاكي من الناحية الشكلية -من وجهة نظر "ميراي جينيكس" (Murray E. Jennex)- تلك الوصفات الموجودة في كتاب الطبخ لإعداد أطباق الأكل المختلفة. لكن هذه الفكرة ليست جديدة في النظرية الاستراتيجية السيبرانية، وإنما لها جذورها المعرفية في تراث النظرية الظاهرية المطوّرة من قبل علماء الاجتماع، المتضمنة مجموعة من المفاهيم السوسيولوجية المقترحة لتحليل الظواهر الاجتماعية، مثل مفهوم «ذخائر الخبرة» المقترح من قبل "ألفريد شوتز"، التي شبهها بكتاب الطبخ المتضمن نماذج مختلفة من أشكال السلوك والخبرات التي تزوّد الفرد بالقدرات على مواجهة المواقف الاجتماعية المختلفة ضمن عملية التفاعل الاجتماعي⁽³⁵⁾. المعرفة من المنظور السوسيولوجي هي «التي تزودنا بالإطار التأويلي، أو بالإطار المرجعي، والذي نستطيع بواسطته أن نطبق خبرة الماضي، ونجعل منها أساساً للأفعال البديلة أو الأفعال الممكنة»⁽³⁶⁾.

كل الأفكار السابقة كيفية بطريقة ما لتطبيقها في مجال الدفاع السيبراني، من خلال جعل برمجات الدفاع تتعرف على التهديدات وتشخص طبيعة الخطر عبر بنية نمطية من المعايير الرقمية المحددة مسبقاً، ثم يتم انتقاء الأسلوب المناسب لمكافحتها. التحدي الرئيسي -وهو العنصر الذي تركّزت عليه معظم الانتقادات- الذي يواجه نموذج الاتجاه العام في الدفاع هو الخاصية النمطية الرقمية التي يطبقها في مكافحة الهجمات السيبرانية، بحيث أن الهجمات والتهديدات غير المنمّطة في النموذج تستطيع أن تخترق النظام وتهاجم البيانات، لأن البرنامج لا يستطيع التعرف عليها بناءً على قاعدة البيانات أو ذخائر المعرفة التي يحملها. بعبارة أخرى، أن الهجمات السيبرانية ذات الخصائص الفريدة أو الخلاقة لا يتعامل معها هذا النموذج، مما يجعل البوابة عرضة للاختراق وعطب الأنظمة أو سرقة المعلومات؛ السبب في ذلك ببساطة هو أن قوائم الفحص (ذخائر المعرفة وطرق الإجراء في علم الاجتماع) لا تتضمن كل أشكال وخصائص التهديد الفعلية والمحتملة، كما هي غير مزودة بحجم هائل من الاحتمالات؛ وبالتالي المحدودية في نماذج الفحص هي الثغرة الأمنية التي تتسلل عبرها الهجمات السيبرانية. لقد جعلت خاصية النمطية المعيارية النموذج يتعامل مع الأخطار بطريقة ميكانيكية التي لا تكون فعالة في كل حالات التهديد، مما يعني بطريقة أخرى ظهور الحاجة إلى نماذج دفاعية أخرى أساسية أو مكملّة لحماية المنشآت والبنية التحتية السيبرانية الحساسة الخاصة بنظم الحاسوب وأمن الشبكات.

(2) نموذج تحليل الحاجز السيبراني

يعتبر الحاجز السيبراني أحد المقاربات الدفاعية لمنع الاختراقات أو انتهاك نظم الحماية الخاصة بالمعلومات الحساسة أو عالية السرية، فهو -من الناحية النظرية- العتبة السيبرانية التي تتحطم أو تتلاشى عليها الهجمات السيبرانية ومحاولات التسلل أو التطفل وكل الأنشطة الخبيثة الأخرى. من الناحية الاصطلاحية، يرى ميراي جينيكس Murray E.

Jennex أن «الحاجز Barrier» يعني عمليا القيام بتركيب الفحوصات [السيبرانية] ضمن الطبقة الأمنية [من أجل منع وقوع الاختراقات أو الهجمات]⁽³⁷⁾. أما مفهوم «تحليل الحاجز Barriers Analysis» (كذلك يُعرف بمصطلح «الرسوم البيانية للحاجز Barrier Diagrams»)، فهو عبارة عن «أداة مستخدمة في أصل النظام للقيام بتحليل الرسوم البيانية للحاجز. تحليل الحاجز هو عملية تحديد وتنظيم إجرائي وإداري وما إلى ذلك من الحواجز الموجودة لمنع عمل معين من الحدوث»⁽³⁸⁾. أو هو: «طريقة لتحديد الأخطار أو التهديدات، وتحديد فعالية عوامل منع/تلطيف حدوث الخطر/التهديد. كذلك يمكن أن يستخدم تحليل الحاجز بعد وقوع الحادثة من أجل تحديد أصل السبب والمساعدة على تطوير حواجز [جديدة] لمنع حدوث التهديدات مرة أخرى»⁽³⁹⁾.

إن الحاجز السيبراني يحاكي نقاط التفتيش التي توضع على طرق أو مداخل المدن للقيام بعمليات التحقق والفحص الأمني كإجراء وقائي، من أجل منع وقوع جرائم أو هجمات إرهابية ضد المصالح العامة للدولة أو المواطنين الأبرياء، وإسقاط شروط السيطرة الأمنية على مناطق البلاد؛ كذلك الأمر بالنسبة للحاجز السيبراني، الذي هو عبارة عن برمجيات تتركب لفحص عمليات الدخول إلى أنظمة المعلومات أو الشبكات أو الأنشطة السيبرانية بصفة عامة، في سبيل تحديد المخاطر الأمنية ومقاومة أو على الأقل الحد من التهديدات الأمنية. إنه عبارة عن عملية وقائية تتخذ لحماية الموجودات والأصول المخزنة في نظم الحاسوب، تحاكي تلك الإجراءات المتخذة في العالم المادي مثل اتخاذ الأبواب للبيوت، وجود خزنة فولاذية لحماية الوثائق والأموال من السرقة، وضع جهاز إنذار على الأبواب، وغيرها من الإجراءات المتخذة من أجل تأمين الأملاك المادية.

تعتبر كلمات المرور، اسم المستخدم، ترميز الملفات، المفتاح العام، المفتاح الخاص، اسم الوظيفة، وترميز الحاسوب في حد ذاته أمثلة للحواجز السيبرانية؛ التي تمثل طبقات من الإجراءات الأمنية الهادفة إلى منع وصول المتسللين أو الأشخاص غير المرخصين إلى المعلومات السرية، وبالتالي منع وقوع الأحداث الأمنية الخطيرة كاختراق محميات البيانات الحساسة للمنظمة أو سرقة براءات الاختراع وغيرها من الأصول التي تمثل قيمة حيوية للدولة أو الهيئة المعنية. تكمن أهمية تعدد الحواجز السيبرانية في إعاقة العدو دون الوصول إلى المعلومات الحساسة أو قاعدة بيانات النظام، بحيث أنه إذا تمكن من تخطي الحاجز الأول، سوف يتعطل في الحاجز الثاني أو الثالث؛ بالطبع هذا من الناحية النظرية، لأن من الناحية العملية يمكن تخطي كل الحواجز السيبرانية وتحقيق الاختراق الأمني بواسطة التحايل على نظام الحاسوب، استغلال الثغرات الأمنية، استخدام هويات مزيفة أو مسروقة، سحق أو تفكيك كلمات المرور، وغيرها من التكتيكات المستخدمة من قبل القراصنة المحترفين. لكن لا تلغي هذه العيوب الوظيفية أهمية استخدام الحواجز السيبرانية لتأمين نظم الحاسوب والشبكات وحتى الحواسيب الشخصية للأفراد.

للتغلب على العيوب الوظيفية السابقة الذكر وأخرى في تأمين نظم الحاسوب، يتم تبني إجراء «حاجز متعدد الطبقات Barrier Multilayered». تعني الطبقة Layer من الناحية الاصطلاحية أي «معلم/حد دفاعي، يتضمن مجموعة من الفحوصات توضع لحماية أصول معينة أو مجموعة أصول»⁽⁴⁰⁾. يؤدي هذا النوع من الحواجز وظيفة ما سَمَاه ميري جينيكس «بالدفاع في العمق Defense in Depth»، الذي هو عبارة عن «مقاربة أمنية التي تعتمد على التكنولوجيات المتعددة والمقاربات المتعددة لتلطيف الخطر [على شبكات الحاسوب]»⁽⁴¹⁾؛ وهو مفهوم مشتق من النظرية الاستراتيجية التقليدية السوفياتية في الدفاع، إنه عبارة عن أي مقاومة للاختراقات السيبرانية في النقاط المتقدمة قبل أن تصل إلى المعلومات الحساسة عبر طبقات متعددة من الحواجز، اشتقاقا من المذهب السوفياتي في الدفاع عن الحدود السوفيتية خلال الحرب الباردة بواسطة نشر القوات العسكرية عبر المناطق المجاورة.

يعني مفهوم «الدفاع في العمق» في النظرية التقليدية، «الاستخدام المنسق للمنشآت والتجهيزات العسكرية من أجل اكتشاف الصاروخ [المهاجم] وتعقبه والتعامل معه في أثناء كل مرحلة من مراحل تحليله في مساره»⁽⁴²⁾، وذلك قبل وصوله إلى نهايته المقصودة؛ وهو معنى قريب من تكتيك «أشبك وقاتل Plug-and-fight» في القتال البري. نفس المعنى تقريبا يطبق في الفضاء السيبراني، عن طريق مقاومة الاختراقات أو الهجمات السيبرانية بواسطة نقاط متقدمة من الفحص المصففة في شكل طبقات، وذلك قبل أن تصل الهجمات إلى الحاجز الأخير. لضمان فعالية قتال الهجمات السيبرانية عبر طبقات متعددة أو بواسطة تكتيك الدفاع في العمق، «يستخدم المصممون فحوصات متعددة التقنية، الإدارية، والعملياتية لحماية الأصول. وضع الفحوصات ضمن طبقات يسمح للمصممين بتثبيت سلسلة من المَعْلَمَات الدفاعية التي تعزز بعضها البعض، ولا تسمح باختراق بعض الطبقات التي تحمي الأصول الأساسية»⁽⁴³⁾. يفترض أن حاجز الطبقات المتعددة موجه أساسا نحو فحص كل الأنشطة الخبيثة وأشكال الهجمات السيبرانية أو أنواع الاختراقات المحتملة، سواء كانت مقصودة أو عرضية، داخلية أو خارجية، عالية أو متدنية الحدة؛ بشكل يحقق متطلبات وشروط مفهوم أمن المعلومات وحماية الشبكات؛ غير ذلك، يكون النظام بدون معنى أو يفقد قيمته الدفاعية.

3) نموذج الدفاع الوقائي

يتضمن هذا النموذج مجموعة من الإجراءات الدفاعية الموجهة أساسا نحو إحباط هجمات حرمان الخدمة السيبرانية الموزعة، التي تقف عائقا أمام فعالية تدفق الوفرة المطلوبة من الخدمات نحو المستهلكين؛ يمكن تصنيف هذه الإجراءات ضمن مجموعة النقاط التالية:

أ) **الوقاية** تستهدف الهجمات السيبرانية تعطيل أنظمة الحاسوب عن العمل ومن وراء ذلك عطب كل الأنشطة التجارية، لكن ليست هذه الأخيرة هي المتضرر الوحيد من هذا النوع من الهجمات، وإنما هناك قطاعات أخرى أكثر حساسية يمكن أن تُمنى بخسائر مالية كبيرة مثل قطاع النقل الجوي والبحري، نظم الصيرفة والمال، والخدمات العامة في المجتمع كنظام البريد والصحة. بناءً على ذلك، تكمن فعالية الدفاع السيبراني ضد تعطيل مثل هذه الخدمات في تلك الأنشطة والإجراءات الفنية القبلية التي تحصّن نظم الحاسوب والشبكات ضد قابليات للعطب، أو ما يمكن تسميته بالدفاع الوقائي الموجه نحو تأمين تدفق الخدمات بشكل سلسل ووفرة كافية، والمحافظة على البنية التحتية للخدمات السيبرانية سالمة وتعمل بكل طاقتها؛ على اعتبار أن جوهر عمل هجمات حرمان الخدمة الموزعة مثلاً هو إغراق الشبكات والروابط بطلبات الخدمة المزيفة بهدف إثقالها عن العمل بالسرعة المطلوبة، وبالتالي تعطيلها عن الاستجابة لطلبات المستخدمين الشرعيين أو الحقيقيين في الفضاء السيبراني. جوهر الوقاية بصفة عامة مُركّز حول التعهد المستمر بالنظم الاحترازية وتحديثها باستمرار من أجل منع وقوع الهجمات أو على الأقل لتلطيف آثارها، بحيث يمكن إصلاح العطب بطريقة آلية وسريعة أو إطلاق نظم الصيانة السريعة؛ هذا يعني من الناحية العملية وجود فريق ماهر ومتخصص في مراجعة إجراءات الوقاية واقتراح تقنيات دفاعية أخرى أو بالأحرى تطبيقات جديدة، عندما تكون النظم المثبتة على الحواسيب ضعيفة أو تعاني من ثغرات فنية تنفذ عبرها الهجمات السيبرانية.

