فهد حمد العذبة | *Fahad Hamad Aladba

استشراف أثر التطوّر التكنولوجي في الحروب الحديثة والقوة العسكرية للدول الصغرى

Forecasting the Impact of Technological Development on Modern Wars and the Military Power of Small States

التسلم Received	التعديل Revised	القبول Accepted	الرقم التعريفي DOI
2022-09-18	2022-11-14	2022-11-26	https://doi.org/10.31430/DCTR9760

ملخص: تتناول هذه الدراسة أثر التطور التكنولوجي العسكري في مفهوم الحرب، ودوره في تعزيز قوّة الدول الصغرى من خلال امتلاكها الأسلحة المتطورة تكنولوجيًا، والمنظومات الاستراتيجية القادرة على تحييد الدول الكبرى ذات العمق الاستراتيجي أو تعطيلها أو ردعها. وتخلص الدراسة إلى أنّ التطوّر التكنولوجي بات عنصرًا بالغ الأهمية لجميع الدول في الحروب الحديثة؛ لأنه يرفع من قدرة القوات المسلحة على أداء المهمات العسكرية باحترافية ومرونة عاليتَين، إضافة إلى تقليل الاعتماد على العنصر البشري واستبدال التكنولوجيا به، حفاظًا على أرواح الجنود، وتوفير الوقت والجهد.

كلمات مفتاحية: التطور التكنولوجي، الحروب الحديثة، الحرب الإلكترونية، الدول الصغرى.

Abstract: This research paper addresses the impact of military technological development on the concept of war, which has shifted from traditional war, which depends on the number of soldiers, ammunition, and military arsenal, to modern war that depends on technology as an effective strategic weapon that imposes its control on the ground by achieving the desired strategic objectives accurately. It also focuses on studying military technological development in enhancing the power of mini states through their possession of technologically advanced weapons and strategic systems capable of neutralizing, disrupting, or deterring the ambitions of major states with strategic depth. The study concludes that, technological development has become a very important element for all countries and an integral part of modern wars, because it is able to perform military tasks with high professionalism and flexibility, in addition to reducing dependence on the human element and replacing it with technology to preserve the lives of soldiers and reduce the time and effort spent in those operations.

Keywords: Technological Development, Modern Warfare, Electronic Warfare, Mini States.

* طالب دكتوراه في الدراسات الدفاعية والأمنية بأكاديمية جوعان بن جاسم للدراسات الدفاعية، قطر.

Ph.D. Student in Defense and Security Studies at Joaan Bin Jassem Academy for Defence Studies, Qatar.

مقدّمة

ارتبطت قوّة الدول في الماضي ارتباطًا وثيقًا بالأساليب العسكرية التقليدية، واعتمدت اعتمادًا كلّيًا على كثافة العنصر البشري وجاهزيّته البدنية وامتلاكه الأسلحة الثقيلة، كالمدفعية والدبابات والمدرعات؛ ولعلّ خير مثال على ذلك ما وقع خلال الحربين العالميتين الأولى والثانية، والتفوق الحربي الألماني آنذاك؛ فالذي صنع القوة العسكرية لألمانيا هو أولًا، امتلاكها الكثافة البشرية، وثانيًا، الترسانة العسكرية الضخمة، وثالثًا، التصنيع العسكري المتطور والمستمر، ورابعًا، الموارد المتاحة. ومع ذلك، فإنّ الجيش الفرنسي (وحده، ومن دون حساب عدد جيوش الحلفاء) - وهو أكبر جيوش أوروبا آنذاك، ويتفوق على جيش الفيرماخت الألماني بفارق اثني عشرة فرقة في بداية الحرب العالمية الثانية - تلقّى هزيمة لأسباب عدّة.

غير أن هذا المفهوم بدأ يتغيّر شيئًا فشيئًا خصوصًا بعد الحرب الباردة؛ إذ بدأت تطفو على السطح أدوات من نوع آخر عزّزت القوّة العسكرية، مثل استخدام المجال الكهرومغناطيسي الذي لديه القدرة على التحكم بأنظمة العدو، والحرب الإلكترونية التي من شأنها تعطيل أنظمة الاتصالات أو التشويش عليها، والأمن السيبراني القادر على اختراق الشبكات، والأقمار الصناعية التي تُعنى بتأمين الاتصالات المشفرة وتوفير صور المنشآت والمعسكرات، والطائرات بدون طيّار التي تستطيع تدمير الأهداف الاستراتيجية بدقة عالية[1]. وهذا ما أدّى إلى تغيير مفهوم الحروب في العصر الحديث، ومن ثمّ إلى نشأة مفهوم جديد لا يعتمد على الجنود وساحات القتال، بل يركّز على تدمير البنى التحتية والمنشآت الحيوية، مثل سكك القطارات، ومنظومات التبريد والتدفئة، ومراكز البيانات، وأنظمة المستشفيات؛ وهي لا تقل ضراوةً وتأثيرًا عن الحروب التقليدية؛ لأنها تتسبب في الفوضى وعدم الاستقرار للشعوب الذين يشكلون ورقة ضغط على حكوماتهم، من خلال الاحتجاجات والمظاهرات التي تتسبب في ضعف الدول، أو في بعض الأحيان، في فشلها.

أصبح للتطوّر التكنولوجي تأثير كبير في الحروب الحديثة؛ لأنّ التكنولوجيا العسكرية تحوّلت إلى أسلحة استراتيجية قائمة بذاتها، وعنصر رئيس في صناعة التفوق العسكري بالميدان، قادر على ردع بعض الأسلحة الاستراتيجية وتعطيل المنشآت الحيوية، إضافة إلى أهميتها في تعزيز قوّة الدول الصغرى، من خلال معرفة "مراكز ثقل" (Center of Gravity, COG) العدو، وكيفية التعامل معها عن طريق استخدام الأدوات التي ساهم التطور التكنولوجي في إيجادها، مثل أنظمة المراقبة والاستطلاع (ISR)، و"استخبارات الإشارة" (Signals Intelligence, SIGINT)، و"استخبارات الاتصالات" (Communications Intelligence, COMINT)، وأنظمة "الهجوم الإلكتروني" (ElectronicAttack,EA)، و"الطائرات بدون طيّار" (UAV)، وأنظمة "الدفاع الإلكتروني" (Electronic Protection, EP)، و"عسكرة الفضاء" (Space Militarization)، و"الأمن السيبراني" (Cyber Security, CS)، و"المجال الكهرومغناطيسي" (Electromagnetic Field, EF)، و"الاستشعار عن بعد" (Remote Sensing, RS).

