

الحروب السيبرانية بوصفها مجالاً خامساً للحروب: نقاش نظري

الدكتور عشور قشي

جامعة مولود معمري-تيزي وزو

الملخص

برز «الفضاء الإلكتروني Cyber Space»، على مدى العقد الماضي، بوصفه بؤرة مخاوف أمنية بامتياز؛ إذ تضاعفت التهديدات التي يواجهها أمنه، وتعاظمت تكاليف الاستجابات المناسبة لها بسرعة تفوق قدرة الدول على التعامل معها. وتصدر الفضاء الإلكتروني أجندات الأمن القومي للحكومات؛ فالثابت أن الاستخدام العسكري للفضاء الإلكتروني حقيقة واقعة بالفعل، ومن المرجح أن تنمو أهميته خلال العقود المقبلة. فقد عمدت أغلب الدول إلى بناء قدرات دفاعية وهجومية إلكترونية. أما الجيش الأمريكي فقد حاز الاهتمام الأوسع بالفضاء السيبراني وهو يعامل الأخير بوصفه مجالاً خامساً للحرب. ففي شهر مايو عام 2008، تم إنشاء «مركز الامتياز للتعاون في مجال الدفاع السيبراني التابع لحلف الناتو NATO Cooperative Cyber Defense Centre of Excellence»، المعروفة اختصاراً بـ: (NATO CCD COE)، وفي شهر أكتوبر 2010، تم إنشاء «القيادة السيبرانية الأمريكية the US Cyber Command»، المعروفة اختصاراً بـ: (USCYBERCOM)، هذا إضافة إلى الجهود العسكرية والمؤسسية للعديد من الدول الأخرى المتعلقة بإنشاء أطر أمنية مماثلة. ما يشير إلى الأمانة والعسكرة المتعاضمة للفضاء السيبراني.

الكلمات مفتاحية: الحروب السيبرانية، الفضاء الإلكتروني، الأمن القومي، عصر المعلومة.

المقدمة

بالموازاة مع ذلك، ظهرت نقاشات ومناظرات أكاديمية حادة بين المنظرين والعلماء المختصين في الدراسات الأمنية والإستراتيجية حول وسم العمليات الإلكترونية من قبيل: جمع المعلومات الاستخباراتية، والعمليات التي تستهدف المعنويات وجمع المعلومات، والهجمات التي تنفذ في الفضاء الإلكتروني، بأنها حروب سيبرانية ومجال

خامس للحروب من عدمه. ومن أبرز تلك الأدبيات نجد: مؤلف «توماس ريد Thomas Rid»، عام 2013، تحت عنوان «الحرب السيبرانية لن تحدث Cyber War Will Not Take Place»، تساءل «ريد» عبر عمله هذا: هل الحرب الإلكترونية قادمة حقا؟ ثم راح يجادل وبمحااجة قوية أن الحرب السيبرانية «لم تحدث في الماضي، وغير واقعة في الوقت الحاضر، ومن غير المرجح أنها ستزعجنا مستقبلا»؛ إذ يعتقد أن جميع الهجمات السيبرانية التي وقعت في الماضي وتقع حاضرا لا تعدو أن تكون صيغا متطورة من ثلاث أنشطة قديمة من الصراع البشري نفسه: «التخريب sabotage»، و «التجسس -espionage» و «التدمير Subversion». في مقابل هذه الرؤية، جاء مقال «جون ستون John Stone»، عام 2012، بعنوان «الحرب السيبرانية ستحدث»، حيث حاول «ستون» إثبات أنه يمكن تفسير الهجمات الإلكترونية على أنها أعمال حربية، عبر استجلاء مفاهيم: «القوة force»، و «العنف violence»، و «القتل lethality».

بناء عليه، تأتي هذه الورقة لتناقش الطروحات الأكاديمية المتضاربة بشأن طبيعة مفهوم «الحروب السيبرانية»، التي قادت بدورها إلى إثارة النقاش حول طبيعة مفهوم الحرب نفسه، وبالتالي علاقة ما يقع على مستوى الفضاء السيبراني من هجمات إلكترونية بنظرية الحرب وموقعه منها.