بشكل عام، يمكن إحصاء قائمة من إجراءات الوقاية السيبرانية المعتمدة في الحد من تأثير هجمات حرمان الخدمة الموزعة، والمحددة في مجموعة النقاط التالية:

(1) تنسيق نظم الحاسوب والبرمجيات والتطبيقات المثبتة في المعدات السيبرانية بشكل يجعلها تقوم بعمليات الصيانة والتحديث واستعادة الملفات المتلفة بطريقة آلية وذاتية؛ ولو أن الكثير من هذه الإجراءات أصبحت تتركب في الحواسيب من قبل الشركات التي تصنعها، إلا أن التطبيقات الجديدة أو الإضافية يجب أن تنسق بطريقة يجعلها تعمل من تلقاء نفسها بمجرد تشغيل الحاسوب وتقوم بوظائف الصيانة والمحافظة بطريقة آلية. بالطبع هذا يتطلب أن تكون ذاكرة الحواسيب قوية وحجم التخزين كبيراً بشكل يستطيع حمل كل التطبيقات الوقائية الجديدة، في مقابل ذلك لا بد من حذف كل التطبيقات والبرمجيات الخاملة أو غير الوظيفية التي تثقل قدرة الحواسيب على العمل بسرعة.

(2) يرتبط الإجراء الوقائي الثاني بسابقه من حيث دعم وتقوية نظم الحماية الموجودة عن طريق تحميل التحديثات السيبرانية بشكل لحظي، لسد الفجوات الأمنية التي خلفتها أي هجمات، أو هي موجودة أصلاً في نظم الحماية الأمنية؛ عادة تحمل التحديثات الجديدة قطع الغيار السيبرانية للملفات المتلفة، وإضافة امتيازات جديدة لاستكمال عناصر النقص

وتقوية نقاط الضعف الموجودة في النظام. تعمل التحديثات السيبرانية في اتجاهين، الأول هو القيام بأعمال الصيانة وتوفير قطع الغيار للملفات المتلفة، والثاني هو القيام بعمليات الدعم للإجراءات المثبتة وتوفير الاحتياط الأمني ضد الهجمات المحتملة، بحيث تصبح نظم الحاسوب في وضع دفاعي جيد ومتأهبة لاحتواء أي تهديدات سيبرانية. يحاكي هذا المبدأ مفهوم الدفاع في النظرية الاستراتيجية التقليدية لكارل فون كلاوزفيتز، الذي يرى أن معنى الدفاع هو انتظار قدوم العدو، بحيث يكون المدافع متأهبا تماما للقتال لحظة وقوع الهجوم.

(3) تبني خيار «الاتصالات الرمزية المموهة Encrypt Communication»، التي تكون المعلومات فيها محصنة ضد الاختراقات أو التعطيل خلال رحلتها عبر النظم السيبرانية، وبالتالي يضمن هذا الإجراء تدفق الخدمات بشكل سلس وآمن وبوفرة كافية لكل للزبائن. بالرغم من الامتياز الذي يوفره هذا الإجراء في احتواء هجمات حرمان الخدمة الموزعة، إلا أن هناك إمكانية لجوء المهاجمين إلى التحايل أو فك الترميز المموه بواسطة سحق كلمات المرور أو إطلاق برمجيات خبيثة مضادة لنظم الترميز.

(4) بناءً على التحدي المشار إليه سابقاً حول إمكانية لجوء المهاجمين إلى فك الترميز المموه للاتصالات، يمكن تبني إجراء آخر للدفاع الوقائي المتعلق «بتنسيق المراقبة للممرات Control Configuration of Routers» التي ترحل عبرها الاتصالات السيبرانية، وذلك من خلال زيادة القدرة على التحقق من رزم الرسائل الاتصالية حول عدم حملها أي برمجيات خبيثة، أو أنها رسائل خادعة تستهدف عطب النظام عن العمل؛ على اعتبار أن التكتيك الذي يعتمد عليه كثيرا المنفذون لهجمات حرمان الخدمة، هو التظاهر بأنهم مصادر اتصالية أصلية أو أنهم يحملون خدمات سيبرانية واعدة من أجل إغراء ضحاياهم. لذلك، الإجراء المناسب في تجنب مثل هذه المطبات الأمنية هو تركيب ما يسمى «بمصافي الدخول Ingress Filters» على بوابات الممرات الاتصالية لفحص رزم الرسائل القادمة، وكذلك تركيب «مصافي الخروج Egress Filters» للتحقق من عدم وقوع أخطاء أو ثغرات أمنية أو عمليات خداع ومنع تسويقها إلى محطات سيبرانية أخرى أو إرسالها إلى مستخدمين آخرين.

(5) يجب أن تهتم الهيئات الحكومية والشركات وكل الفواعل التي لديها مصالح حيوية في الفضاء السيبراني، بإعداد ما يسمى «بخطط الطوارئ»⁽⁴⁴⁾ Emergency Plans، التي تشمل مجموعة من الإجراءات الدفاعية والتنظيمية وعمليات الإنقاذ والتعافي في حالة التعرض لهجوم سيبراني كبير، يخترق كل الدفاعات الأمامية ويتخطى الإجراءات الوقائية. عادة تكون خطط الطوارئ جاهزة للرد على الهجمات المفاجئة في شكل حاسوب الرد على الطوارئ، الذي يتولى تنسيق معظم الوظائف والمهام والاتصالات الخاصة بالعمل خلال الطوارئ؛ فهو الحاسوب البديل الذي يُشغل عندما تشل الهجمات السيبرانية الحواسيب العادية وتوقف

الشبكات عن العمل. يستلزم وجود حاسوب الرد على الطوارئ فريقاً فنياً متخصصاً في القيام بهذه المهمة شبيهاً بفريق خدمة الطوارئ في العالم الواقعي، يسمى «بفريق الرد على طوارئ الحاسوب Computer Emergency Response Team»، الذي يتضمن «جماعة من خبراء أمن الإنترنت، الذين هم أعضاء في دراسة قابليات عطب أمن الإنترنت، بحث التغيرات طويلة المدى في الأنظمة المشبكية، وتطوير المعلومات والتدريب لتحسين الأمن [السيبراني]⁽⁴⁵⁾؛ أو هو عبارة عن «مركز تنسيق الفريق للرد على الطوارئ الحاسوبية .. [يوظف] الخبرة الأمنية للإنترنت [من أجل التعامل مع كل أشكال التهديد السيبراني]». في حالة الولايات المتحدة، تم تأسيس أول فريق للطوارئ في شكل مؤسسة قائمة بذاتها من قبل جامعة كارنيجي-ميلن Carnegie-Mellon عام 1988، يقع مقرها في «معهد هندسة البرمجيات Software Engineering Institute» داخل الجامعة⁽⁴⁶⁾. الهدف الرئيسي لهذه المؤسسة وغيرها هو إيجاد البدائل المختلفة لضمان تدفق الخدمات السيبرانية الموزعة خلال فترات الأزمات، أو خلال وقوع الهجمات السيبرانية الكبرى التي تشل البنية التحتية الحساسة عن العمل.

ب) تطوير أنظمة الإنذار المبكر. إحدى المقاربات الدفاعية الفعالة في الرد على التهديدات السيبرانية هي الاكتشاف المبكر للهجمات قبل أن تخترق الإجراءات الأمنية الأمامية، وذلك بواسطة تركيب نظام إنذار مبكر بوقوع هجوم معين أو وجود محاولات لاختراق أنظمة الحماية في الحاسوب من أجل الوصول إلى المعلومات السرية. الخاصية المميزة لنظام الإنذار المبكر هي توفير الوقت الكافي للرد على التطفلات، واتخاذ التدابير الوقائية من أجل تقليص الخسائر أو تلطيف قوة الهجمات والحد من آثارها الأمنية؛ بالطبع يتطلب هذا التفات الشركات والهيئات الحكومية إلى الاستثمار في تطوير نظم الإنذار المبكر وليس فقط نظم الدفاع وإجراءات الوقاية. فهي عملية تحاكي نظم الرادار والاستشعار عن بعد في النظرية الاستراتيجية التقليدية⁽⁴⁷⁾، التي تنبه بوقوع انتهاك للأجواء الوطنية أو التنبيه بوقوع هجوم وشيك على مصالح الدولة في الداخل أو الخارج. الحقيقة أن مسألة الإنذار المبكر في النظرية الاستراتيجية التقليدية أو السيبرانية هي معقدة ومثيرة للجدل، بسبب وجود مخاطر عالية لوقوع الاختراق لنظم الدفاع أو التحايل على نظم الإنذار المبكر أو يمكن أن يقع الاختراق بسبب الإهمال البشري والتعقيدات البيروقراطية في المنظمات الأمنية.

ج) تلطيف الهجمات وضمان تدفق نوعي للخدمة. تفترض هذه المقاربة أو الطريقة في الوقاية السيبرانية ضرورة العمل على جعل أنظمة الحاسوب والشبكات تتكيف مع الهجمات السيبرانية مثل الجسم الذي يتكيف مع الأمراض أو الهجمات الفيروسات البيولوجية، وبدلاً من العمل على وقفها تماماً (وهو أمر مستحيل)، يجب تركيز الاهتمام على تلطيفها أو تخفيف حدتها إلى المستوى الذي لا تؤثر فيه على عمل نظم الحاسوب، وتضمن استمرار تدفق الخدمة الموزعة للمستخدمين الشرعيين.

(د) **تعقب مصدر الهجمات.** تعتبر عملية «تعقب مصدر الهجمات traceback the source of attacks» أكثر المهام صعوبة وتعقيدا أمام المصممين الدفاعيين السيبرانيين، وذلك بسبب أن في معظم الأحيان يهتم المهاجمون بتبني مقاربات هجومية تضلل تقفي أثرهم أو تموّه أعمالهم الهجومية، بنفس القدر الذي يهتمون فيه بكيفية إبداء مقاربات اختراق الدفاعات السيبرانية والولوج إلى البنية التحتية الحساسة لإنجاز المهمة الهجومية؛ يصطلح البعض على هذه المشكلة «بتحدي العزو»، الذي يعني صعوبة عزو أو ربط الهجمات بمصادرها الحقيقية. لكن مع ذلك، يرى "جورج ديستيرير" (Georg Disterer) وزملاؤه بأن: «كشف مصادر هجمات حرمان الخدمة الموزعة وتلطيف آثارها يجب أن يبقيا دائما على رأس الأولويات الأمنية، ومن ثم يجدر بالشركات أن تحاول تعقب أثر المهاجم وكشف شبكة حرمان الخدمة الموزعة لمنع المزيد من التهديدات..»⁽⁴⁸⁾.