1 Subramaniam Ananthan, "The Elements of National Power and its Relevance to National Security," *Zulfaqar Journal of Defence Management, Social Science & Humanities*, Special Issue: "Social Sciences and Humanities in the 4th Industrial Revolution Issues," (2020), pp. 59-65.

تتجلى أهمية هذه الدراسة، بعد الواقع الجديد الذي بات يفرض نفسه على مستقبل الاستراتيجيات العسكرية، في معرفة إسهامات التطور التكنولوجي في تعزيز قوّة الدول الصغرى، باعتباره أداة ردع محتملة كفيلة بإبعاد بعض الأخطار، وتقليل مستوى تهديدات الدول الكبرى، وذلك من خلال ما وفّرته هذه الطفرة التكنولوجية من منظومات متطورة تشكّل عنصر حسمٍ في الحروب الحديثة.

ركّزت العديد من الأبحاث الأكاديمية والأدبيات السابقة على أثر التطور التكنولوجي في الاستراتيجيات العسكرية للدول الصغرى، لمعرفة تأثير التكنولوجيا العسكرية في تعزيز قوّة الدول الصغرى لمجابهة الدول الكبرى. ومن بين هذه البحوث، نذكر بحث ريتشارد بيتزنغر بعنوان "الابتكار العسكري التكنولوجي في الدول الصغيرة: حالة إسرائيل وسنغافورة"[2]؛ إذ يرى أن إسرائيل وسنغافورة تسعيان إلى خلق ابتكارات عسكرية - تكنولوجية حاسمة وقادرة على تمكين السيادة الاستراتيجية، وحفاظ كلا البلدين على مستويات جيدة من الدعم للبحث والتطوير العسكري لصيانة الصناعات الدفاعية المحلية وإدامتها. إلّا أن إسرائيل كانت أكثر نجاحًا في الابتكار التكنولوجي العسكري، وذلك لأن وضعها الاستراتيجي أكثر هشاشة من وضع سنغافورة بسبب دول الطوق العربية المحيطة بها. في حين أنّ سنغافورة لا تواجه تهديدًا مباشرًا مثل إسرائيل، ومن ثمّ فإن نشاطات الابتكار التكنولوجي العسكري أقل بالمقارنة مع إسرائيل، ويبقى دافعها الوحيد هو الرغبة في امتلاك التكنولوجيا فقط[3].

ومن ثمّ، فإنّ أحد أهداف هذا البحث هو إضافة معلومات وأدبيات بمنظور مختلف لإثراء القيمة الأكاديمية في هذا الحقل المعرفي[4]، ومعرفة كفاءة المنظومات الاستراتيجية المتطوّرة تكنولوجيًا، وقدرتها على مجابهة المنظومات الأخرى، وإثبات أنّ الدول الصغرى التي تمتلك التكنولوجيا العسكرية قادرة على ردع الدول الكبرى ذات العمق الاستراتيجي. مع التركيز على محورَين جوهريين يغطّيان معظم الجوانب المهمة في هذا المجال، والمتعلقة بتجليات تأثير تطور التكنولوجيا العسكرية في الجيوش الحديثة، وكيفية استخدام الدول الصغرى التكنولوجيا العسكرية بوصفها سلاحًا استراتيجيًا لحماية نفسها من بطش الدول الكبرى.

يعتمد البحث كذلك على نظرية الثورة في الشؤون العسكرية؛ إذ إنّ مفهوم الصراع في هذه الحالة يقتضي التعامل مع أسوأ الاحتمالات (Worst Case Scenarios)[5]، ولذلك تبني الدول قراراتها بناءً على التهديدات المحتملة، وطالما أنّ التكنولوجيا العسكرية تخدم الهدف الرئيس لردع المخاطر والتهديدات، فنظرية

2 Richard A. Bitzinger, "Military-technological Innovation in Small States: The cases of Israel and Singapore," *Journal of Strategic Studies*, vol. 44, no. 6 (2021), pp. 873-900.

3 Ibid.

4 Warren Chin, "Technology, War and the State: Past, Present and Future," *International Affairs*, vol. 95, no. 4 (2019), pp. 765-783.

5 عمران عمر علي، "الصراع والتعاون في العلاقات الدولية: الإسهامات النظرية للنقاش بين الواقعية الجديدة وبين الليبرالية الجديدة"، **مجلة العلوم الإنسانية لجامعة زاخو**، مج 8، العدد 4 (كانون الأول/ ديسمبر 2020)، ص 659-670.

الثورة في الشؤون العسكرية أكثر ملاءمة واتساقًا مع الموضوع المطروح وتصب في الإطار نفسه[6]. وكذلك يتوافق البحث مع "نظرية الدول الصغرى" (Small State Theory)، من منطلق أن هذه الدول غير قادرة على التغلب على نقاط ضعفها مثل غياب العمق الاستراتيجي، خصوصًا إذا كانت محاطةً بدول كبرى ذات أطماع، حيث تلجأ الدول الصغرى إلى تعويض ذلك النقص بامتلاك المنظومات الاستراتيجية المتطورة تكنولوجيًا للدفاع عن نفسها من خلال ردع التهديدات ومخاطر الدول المجاورة[7].

أولًا: التطور التكنولوجي ونظرية الثورة في الشؤون العسكرية

يُستخدم مفهوم التطور التكنولوجي الذي مثّل نقاشات أكاديمية وفكرية موسّعة ومستمرّة، بوصفه مزيجًا من المعارف والعلوم والبحث والتطوير المستمرين، لوضع حلول للمشكلات وتسهيل الإجراءات لخلق فرص أفضل ولتحقيق رفاهية الشعوب، إضافة إلى مواكبة الإيقاع السريع للحياة الحديثة، وذلك من خلال تسخير الحواسيب والأجهزة الذكية القادرة على تلبية الرغبات والوصول إلى الأهداف المرجوّة[8]. يضاف إلى ذلك أنّ التطور التكنولوجي زاد من فاعلية الأسلحة العسكرية، ومنحها بعدًا استراتيجيًا؛ ما ساهم في تعزيز نظرية الثورة في الشؤون العسكرية، وأصبحت الأسلحة المتطورة تكنولوجيًا تُعرف بالأسلحة التكنولوجية الذكية.