أولا: الحرب من منظور كلاوزفيتز..مقاربة مفاهيمية

الثابت في دراسات الحرب أن الأخيرة ليست ثابتة بحد ذاتها، رغم أنها سمة ثابتة ومتأصلة في السياسة العالمية. فوفقا لـ: «جاك ليفي Jack S. Levy» و «ويليام تومبسون William R. Thompson»، تتغير طبيعة الحرب من وقت لوقت، ومن مكان لآخر، وفقا لشدها، ومدتها، وأسبابها، وتداعياتها⁽¹⁾، وأبعاد أخرى يضيفها «كالفي هولستي Kalevi J. Holsti»، تتعلق بتوقيت شن الحرب، وآليات إدارتها، وطريقة إنهاؤها⁽²⁾. هولستي، وفي مؤلفه «الدولة والحرب ودولة الحرب»، عام 1996، يشير إلى هذه الطبيعة المتغيرة للحرب، حين ذكر أن حروب القرن 18 ليست هي نفسها حروب القرن 19 أو 20، وحروب القرن 21 قطعاً لن تكون نفسها حروب القرن 20.

ومع ثراء أدبيات الحقل الاستراتيجي بالتحليلات المفاهيمية والنظرية لمصطلح الحرب، إلا أن التعريف الذي قدمه البروسي «كارل فون كلاوزفيتز Carl von Clausewitz» للحرب وضمّنه في كتابه الشهير، والمعنون بـ: «عن الحرب»⁽³⁾ On War، الذي يعد أحد الأعمال الأساسية التي تحتل محور النقاشات الجارية حول طبيعة الحرب،

ولكن أيضا النقاشات الحالية حول طبيعة ما يجري من أعمال خبيثة على مستوى الفضاء السيبراني، يبقى التعريف الذي يحظى باتفاق كبير بين منظري الإستراتيجية.

لقد كانت غاية كلاوزفيتز الأسمى من كتابه المذكور هو التأسيس لنظرية في الحرب عبر تحديد عناصرها الرئيسية. يرى كلاوزفيتز أن الحرب هي: «عمل من أعمال القوة لإجبار العدو على تنفيذ مشيئتنا»⁽⁴⁾، وأنها: «سوى استمرار للسياسة بوسائل أخرى»⁽⁵⁾. ومن لدن هاتين العبارتين يستخلص المحللون ثلاثة عناصر رئيسية تشكل مجتمعة فعل الحرب. الطابع السياسي، والذرائعي، والعنفي للحرب.

أول هذه العناصر هو الطابع السياسي للحرب؛ فالأخيرة عمل من أعمال السياسة، وهذا يعني، من بين أمور أخرى، أن القتال الحربي يحدث بين المجتمعات السياسية التي تمتلك القدرة على فرض الإرادة السياسية. وهذا ما يميز الحرب عن أي نوع من أنواع القتال الأخرى. أما ثاني العناصر الثلاثة فهو الطابع الذرائعي للحرب، فلكل حرب غاية ووسيلة؛ أما وسيلة الحرب فهي القوة أو التهديد باستخدامها. وأما غايتها فهي إجبار العدو على قبول مشيئة المعتدي. وأما ثالث هذه العناصر وآخرها فهو الطابع العنفي للحرب، فالحرب في جوهرها مؤسسة للعنف، والعنف سمة متأصلة في الحرب ومكون لا غنى عنه، يبقى أن درجة العنف تتباين من حرب لأخرى.

غير أن السؤال المطروح ضمن هذا السياق، وفي حدود هذه الورقة، هو: هل بالإمكان اعتبار أن ما حدث ويحدث من هجمات على مستوى الفضاء الإلكتروني، من قبيل التجسس والتخريب وجمع المعلومات، عملا من أعمال الحرب، ومن ثم بإمكاننا الحديث عن حرب سيبرانية تؤسس بدورها لمجال خاص خامس للحروب إلى جانب المجالات الأربع التقليدية: البرية والبحرية والجوية والفضائية؟

بعد مراجعة عدد من الأدبيات ذات الصلة بموضوع الورقة وجدنا أن بالإمكان تجميع تلك الأدبيات في قسمين اثنين:

- قسم أول يرفض إضفاء الطابع الحربي على ما يجري من عمليات تجسس وتخريب على مستوى الفضاء الإلكتروني، وبالتالي يرفض مصطلح «الحرب السيبرانية»، معتمدا في ذلك على تعريف كلاوزفيتز التقليدي للحرب، والشروط الثلاث التي حددها لتوصيف فعل ما على أنه عمل من أعمال الحرب. علماء هذا الطرح رأوا أن التهديد مبالغ فيه، وزعموا أن الأنشطة الخبيثة التي تجري عبر الفضاء السيبراني

لا تلبى الشروط الثلاث، ولا تستجيب لها، ومن ثم ليس بالإمكان أن نطلق عليها صفة الحرب إلا إذا تم توظيف هذا المصطلح بصورة سيئة للغاية.