(هـ) **التدريب الأمني.** إحدى المقاربات الوقائية المتاحة أمام الحكومات والمنظمات الخاصة هي القيام بعمليات «التدريب الأمني السيبراني Cybersecurity Training» المحترفة، أو الموجهة نحو تأهيل فريق عمل متخصص في مهام الدفاع السيبراني وكيفية تأمين المنشآت والبنية التحتية الصلبة واللينة الخاصة بالقوة السيبرانية، وذلك محاكاة مع تلك التدريبات التقليدية في الشؤون العسكرية والأمنية. على المستوى العام، فإن عملية التدريب يجب أن تتوسع لتشمل جميع مستخدمي الفضاء السيبراني، وذلك من خلال التعليمات والنصائح التي تقدم بشكل فوري وآلي عندما يتعرض الحاسوب أو الحسابات الشبكية الخاصة لهجمات سيبرانية؛ إنها تتضمن عملية تثقيف سيبراني حول طرق الحماية الأمنية واتباع إرشادات إصلاح الأعطاب. الافتراض الأساسي المقترح في هذا الصدد أن الأمن السيبراني يتطلب قوات متخصصة ذات مهارة عالية في إدارة شبكة الإنترنت وعلى دراية بعلم الحاسوب، وذلك للعمل بشكل دائم على تشغيل التطبيقات السيبرانية الجديدة، تقييم التهديدات، القيام بالتحديثات المطلوبة في تنفيذ الإجراءات الوقائية؛ وبالطبع التدخل السريع في حالة وقوع الهجمات الكبرى، التي تستهدف شل أنظمة الحاسوب وتعطيل الشبكات عن العمل تماما.

على مستوى احتراف الأمن السيبراني، تتضمن عمليات التدريب تحضير القوات السيبرانية والموارد ذات العلاقة لصد الهجمات السيبرانية على المستوى الكبير، بواسطة تنفيذ عمليات المحاكاة لحرب الدفاع السيبراني، تطوير المهارات الدفاعية في تشغيل التطبيقات السيبرانية المضادة وتعديل البرمجيات القابلة للعطب، وحتى محاكاة الحرب السيبرانية الهجومية؛ التي عادة تكون مطلوبة عندما يكون العدو في وضعية مكشوفة أو منهمك في الإعداد للهجوم. الكثير من عمليات المحاكاة للحرب السيبرانية -أو ما سماها "جورج كوستوبولس" (George Kostopoulos) «بالتمارين والمحاكاة السيبرانية Cyber Simulation and Exercises»-، تقوم بها فرق خاصة تابعة للقوات المسلحة، يتم تنفيذها

بالتزامن مع التدريبات العسكرية الميدانية حول الحرب التقليدية؛ خاصة بالنسبة للجيش التي تتمتع ببنية تحتية سيبرانية متطورة.

حدد كوستوبولوس⁽⁴⁹⁾ عشر مهام لعمليات التدريب الأمني ومحاكاة الدفاع السيبراني وهي:

(1) تقييم إجراءات الإعداد المضاد للهجمات السيبرانية والاختراقات وعمليات التطفل؛
(2) تحسين قدرات الكشف وتشخيص طبيعة وخصائص التهديدات السيبرانية؛ (3) تطوير القدرات الفنية والإنذار المبكر للتعامل مع الكوارث الطبيعية والاضطرابات المناخية؛ (4) تحديد الثغرات التقنية وقابليات عطب التكنولوجيا السيبرانية؛ (5) تمكين السلطات من استغلال قابليات عطب دفاعات العدو واستهداف نقاط ضعف إجراءاته الأمنية؛ (6) تعزيز وتكثيف أوجه التعاون وتبادل المعلومات بين الأطراف المعرضة للتهديدات المشتركة؛ (7) تحديد الإمكانيات المحتملة حول تطوير الشراكات السيبرانية الجماعية وتقوية الاعتماد المتبادل الأمني على المستوى الوطني والدولي؛ (8) تحسين مهارات التخطيط السيبراني المستمر لاحتواء التهديدات المفاجأة؛ (9) تدريب وتعليم الناس الأمن السيبراني عبر نشر الثقافة السيبرانية وتنمية الوعي الأمني؛ (10) خلق مستوى عالي من الثقة في الأمن السيبراني لدى المستخدمين بواسطة إنتاج التطبيقات الفعالة، معالجة الثغرات الأمنية، وتحسين قدرات إصلاح الأعطاب والتعافي السريع من آثار الهجمات السيبرانية.

(9) تحليل البيانات الشخصية. بالرغم من التحدي الكبير المطروح حول صعوبة تعقب مصدر الهجمات السيبرانية، أو ما يمكن تسميته بصعوبة الغزو السيبراني كمشكلة تواجه الأمن السيبراني، إلا أن طريقة استخدام الإنترنت والرغبة في الاستفادة من الخدمات السيبرانية قد جعلتا الكثير من المعلومات الشخصية متاحة أمام محلي الأمن السيبراني، للاستعانة بها في تحديد هوية المهاجم أو القائم بالأنشطة العدائية في الفضاء السيبراني، عبر ما اصطلح عليه "بول روزنزويغ" (Paul Rosenzweig) «بتحليل البيانات الشخصية»⁽⁵⁰⁾ Dataveillance. الحقيقة أن طريقة استخدام الإنترنت ليست العامل الوحيد الذي ساعد على اعتماد عملية تحليل البيانات الشخصية كطريقة لمكافحة الأنشطة السيبرانية المعادية، وإنما هناك عامل آخر سماه روزنزويغ «بثورة التخزين»، التي تعني تطوير أجهزة الحاسوب والشبكات القادرة على تخزين المعلومات فوراً بكميات غير مسبقة، وتنظيمها آلياً بشكل يجعلها سهلة الاستدعاء وقابلة للاستخدام لأغراض متعددة، منها الشؤون الدفاعية والأمنية. لقد تضمنت ثورة التخزين خاصيتين أساسيتين هما: «الزيادة في قوة الحوسبة وتناقص في تكاليف تخزين البيانات»⁽⁵¹⁾، وهذا ما يجعل البحث في ملايين المعلومات حول البيانات الشخصية عملية سهلة تتم في فترة زمنية وجيزة؛ الأكثر من ذلك أهمية، توسيع عمليات التتبع والبحث عبر كميات كبيرة من البيانات المخزنة، بشكل يجعل احتمال الوصول إلى تحديد مصادر التهديد عالياً في وقت وجيز.

ثالثاً: إدارة الحرب السيبرانية

إذا كانت الأمم تحارب من أجل المحافظة على أوطانها مندمجة، فإنها كذلك تفعل في البيئة السيبرانية من أجل تحقيق نفس الغاية الاستراتيجية بطريقة مغايرة، بغض النظر عن الجدل القانوني حول طبيعة الحرب السيبرانية ووجودها من عدمها. الفكرة الجوهرية المراد التأكيد عليها أنه طالما أن الفضاء السيبراني يحمل مصالح وطنية حيوية للدول بالتوازي مع وجود منافسة كبيرة تتمظهر في صورة متعددة، فإنه قد تحول إلى مسرح حيوي لإدارة العمليات الاستراتيجية المختلفة: الدفاع عن المصالح والأصول الحيوية للدولة، دعم إدارة الحرب التقليدية، التجسس، التطفل، القرصنة، ضرب البنية السوسولوجية للعدو، والتحضير للحرب السيبرانية البحتة بواسطة الفيروسات والتطبيقات الهجومية. تندرج كل العمليات الاستراتيجية السابقة الذكر وأخرى ضمن المفهمة الواسعة للحرب السيبرانية التي يحتمل أن تواجهها الدولة في طريقها نحو تشييد وطنها السيبرانية. ليس هناك شيء متاح مجاناً، كما أنه ليس هناك مصالح حيوية لا تستلزم كلفة لحمايتها والدفاع عنها؛ تشكل هذه المعاني المنطق الاستراتيجي الذي يحكم الدول في بيئتها المادية أو الافتراضية.

يعتبر التراث الاستراتيجي والأمني الذي كُتب حول الفضاء السيبراني بصفة عامة، وكل الموضوعات الفرعية ذات العلاقة (كالهرب السيبرانية) ناشئاً، بسبب أن استخدام القدرات السيبرانية في الشؤون الاستراتيجية والعسكرية مازال غير واضح المعالم؛ الأكثر أهمية من ذلك، تصاعد الشكوك والتأكدات بشكل متلازم حول قابلية استخدام القوة السيبرانية في الحروب والنزاعات الحديثة بين الدول لتدمير بعضها البعض، وذلك بسبب حالة قابلية العطب الجماعي الآلي بغض النظر عن مستوى تقدم التفوق العسكري المادي لأطراف النزاع. إذا كان الافتراض الشائع حول استخدام القوة التقليدية أو النووية يقضي بأن العطب الجسيم سوف يكون من نصيب الطرف الضعيف، فإن الضحايا والآثار عند استخدام القوة السيبرانية سوف تكون عامة، طالما أن كل الدول تتربط مع نفس الشبكة. في مقابل ذلك، يعتقد المدافعون عن فرضية الحرب السيبرانية Cyberwar أن الدول يمكن أن تلجأ إلى القوة السيبرانية من أجل شلّ بعضها البعض أو الحرمان من التفوق العملياتي فوق مسرح العمليات، كتعطيل الأقمار الصناعية، عزل القوات في ساحة المعركة عن مركز القيادة، شلّ عمل الأسلحة الموجهة بواسطة القوة السيبرانية (الأسلحة الذكية) وهكذا. الأكثر من ذلك، أن تحت تأثير مفردات الريبة، المساعدة الذاتية، المنافسة الأمنية، وباقي المفردات المقترحة من قبل أنصار النظرية الواقعية/الواقعية الجديدة⁽⁵²⁾، فإن الدول لا تنتظر التأكد من حقيقة الحرب السيبرانية من عدمها، وإنما تستعد دائماً وتحضّر نفسها للأسوأ، حتى ولو كان هذا النوع من الحرب خدعة أو وهما على شاكلة الحرب النووية وحرب النجوم خلال فترة الحرب الباردة؛ وإلا يجب عليها دفع ثمن الاعتداء، حتى ولو كان احتمال وقوع هذا الأخير بنسبة واحد بالمائة. الاعتبار الاستراتيجي الذي يؤخذ جدياً في الحسبان مفاده أن

الحرب السيبرانية هي كل الأعمال العدائية الفعلية أو المحتملة ذات المضامين المختلفة (تخريب، تضليل، تجسس، قرصنة، سرقة معلومات، تعطيل الشبكة عن العمل ..)، الموجهة ضد أنظمة الحاسوب والشبكات السيبرانية المتحركة في البنية التحتية الحساسة للدولة (إدارة منظومات الأسلحة، مراكز توليد الطاقة، النقل، تنظيم حركة المرور، شبكة وزارة الدفاع والأمن ...).

من ناحية أخرى، ضمن المعنى الاستراتيجي العام، الحرب هي «عنف بين جماعات الذي عادة يتضمن ضربة القتل و[إحداث] الإصابة ضد الجانب الآخر.. بدون العنف، الإصابة، والقتل، يفقد المصطلح معناه ومضمونه»⁽⁵³⁾. يستلزم وقوع العنف وجود عالم مادي للاشتباك بين القوات المسلحة للطرفين عادة يسمى بحقل المعركة، الذي هو الآخر -وفق كلاوزفيتز- يخضع لتنظيم معين وفق معايير عسكرية محددة مثل المعرفة بالأرض، الطقس، العدو، الطريقة المناسبة للاحتشاد وغيرها من المعايير التي عادة تكون معروفة أو متوقعة من قبل جانبي القتال. في الحرب السيبرانية، لا يوجد حقل معركة مادي محدد كما لا يوجد احتشاد عسكري مثل ما هو معروف في الحرب التقليدية، وإنما هناك معركة مفتوحة يمكن أن تمتد لتشمل العالم ككل. كما أن حقل المعركة السيبرانية لا يتطلب أن تكون الدول محتكرة لأدوات العنف، إذ يمكن للأفراد والجماعات أن تبدأ هذه الحرب سواء من تلقاء نفسها أو بالوكالة عن الآخرين. لذلك يرى كل من "كلارك" و"كناك" أن: «الحرب السيبرانية هي عالمية: في أي نزاع، الهجمات السيبرانية تنتشر بسرعة عبر العالم، تكتسب أو تقرصن خفية الحواسيب والخوادم عبر العالم وتعطل الخدمة. الكثير من الدول تتورط فيها»⁽⁵⁴⁾. بالنسبة لـ "إلينور سلوان" (Elinor C. Sloan)، فإن الحرب السيبرانية تعني: «استخدام الأعمال المتعمدة -بالطبع على فترات طويلة من الزمن- لتعديل، تمزيق، خداع، تخريب، أو تدمير أنظمة حاسوب الخصم أو الشبكات أو البرامج المخزنة أو نقل هذه الأنظمة أو الشبكات»⁽⁵⁵⁾. أو هي: مجموعة «الهجمات [السيبرانية] على أنظمة الحاسوب والشبكات بواسطة أدوات البرمجيات والبيانات»⁽⁵⁶⁾. يمكن أن تتضمن الحرب السيبرانية عمليات «إلحاق الضرر ببيانات العدو وشبكاته الإلكترونية أو تعطيلها، أو إلحاق مزيد من الضرر المادي بأفراد العدو أو عتاده»⁽⁵⁷⁾.