إلّا أن الأمر قد يصبح أكثر تعقيدًا عندما يتعلّق بمفهوم الحروب الحديثة، تلك الحروب التي يصعب التنبؤ بحدوثها أو تقييم أضرارها، خصوصًا أنّها مخفيّة نوعًا ما، وتتّصف بالضبابية وعدم اليقين. فالحروب الحديثة تحتاج إلى الأسلحة التقليدية، كالدبابات، والمدرعات، والأسلحة الثقيلة، والترسانات العسكرية الضخمة، ولكن ليس بالشكل الذي كان عليه الحال في الحروب التقليدية؛ لأن استخدام السلاح التقليدي سيكون أقل نوعًا ما في الحروب الحديثة، وستحلّ محلّه تدريجيًا الأسلحة التكنولوجية المتطورة. ويرى وسيم أحمد أن الادوات المستخدمة في الحروب الحديثة التي تعتمد على التقنية والتكنولوجيا المتطوّرة كفيلة بتدمير اقتصاد الدول وتجويع الشعوب[9]، وتدمير البنى التحتية، كالحروب السيبرانية على شبكات الاتصالات ومراكز البيانات، وتعطيل سكك القطارات، من خلال التلاعب بالأنظمة التي من الممكن أن تتسبب في ضرر الممتلكات والأرواح والتلاعب بأنظمة

6 James E. Dougherty & Robert L. Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey*, 3rd ed (New York: Longman, 2001), p. 82.

7 Christine Ingebritsen et al. (eds.), *Small States in International Relations*, Series: New Directions in Scandinavian Studies (Seattle: University of Washington Press/ University of Iceland Press, 2006), pp. 300-342.

8 Mihaela Diaconu, "Technological Innovation: Concept, Process, Typology and Implications in the Economy," *Theoretical and Applied Economics*, vol. XVIII, no. 10 (2011), pp. 127-144.

9 Waseem Ahmad Qureshi, "Fourth-and Fifth-Generation Warfare: Technology and Perceptions," *San Diego International Law Journal*, vol. 21, no. 1 (Fall 2019), p. 187.

التدفئة في الدول الباردة[10]. ولعل ما قامت به روسيا في مطلع عام 2022 من أنشطة سيبرانية وكهرومغناطيسية ضد أوكرانيا وبعض الدول المجاورة خير دليل على ذلك.

كل ذلك ممكن أن يحصل بدون خسارة العديد من الجنود أو ربما بدون أرض معركة، وهنا يكمن خطر تلك المنظومات المطوّرة تكنولوجيًا؛ إذ إنها نوعًا ما أقل تكلفةً وأكثر فاعلية[11]. إضافة إلى حروب القوى الحادة (Sharp Power)، مثل القنوات الإخبارية ومنصّات التواصل الاجتماعي، التي تعمل على تأليب الرأي العام، وتشكيل التحالفات من أجل التضييق على بعض الدول، كالحصار والعقوبات الاقتصادية[12]، والعديد من الوسائل الأخرى بالغة الضرر التي لا تقل تأثيرًا عن التدمير والقتل. هذا مع عدم نكران أن الحروب التقليدية ما زالت قائمة، كالحرب في سورية، وحرب اليمن، وحروب إسرائيل على فلسطين، على غرار الحرب الأخيرة على غزّة عام 2021.

1. الثورة في الشؤون العسكرية

عرّف روبرت توماس (Robert R. Tomes) الثورة في الشؤون العسكرية بأنها "التغير الذي طرأ على طبيعة القتال بسبب استخدام التطبيقات التكنولوجية الجديدة، إضافة إلى التغيرات في إدارة العمليات العسكرية"[13]. كما عرّفها وزير الدفاع الأميركي في إدارة بيل كلينتون (Bill Clinton) خلال فترة التسعينيات من القرن الماضي وليام كوهين (William S. Cohen) حين قال: إن "الثورة في الشؤون العسكرية أعطت جيوش الدول فرصةً لتحويل استراتيجياتها، مثل المذاهب العسكرية، والتدريب، والتعليم، والتنظيم، والتجهيز، والعمليات والتكتيكات لإنجاز النتائج العسكرية الحاسمة بطرق جديدة"[14]. أمّا الباحث الأميركي كولن غراي (Colin S. Gray)، فقد قدّم تعريفًا عامًا يتمثّل في "التغير الراديكالي في خاصية وسلوك الحرب"[15].

وعلى غرار العديد من الظواهر التي تظهر بين الفينة والأخرى، مرّت ظاهرة "الثورة في الشؤون العسكرية" بعدة مراحل؛ إذ بدأت بثورة البارود في القرن الثالث عشر، تلتها ثورة المشاة، وتسارع التطور بدخول مرحلة الثورة الصناعية التي كان لها إسهامات في تعزيز المنظومات الدفاعية، بوساطة صناعة المدرعات والطائرات، وصولًا إلى الثورة النووية في نهاية الحرب العالمية الثانية في عام 1945، وأخيرًا، دخول مرحلة ثورة المعلومات التي تزعّمتها الولايات المتحدة الأميركية، حيث اعتمدت اعتمادًا كليًا على الاتصالات ورقمنة ساحات المعارك والقتال الشبكي المرتبط مع مراكز

10 رياض مهدي عبد الكاظم وآلاء طالب خلف، "المعلوماتية والحروب الحديثة: دراسة حالة الحرب الأمريكية على العراق عام 2003"، **مجلة واسط للعلوم الإنسانية**، مج 11، العدد 30 (2015)، ص 181-212.

11 المرجع نفسه.

12 منعم صاحي العمار وعلي محمد امنيف الرفيعي، "المتغيرات المؤثرة في استخدام الولايات المتحدة الأمريكية للقوة الناعمة بعد أحداث 11 أيلول 2011"، **قضايا سياسية**، العدد 42 (2015)، ص27-48.

13 مصباح عامر، **تطور علم الاستراتيجية** (القاهرة: دار الكتاب الحديث، 2017)، ص 500-550.

14 مصباح عامر، **نظرية العلاقات المدنية العسكرية: الحالات التطبيقية في التحليل الاستراتيجي** (القاهرة: دار الكتاب الحديث، 2018)، ص 300-314.

15 المرجع نفسه.

القيادة والسيطرة والبرمجيات[16]، وأصبح القادة وجنرالات الجيش الأميركي قادرين على قيادة المعارك عن بعد (Remotely) من خلال غرف العمليات الموجودة في الولايات المتحدة من خلال الربط الإلكتروني، حيث يجري توجيه الألوية والكتائب المقاتلة المزودين بكاميرات تتيح للقادة التوجيه والقيادة من الخلف وكأنهم على أرض المعركة الحقيقة. كما في حرب الخليج الثانية عام 1991، التي استُخدمت فيها أنظمة الاستخبارات بشقّيها (SIGINT & ELINT) والمراقبة والاستطلاع (C4ISR)، والصواريخ الموجهة عن بعد (Guided Missiles).