- أما القسم الثاني من الأدبيات الصادرة حول الموضوع فتؤكد على أن الحروب القادمة ستكون حروبا سيرانية بامتياز، وأعابت على أدبيات القسم الأول اعتمادها تعريف كلاوزفيتز التقليدي للحرب في دراستها لواقع جديد يتعلق بهجمات الفضاء السيبراني، وترى أن السياق الحالي يستدعي بالضرورة تجاوز التعريفات التقليدية الضيقة للحرب، وتبني تعريفات جديدة موسعة لها تتلاءم وحقائق عصر المعلومة.

ثانياً: الحرب السيرانية القادمة: الفضاء السيبراني كمجال خامس للحروب

لقد باتت مفردة «ساير Cyber» المفردة السائدة، على الأقل خلال العقد الأخير؛ إذ صارت تضاف كبادئة لكل نشاط بشري. فقد تحول الإرهاب إلى «إرهاب سيبراني»، والأمن إلى «أمن سيبراني»، والاحتيايل إلى «احتيايل سيبراني»، والجريمة إلى «جريمة سيرانية»، والأسلحة إلى «أسلحة سيرانية» والحرب إلى «حرب سيرانية»، وهكذا، حتى تم إنشاء قاموس مصطلحات كامل يتعلق بقضايا عالم الأنترنت⁽⁶⁾.

خلال العام 2010، كتب ويليام لين William J. Lynn، نائب وزير الدفاع الأمريكي الأسبق، في مقال له في دورية الشؤون الخارجية ما يلي: «على الرغم من أن الفضاء الإلكتروني هو مجال من صنع الإنسان، إلا أنه أصبح بالغ الأهمية للعمليات العسكرية مثل البر والبحر والجو والفضاء»⁽⁷⁾. وفي فيفري 2011، حذر مدير وكالة الاستخبارات المركزية الأمريكية، آنذاك، ليون بانيتا Leon Panetta، اللجنة المختارة الدائمة المعنية بالاستخبارات، من أن هجوم «بيرل هاربور القادم قد يكون هجوماً سيرانياً»⁽⁸⁾. كما أن البنتاغون الأمريكي اعترف رسمياً بالفضاء السيبراني بوصفه مجالاً جديداً للحرب⁽⁹⁾.

علاوة على ذلك، أضفت، على مدى العقدين الماضيين، عناوين بعض المنشورات الأكاديمية والصحفية، مثل: «الإعداد لبيرل هاربور رقمي» لـ: «جون شواتز John Schwatz» عام 2007⁽¹⁰⁾، و«الاستعداد لـ 11 سبتمبر رقمي» لـ: «كاران غرينبيرغ Ka-ren J. Greenberg» عام 2012⁽¹¹⁾، طابعاً خاصاً على سجل ناشئ بدأ يلوح في الأفق بين عدد من الأكاديميين المختصين في مجال الدراسات الأمنية والإستراتيجية، لتأت بعد ذلك سلسلة من الهجمات الإلكترونية الممتدة إلى اليوم، من بينها ثلاث حالات كبرى،

استند إليها البعض لدعم رأيه القائل بأطروحة «الحرب السيبرانية»، واستدلوا بها لتعزيز الفكرة القائلة أن الحرب دخلت فعلا عصرا جديدا في سياق الهجمات السيبرانية، في الوقت الذي وظف فيه البعض الآخر هذه الحالات الثلاث، وحالات أخرى عديدة، لدحض أطروحة البعض الأول. هذه الحالات الثلاث هي:

1. الهجوم السيبراني على استونيا عام 2007.
2. الهجوم السيبراني على جورجيا عام 2008.
3. فيروس ستاكسنت Stuxnet عام 2009 ضد البرنامج النووي الإيراني.