للسياق الاستراتيجي دور مهم في تحديد مدى ومكونات وأنشطة الحرب السيبرانية، إذ خلال فترات النزاع الحاد بين الدول، فإن كل الأنشطة التي تجري على الفضاء السيبراني عادة تصنف تحت فئة الأعمال العدائية التي يجب الرد عليها؛ سواء تضمنت عمليات استغلال شبكة الحاسوب أو القيام بالهجمات ضدها. على عكس فترات السلم، التي يتم التعامل مع عمليات استغلال شبكة الحاسوب كالتجسس وسرقة المعلومات الحيوية وغيرها بواسطة الإجراءات العادية المضادة للاختراق والمحافظة على أمن المعلومات. الحرب السيبرانية معنية على وجه التحديد باستخدام الأسلحة الرقمية المعروفة والمحملة في المستقبل

من أجل تحقيق هدف التخريب المتعمد للمعلومات، أو التسبب في التدمير المادي للبنية التحتية وإيقاع الإصابات في صفوف العدو.

يمكن النظر للحرب السيبرانية على أنها ظاهرة جديدة في الشؤون الاستراتيجية والعسكرية تختلف عن نظيرتها التقليدية، وتشتمل مضمون هذا الاختلاف من طبيعتها المكونة من الشبكات والبرمجيات وكل أشكال القوة اللينة، وليس القوة الصلبة كما هو مألوف في الحرب العادية؛ تعتبر هذه المحاجة متماسكة إلى حد كبير، إلا أن جانب النقص فيها يكمن في أن البرمجيات والشبكات مرتبطة وظيفيا وعمليا بالبنية التحتية الحيوية المادية للدولة بما فيها العسكرية والأمنية، خاصة فيما يتعلق بمضامين ثورة المعلومات في الشؤون العسكرية. في كل الأحوال، هناك اختلاف مهم بين الحرب السيبرانية والحرب التقليدية، المحدد أساسا في الانتقال من مفهوم هيمنة حشد القوات فوق حقل المعركة إلى هيمنة المعلومات وتبديد مفهوم «ضباب الحرب» المطروح من قبل كارل فون كلاوزفيتز⁽⁵⁸⁾.

النتيجة المهمة المستخلصة من هذه المناقشة أن ليس هناك حدود فاصلة تماما بين الحرب التقليدية ونظيرتها السيبرانية، حتى ولو غلبت على الأولى الاستخدام المهيمن للقوة النارية، وتميزت الثانية جوهريا بإدارة وتوظيف المعلومات لغايات عسكرية. من منظور "مارتن ليبكي" (Martin Libicki)، يمكن تحديد المضمون المفاهيمي للحرب السيبرانية من خلال الأشكال السبعة التي تتمظهر بها، وهي: «قتال القيادة والسيطرة على رأس وعنق العدو، سواء عبر الهجوم المادي أو هجوم شبكات الحاسوب على الأهداف العسكرية؛ القتال الأساسي-للاستخبارات؛ القتال الإلكتروني؛ القتال السيكلوجي؛ قتال القرصان، هذا يعني هجوم شبكة الحاسوب على الأهداف المدنية؛ قتال المعلومات الاقتصادية؛ والقتال السيبراني»⁽⁵⁹⁾.

بالرغم من أن المفهمة السابقة قد وسعت المجال العملياتي للحرب السيبرانية، إلا أنها في نفس الوقت أدرجت مجالات غير مرتبطة بالفضاء السيبراني وتكنولوجية المعلومات، وأخرى تتعلق بالحرب التقليدية من حيث الجوهر أو هي مجرد تكتيكات لها، مثل مقارنة قطع الرأس التي هي خاصة بنظرية القوة الجوية⁽⁶⁰⁾، ومقاربة الحرب النفسية التي هي أسلوب قديم متلازم مع ظاهرة الحرب نفسها في العلاقات الاستراتيجية الدولية؛ إنما الشيء المتغير هو الأدوات المستعملة.

خاصيات الحرب السيبرانية

يتطلب الفهم الجيد لموضوع الحرب السيبرانية -كجزء ملازم لعملية تشييد الوطن السيبراني- والتحكم في توظيف مفردات التحليل وأدوات البحث، تشخيص الظاهرة بواسطة شرح وتفسير خاصياتها الجوهرية من حيث التفاعل، التطور، الفواعل، وفعالية التأثير في

القطاعات الأخرى؛ من أجل الحصول في النهاية على تصور عام لفهم الظاهرة. يمكن تصنيف هذه الخصائص ضمن النقاط التالية:

أ) تمدد مسرح العمليات. إحدى الخصائص المميزة للفضاء السيبراني في العلاقة بالحرب وشؤون الدفاع هي عدم محدودية مسرح العمليات، بحيث أنه يمتد لكل نقطة من العالم لها ارتباط بشبكة الإنترنت، ومن ثم تستثنى فقط المجالات المعزولة أو المفصولة عن الشبكة. وفق هذا المنطق، معظم المجتمعات ذات الثقل الصناعي والتجاري وحتى العسكري في العالم تكون مسرحاً للعمليات القتالية السيبرانية، لأنها طورت -ولازالت- بنيتها الدفاعية والهجومية وفق مفردات ثورة المعلومات وتكنولوجيا الرقمية في الشؤون العسكرية⁽⁶¹⁾. لحد الآن لم تحدث حرب سيبرانية ذات كثافة عالية تشمل العالم ككل، ولكن احتمال الانتشار والتمدد لكل ركن شبكي عبر العالم عالي جداً في حالة وقوعها، حتى ولو كانت العديد من الدول غير معنية بهذه الحرب من الناحية السياسية والعسكرية، إلا أنها تجد نفسها مقحمة فيها عنوة بسبب خاصية التمدد السيبراني لمسرح العمليات.

ب) صعوبة السيطرة. على الأقل من الناحية النظرية، تولّد خاصية التمدد السيبراني لمسرح العمليات خاصية أخرى ملازمة وهي صعوبة السيطرة على حقل المعركة بسبب اتساع حجمه من جهة، وعدم القدرة على تحديد مصادر النيران السيبرانية للرد عليها بفعالية من جهة أخرى؛ الأسوأ من ذلك، صعوبة معرفة الأطراف المنخرطة في القتال السيبراني، التي تعكس بدورها خاصية اللاتماثلية في أطراف القتال. صحيح -من الناحية الشكلية- تبدو السيطرة السيبرانية إلى جانب الأطراف المتحكمة في التكنولوجيات الرقمية ولديها موارد كبيرة موجهة نحو التطوير المستمر والمتسارع لقدراتها الدفاعية والهجومية السيبرانية، لكن هذا التفوق مقوض بواسطة قدرة الأطراف الضعيفة وحتى المنظمات والأفراد على الانخراط بشكل نشط في هذا النوع من الحروب، ولديها احتمال كسبها أو الأقل التسبب في إحداث أضرار جسيمة ضد الأعداء. بالرغم من أن الدول تطوّر تقنيات عالية الدقة في تحديد مصادر النيران السيبرانية، إلا أنه لحد الآن مازالت العملية دون مستوى الدقة المطلوبة التي تمكّن من تحديد المسؤولية وتغريم المهاجمين أو معاقبتهم؛ الأكثر من ذلك، هذا التحديد -على بساطته- يتم فقط بعد حدوث الهجوم والقيام بعملية تقييم الأضرار.

ج) المفاجأة. تتمثل هذه الخاصية في عدم القدرة على تحديد موعد إطلاق الحرب السيبرانية، عندئذ تكون المفاجأة والخداع والتضليل العناصر الرئيسية المشكلة لمناخ البيئة الاستراتيجية السيبرانية، في غياب نظام الإنذار المبكر وعدم القدرة على معرفة متى ومن أين تأتي الهجمات المعادية؛ وبالتالي سيطرة الحالة الكلاوزفيتزية المحددة في «ضباب الحرب»⁽⁶²⁾. تشكّل هذه الخاصية عنصر التناقض في الفضاء السيبراني من حيث أن هذا الأخير يفترض المعرفة الشاملة بواسطة توظيف التكنولوجيا الرقمية المتطورة، لكن عدم

القدرة على معرفة توقيت إطلاق الحرب السيبرانية يقوض ادعاءات أنصار ثورة المعلومات في الشؤون العسكرية حول افتراض المعرفة الشاملة⁽⁶³⁾. الاعتبار الأساسي حول التناقض بين المعرفة السيبرانية الشاملة وعدم القدرة على معرفة زمن إطلاق الحرب السيبرانية أو تحديد بدقة مصادر النيران في الوقت المناسب لتدميرها، محدد في غياب معلّات واضحة تحدد مجال تفاعل الفضاء السيبراني؛ في مقابل ذلك، يعطي قيمة لمعنى المفاهيم التقليدية في الاستراتيجية مثل السيطرة، التحكم، القيادة، المبادأة، وغيرها من المصطلحات المقترحة في طريقة قتال الجيش الرقمي. على عكس المجالات الأخرى لتفاعل القوة العسكرية (البر، البحر، الجو)، فإن الفضاء السيبراني هو عبارة عن «بقعة للتغير بشكل واسع، مقارنة بالمجالات الأخرى. أقسام من الفضاء السيبراني تتغير بشكل مستمر، تنبعث وتتمدد مع الإبداع التكنولوجي بالإضافة إلى محو، تعويض، أو إعادة برمجة الشبكات»⁽⁶⁴⁾؛ فهو عالم موجود بلا حدود ولا معلّات مادية، لكن يؤثر بشكل متزايد في مخرجات الاستراتيجية ويساهم في صنع السياسة والأشكال الأخرى من التأثير الاجتماعي والنفسي.

د) السرعة. خاصية أخرى جد مميزة للحرب السيبرانية وهي السرعة غير المسبوقة في الهجوم على الأهداف عبر العالم، تقاس بسرعة الضوء أو حركة الذبذبات عبر الأثير؛ لأنه ببساطة لا وجود لتأثير البعد الجغرافي على مكونات القتال السيبراني، كما لا تدخل الحسابات الطبوغرافية ولا المناخية (وغيرها من العناصر المطروحة من قبل المنظرين للحرب التقليدية) في تصميم وإدارة تكتيكات القتال السيبراني؛ إنها خاصية «الفورية Instantaneous» والتأثير المتزامن على بيئة القتال دون تحديد واضح لمسرح القتال، وهذا يعني أن الحرب السيبرانية تشمل المحاربين وغير المحاربين، الأطراف الحكومية وغير الحكومية، وكل من له رابطة اتصالية بالفضاء السيبراني. بالطبع ولدت هذه الخاصية بدورها استراتيجية القتال (في صورتها الدفاعية أو الهجومية)، القائمة على فكرة إدارة الاشتباك على المستوى العالمي وبشكل تزامني وفوري؛ مما يعني بطريقة أخرى، الخطورة المتزايدة لمثل هذه الحرب، خاصة مع الرقمنة المتزايدة لكل القطاعات الحيوية وغير الحيوية في الدولة والمجتمع، بدءاً من تنظيم أضواء المرور إلى التحكم في منشآت ومعدات تشغيل الأسلحة النووية.

هـ) الشمولية. كعلاقة تلازمية، الحرب السيبرانية شاملة في طبيعتها وفي نفس الوقت تستلزم الانتقام الشامل، الذي بدوره لا يكون محدوداً ضمن مصادر التهديد ولا يستهدف فقط الأطراف المعادية، وإنما يشمل أيضاً الأهداف البريئة عبر العالم أو الأطراف غير المحاربة وغير المعنية أصلاً بالنزاع؛ على افتراض أن مسرح العمليات القتالية غير محدد بأبعاد معينة تساعد على التحكم في النزاع ضمن نطاق معين. يشكل «مبدأ الرد الانتقامي» إحدى المفردات الرئيسية لنظرية الردع النووي، لكنه محدد ضمن مسرح عمليات واضح وموجه ضد أعداء واضحين من حيث مجال الاستهداف ومن حيث المجال الجغرافي؛ ومن

ثم يمكن تركيز القتال على أراضي الطرف المعتدي، حتى ولو كان له أضرار جانبية فإنها تكون محدودة مقارنة بما يحدث في حالة الانتقام السيبراني الشامل، على الأقل من الناحية النظرية.