لا غرابة إذًا في أنّ بعض الدول تسعى إلى تعزيز قدراتها والحصول على موطئ قدم في ثورة الشؤون العسكرية بهدف مجاراة قوة المتنافسين ومحاولة التفوق على الأعداء وتعزيز قوة الردع (Deterrence). فقد نشأت ظاهرة "الثورة في الشؤون العسكرية" بسبب المنافسة المحمومة والمستمرة بين الفواعل الدولتية والفواعل غير الدولتية؛ إذ إن الدول والمنظمات الدولية بوصفها فواعل دولتية في تنافس مستمر مع الفواعل غير الدولتية مثل المنظمات الإرهابية، ولذا تحرص الفواعل غير الدولتية على الحصول على الأسلحة المتطورة والتكنولوجيا الحديثة التي تضاهي ما تمتلكه الفواعل الدولتية، مثل ما حصل في العراق عندما استطاع تنظيم الدولة الإسلامية في العراق والشام "داعش" الحصول على الصواريخ الحرارية الموجهة. وفي المقابل، نجد أن الفواعل الدولتية تحاول منع تلك المنظمات من امتلاك الأسلحة بالتعاون مع المنظمات الدولية، من خلال حظر الأسلحة، وتنفيذ العقوبات على المنظمات والجماعات ذات الصلة؛ ما دفع العديد من الدول إلى التحديث المستمر لمنظوماتها العسكرية، وتعديل استراتيجياتها الدفاعية بما يتناسب مع التحديات الجديدة، إضافة إلى التنافس بين الفواعل الدولاتية الذي نشهده بين الفينة والأخرى على الساحة الدولية[17].

بعد التمعّن في هذه التعريفات والمفاهيم والتسلسل التاريخي والمقاربات، نستنتج أن الثورة في الشؤون العسكرية قد تكون عبارةً عن تطوير الجانبين النظري والتطبيقي من خلال التطور التكنولوجي للحصول على أسلوب حربي أو قتالي يمكن استخدامه في المعارك، والذي قد يؤثر إيجابيًا في المفاهيم العملياتية للجيوش في إدارة العمليات العسكرية لتحقيق الأهداف المرجوة بفاعلية ومرونة عاليتين، إضافة إلى حماية أرواح الجنود والخروج من المعارك بخسائر أقل وتحقيق أهداف أكثر[18].

2. العلاقة بين التكنولوجيا والحروب الحديثة

ركّز ورين شين في تناوله العلاقة بين التكنولوجيا والحروب الحديثة على ازدهار العلاقة التي نشأت بين الدولة والحرب على مدى القرون الأربعة الماضية. ومع ذلك، فقد جرى كبح هذا التوسع من خلال انخفاض وتيرة الحرب

16 حنان دريسي، "الثورة في الشؤون العسكرية وتداعياتها على السياسات الدفاعية للدول"، **المجلة الجزائرية للدراسات السياسية**، مج 8، العدد 2 (2021)، ص 184-201.

17 المرجع نفسه.

18 المرجع نفسه.

بين الدول وحجمها بعد عام 1945؛ ما سمح في النهاية بظهور أولويات سياسية واقتصادية جديدة أدت إلى إعادة تشكيل الدولة وتغيير دورها. ويرى الكاتب أن دور التكنولوجيا في الحرب زاد على نحو كبير بسبب الثورة النووية. وفي هذا السياق، قلل التطور التكنولوجي من فرص الحرب، علمًا أنّ سباق التسلح أدى أيضًا إلى ظهور تقنيات جديدة، وأثرت هذه التطورات في فهم طبيعة الحرب وتفاعلها مع الدولة[19].

ويرى محمد كريم كاظم وبراء عبد القادر وحيد في بحثهما المعنون بـ "التطور التكنولوجي والحرب" أنّ تأثير التطور التكنولوجي في الحروب الحديثة هو أهم ما يميز العالم المتطور هذه الأيام؛ لأنّ عامل التفوق الذي غيّر مجرى الحروب ولّدته القدرة التكنولوجية العسكرية[20]. وبسبب التغيّر المستمر في وسائل الحروب وأساليبها، تجلّى الدور الحيوي للتكنولوجيا في كفاءة المؤسسات العسكرية، وأصبحت كذلك من أولويات قادة الحروب وواجباتهم؛ الأمر الذي شجّع العديد من الدول على استغلال طاقاتها في التطور التكنولوجي. ولعلّ من أبرز ما جاء في هذا البحث أنّ "تكنولوجيا عالية ومتفوقة تعني النصر، وتكنولوجيا متدنية تعني الهزيمة"؛ بيد أنّ تلك المقولة ليست قاعدةً حربية يمكن الاعتماد عليها، وهي غير صحيحة في أغلب الأحيان[21].

كما ظهر على السطح نوعٌ آخر من الحروب الطاحنة التي تواكب العصر الحديث، وقد أُطلق عليها العديد من المسمّيات مثل "الحروب الحديثة"[22]، وهي كما يرى العديد من الخبراء العسكريين، مثل بارت شورمان، لا تقل خطرًا عن الحروب التقليدية[23]، حتّى إن لم تكن هناك مشاهد دموية تُبثّ على وسائل الإعلام[24]؛ ومنها "الحروب الإلكترونية" التي ساهم التطور التكنولوجي في وجودها. ولم تعد الحروب الحديثة - نوعًا ما - بحاجة إلى الجنود في أرض المعركة (Foot On Ground) لإحداث الضرر في صفوف العدو[25]، بل أصبح من السهل تعطيل المنظومات العسكرية وتدميرها من خلال زرع البرمجيات الخبيثة فيها[26]، أو التضليل الإلكتروني من خلال إرسال عدد هائل من البيانات الرقمية

19 Chin.

20 محمد كريم كاظم وبراء عبد القادر وحيد، "التطور التكنولوجي والحرب"، **مجلة دراسات دولية**، العدد 45 (2010)، ص 153-158.

21 المرجع نفسه.

22 Stephenie Gosnell Handler, "New Cyber Face of Battle: Developing A Legal Approach to Accommodate Emerging Trends in Warfare," *Stanford Journal of International Law*, vol. 48, no. 1 (2012), pp. 209-237.

23 Bart Schuurman, "Clausewitz and the 'New Wars' Scholars," *The US Army War College Quarterly: Parameters*, vol. 40, no. 1 (2010), pp.. 89-100.

24 نواف موسى مسلم الزيدين، "مدى مشروعية الحرب الوقائية على أفغانستان والعراق في القانون الدولي"، **مجلة كلية الشريعة والقانون بتفهنا الأشراف - دقهلية**، العدد 23، ج 4 (2021)، ص 3033-3060.

25 Daniel E. Sutherland, *A Savage Conflict: The Decisive Role of Guerrillas in the American Civil War* (Chapel Hill: University of North Carolina Press, 2006), pp. 1-46.