في مقال مشترك لهما صادر عن مؤسسة راند الأمريكية عام 1993، أعلن المحللان البارزان بالمؤسسة نفسها، «جون أركيلا John Arquilla» و «ديفيد رونفيلت David Ronfeldt»، عن بزوغ فجر الحروب الالكترونية، وأن الأخيرة قادمة لا محالة. وقد جادل الباحثان، وبمحااجة قوية، أن شبكة الأنترنت الناشئة ستغير مجرى الحروب ومسارها بصورة جذرية للغاية، وذكر أن النصر في الحروب المقبلة سيكون من نصيب أولئك الذين يحوزون قدرا أكبر من المعلومة.

الفكرة التي أعلنها الباحثان بدت آنذاك ضربا من ضروب الخيال، وكان يتعين على عقد من الزمن أن يمر حتى يدرك صناع القرار في الولايات المتحدة، وأعضاء مؤسسة الأمن القومي الأمريكية، الفكرة. وبمجرد استيعابهم لها، تلقفتها أصوات شتى في وسائل الإعلام معلنه عن بروز مرحلة جديدة من الحروب وسمائها البعض بـ: «الحروب السيبرانية»، مثل ما كتبه «شواتز» و«غرينبيرغ» على النحو المذكور أعلاه.

في وقت لاحق، انساق عدد من العلماء البارزين في حقل العلاقات الدولية مثل: جوزيف ناي⁽¹²⁾ Joseph S. Nye، و مايكل شميت⁽¹³⁾ Michael N. Schmitt، وراء ادعاء أركيلا وزميله رونفيلت، وأكدوا أن ما يحدث على مستوى الفضاء السيبراني من عمليات هجومية إنما يدخل تحت عنوان الحرب لا غير. ونادوا بضرورة إعادة مفهمة الحرب وإعادة ضبط تعريف دقيق وسليم للمصطلح بغية رسم حدوده المفاهيمية قبل النظر فيما إذا كان ما يطلقون عليه وصف «الحرب السيبرانية» يتفق مع تعريف كلاوزفيتز للحرب من عدمه. كما رأوا أن التأثير الطاعى لتصور كلاوزفيتز للحرب لا يترك مساحة كافية لتفسير جديد للظاهرة. كما تزعم هذه المدرسة الفكرية الناشئة أن السياق السياسى الجديد، الذى تحدده تكنولوجيات الاتصال الجديدة، يفرض علينا

إعادة مفهمة الحرب والقوة العسكرية ومفاهيم أخرى ذات صلة كمفهوم القوة والعنف وغيرهما.

ضرورة إعادة صياغة تعريف دقيق للحرب يتواءم وتطورات العصر، تفرضه حقيقة أن الحرب ليست ثابتة بحد ذاتها، رغم أنها سمة ثابتة ومتأصلة في السياسة العالمية. فطبيعة الحرب تتغير من وقت لوقت، ومن مكان لآخر، وفقا لشدتها، ومدتها، وأسبابها، وتداعياتها⁽¹⁴⁾، وأبعاد أخرى من قبيل: توقيت شنها، وآليات إدارتها، وطريقة إنهاؤها⁽¹⁵⁾. حتى أن هولستي في مؤلفه «الدولة والحرب ودولة الحرب»، عام 1996، يشير إلى هذه الطبيعة المتغيرة للحرب حين ذكر أن حروب القرن 18 ليست هي نفسها حروب القرن 19 أو 20، وحروب القرن 21 قطعاً لن تكون نفسها حروب القرن 20. لقد تطورت الحرب بتطور الإنسان والمجتمعات؛ فمن الحرب القبلية إلى الحرب النووية، ومن حرب الاستقلال إلى الحرب الأهلية، ومن الحرب المحلية إلى الحرب العالمية. لذلك، يعتقد البعض أن «الحرب السيبرانية» أحدث نماذج الحرب خلال القرن الحالي. العلة في ذلك، أن مجتمعنا العالمي مجتمع سلكي بالكامل تقريباً، وهذا المجتمع السلكي قد يصبح عرضة للعطب في حال حدوث هجمات إلكترونية.