9) عمومية الأضرار. تشكل عمومية الأضرار الناجمة عن الهجوم السيبراني الخاصة الفرعية الإضافية لهذا النوع من الحروب، بحيث أنها تشمل القطاعات المدنية والعسكرية على حد سواء. مهما قلنا أن هذه الخاصة تحاكي مفهوم «الحرب الشاملة»⁽⁶⁵⁾ في الثقافة الاستراتيجية البريطانية أو مفهوم «الاشتباك العالمي»⁽⁶⁶⁾ في الثقافة الاستراتيجية الأمريكية، فإن الشمولية السيبرانية تمتد لكل العناصر الدقيقة في المجتمعات بما فيها الهواتف الخلوية للأفراد؛ إنها تدمر القدرات العميقة المسؤولة عن إدارة شؤون المجتمعات، بشكل تجعلها بدون ذاكرة وتفقد حقيقتها وجودها. إن هذا النوع من الحروب يحاكي في آثاره الأمنية والعسكرية مرض زهايمر أو الخرف الذي يصيب الإنسان ويفقده كل شيء، بما في ذلك وجوده الآدمي داخل المجتمع؛ الكثير من الخسائر السيبرانية يمكن أن لا يكون لها محتوى مادي، لكن محتواها المعنوي أكثر كلفة ولا يقدر بأي حساب مادي مثل تخريب ذاكرة الحواسيب، محو الحسابات المالية، وخسارة بشكل عام العقل الإلكتروني للدولة والمجتمع.

تجري عملية تجريد الخصوم والأبرياء من قدراتهم السيبرانية المخزنة في الشبكات بسرعة كبيرة ومتزامنة، بشكل تفوق كثيرا مضامين مبدأ الهيمنة السريعة المقترحة من قبل أنصار نظرية المعلو-اتصالية⁽⁶⁷⁾؛ الأسوأ من ذلك، أن الأضرار السيبرانية المقصودة أو الجانبية غير قابلة للاستعادة من جديد، على عكس أضرار الحرب التقليدية التي يمكن بعد انتهائها إعادة إعمار المدن واستعادة الناس لحياتهم من جديد. عندما يتم تدمير المعلومات أو تخريب الشبكات، فإنه من الصعب استعادتها لأنها قد تلاشت وأصبحت عدما. لذلك، تعكف الدول على تطوير الدفاعات السيبرانية التي تمكّنها من الاحتفاظ بالنسخ الأصلية للشبكات والذاكرة بعيدا عن الهجمات السيبرانية، وهذا متاح فقط للدول (وهي قليلة) التي تتحكم في التكنولوجيا عالية التعقيد، أما باقي الدول التي تشكل معظم العالم سوف تكون مجبرة على دفع ثمن حرب ليست مسؤولة عنها.

ربما يبدو أن هناك مبالغة كبيرة في تشخيص خاصيات الحرب السيبرانية من المنظور النقدي، وهو انتقاد وجيه وربما يكون متماسكا بسبب أن الأمم لازالت لم تختبر فعليا - على عكس الحرب التقليدية- هذا النوع من الحروب فوق مسرح العمليات السيبرانية، وأن ما حدث لحد الآن هو مجرد مناوشات سيبرانية تظهر وتختفي بسرعة. لكن مع وجاهة ومنطقية هذه الأطروحة، فإن تأثير مفردات الريبة، الخوف، المنافسة الأمنية، والمساعدة الذاتية (المقترحة من قبل أنصار النظرية الواقعية/الواقعية الجديدة⁽⁶⁸⁾)، وحتى المناوشات

السيبرانية في حد ذاتها (الاتهامات الأمريكية لروسيا بالتدخل في الانتخابات الرئاسية عام 2017، واتهام روسيا للولايات المتحدة بالتدخل السيبراني في الانتخابات البرلمانية عام 2021) تجعل الدول تستعد للأسوأ؛ وبنفس المنطق الواقعي، إذا لم تفعل ذلك، فيجب عليها دفع ثمن الاعتداء وحدها.

بقدر ما حمل الفضاء السيبراني مصفوفة غير متناهية من الامتيازات متعددة الخواص شملت كل مجالات الأنشطة الإنسانية، حمل معه أيضا مخاطر كبيرة تفوق في بعض جوانبها تلك المترتبة عن الحروب التقليدية. طالما أن الفضاء السيبراني وضع المصالح الحيوية للدولة والمجتمع تحت التهديد الخطير، فإن المنطق الاستراتيجي يفرض مفرداته على طريقة تفكير صناع القرار والمخططين الدفاعيين حول الشؤون الأمنية. الجانب الأكثر إثارة للمفارقة الاستراتيجية، أن كل المجتمعات مدمنة بطريقة مستمرة على تطوير بنيتها التحتية وإدارة شؤونها الخاصة وفق مفردات ومنطق عمل الفضاء السيبراني (الحكومة الإلكترونية، التحكم الشبكي في الشؤون الخاصة للمجتمعات، الدور المتزايد لمواقع التواصل الاجتماعي في توجيه والتأثير على حياة الناس العامة، وهكذا)، وبالتالي هي مجبرة على تطوير مذهبها في القتال السيبراني بشكل متزامن ومتناسب مع التهديدات والمخاطر الناجمة عن الخصائص الجوهرية لهذا الفضاء.

(ن) خصوصية الأهداف. من الناحية السياسية، هناك تشابه يكاد يكون متطابقا بين أهداف الحرب السيبرانية ونظيرتها التقليدية، لأنها في المقام الأول هي أهداف سياسية؛ لكن من الناحية العملية هناك تباين بينهما. وفق المفهمة الكلاوزفيتزية، هدف الحرب هو تدمير قوات العدو وتجريده من أسلحته؛ في مقابل ذلك، أهداف الحرب السيبرانية هي تحقيق السيطرة وحرمان العدو من الاستفادة من الامتيازات العملية والتكتيكية السيبرانية. طالما أن أهداف الحرب السيبرانية هي سياسية في المقام الأول، فإن بدورها يجب أن تبنى الاستراتيجية بشكل يساعد على تحقيق أهداف السياسة؛ بالطبع هذا ليس متاحا بسهولة، لإمكانية حدوث إضرار بمصالح ومنشآت الأطراف الحليفة أو الصديقة، بل إن احتمال تعرض البنية التحتية الحساسة في تلك الدول لهجمات سيبرانية صديقة هو عالي جدا؛ السبب في ذلك هو افتقار الفضاء السيبراني لحدود ثابتة، وبالتالي يمكن أن تخترق الهجمات كل البنيات التحتية بشكل فوري ومتزامن.

لا تهدف الحرب السيبرانية إلى السيطرة أو احتلال مجال سيبراني لدولة معينة، لأن ذلك ليس متاحا من الناحية العملية لفترة طويلة من الزمن، وإنما الهدف الأولي هو التخريب أو الإضرار بالمنشآت الحساسة للطرف المعادي وعطبها عن العمل؛ مما يعني بطريقة أخرى حرمان العدو من استغلال الامتيازات السيبرانية في تحقيق أي تفوق أو انجاز عسكري. هناك حالة فريدة في الحرب السيبرانية التي يملك فيه طرف واحد التفوق

العملياتية كلية، وهي عندما تكون الولايات المتحدة الأمريكية إحدى أطراف هذه الحرب، فإن عنصر التفوق لديها هو إمكانية استغلال الإنترنت عندما يصل مستوى تصعيد النزاع إلى الحرب الشاملة؛ العيب في هذا الامتياز العملياتي هو حرمان وشل قدرات الدول الصديقة في الدفاع عن نفسها، ومن ثم لا يتم اللجوء إلى هذا الخيار إلا في حالة اليأس بشكل مشابه لما طرحه أنصار نظرية الردع النووي⁽⁶⁹⁾ حول استخدام الأسلحة النووية في حالة تعرض أراضي الدولة لهجوم تقليدي شامل أو هجوم بالأسلحة النووية، يستلزم تنفيذ الرد الانتقامي. في كل الأحوال، على عكس الحرب التقليدية، خيار التدمير الشامل للقدرات السيبرانية المعادية غير عملي وغير منطقي؛ عندئذ تبقى خيارات الأطراف المتحاربة مركزة حول الأهداف دون التدمير الشامل. السبب الرئيسي المتماسك في هذه الأطروحة هو وجود مصلحة مشتركة في الاستفادة من الفضاء السيبراني للأغراض المدنية أو العسكرية خلال فترة النزاع، خاصة فيما يتعلق بالاتصالات والحصول على المعلومات أو حتى إدارة شؤون الحرب نفسها؛ على اعتبار أن تفعيل العمليات السيبرانية المختلفة (التخريب، التجسس، القرصنة، الدعاية...) ضد العدو يستدعي بالضرورة المحافظة على بقاء الفضاء السيبراني قائماً.

باختصار، تفرض طبيعة الفضاء السيبراني وعمليات إدارة الحرب على الأطراف المختلفة التباري الاستراتيجي ضمن مستوى الأهداف التكتيكية، التي تعمل باتجاه تعزيز التفوق العملياتي أو حرمان الخصم الاستفادة من الامتيازات السيبرانية في الدفاع أو الهجوم؛ أو على الأقل منع العدو من أن يقاتل بحرية في الفضاء السيبراني. لقد عرض **إلينور سلوان Elinor C. Sloan** أمثلة عن الأهداف التكتيكية في الحرب السيبرانية بقوله: "يمكن أن يكون الهدف الفوري إعماء الخصم بواسطة خلق ضجيج.. تمزيق البيانات، إفساد المعلومات بواسطة إضافة البيانات الخاطئة إلى الموجود منها، .. تشويش أو تضليل الخصم بواسطة تقويض مصداقية المعلومات؛ سرقة المعلومات؛ والتلاعب بأنظمة الخصم من خلال جعلها تقوم بالأشياء التي لا يريد مصمموها القيام بها"⁽⁷⁰⁾. القائمة ليست نهائية حول الأهداف التكتيكية، لكن يجب أن تؤدي في النهاية إلى تحقيق الأهداف الاستراتيجية، أو على الأقل تساهم في تعزيز الموقف القتالي للدولة من أجل تحقيق الغايات النهائية.

(ي) طبيعة فواعل الحرب. تشمل قائمة فواعل الحرب الدول وغير الدول، لكن ما هو مميز أن أهداف الفواعل ليست دائماً سياسية كما هو الحال في الحرب التقليدية، إذ يمكن أن تدار الحرب من أجل سرقة الملكية الفكرية، التكنولوجيا الدقيقة، تحطيم قدرات الشركات على المنافسة، تسويق أنظمة دفاعية سيبرانية جديدة، إثبات القدرات العقلية، بالإضافة إلى الأهداف السياسية التي عادة تكون متلازمة مع نوعين من الفواعل: الدول والجماعات الإرهابية، التي عادة تقاتل في كل أشكال الحروب من أجلها. يمكن أن تدار بعض العمليات القتالية -التي تبدو أنها غير سياسية- من قبل أنواع مختلفة من الفواعل، لكن من حيث الجوهر لها أهداف سياسية مثل عمليات التشويش والتضليل والدعاية وغيرها. لكل هذه

الاعتبارات وأخرى، تنطوي عملية تحديد طبيعة الفواعل والأهداف التي يحملونها على مسألة مهمة في إدارة الحرب السيبرانية؛ لأنها تتحكم في مضمون الرد العقابي أو الانتقامي الذي سيقوم به المدافع جراء الهجمات التي تعرضت لها منشآته وحجم الخسائر التي تكبدها. فعلى سبيل المثال، الهجمات السيبرانية التي تقف وراءها دولة، جماعة إرهابية، شركة منافسة، وقرصان هاوي، تستدعي ردا انتقاميا متباينا وفق كل حالة.