26 البرامج الخبيثة هي برامج رقمية يجري إعدادها سلفًا بوساطة مبرمجين ذوي خبرة في مجال الاختراقات، وهم يضعون تلك البرامج في المنظومات المستهدفة، إمّا يدويًا وإمّا من خلال إرسال الروابط إلى الجهة المستهدفة، بغرض تعطيلها أو تدميرها بالكامل. يُنظر: قاسم قبلان وأحمد عاقل، "تحليل وكشف البرمجيات الخبيثة في أنظمة التشغيل للهواتف الذكية دراسة حالة نظام التشغيل (أندرويد)"، **مجلة جامعة تشرين للبحوث والدراسات العلمية**، مج 39، العدد 3 (2017)، ص 425-437.

المتداخلة من أجل إعطاء قراءات خاطئة، أو حجب تلك المعلومات عن الطرف المستخدم لتلك الأنظمة[27]، أو الحصول على معلومات العدو من خلال الهجمات الإلكترونية التي تقوم بها أجهزة الحواسيب عبر الشبكة العنكبوتية والاتصالات الرقمية بهدف تعطيل البرامج أو التلاعب بها أو استهداف البيانات بغرض سرقتها أو تدميرها، واختراق الأنظمة وأوامر التحكم، بهدف إلحاق الأضرار البالغة بأنظمة برامج الطرف الآخر وحواسيبه[28]، إضافة إلى استخدام السلاح الكهرومغناطيسي؛ إذ تُستخدَم طاقة الإشعاع الكهرومغناطيسي لتسريع القذيفة بغرض ضرب الهدف وتدميره[29]، كما يُستخدم بديلًا من المتفجرات، مع إمكانية استخدامه لتحريض التيارات عالية الجهد، وتعطيل المعدات والآلات الكهربائية والإلكترونية بسبب الجهد العالي، أو التسبب بآلام البشر وأوجاعهم؛ إضافة إلى وجود أسلحة كهرومغناطيسية آمنة لاستخدام البشر، تُستعمَل لتعطيل آليات العدو[30].

في خضمّ هذا التطور التكنولوجي والتقني الذي أحدث قفزةً نوعية في الحروب الحديثة، ما زال العنصر البشري هو العنصر الأساسي في كسب الحروب، وليس الآلة أو السلاح المطوّر تكنولوجيًا؛ لأنه هو الذي يبتكر الأسلحة ويُطوِّر من خلال تطويع التكنولوجيا (Technology Adaptation) لتحقيق الأهداف والأغراض العسكرية، وهو المسؤول الأوّل عن الصيانة والإدامة للوصول إلى الاستخدام العملياتي ذي الكفاءة العالية، ويوظّف التكنولوجيا من خلال تحويلها من الطابع المدني إلى الطابع العسكري، مثل الاستخدام في الأغراض العسكرية، كما جرى مؤخرًا في الحروب الحديثة؛ كاستخدامها للاستطلاع والمراقبة أو تحميلها قنابل أو متفجرات[31]. وما زالت التكنولوجيا تحتاج إلى المخطط والمفكّر العسكري صاحب الخلفية التقنية، كالمهندسين وخبراء الأمن السيبراني وتقنية المعلومات الذين يستطيعون أن يستخدموا تلك التكنولوجيا الاستخدام الأمثل، مثل توظيف الذكاء الاصطناعي (Artificial Intelligence) للأغراض العسكرية، وذلك من خلال تغذية منظومات الذكاء الاصطناعي بالمعلومات المراد معرفتها، وتحليلها؛ مثل الطائرات المقاتلة والدبابات والصواريخ والآليات العسكرية[32]، بحيث تحفظ تلك المنظومات المعلومات والبيانات التي جرى استقبالها في قواعد البيانات الخاصة بها (Data Center)، وتجري معرفتها وتحليلها في العمليات العسكرية الحقيقية؛ وهذه العملية تُسمّى عملية تأهيل المنظومة وتعليمها (Machine Learning).

27 بشرى معلا وهيثم الرضوان وعلاء محفوض، "دراسة تحليلية لتأثير أنواع هجوم التشويش على أداء شبكات Ad Hoc"، **مجلة جامعة تشرين**، مج 41، العدد 5 (2019)، ص 81-98.

28 سارة عبد العزيز، "الحرب السيبرانية: التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية"، مجلة **اتجاهات الأحداث**، العدد 20 (2017)، ص 1-12.

29 Martin van Creveld, "Modern Conventional Warfare: An Overview," *Hebrew University, Jerusalem* (2004), pp. 1-14.

30 Tom E. Bearden, "Scalar Electromagnetic Weapons and Their Terrorist Use," *World Affairs: The Journal of International*, vol. 9, no. 4 (2005), pp. 58 - 85.

31 Ibid.

32 سامح راشد، "الذكاء الاصطناعي في مواجهة الإرهاب: فرص وتحديات"، مجلة **درع الوطن** (2022)، ص 89-95.

ثانيًا: خصائص الحروب الحديثة وأدواتها

يقول المنظر العسكري في القرن التاسع عشر كارل فون كلاوزفيتز (Carl von Clausewitz): إن "الشكل السائد للحرب يعكس دائمًا العصر الذي يحدث فيه"[33]؛ لذلك تجد أنّه في كل فترة زمنية قصيرة يجري الإعلان عن دخول سلاح متطور جديد لساحات المعارك تحت مُسمَّى جديد، أو أسلوب جديد، أو كيفية جديدة، إلى أن أصبحت هناك أسلحة ذكية يُستخدَم فيها الذكاء الاصطناعي. ولأن الحروب الحديثة ترتبط ارتباطًا وثيقًا بالعصر التي تحدث فيه، فإن التطور التكنولوجي فرض عليها العديد من المتغيرات والمتطلبات الملحّة التي لا يستغني عنها المحللون والمخططون الاستراتيجيون والقادة المعنيون بخوض تلك الحروب في ساحات المعارك، ومن أهمها سرعة الحركة، ودقة التصويب، والاستطلاع الاستخباري، والتحليل الدقيق للمواقف العسكرية بهدف الوصول إلى تقدير دقيق للمواقف العسكرية، والتخطيط السليم للعمليات العسكرية المضادة[34].

ومن ثمّ، لا بدّ من تطويع التكنولوجيا بطريقة معينة تكفل الحصول على سلاح ذكي أو منظومة استراتيجية قادرة على التعامل مع التحديات والمخاطر على أرض الواقع، والتي تتغير بتغير المكان والزمان[35]؛ وهو ما أزاح الستار عن العديد من المنظومات العسكرية المتطورة تكنولوجيًا، والتي جرى ذكرها في بداية هذا البحث.