أما جون ستون فقد رأى أن الجهود التي تم بذلها لتحديد ما إذا كانت الهجمات التي تقع على مستوى الفضاء السيبراني يجب اعتبارها عملاً من أعمال الحرب، أو على أنها مجرد أعمال إجرام، أو تجسس، أو تخريب، وما إلى ذلك، تتعطل بسبب فهمنا الواسع والفضفاض لماهية الحرب نفسها⁽¹⁶⁾. لذلك، يدعو «ستون» ومن معه من الدارسين المختصين، مثل «رونفيلت»⁽¹⁷⁾، إلى ضرورة إعادة النظر في مفاهيم العنف والقوة وعلاقتها بالقتل.

وفي سياق رده على ادعاءات «ريد»، يرى ستون أن الأخير يخلط بين مفاهيم القوة والعنف والقتل. فالحرب وفقاً لستون لا تتطلب أي علاقة سببية بين المفاهيم الثلاث؛ لأن كل الحروب تتطلب القوة، لكن الأخيرة لا تعني بالضرورة العنف - لا سيما إذا كان العنف يتضمن القتل. وعليه، فإن القوة، من منظور «ستون»، يمكن أن تتجاوز مجرد إلحاق الضرر بالأجساد البشرية. ومصطلح «الضرر damage» يشير إلى أن العنف قد يكون موجهاً إلى الأجهزة كما الأشخاص، مما يعني أن الضرر لا يجب أن يكون دائماً قاتلاً بالضرورة⁽¹⁸⁾. لذلك، يرى «ستون» أن القيمة العسكرية لأي هجوم على نتائج الحرب، سواء كان هجوماً سيبرانياً أم لا، لا ينبغي تقييمه على أساس مقدار عدد القتلى.

ضمن هذا السياق، وبغرض التوضيح، صاغ «ستون» مثالا ينفي من خلاله وجود ارتباط سببي بين العنف والقتل، وأن العنف لا يحمل طابعا دمويا بالضرورة. يتعلق المثال بالغارتين الجويتين اللتين شنتهما القوات الجوية الأمريكية الثامنة عام 1943 على مدينة شفاينفورت الألمانية، وفي كلتا الحالتين كان الغرض من الهجوم شل مصانع الفولاذ الألمانية. الغارة الأولى قتل فيها 203 أشخاص، وفي الثانية قتل 276 شخصا. هنا، يذكر «ستون» أن هذه الوفيات كانت عرضية بالنسبة للحلفاء للهدف المنشود المتمثل في تدمير قدرة العدو على تصنيع كرات الفولاذ⁽¹⁹⁾. المغزى من المثال الذي ساقه ستون هو أن القوة قد تنطوي على العنف غير أن العنف لا ينطوي بالضرورة على القتل لتحقيق الطابع الدموي وتحقيق الغاية من الحرب.

هذا الطرح ينساق معه «أركيلا» وزميله «رونفيلت» حينما ذكرا، في مقالهما عام 1993، أن المسيطر على المعلومة، والمتحكم فيها، سيثبت على نحو مستقل أنه قادر على ضمان النصر في أي صراع قادم، وبالتالي نزع طابع العنف والقتل والتدمير عن فعل الحرب⁽²⁰⁾.

وعليه، يرى المدافعون عن أطروحة الحرب السيبرانية أن الدول التي تمكنت من تخصيص قوات منظمة في المجالات البرية والبحرية والجوية والفضائية، تخصص اليوم جيوشا منظمة ومتخصصة مهمتها القتال عبر الفضاء الإلكتروني وهو ميدان حربهم، وأسلحتهم في ذلك الحواسيب بدلا من البنادق. فبنقرة واحدة على زر من أزرار لوحة المفاتيح الخاصة بالحواسيب بالإمكان شل مجتمعات بأكملها تعتمد اعتمادا كبيرا على شبكة الانترنت.

ثالثا: الحرب السيبرانية لن تحدث: نزع الطابع الحربي عن الأنشطة السيبرانية

على النقيض من الطرح الأول الذي حاول إضفاء الطابع الحربي على النشاطات الخبيثة التي تحدث على مستوى الفضاء السيبراني، جاءت أدبيات الشق الثاني من هذا النقاش الناشئ لدحض ذلك الطرح ونفيه، منادية بضرورة الالتزام بالتصور التقليدي للحرب، الذي صاغه كلاوزفيتز قبل نحو قرنين من الزمن، وعدم الإساءة للمصطلح عبر التوظيف السيئ له، مؤكدة أن جميع الهجمات السيبرانية التي وقعت في الماضي، وتقع حاضرا، لا تعدو أن تكون صيغا متطورة من ثلاث أنشطة قديمة من الصراع البشري نفسه، وهي: التخريب، والتجسس، والتدمير.