الأبعاد العملية للحرب السيبرانية

تتضمن الأبعاد العملية تلك التحضيرات والترتيبات الضرورية لإدارة المعركة فوق الحقل السيبراني بنجاح سواء في صورتها الدفاعية أو الهجومية، بشكل يولد الفعالية القتالية المؤدية في نهاية المطاف إلى تحطيم هجوم العدو أو قدراته الدفاعية. وإذا كان فن العمليات في الحرب التقليدية يعني «استخدام القوات المسلحة في الحملات لإنجاز النتائج السياسية والعسكرية في مسرح جغرافي مميز»⁽⁷¹⁾، فإن فن العمليات السيبراني يعني تحضير القوات والمعدات والاستراتيجيات أو المقاربات المطلوبة، من أجل تحقيق الأهداف الدفاعية أو الهجومية فوق الحقل السيبراني وإبقاء البنية التحتية الحساسة بعيدة عن التهديد السيبراني الخطير. يتضمن حقل المعركة القوى السيبرانية البشرية، البرمجيات، الأسلحة، المقاربات أو الاستراتيجية، أنظمة الحاسوب، والتحكم والسيطرة؛ يجب أن تتكامل كل هذه العناصر ضمن اتجاه واحد للقتال، وهي المهمة المحددة لفن العمليات السيبرانية، أي كيفية جعل كل القوى والعناصر والقدرات والأفكار تتفاعل بشكل منسجم ومتناغم من أجل تحقيق أهداف الحرب. إن حقل المعركة السيبرانية هو القتال عبر شبكات الحاسوب، ومن ثم فن العمليات يجب أن يتفاعل ويأخذ خاصياته الجوهرية من الشبكات مثل البرمجة الآلية، الرقمنة، قوة الروابط، الاتصالات الافتراضية، بالإضافة إلى المعدات الصلبة كالحواسيب والهواتف والكابلات ومحطات البحث فوق الأرض أو في الأجواء.

نظرا لأهمية الأبعاد العملية في الحرب السيبرانية، ظهرت أشكال التنظيم العسكري والمذاهب القتالية والتكتيكات التي تلبي حاجات هذا النوع من القتال. أنشأت وطوّرت معظم الدول (الكبرى على وجه التحديد) الكثير من البنيات التنظيمية والقانونية والاستراتيجية، من أجل توفير القاعدة المفاهيمية لإدارة هذا الشكل من القتال؛ مدفوعة في ذلك بواسطة مخاوف متعددة الخواص، يتعلق البعض منها بالتحضير لقتال بعضها البعض (الحالة الأمريكية-الصينية)، والبعض الآخر خاص بمواجهة التهديدات غير التقليدية مثل الإرهاب السيبراني، الجريمة المنظمة، القرصنة، التجسس، التطفل وغيرها. ففي حالة الولايات المتحدة الأمريكية مثلا، أنشأت وزارة الدفاع العديد من الهيئات ذات الاختصاص بشؤون الدفاع السيبراني، منها تأسيس ما يسمى «بقوة المهمة المشتركة لشبكة دفاع الحاسوب The Joint Task Force-Computer Network Defense» عام 1998، ثم تبعت

بعد سنتين بإنشاء هيئة أخرى متخصصة في حماية شبكات الحاسوب تسمى «قوة المهمة Task Force» عام 2000؛ الخاصة التي تجمع بين الهيئتين هي تحضير القدرات المحوسبة الأمريكية لتنفيذ العمليات الدفاعية والهجومية على حد سواء.

الحقيقة أن التحضير العملياتي للقدرات السيبرانية كان متسارعا منذ ظهور ما يسمى «بثورة المعلومات في الشؤون العسكرية»⁽⁷²⁾، حتى ولو أن الولايات المتحدة الأمريكية كانت متقدمة على الآخرين في كل المجالات السيبرانية، إلا أن الأطراف الأخرى انخرطت أيضا بسرعة في سباق التسلح السيبراني بهدف التحضير العملياتي للقتال السيبراني، وفي مقدمة هذه الدول نجد الصين وروسيا. من أجل تجريب القدرات السيبرانية واختبار فعالية القتال السيبراني فوق الحقل السيبراني الفعلي، قامت روسيا في سنوات 2007 و2008 بتنفيذ هجمات سيبرانية منسقة ضد كل من إستونيا وجورجيا على التوالي، كجزء من استراتيجيتها التقليدية في مقاومة النفوذ الأطلسي على حدودها الغربية. مع ظهور بؤادر تنامي خطر الحرب السيبرانية خلال العشرية الأولى من القرن الحادي والعشرين، اتخذت وزارة الدفاع الأمريكية خطوة متقدمة باتجاه دعم القدرات العملياتية للقتال السيبراني، وذلك بإنشاء قيادة متخصصة في الحرب السيبرانية عام 2010 تحت اسم «القيادة السيبرانية الأمريكية» كفرع من القيادة الاستراتيجية التقليدية، موجهة أساسا نحو القيام بمهمة «إعادة توحيد المهام السيبرانية الدفاعية والهجومية .. ليس فقط [من أجل تحقيق مهام] الدفاع، ولكن كذلك أن تكون موجهة نحو القيام بالهجوم ضد الخصوم بأمر من الرئيس»⁽⁷³⁾.

يهدف التكيف والإنشاء التنظيمي والمذهبي والاستراتيجي إلى تحقيق عملية تكامل القوة السيبرانية مع مجالات القوة العسكرية الأخرى، كجزء من مهام فن العمليات السيبرانية لتحقيق التناغم القتالي مع القطاعات الأخرى وإنتاج الفعالية القتالية المطلوبة في إنجاز النصر. يتطلب كل هذا تطوير قدرة «الهجوم المتكامل Integrated Attack»، الذي يعني من وجهة نظر فن العمليات: تحقيق «تكامل ليس فقط بين القوة الجوية والفضائية، ولكن كذلك القدرات السيبرانية ضمن العمليات المشتركة. .. تصطف خيارات الهجوم السيبراني الممكنة من الاختراقات السيبرانية «الأدنى كثافة» مثل التنصت على اتصالات الخصم، إلى الهجوم «العالي الكثافة» الذي يشل نظام الدفاع الجوي للعدو لفتح الطريق أمام الهجوم الحاسم»⁽⁷⁴⁾. أكثر الأمثلة التي يستشهد بها المنظرون حول تكامل القوة السيبرانية مع القدرات الأخرى هي حملة «تحالف القوة» في حرب كوسوفو عام 1999، عندما اعتمدت القوات الأطلسية على القوة السيبرانية في إنتاج فعالية تنسيق الأنشطة القتالية وتوفير مستوى الدقة في تحديد الأهداف وتقليص حجم الأضرار الجانبية. تجدر الإشارة إلى أن القوة السيبرانية في هذه الحرب كانت محددة في تعزيز فعالية اللوجستيك والمعلومات، ولم تستخدم بطريقة هجومية كما هو مصوّر على الأقل من الناحية النظرية⁽⁷⁵⁾، لأن جوهر الحملة العسكرية كان قتالا حركيا يستهدف تدمير البنية المادية وليس الافتراضية للقوات

الصربية، وإجبار الرئيس الصربي "سلوبودان ميلوسوفيتش" على الانسحاب من إقليم كوسوفو.

ضمن سياق التحليل العملياتي، تتركز المخاوف الأمريكية -وبشكل أقل الغربية- حول قدرات كل من الصين وروسيا في شن الحرب الهجومية السيبرانية ضد مكونات القوة الأساسية، سواء كانت مدنية أو عسكرية. بالرغم من وجود احتمال أن مثل هذه المخاوف مبالغ فيها لأجل الحصول على الموارد المالية الإضافية في تطوير القدرات الجديدة، إلا أن هذا لا ينفي أن الدول الكبرى تعكف على تطوير قدراتها السيبرانية الهجومية بشكل حثيث؛ يظهر ذلك من خلال المذاهب القتالية التي تتبناها في إدارة الحرب المستقبلية. فإذا أخذنا الصين على سبيل المثال، نجد أن سجل التاريخ الاستراتيجي يؤكد على أن الصين لم تشن حروبا خارج حدودها الوطنية لفترة طويلة من الزمن، وليست دولة استعمارية، وأنها تبنت خلال الحرب الباردة مذهب «الدفاع النشط Active Defense»، الذي يتطلب الرد الحاسم في حالة تعرض أراضيها لاعتداء خارجي؛ لكن في الفترة الأخيرة، تبنت مذهباً جديداً وهو «الهجوم النشط Active Offense» في إدارة الحرب الحديثة بشكل عام. يتضمن مذهب الهجوم النشط فكرة: «أن مفتاح العمليات السيبرانية الفعالة هو أخذ المبادرة، إطلاق الهجمات السيبرانية وحتى القيام بالعمل الوقائي.. [وهذا يتطلب] دمج التكنولوجيات المتقدمة في العمليات العسكرية، وكل الأنشطة التي تهدف إلى ربح التفوق المعلوماتي فوق حقل المعركة»⁽⁷⁶⁾.

ترجمت الصين هذا المذهب من الناحية العملية بواسطة قيام «جيش التحرير الشعبي The People's Liberation Army» الصيني بتطوير استراتيجية خاصة بالقتال السيبراني تحمل اسم «شبكة القتال الإلكتروني المندمجة Integrated Network Electronic Warfare»، التي تتضمن منظومة أسلحة سيبرانية متنوعة ومتكاملة، توجه نحو تدمير القدرات الشبكية وأنظمة المعلومات للعدو؛ فهي ليست موجهة نحو إشباع الحاجات الدفاعية للأمن القومي الصيني، وعوضاً عن ذلك تتضمن تطوير القدرات الهجومية القادرة على تدمير البنية التحتية السيبرانية للعدو في حالة وقوع الحرب. العامل الإمبريقي الذي يعطي قيمة عملياتية لهذه الاستراتيجية هو استمرار الخلاف بين الصين الشعبية والصين الوطنية (تايوان)، وأن للأخيرة بنية تحتية سيبرانية متقدمة جداً سوف تكون هدفاً أولياً للقوات السيبرانية الصينية، إذا ما حاولت الصين ضم الجزيرة لسيادتها بواسطة استخدام القوة المسلحة. في حالة ما نفذت الصين هذا السيناريو في المستقبل (قامت بتدريبات جوية على ذلك في نهاية سبتمبر من عام 2021 عندما حلقت عشرات الطائرات الحربية فوق الأجواء التايوانية، تراهن الصين على انهيار جيش تايوان على غرار انهيار جيش أفغانستان في أوت 2021)، فإن مجال تفاعل القتال السيبراني يكون مركزاً بالذات على استهداف البنية التحتية لأنظمة المعلومات التايوانية؛ والتي تشمل على وجه الخصوص «القيادة

Command، السيطرة Control، الاتصالات Communications، الحواسيب Computers، الاستخبارات Intelligence، المراقبة Surveillance، الاستعلام Reconnaissance، وشبكات أنظمة اللوجستيك»⁽⁷⁷⁾. وإذا كانت تايوان الهدف الأولي للصين في أي حرب قادمة، فإنها تستدعي بالضرورة تدخل الولايات المتحدة الأمريكية، لأن جزءاً من البنية التحتية الحساسة التايوانية يشغل من قبل القوات المسلحة الأمريكية والاستخبارات المركزية؛ بالإضافة إلى ذلك، أن كل مكونات الحرب السيبرانية وما يندرج تحت ما يسمى «بثورة المعلومات في الشؤون العسكرية» في تايوان هو من إبداع الجيش الأمريكي؛ على اعتبار أن تايوان تمثل الخط المتقدم للولايات المتحدة في احتواء أي توسع صيني شرق آسيا. ليس هذا فحسب، وإنما مازالت تايوان في الثقافة الاستراتيجية الصينية⁽⁷⁸⁾، تابعة للصين تخضع إدارة شؤونها إلى القيادة العسكرية الشرقية لجيش التحرير الصيني.

ضمن المنظور الاستراتيجي، الهجوم السيبراني يجب أن يستهدف مفاصل بنية نظام العدو المدنية والعسكرية، وكل حلفائه في المنطقة، بشكل يضمن التفوق الاستراتيجي والسيطرة على البيئة الاستراتيجية؛ ومن ثم، يكون التحضير العملياتي للقتال السيبراني قائماً على فكرة الاستهداف الشامل للقدرات العسكرية والمدنية، التي يقيّم القادة العسكريون في الجيش الصيني أنها تشكل مفاصل قوة النظام وتؤثر على عمليات صناعة القرار ومعنويات العدو. إن مكونات القوة السيبرانية موجودة في القطاع المدني والعسكري، وفي حالة الولايات المتحدة الأمريكية، يعتبر القطاع المدني الخاص أكثر استحواذاً على مكونات القوة السيبرانية من القطاع العسكري؛ أخذ المذهب الصيني السيبراني كل هذه المعطيات في الحسبان وفق ما شرحه إيلينور سلوان بقوله: «تبحث الصين عن السيطرة المعلوماتية أو التفوق بواسطة مهاجمة البنية التحتية لـ (C4ISR) [المشار لها سابقاً] الخاصة بالعدو لمنع حصوله على المعلومات أو تمزيق حصوله عليها، معالجتها، أو نقلها من أجل دعم العمليات القتالية. أخيراً، حدد جيش التحرير الشعبي الصيني مطلباً للهجمات المنسقة أو المتزامنة على شبكات العدو والأنظمة، والمتمثل في إعطاء قيمة للعمليات الصامتة أو الخفية المتمثلة في سرقة أو التلاعب بالمعلومات»⁽⁷⁹⁾.