1. أثر استخدام الأقمار الصناعية وأنظمة المراقبة والاستطلاع

لم يكن للولايات المتحدة الأميركية عنصر السبق في ما يخص جمع المعلومات وتحليلها؛ إذ لم تبدأ في هذا المجال إلّا في الفترة التي أعقبت الحرب العالمية الثانية، وتحديدًا مع بداية الحرب الباردة؛ ما أتاح الفرصة للمملكة المتحدّة والاتحاد السوفياتي اللذين أسّسوا وكالاتهم الاستخباراتية في العقدين الأول والثاني من القرن العشرين التفرّد بتلك الميزة حتى ذاك الحين، وهو ما لاحظه الرئيس الأميركي آنذاك هاري ترومان (Harry Truman) من خلال خوض بريطانيا غمار العمليات الاستخبارية في الحرب العالمية الثانية التي انتهت لصالحها وصالح قوّات الحلفاء[36]؛ لذلك قرر ترومان البدء في تأسيس جهاز الاستخبارات الخارجية الأميركية في عام 1941، وسُمِّي بمكتب الخدمات الاستراتيجية في عام 1942، ثم لاحقًا سُمِّي بـ "وكالة المخابرات المركزية" (CIA)، مستفيدًا من خبرة أصدقائه في جهاز الاستخبارات البريطانية الذين ساهموا في تأسيس وكالة الاستخبارات الأميركية من خلال نقل الخبرة (Knowledge Transfer) إلى عناصر الاستخبارات الأميركية، وإعدادهم إعدادًا جيدًا يمكّنهم من العمل على نحو احترافي[37].

33 Carl von Clausewitz, *On War*, Michael Howard & Peter Paret (Trans.) (Oxford & New York: Oxford University Press, [1976] 2006), pp. 50-87.

34 عبد الكاظم وخلف.

35 فيفيان والت، "كيف يتم تطويع التكنولوجيا في الدفاع عن أوكرانيا؟"، **فورتشن العربية**، 2022/5/18، شوهد في 2023/1/2، في: https://bit.ly/3CfUGBL

36 زلمي خليل زاد وجون وايت (محرران)، **الدور المتغير للمعلومات في الحرب**، سلسلة دراسات عالمية، العدد 53 (أبوظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2004)، ص 28.

37 Richard E. Schroeder, *The Foundation of the CIA: Harry Truman, the Missouri Gang, and the Origins of the Cold War* (Columbia, Missouri: University of Missouri Press, 2017), pp. 107-145.

فالمعلومات مهمّةً جدًا لصناعة كل قرار سليم يصدر من رأس الدولة أو القيادات العليا للجيش، وبدون المعلومة الصحيحة لن يكون باستطاعة صانعي القرار من السياسيين أو العسكريين اتخاذ القرارات الصحيحة مهما بلغت براعتهم وحنكتهم، فالمعلومات الصحيحة ترسم الطريق الصحيح؛ ومن ثمّ، تكمن أهمية المعلومة الاستخباراتية بحساسيتها وقدرتها على قلب موازين المعارك، والحربان العالميتان الأولى والثانية خير دليل على ذلك[38].

توصّلت التكنولوجيا الحديثة إلى أدوات ووسائل ساعدت على تطوير فاعلية الاستخبارات، مثل المراقبة والاستطلاع، وهي المنظومة الأساسية للجيوش الرقمية الحديثة، وتستطيع هذه المنظومة القيام بعدد من المهمات والقدرات الاستخبارية، مثل استخبارات الإشارة (Signals Intelligence, SIGINT)، وهي استخدام منصات التجسس الإلكتروني مثل الأقمار الصناعية وطائرات التصوير والإنذار المبكر والرادارات ومحطات التجسس الأرضية للحصول على المعلومات والبيانات المهمة، علمًا أنّ استخبارات الإشارة تُقسم قسمين أساسيين: استخبارات الاتصالات (Communications Intelligence, COMINT)، والاستخبارات الإلكترونية (Electronic Intelligence, ELINT)[39].

الهدف الرئيس لمنظومات الاستخبارات الخاصة بالاتصالات هو اعتراض الإشارات والاتصالات للجيوش المعادية، بغرض استخلاص المعلومات عن طريق التنصّت عليها، وتحديد أماكن الوحدات المقاتلة وكشف مواقع الدبابات والطائرات والرادارات، إضافة إلى اعتراض اتصالات الأقمار الصناعية وفكّ تشفيرها (Encryption) بوساطة أنظمة برمجية متطوّرة تعمل على فك رموزها (Decryption) وتحويلها إلى أصوات مسموعة ورسائل نصيّة[40]. كما تتتبّع أنظمة الاستخبارات الإلكترونية الموجات الكهرومغناطيسية المنبعثة من أنظمة مجسّات العدو، مثل الرادارات الأرضية والبحرية والجوية، وتحدد مواقعها وترددداتها. لذلك فإن المحطات الأرضية (Ground Segment) تتلقّى الإشارات من المحطات الفضائية بوساطة العديد من القباب الكروية وصحون الاتصالات التي تحتوي على الإلكترونيات والبرمجيات المتطورة، وتستخدم للتتبع والتنصت على المكالمات الهاتفية والبريد الإلكتروني، إضافة إلى طائرات القيادة والسيطرة والاستخبارات الإلكترونية المجهزة بمجسّات لرصد الأهداف العدائية من مسافات بعيدة تضمن توفير درجة كافية من الإنذار المبكر، من أجل أن تكون القوات المضادّة على أهبة الاستعداد[41].

وبفضل التكنولوجيا المتطوّرة التي أوجدت المنظومات المذكورة أعلاه، جرى التوصّل إلى حلول لتلك المشاكل من خلال استخدام الأقمار الصناعية لتقنية المستشعرات، أو ما يُسمّى

38 علي علواني، "دور أنظمة القيادة والسيطرة في الحروب الحديثة: مستقبل أنظمة القيادة والسيطرة"، **درع الوطن**، العدد 480 (2021)، ص 60-69.

39 Linda Dawson, *War in Space: The Science and Technology Behind Our Next Theater of Conflict* (Cham: Springer-Praxis Books, 2018), pp. 131-157.

40 قبلان وعاقل.

41 مصباح عامر، **تطور علم الاستراتيجية** (القاهرة: دار الكتاب الحديث، 2017)، ص 500-550.

بأنظمة الاستشعار عن بعد التي تستطيع أن تزوّد أصحاب القرار والقادة العسكريين بالصور ذات الجودة العالية، وبسرعة كبيرة ودقّة عالية تشمل كل التفاصيل التي تمكّنهم من معرفة تحركات العدو، وقوام جيشه، والقوات المستخدمة فيه، وتقدير الوقت المستغرق لوصوله للمناطق الحدودية، بهدف الاستعداد وكيفية التعامل مع الأسلحة المستخدمة[42].