علماء هذا الطرح حاولوا بكتاباتهم وضع النقاش حول «الحرب السيبرانية» على المسار الصحيح، عبر التأكيد أن «الحرب السيبرانية لن تحدث»⁽²¹⁾، وأن «الحرب السيبرانية لن تأت»⁽²²⁾. الحجة التي ساقها علماء هذا الطرح، وعلى رأسهم الباحث الأكاديمي «توماس ريد»، و«ديفيد بيتز David J. Betz»، و«تيم ستيفنز Tim Stevens»، «أमित يوران»⁽²³⁾ Amit Yoran، «مارتن ليبكي»⁽²⁴⁾ Martin C. Libicki، هي أنه لا يوجد شيء اليوم يدعى «حرب سيبرانية»، ومن غير المرجح أن تحدث في المستقبل. والعلّة في ذلك، أن نماذج الهجمات الالكترونية التي وقعت حتى اليوم لم ترق إلى مستوى الحرب، لعدم استيفائها المكونات اللازمة لتوصيف الحروب استنادا لمنظور كلاوزفيتز للحرب الذي يحدد ثلاث معايير أساسية يجب أن تتوافر في أي عمل عدواني أو هجومي كي يعتبر عملا حربيًا، وهي:

1. المكون الأول: الطابع السياسي للحرب، وهذا ما يميز الحروب عن غيرها من أشكال القتال الموجودة بين مختلف الأفراد والجماعات غير السياسية؛
2. المكون الثاني: الطابع الذرائعي للحرب، فالحرب أداة لتحقيق الغاية التي تتمثل في إجبار الخصم على الاستجابة لرغبة المهاجم ومشئته؛
3. المكون الثالث: الطابع العنفي للحرب الذي ينطوي بدوره على طابع دموي.

لذلك، يرى «ريد» أن أي عمل عدواني، أو دفاعي، يطمح إلى أن يكون عملاً حربياً قائماً بذاته، أو أن يتم تفسيره على ذلك النحو، ينبغي أن يستوفي المعايير الثلاثة جميعاً، وهي: الحافز السياسي، والعامل الذرائعي، وإمكانية القتل. «توماس ريد»، ومن نهج نهجه، ينفون وجود المكونات الثلاث في حال الهجمات السيبرانية التي وقعت فعلاً. فلا الطابع السياسي للحرب تحقق نتيجة عدم التيقن من تحديد هوية المهاجم إن كان فعلاً وحدة سياسية أم لا، ولا الطابع العنفي الدموي، ولا الطابع الذرائعي قد تحققاً أيضاً، ناهيك عن عدم حدوث خسائر كبيرة في الأرواح بسبب الهجمات التي حصلت حتى اليوم⁽²⁵⁾.

بالنسبة لمعيار الطابع العنفي للحرب، يرى كلاوزفيتز أن «الحرب هي عمل من أعمال القوة لإجبار العدو على الخضوع لمشيئتنا». لذلك، يرى «ريد» أن كل الحروب عنيفة بطبيعتها. وإذا كان الفعل غير عنيف، أو لا يحتمل العنف، فهو ليس فعل حرب. بل يتم التخفيف من حدة هذا المصطلح ويتحول إلى مجرد تعبير مجازي، كما هو الحال

في «الحرب» على السمعة أو «الحرب» على السرطان. لأن الفعل الحقيقي للحرب، وفقا «لريد»، ينبغي أن يكون دائما قاتلا، على الأقل بالنسبة لطرف من الأطراف المشاركة.

أما المعيار الثاني من معايير فعل الحرب فهو الطابع الذرائعي. فلكي يكون فعل الحرب ذرائعيا، ينبغي أن تكون هناك وسيلة وغاية. فالقوة أو التهديد باستخدامها هي الوسيلة. وأما الغاية فهي إجبار طرف على قبول إرادة الطرف الآخر. ولتحقيق الغاية من الحرب، يتعين على أحد الخصوم أن يتبنى موقفا دفاعيا.