ما يقال على الصين، ينطبق نوعاً ما -وربما أكثر كثافة وتأکیداً- على الولايات المتحدة الأمريكية، التي يحتل فيها فن العمليات السيبرانية حيزاً كبيراً من الاهتمامات الاستراتيجية والتطبيقات العملية، سواء في الصورة الهجومية أو الدفاعية؛ يبنى كل ذلك على التوقعات المحتملة والفعالية حول تصرفات العدو في هذا النوع من القتال. بالرغم من أن الحرب السيبرانية -بالمفهوم الواسع- لم تحدث لحد الآن، إلا أن التفكير الاستراتيجي مبني على ضرورة تحضير القوات السيبرانية لإدارة القتال الهجومي ضد العدو في حالة نشوب الحرب؛ ومن ثم، فن العمليات يجب أن يشمل وضعية الهجوم والدفاع على حد سواء، حتى ولو أن الأدلة الإمبريقية حول المسائل الدفاعية أكثر شيوعاً وألفة لدى الناس من نظيرتها الهجومية.

عند التمعن في السياسة الدفاعية السيبرانية للولايات المتحدة الأمريكية، نجد أنها لا تحمل فقط المعاني الدفاعية في منظورها السلبي (منع الأعداء من الوصول إلى شبكات الحاسوب وصد الهجمات السيبرانية)، وإنما الجزء الأكبر منها مركز حول مفهوم «الدفاع النشط Active Defense»؛ الذي يعني البحث عن الأعداء وتحديد مصادر التهديد ومهاجمتها قبل أن تتحول إلى وضعيتها النشطة. وهذا يعني بطريقة أخرى، أن مفهوم الدفاع يتخطى حدود إجراءات مراقبة الدخول وكشف التطفل وجدران النيران، ليشمل الضربات الوقائية قبل أن تتحول التهديدات إلى الحالة النشطة عالية الكثافة؛ خاصة فيما يتعلق بالهجمات السيبرانية الإرهابية والجريمة المنظمة وحتى التمرد السيبراني. بالنسبة للمخططين الدفاعيين، يستلزم مبدأ الدفاع النشط البحث ومهاجمة مصادر التهديد قبل أن تأتي، مما يعني بطريقة أخرى أنه يتجاوز المفهوم التقليدي المركز حول تعزيز الدفاعات المضادة للاختراقات، التجسس، الفيروسات، القرصنة وغيرها؛ إنه يتضمن القيام بالضربات الوقائية مثل غلق المواقع الشبكية المعادية، اختراق الحسابات السيبرانية المشبوهة، تعقب الاتصالات وتفكيك الرسائل المشفرة وغيرها. إذا بدت مثل هذه الأنشطة في الظاهر أعمالاً هجومية، إلا أن في جوهرها هي من أجل الأغراض الدفاعية؛ وهي الفكرة المستمدة من تفكير كلاوزفيتز حول الهجوم من أجل الدفاع.

في هذا الصدد، يحاكي مفهوم «الدفاع السيبراني النشط» في المنظور الاستراتيجي الأمريكي، مفهوم «سمة الدفاع الاستراتيجي»⁽⁸⁰⁾ المقترح من قبل كارل فون كلاوزفيتز، الذي يعني نقل المعركة إلى ما وراء حدود الدولة للقضاء على المصادر الهجومية الرئيسية للعدو، وتكون بذلك جهود منع استعادة العدو أنفاسه أو إعادة بناء قواته هدفاً دفاعياً مركزياً، لا تتم الغاية العظمى للاستراتيجية الدفاعية إلا بتحقيقه. من هذا المنظور، لا يتحقق معنى الدفاع بمجرد كسب التفوق الاستراتيجي الدفاعي، وإنما يتمدد ليشمل السيطرة على موارد المهاجم وتجريده من سلاحه؛ اشتقاقاً من مفهومة كلاوزفيتز للدفاع عندما قال: «فإن كنا نريد تصور وتفهم الدفاع كما ينبغي أن يكون، فهو كما يلي: تهيئة قصوى وشاملة لكل الوسائل»⁽⁸¹⁾. استخدم هذا المفهوم بصيغة جديدة تناسب متطلبات البيئة الاستراتيجية السيبرانية، وصيغ في مبدأ «الدفاع النشط» الذي يتطلب تنفيذ بعض الأعمال الهجومية من أجل تعزيز قدرات الدفاع عن المصالح الحيوية للأمن القومي، وفي مقدمتها إبقاء البنية التحتية السيبرانية الحساسة بعيدة عن الهجمات السيبرانية المعادية؛ لا تتحقق هذه الغاية الدفاعية إلا بواسطة الذهاب إلى العدو قبل أن يأتي، والمبادرة بالهجوم على مصادر التهديد قبل أن تصبح نشطة. لذلك، يعتقد محللو الدفاع في الولايات المتحدة الأمريكية بأن الدفاع النشط «لا يستلزم فقط تحصين شبكة الحاسوب بواسطة جُدر النيران والبرمجيات المضادة للفيروسات، وإنما يستلزم أيضاً رؤية التهديدات قبل أن تأتي، وبالطبع السماح للجيش الأمريكي القيام بالبحث في الأنظمة السيبرانية للخصم باستخدام هجوم شبكة الحاسوب، من أجل تنفيذ الرد السيبراني [على الهجمات المحتملة]»⁽⁸²⁾.

المحددات العملية للدفاع النشط

يمكن تلخيص العناصر العملية لمفهوم الدفاع السيبراني النشط في مجموعة العناصر التالية: (1) لا معنى للدفاع الإيجابي في ضمان الأمن ما لم يتم جعل العدو يدفع ثمن تهديداته أو هجماته الفعلية؛ (2) استخدام هجمات شبكة الحاسوب لتحقيق الغايات الدفاعية، مثل تحييد التهديد السيبراني قبل وصوله إلى البوابات الدفاعية أو الخطوط الأمامية للدفاع السيبراني (محاولات القرصنة أو التطفل)؛ (3) المبادرة باستخدام الهجوم السيبراني خلال المراحل الافتتاحية للأزمات الأمنية أو قبل أن يصل النزاع إلى مرحلة الكثافة؛ (4) التأكيد على أهمية عامل السرعة في إدارة الحرب السيبرانية، بحيث يتم جمع وتحليل وتوزيع المعلومات ونقل المعركة إلى شبكات العدو في حدود سرعة الضوء؛ (5) اعتبار السرعة العملية مصدر قوة القتال السيبراني ومظهر فعالية السيطرة على مصادر التهديد؛ (6) المحافظة على التأهب وقابلية المبادرة بالهجوم والتفاعل ضمن دائرة صناعة القرار في حكومة العدو؛ (7) المحافظة على الخاصيات الأساسية للدفاع السيبراني النشط مثل المناورة القتالية، السرعة والرشاقة أو المرونة العملية، المفاجأة، واقتصاد القوة (يحاكي معظمها طريقة القتال ضمن منظور ثورة المعلومات في الشؤون العسكرية⁽⁸³⁾)؛ (8) التأكيد على مقاربة السرية وعدم لفت الانتباه عند تنفيذ الأعمال القتالية السيبرانية النشطة؛ (9) أحسن مقاربة للدفاع النشط، القيام بعمليات اختراق حواسيب العدو والشبكات والتجسس عليها واعتراض اتصالاته بطريقة سرية لمعرفة في ماذا يفكر، حول ماذا يخطط، ومتى يقوم بالتنفيذ⁽⁸⁴⁾.

نتائج البحث

من خلال البلورة النظرية لمفهوم الوطن السيبراني كمقدمة لتطوير العقيدة السيبرانية في الدفاع والأمن، يمكن استخلاص مجموعة من النتائج المصنفة ضمن النقاط التالية:

1. تمتد الأمم من حيث خاصياتها الوطنية، نفوذها السياسي، تأثيرها الاستراتيجي، وتواصلها الثقافي والرمزي إلى الحدود التي ترسمها عناصر قوتها الوطنية المتعددة المجالات، وذات النوعية القابلة للمنافسة مع الآخرين؛ والفضاء السيبراني ليس استثناءً من هذه القاعدة؛

2. تتفاعل الأمم عبر أوطانها السيبرانية لغايات سياسية متعددة، تشمل التسويق الثقافي والحضاري، دعم التماسك السوسيو-ثقافي الوطني، النفوذ الاستراتيجي، التعلم ونقل الخبرات، الدفاع والأمن، صناعة السمعة، والتأثير الاتصالي في عقول ومشاعر الآخرين.

3. تستلزم عملية بناء الوطن السيبراني تطوير البنية التحتية للأغراض الاقتصادية والتجارية والتنظيمية، الأغراض الدفاعية، التسويق السيبراني، وحرب الأفكار ضد الخصوم وكسب الأصدقاء؛
4. الأبعاد العملية للحرب السيبرانية مفعلة على مستويات عالية جدا، تشمل قدرات الإعداد والتحضير، التكيف والتعديل المذهبي والاستراتيجي، سباق التسلح، الاختبارات على مستوى النزاعات المتدنية والعالية الكثافة؛ وذلك فقط من أجل التحضير لمواجهة خيارات الأسوأ في المستقبل؛
5. على عكس الأسلحة التقليدية، فإن الدول لحد الآن لم تعلن أنها طورت أو تعمل على تطوير أسلحة سيبرانية هجومية، وإنما مازال التأكيد مستمرا حول تطوير القدرات الدفاعية لحماية أنظمة الحاسوب والشبكات السيبرانية والبنية التحتية الحساسة للدولة بشكل عام؛ لكن هذا لا يضمن أن هذا الخيار مستبعد أو يبقى مهملا من أجندة السياسة الدفاعية للأمم؛
6. إذا كان التحضير العملي للحرب السيبرانية الهجومية غير شائع في خطابات صناع القرار أمام الرأي العام، فإنه حاضر في كتابات المنظرين والحوارات الاستراتيجية حول حقيقة وجودها من الناحية القانونية والعملية؛ بحيث مال الكثير منهم نحو التأكيد على حتميتها في المستقبل وأنها جزء مهم من الحرب المتحركة؛
7. لا يُختزل مسرح الحرب السيبرانية ضمن عمليات قتال الشبكات لعطب أو شل قدرة العدو على القتال، وإنما يتمدد ليشمل الأنشطة الحربية الصامتة والمستمرة عبر الزمن، التي تستهدف تحقيق غاية هزيمة استراتيجية العدو وربح الحرب بدون قتال، عبر ضرب التماسك السوسولوجي، خلق الاضطرابات الاجتماعية، تسويق الإشاعات وعمليات التضليل، نشر الأخبار الزائفة، التشكيك في الثوابت الوطنية، إضعاف الولاء الشعبي للدولة، نشر الثقافة الاستراتيجية المضادة، وغيرها من العناصر التي تدرج ضمن أهداف قتال القوة الرمزية ■

الهوامش

- 1- John J. Mearsheimer, The Tragedy Of Great Power Politics, (New York, London: W. Norton & Company, 2003), pp. 36 - 37.
- 2- Elinor C. Sloan, Modern Military Strategy : An Introduction, (London and New York: Routledge Taylor & Francis Group, 2012), pp. 85-87, pp. 28-30.

3 - محمد عزيز الحبابي، ابن خلدون معاصراً، تر. فاطمة الجامعي الحبابي، (بيروت: دار الحداثة للطباعة والنشر والتوزيع، 1984)، ص ص. 55-57.

4- Thucydides, the History of the Peloponnesian War, Translated by Richard Crawley, (New York, London: E.P.Dutton and Company, INC., J. M. Dent and Sons, Limited 1950), pp. 01-58.