2. أثر أنظمة الهجوم والدفاع الإلكتروني

تقوم أنظمة الهجوم الإلكتروني (EA) بعد استقبالها المعلومات من نظم الدعم والإسناد الإلكتروني في استخبارات الاتصالات (COMINT) والاستخبارات الإلكترونية (ELINT) بمحاولة تحييد الدفاعات الجوية للعدو، وتعطيل أنظمة الشبكات والاتصالات الخاصة به[43]، ويعود الفضل إلى حواضن التشويش والإعاقة التي لديها المعلومات الدقيقة عن مواقع الوحدات المقاتلة ومراكز سيطرتها ونطاق عملها وشفراتها وتردداتها، وهذا يعطي المنصات الهجومية الإلكترونية فرصة إطلاق حزمات موجية كهرومغناطيسية مباشرة عالية التردد تشوّش على اتصالات مراكز قيادة العدو وسيطرته؛ وقد يطول التشويش منظومات الأقمار الصناعية والدفاع الجوي والرادارات والإنذار المبكر؛ ما يؤدي إلى التحييد الجزئي أو الكلي، مسببًا إرباكًا لحركة القوات بسبب عدم الانسجام وتداخل القرارات وغياب التنسيق بين أفرع الجيش المختلفة[44].

كما تؤدي موجات التشويش التي تبثُّها أنظمة العدو باستمرار إلى انقطاع الاتصالات وتوقّف الرادارات عن العمل، وهذا يؤدي إلى تعطّل صواريخ الدفاع الجوي والمنظومات الأخرى، ممهّدًا الطريق لقوات العدو لشنّ الهجوم المُخطط له سلفًا، بعد التأكّد من فاعلية الهجمات الإلكترونية بتدمير أنظمة الأهداف الحيوية والمنشآت والمطارات ومنصّات الدفاع الجوي ومراكز القيادة والسيطرة (C2) ومقرّات الإعداد والتعبئة وقواعد الصواريخ ومراكز المخابرات وتحييد رادارات الإنذار المبكر والرادارات الأرضية والبحرية، وأخيرًا، تبدأ الضربات الصاروخية على الأهداف الحيوية وتتقدم القوات البرية محدثةً ثغرات في الصفوف الأولى بوساطة الدبابات والمدفعية والمشاة بغية احتلال الأرض وفرض سياسة الأمر الواقع[45]. لذلك لا شك في أن التفوق العسكري الإلكتروني يحتوي على مزايا استراتيجية تمهّد للتعامل مع الجيوش القوية بكفاءة عالية وبأقل قدر ممكن من التكلفة المادية والبشرية. ولذا تهتم الجيوش بأنظمة الحرب الإلكترونية (EW)، وتضمّها إلى منظوماتها؛ كطائرات الحرب الإلكترونية (RC-135) و(EC-130) و(Beechcraft)[46].

وتعتبر أنظمة الدفاع الإلكتروني خطّ الدفاع الأول لحماية منظومات الاتصالات والصواريخ،

42 Jesse Casana & Elise Jakoby Laugier, "Satellite Imagery-Based Monitoring of Archaeological Site Damage in The Syrian Civil War," *PLOS ONE*, vol. 12, no. 11 (2017).

43 جاد، ص 28-30.

44 المرجع نفسه.

45 James M. Acton, "Debating Conventional Prompt Global Strike," *Carnegie Endowment for International Peace* (October 3, 2013), pp. 1-8.

46 Ibid.

وتقوم بالعديد من الاحترازات والإجراءات الإلكترونية في سبيل الوقاية من الهجمات الإلكترونية وتقليل الآثار السلبية للتشويش، وتقلل كذلك من محاولة التتبع والاختراقات، كما توّفّر الحماية من الهجمات الصاروخيّة؛ إذ تزوّد الطائرات العسكرية بأنظمة الحماية الإلكترونية التي تُطلق تحذيرًا ينبئ بوجود صواريخ حرارية موجّهة في نطاق معيّن، إضافة إلى أنها قادرة على تضليلها بوساطة مجسّات الليزر التي توجّه صواريخ العدو إلى مطاردة أهداف غير حقيقة في سبيل توفير نطاق آمن لطائراتها والطائرات الصديقة، مثل المنظومة الفرنسية (Spectra)، والمنظومة الإسرائيلية (C-Music)، والمنظومة الروسية (President). وكذلك تقوم منظومات الدفاع الإلكتروني بعملية الشراك الخداعية الصوتية التي تحدث مصدرًا ضوضائيًا مزيّفًا يعمل على تضليل صواريخ وطوربيدات العدو، ويدفعها للخروج بعيدًا عن مسار حركة الغواصات والسفن[47]، وأخيرًا، القدرة على إنشاء مراكز القيادة والسيطرة والاتصالات المتحركة البديلة لتعمل بوصفها مراكز قيادة بديلة في حال قصف مراكز القيادة والسيطرة والاتصالات الرئيسة أو تدميرها، وضمان تواصل القيادة مع أفرع الجيش كافة في أثناء العمليات العسكرية[48].

47 Antonio Grilo et al., "Electronic Protection and Routing Optimization of MANETs Operating in An Electronic Warfare Environment," *Ad Hoc Networks*, vol. 5, no. 7 (September 2007), pp. 1031-1045.

48 Shubhashis Sengupta & K. M. Annervaz, "Multi-Site Data Distribution for Disaster Recovery: A Planning Framework," *Future Generation Computer Systems*, vol. 41 (December 2014), pp. 53-64.

3. استخدام قوّات الحرب الإلكترونية والفضاء السيبراني

تعدّ قوات الحرب الإلكترونية ذلك السلاح الصامت من أهم مقوّمات النجاح التي تُستخدم على نطاق واسع في الحروب الحديثة؛ لأنها أصبحت من الضروريات، ولا تقلّ أهميةً عن الصاروخ والقنبلة وباقي الأسلحة الأخرى ذات الضرر البالغ. ولعل ما يمكن أن يُستشهد به في هذا الجانب تدخّل روسيا في حرب سوريا في عام 2015[49]؛ إذ إنّ الولايات المتحدة لم تكن على دراية تامة بقوّة الروس في مجال الحرب الإلكترونية، حيث استطاعت قوّة الحرب الإلكترونية الروسيّة التعامل مع الأسلحة الأمريكية الحديثة التي كلّف تصنيعها مليارات الدولارات من خلال التشويش المستمر على الرادارات الأمريكية؛ ما أدّى إلى بعض الصعوبات التي واجهها الطيارون الأميركيون، مثل فقد الاتصال المؤقت مع غرف العمليات[50].