أما المعيار الثالث، فهو الطابع السياسي للحرب. فالأخيرة لم تكن يوما فعلا منعزلا، وهي ليست سوى استمرار للسياسة بأدوات أخرى مغايرة. فالغاية الأسمى من الحرب تبقى دائما غاية سياسية.

وعليه، يجادل «ريد» بالقول أنه إذا كان استخدام القوة في الحرب يحمل طابعا عنيفا، وذرائعيا، وسياسيا، فلا وجود إذن لأي هجوم وقع عبر الإنترنت تجتمع فيه هذه المعايير الثلاث. بل أكثر من ذلك، يرى ريد أن هناك عددا قليلا جدا من الهجمات السيبرانية التي وقعت فعلا، والتي لا تستجيب إلا لمعيار واحد في أحسن الحالات، ما يجعلها بعيدة كل البعد عن أن يتم إضفاء الطابع الحربي عليها، أو أن يتم وسمها بـ«الحرب السيبرانية».

أما بيتز وستيفنز فقد أشارا إلى هامشية القدرات الإستراتيجية للحرب السيبرانية كوسيلة سياسية للدول لفرض مشيئتها على خصومها، ويرجع ذلك أساسا إلى مشكلة الإحالة أو العزل، والتي تعني صعوبة، إن لم تكن استحالة، تحديد هوية المهاجم إن كان فعلا وحدة سياسية أم لا. وهي الحالة التي وصفها بـ: «الهجوم اليتيم orphan attack»، أو الهجوم مجهول الهوية الذي لا ينطلق من كيان سياسي يمكن تحديده دوليا.

الخاتمة

المستخلص من هذه الورقة أن هناك وفرة في الأدبيات والأفكار التي تتعلق بالطابع المستقبلي للحرب في عصر المعلومة، والاستخدام المتعاظم للفضاء السيبراني، وما يقع داخله من عمليات تخريب وتجسس وتدمير. وقد انقسمت هذه الأدبيات والأفكار إلى قسمين اثنين: قسم أول مدافع عن أطروحة الحرب السيبرانية ومنافع عنها، أقر بوجودها فعلا، ورأى أنها باتت تمثل مجالا خامسا من مجالات الحروب، بعد مجالات

البر والبحر والجو والفضاء. مثلت هذا القسم رؤى كل من أركيلا ورونفيلت، وستون، وناي، وشميت، وآخرون. هؤلاء كلهم نادوا بضرورة توسيع مفهوم الحرب، والابتعاد عن الفهم التقليدي الضيق له، والابتعاد عن التطبيق الصارم والعنيد للمنظور الكلاوزفيتزي للحرب، مع إعادة النظر، طبعا، في مفاهيم القوة والعنف وتحديد ما ينطويان عنه. العلة في ذلك، أن العالم تغير، وطبيعة الحرب تغيرت معه، مع بقاء الأخيرة سمة ثابتة ومتأصلة في السياسة الدولية.

أما القسم الثاني فيقع على النقيض من مذهب القسم الأول. ويمثله كل من: توماس ريد، شنابر، يوران، بيتز، شنابر، ستيفنز، ليبكي، وآخرون، الذين رأوا أن التهديد السيراني قد تم المبالغة فيه، ومُنح من الاهتمام أكثر مما ينبغي، ورأوا أن ليس هناك ما يدعو إلى التنبؤ بمثل هذه الحرب مستقبلا، وليس على الجيوش أن تتجهز لها. علاوة على ذلك، جادلوا، وبمحااجة قوية، أن الحرب السيرانية كمفهوم، لا يمكن أن تكون حرباً من منظور التصور الكلاوزفيتزي التقليدي للحرب.