5- Collin S. Gray, War, Peace and international Relations : An Introduction to Strategic History, (London and New York : Routledge Taylor & Francis Group, 2007), pp.115-16.

6 - عبد الرحمن بن محمد بن خلدون، كتاب العبر وديوان المبتدأ والخبر في أيام العرب والعجم والبربر ومن عاصرهم من ذوي السلطان الأكبر، 7 أ.ج. (بيروت: دار الكتب العلمية، 1992)، ص. 313.

7- Sylvia Mercado Kierkegaard, «Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism: The European Response», in Cyber Warfare and Cyber Terrorism, ed. Lech J. Janczewski and Andrew M. Colarik, (New York: Andrew Colarik. com, 2007), p. 438.

8- سون أنزو، فن الحرب، تق. وت. أحمد ناصيف، (دمشق، القاهرة، لبنان: دار الكتاب العربي، 2010)، ص ص. 164-65.

9- نفس المرجع، ص. 23.

10- Christopher Paul, Information Operations Doctrine and Practice: A Reference Handbook, fo. Charles A. Krohn, (London : PRAEGER SECURITY INTERNATIONAL Westport, Connecticut, 2008), p. 02.

11- Elinor C. Sloan, Op. Cit., pp. 85-87.

12- Christopher Paul, Op. Cit., p. 01.

13- Barry Buzan and Ole Waever, Regions and Powers: The Structure of International Security, (Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo: Cambridge University Press, 2003), pp. 45-50.

14- Robert R. Tomes, US Defense Strategy from Vietnam to Operation Iraqi Freedom : Military innovation and the new American way of war, 1973-2003, (New York: Routledge Taylor & Francis Group, 2007), pp. 01-04.

- 15- حسن توركماني، المذاهب العسكرية في العالم، تر. مصطفى طلاس، ط.1، (دمشق: طلاس للدراسات والترجمة والنشر، 1995)، ص ص. 38-39.
- 16- Gene H. McCall and John H. Darrah, «Space Situational Awareness Difficult, Expensive—and Necessary», Air Space Power Journal, (November-December 2014), V. 28, N. 06 : 15.
- 17- روبرت شيالديني، التأثير: وسائل الإقناع، تر. سعد جلال، (القاهرة: دار الفكر العربي، 1988)، ص ص. 33-73.
- 18- كارل فون كلاوزفيتز، عن الحرب، تر. سليم شاكور الإمامي، (بيروت: المؤسسة العربية للدراسات والنشر، 1997)، ص. 294.
- 19- M. V. SMITH, Ten Propositions Regarding Spacepower, (Alabama : Maxwell Air Force Base, 2002), p. 49.
- 20- Colin S. Gray, Op. Cit, p.69.
- 21- Thomas G. Mahnken, «U. S. Strategic and Organizational Subcultures», in Strategic Culture and Weapons of Mass Destruction: Culturally Based Insights Into Comparative National Security Policymaking, ed. Jeannie L. Johnson, Kerry M. Kartchner, and Jeffrey A. Larsen, (United States: PALGRAVE MACMILLAN, 2009), pp. 70-73.
- 22- Brandon Valeriano and Ryan C. Maness, Cyber War versus Cyber Realities Cyber Conflict in the International System, (New York: Oxford University Press, 2015), p. 25.
- 23- Brandon Valeriano and Ryan C. Maness, Op. Cit. p. 28.
- 24- Colin S. Gray, Strategy For Chaos : Revolutions in Military affairs and The Evidence of History, for. Williamson Murray, (London : Frank Cass, 2005), pp. 130-55.
- 25- Ibid., p. 02.
- 26- Robert R. Tones, Op. Cit., pp. 67-68.
- 27- John Mearcheimer, «Strategies for survival», in Perspectives on World politics, 3rd ed. Ed. Richard Little and Michael Smith, (London and New York: Routledge Taylor & Francis Group, 2006), pp. 69 -78.

28- كارل فون كلاوزفيتز، مرجع سبق ذكره، ص. 501.

29- نفس المرجع، ص. 527.

30- Jason B. Barlow, Strategic Paralysis : An Airpower Theory For the Present, (Albama: School of Advanced Airpower Studies, 1992), p. 24.

31- Neville Brown, Global Instability and Strategic Crisis, (London and New York : Routledge, 2004), p. 02.

32- Ka Po Ng, Interpreting China's Military Power Doctrine makes readiness, (USA and Canada: Frank Cass, an imprint of Taylor & Francis, 2005), pp. 16-17.

33- Robert R. Tomes, Op. Cit., p. 117.

34- ريتشارد ريتير وديفيد مارتين، «الدفاع الصاروخي الإقليمي في منطقة الخليج العربي: الاعتبارات المتعلقة بالإنذار المبكر والاستطلاع وإدارة المعارك والقيادة والسيطرة والاتصالات والحواشيب والاستخبارات»، في الدفاع الجوي الصاروخي ومواجهة انتشار أسلحة الدمار الشامل وتخطيط السياسة الأمنية، تح. جاكين ديفس، شارلز بيرري، وجمال سند السويدي، (أبو ظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2000)، ص. 118.

35 - معنى خليل عمر، نظريات معاصرة في علم الاجتماع، (الأردن: دار الشروق للنشر والتوزيع، 1997)، ص. 36-23.

36 - السيد علي شتا، التفاعل الاجتماعي والمنظور الظاهري، ط. 1، (الإسكندرية: المكتبة المصرية، 2000)، ص. 246.

37- Murray E. Jennex, «Cyber War Defense: Systems Development With Integrated Security», in Cyber Warfare and Cyber Terrorism, ed. Lech J. Janczewski and Andrew M. Colarik (New York: Andrew Colarik. com, 2007), p. 253.

38- Ibid., p. 253.

39- Ibid., p. 242.

40- Ibid., p. 253

41- Ibid., p. 253.

42 -ريتشارد ريتير وديفيد مارتين، مرجع سبق ذكره، ص. 119.

- 43- Murray E. Jennex, Op Cit., p. 245.
- 44- Georg Disterer, Ame Alles, Axel Hervatin, "Denial-of-Service (DOS) Attacks: Prevention, Intrusion Detection, and Mitigation", in Cyber Warfare and Cyber Terrorism, ed. Lech J. Janczewski and Andrew M. Colarik (New York: Andrew Colarik. com, 2007), pp. 267-68.
- 45- Richard J. Kilroy, Jr., «The U.S. Military Respnse to Cyber Warfare», in Cyber Warfare and Cyber Terrorism, ed. Lech J. Janczewski and Andrew M. Colarik, (New York: Andrew Colarik. com, 2007), p. 444.
- 46- Kenneth J. Knapp and William R. Boulton, «Ten Information Warfare Trends», in Cyber Warfare and Cyber Terrorism, ed. Lech J. Janczewski and Andrew M. Colarik, (New York: Andrew Colarik. com, 2007), p. 25.
- 47- Thomas M. Kane and David J. Lonsdale, Understanding Contemporary Strategy, (London and New York : Routledge Taylor & Francis Group, 2012), pp. 181-82.
- 48- Georg Disterer, Ame Alles, Axel Hervatin , Op. Cit., p. 269.
- 49- George Kostopoulos, Cyberspace and Cybersecurity, 2nd, (London, New York: CRC Press Taylor & Francis Group, 2018), pp. 235-36.
- 50- Paul Rosenzweig, Cyber Warfare: How Conflicts in Cyberspace: Are Challenging America and Changing the World, (Santa Barbara, California: Praeger An Imprint of ABC-CLIO, LLC, 2012), p. 106.
- 51- Ibid., p. 106.
- 52- John J. Mearsheimer, The Tragedy Of Great Power Politics, (New York, London: W. Norton & Company, 2003), pp. 30 - 41.
- 53- Brandon Valeriano and Ryan C. Maness, Op. Cit., pp. 28-29.
- 54- Ibid., pp. 30-31.
- 55- Elinor C. Sloan, Op. Cit., p. 85.

56- Neil C. Rowe, «Ethics of Cyber War Attacks», in Cyber Warfare and Cyber Terrorism, ed. Lech J. Janczewski and Andrew M. Colarik, (New York: Andrew Colarik. com, 2007), p. 111.

57 - أوستن لونج، «الحروب اللامتماثلة في القرن الحادي والعشرين: الإرهاب الدولي، والتمرد، وحرب الطائرات من دون طيار»، في الحروب المستقبلية في القرن الحادي والعشرين، (أبو ظبي: مركز الإمارات للبحوث والدراسات الاستراتيجية، 2014)، ص. 56.

58 - كارل فون كلاوزفيتز، مرجع سبق ذكره، ص. 757.

59- Elinor C. Sloan, Op. Cit., p. 86.

60 - أنتوني زيني، «تطوير نظام دفاع جوي وصاروخي مشترك من منظور القيادة المركزية الأمريكية»، في الدفاع الجوي الصاروخي ومواجهة انتشار أسلحة الدمار الشامل وتخطيط السياسة الأمنية، تح. جاكين ديفس، شارلز بير، وجمال سند السويدي، (أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2000)، ص. 17 - 19.

61- Robert R. Tones, Op. Cit., pp. 54-72.

62 - كارل فون كلاوزفيتز، مرجع سبق ذكره، ص. 166.

63 - ديفيد جومبرت، «الحرية والقوة في عصر المعلومات»، في دراسات عالمية: الدور المتغير للمعلومات في الحرب، تح. زلمي خليل زاد وجون وايت، ر. 53، (أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2004)، ص. 13-14.

64- Elinor C. Sloan, Op. Cit., p. 89.

65- Colin S. Gray, War, Peace and international Relations : An Introduction to Strategic History (London and New York : Routledge Taylor & Francis Group, 2007), pp.282-84.

66- Neville Brown, Op. Cit., p. 128.

67 - هارلان أولمان وجيمس بي. ويد، «الهيمنة السريعة: ثورة حقيقية في الشؤون العسكرية: التقنيات والأنظمة المستخدمة لتحقيق عنصري الصدمة والترويع»، في دراسات عالمية، ع. 31، (أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2000)، ص. 62-66.

68- Paul R. Viotti & Mark V. Kauppi, International Relations Theory: Realism, Pluralism, Globalism, 2nd ed. (New York: Mac Millan Publishing Company, 1993), pp. 59-61.

69 - ديفيد تانكس، «الاتجاهات الرئيسية في مجال انتشار أسلحة الدمار الشامل وآثارها المحتملة على توازن القوى في منطقة الخليج العربي: تقويم مركز»، في الدفاع الجوي الصاروخي ومواجهة انتشار أسلحة الدمار الشامل وتخطيط السياسة الأمنية، تح. جاكليين ديفس، شارلز بيرري، وجمال سند السويدي، (أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2000)، ص ص. 40-55.

70- Elinor C. Sloan, Op. Cit., p. 90.

71- Colin S. Gray, Modern Strategy, (Oxford New York : Oxford University Press, 1999), p.18.

72 - ديفيد جومبرت، «الحرية والقوة في عصر المعلومات»، في دراسات عالمية: الدور المتغير للمعلومات في الحرب، تح. زلمي خليل زاد وجون وايت، ر. 53، (أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2004)، ص ص. 13-22.

73- Elinor C. Sloan, Op. Cit., p. 88.

74- Ibid., pp. 88.

75 - بيتر سينجر، «دروس الحروب الماضية والاتجاهات التكنولوجية المستقبلية»، في الحروب المستقبلية في القرن الحادي والعشرين، (أبو ظبي: مركز الإمارات للبحوث والدراسات الاستراتيجية، 2014) ص. 81.

76- Elinor C. Sloan, Op. Cit., p. 92.

77- Ibid., p. 92.

78- Lawrence Sondhaus, Strategic Culture and Ways of War (New York: Routledge is an imprint of the Taylor & Francis Group, an informa business, 2006), p. 98.

79- Elinor C. Sloan, Op. Cit., p. 92.

80 - كارل فون كلاوزفيتز، مرجع سبق ذكره، ص. 517.

81 - نفس المرجع، ص. 518.

82- Elinor C. Sloan, Op. Cit., p. 93.

83- Thomas K. Adams, The Army after Next : The First Postindustrial Army (London : Praeger Security International, 2006), p. 07.

84- Elinor C. Sloan, Op. Cit., pp. 92-94.