ما يمكن التشديد عليه هنا من خلال عرض الطرحين وحججهما، أن الحرب السيرانية ممكنة؛ بمعنى أن الهجمات السيرانية يمكن أن تشكل أعمال حرب، شرط أن نكون واضحين بشأن مفهوم الحرب، وما تتضمنه مصطلحات «القوة» و «العنف»، وحول علاقتهما بمسألة القتل. فأعمال الحرب تنطوي على تطبيق القوة من أجل إحداث آثار عنيفة. غير أن هذه الآثار العنيفة لا ينبغي أن تكون قاتلة ومميتة في طبيعتها؛ فهي يمكن أن تكسر الأشياء وتدمرها، بدلاً من أن تقتل الناس وتريق دماءهم، لكنها تظل دائماً تحت عنوان الحرب. وعليه، فإن العالم سيشهد حروبا بين مجموعات متخصصة تهدف إلى تحقيق الغايات التي وضعتها الوحدات السياسية، وبذلك نكون أمام مجال خامس من مجالات الحرب، إلى جانب المجالات التقليدية الأربع: البرية والبحرية والجوية والفضائية. غير أن الاستنتاج الأهم من هذه الورقة هو أن النقاش الأكاديمي الجاري حول الحرب السيرانية قد فتح الباب واسعا أمام ضرورة إعادة النظر والتفكير مرة أخرى في مفهوم الحرب وطبيعتها.

الهوامش

1. Jack S. Levy, William R. Thompson, The Arc of War: Origins, Escalation, and Transformation (London: The University of Chicago Press, 2011), p. 01.
2. Kalevi J. Holsti, The state, war, and the state of war (Cambridge: Cambridge University Press, 1996).
3. كارل فون كلاوزفيتز، عن الحرب، تر. سليم شاكراً الإمامي، ط. 1 (بيروت: المؤسسة العربية للدراسات والنشر، 1997).
4. المرجع نفسه، ص. 103.
5. المرجع نفسه، ص. 121.
6. NCAFP, « Cyberpower and National Security », The Journal of the National Committee on American Foreign Policy, No. 35, Vol. 1 (2013), p. 50.
7. William J. Lynn, «Defending a New Domain The Pentagon's Cyberstrategy», Foreign Affairs Vol. 89, No. 5 (September/October 2010), p. 101.
8. Lisa Daniel, « Panetta: Intelligence Community Needs to Predict Uprisings », American Forces Press Service, 11 Feb. 2011. (<http://archive.defense.gov/news/newsarticle.aspx?id=62790>)
9. William J. Lynn, Op. Cit., p. 101.
10. John Schwatz. Preparing for a digital Pearl Harbor. New York Times, 24 JUNE, 2007. (<https://www.nytimes.com/2007/06/24/business/worldbusiness/24iht-cyber.1.6299676.html>)
11. Karen J. Greenberg, Preparing for a digital 9/11: Fear of a cyber attack is eroding US civil liberties and the constitution, the nation, 22 OCTOBER 2012. (<https://www.thenation.com/article/preparing-digital-911/>).
12. Joseph S. Nye, Nuclear lessons for cyber security? Strategic Studies Quarterly, Vol. 5, No. 4 (2011), pp. 18–38.
13. Michael N. Schmitt, Tallinn manual on the international law applicable to cyber warfare (Cambridge: Cambridge University Press, 2013).
14. Jack S. Levy, William R. Thompson, The Arc of War: Origins, Escalation, and Transformation (London: The University of Chicago Press, 2011), p. 01.
15. Holsti K. J, The state, war, and the state of war (Cambridge: Cambridge University Press, 1996).

16. John Stone, « Cyber War Will Take Place! », Journal of Strategic Studies, Vol. 36, No. 1 (2013), p. 101.
17. Carsten F. Roennfeldt, « Productive war: a re-conceptualisation of war », Journal of Strategic Studies, Vol. 34, No. 1 (February 2011) pp.39-62.
18. John Stone, Op. Cit., p. 104.
19. Ibid., pp. 104-105.
20. Arquilla and Ronfeldt, Op. Cit., p. 23.
21. Thomas Rid, Cyber war will not take place, The Journal of Strategic Studies, Vol. 35, No. 1 (February 2012), pp. 5-32.
22. David J. Betz, Tim Stevens, Cyberspace and the State: Towards a Strategy for Cyber-Power (London: Routledge, 2011), p. 88.
23. Amit Yoran, Cyberwar or not cyberwar? And why that is the question? », Forbes, 25 Mar 2010. (<http://www.forbes.com/sites/firewall/2010/03/25/cyberwar-or-not-cyberwar-and-whythat-is-the-question/>).
24. Martin C. Libicki , Conquest in cyberspace: national security and information warfare, 1st ed. (Cambridge: Cambridge University Press, 2007).
25. Thomas Rid., Op. Cit.