يرى باتريك سميث أنّ الحرب الإلكترونية الروسية تعتبر تهديدًا للسيطرة الأميركية على ساحات الحروب؛ إذ إن الروس استفادوا من التجارب السابقة، خصوصًا بعد الفشل خلال الحرب الروسية - الجورجية بسبب سوء الإدارة والفساد المشتري والمعارضين للإصلاح قبل استلام فلاديمير بوتين الحكم[51]؛ إذ استفادت روسيا من

49 Dina Smeltz, Stepan Goncharov & Lily Wojtowicz, "US and Russia: Insecurity and Mistrust Shape Mutual Perceptions," *Chicago Council on Global Affairs* (November 2016), pp. 1-11.

50 Ibid.

51 Patrick Smith, "Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy," *American Security Project - Perspective* (April 2020), p. 3.

هذا الفشل واستغلته لصالحها من خلال التركيز على الابتكار وتطوير أسلحة الحرب الإلكترونية، خصوصًا أنه أتيحت الفرصة لتجربتها على الساحة السورية، من خلال تعطيل أجهزة الرادارات والصواريخ الموجهة الأميركية التي لم تكن قادرة على مواكبتها من خلال سباق التسلح وتفوّق القدرات العسكرية الأميركية. ويبيّن سميث استشعار المؤسسة العسكرية الأميركية الخطر الروسي المقبل من خلال قدرات الحرب الإلكترونية المختلفة التي تتمتّع بها روسيا، وكيف أن ذلك من الممكن أن يقلب الموازين بين القوى الكبرى، خصوصًا في ظل دخول دول قوية في هذا المعترك، مثل الصين، ومنح الأفضلية لروسيا. كما بيّن الكاتب قلق الولايات المتحدة ودقها ناقوس الخطر من هذه الحرب غير المرئية التي من الممكن أن تكبّدها خسائر باهظة، سواءً في الأرواح أو الممتلكات، أو في بسط النفوذ والسيطرة والسيادة[52].

ويسلط جيرمي هوفستر وآدم ويشوسكي الضوء على روسيا، وقدرتها على اكتشاف مواقع القيادة الأوكرانية، والتشويش عليها من خلال استخدام منصات الحرب الإلكترونية الخاصة بها. وربما يُعزى تراجع الأميركيين في مجال الحرب الإلكترونية إلى مكافحة الولايات المتحدة لأكثر من عشرين عامًا حروب مكافحة التمرد؛ ما أدّى إلى تضاؤل تركيز الجيش الأميركي على ممارساته وإجراءاته في الحرب الإلكترونية، بسبب انتقال الجيش للقتال في عمليات واسعة النطاق ضد هذه التهديدات. ويجادل هذا المقال بأنّ الجيش الأميركي كان يمتلك الخبرة والهيمنة الساحقة في الحرب الإلكترونية خلال سنوات الحرب في أفغانستان والعراق[53].

من الأمثلة التي يُستدلُّ بها: الحادثة التي وقعت عام 2014 للمدمّرة الأميركية (USS Donald Cook) في البحر الأسود في أثناء واجب تفتيشي دوري لحلف شمال الأطلسي (الناتو)، عندما قامت قوّة الحرب الإلكترونية الروسية بتعطيل الأجهزة والأنظمة الإلكترونية فيها[54]؛ وذلك بسبب مرور طائرة من طراز (SU-24) بالقرب من المدمّرة الأميركية عام 2014 في البحر الأسود؛ إذ أظهر الطيار البراعة والخبرة في الحرب الإلكترونية الروسية[55]؛ لأنه بمجرد اكتشافه المدمّرة، شغّل المعدات، وأبطل الموجات الإلكترونية الراديوية القوية لأنظمة السفينة، علمًا أنّه لا يوجد دليل واضح على استعمال حرب إلكترونية ضد السفينة[56]، بيد أن ذلك نبّه جنرالات الجيش الأميركي على ضعفهم الإلكتروني واستشعار الخطر الروسي القادم، وضرورة البدء فورًا في تطوير أنظمة هجومية مضادة للحرب الإلكترونية الروسية[57].

52 Ibid., p. 6.

53 Jeremy Hofstetter & Adam Wojciechowski, "Electromagnetic Spectrum Survivability in Large-Scale Combat Operations," *Infantry* (Winter 2020-2021), pp. 21-24.

54 Pavel Gudev, "Learning Lessons of Donald Cook," *Russia in Global Affairs*, 17/6/2016, accessed on 25/11/2022, at: https://bit.ly/3ieuShV

55 Ibid.

56 Sharyl Cross, "NATO–Russia Security Challenges in the Aftermath of Ukraine Conflict: Managing Black Sea Security and Beyond," *Southeast European and Black Sea Studies*, vol. 15, no. 2 (2015), pp. 151-177.

57 Ibid.

وفي حين أن قدرات الحرب الإلكترونية الروسية ظلّت غامضة (ربما بغرض التهويل والتخويف)، إلّا أن هذا لا يعني أن الولايات المتحدة لا تكترث بالتهديد الذي تشكله قوّة الحرب الإلكترونية الروسية، بل إنها أخذت هذا التهديد المحتمل على محمل الجد[58]. وفي هذا الصدد، يقرّ الخبيران يان كالبيرغ وستيفن هاملتون بأنّ روسيا قد طورت قدراتها القتالية في مجال الحرب الإلكترونية التي أضحت تؤدي دورًا حاسمًا في كيفية عمل الجيش الروسي[59]، ويبدو أن استخدامها الحرب الإلكترونية يشير إلى أن الكثير من هذا الاستثمار قد أسفر عن مزايا عملية. كما أن القائد السابق لوحدات الجيش الأميركي في أوروبا فيليب بريدلاف وصف "قدرة الحرب الإلكترونية الروسية في أوكرانيا بأنها قوية"[60]. وفي الواقع، يلاحظ بعضهم أن أسلحة الحرب الإلكترونية الروسية تتفوق على الأسلحة الأميركية من عدة جوانب[61].

فيما يخصّ الحروب السيبرانية، تغيّرت تلك الصورة النمطية التي تتجسّد في تسلسل الجنود إلى ما خلف خطوط العدوّ واختراق صفوفه بغية تدمير منشأة حيوية أو مقر مهم ذي قيمة عالية، كاختراق قناة إخبارية بهدف بث الإشاعات والأخبار الكاذبة، مثل ما حصل في اختراق وكالة الأنباء القطريّة "قنا" سنة 2017، وذلك لتسييس القضية من دول الحصار الأربع بغية كسب موقف سياسي، أو الحصول على تنازلات، أو تأليب الرأي العام من خلال شيطنة الخصم أمام المجتمع الدولي[62].

كما يرى دومنيك هيرمان أن الدول القومية تنخرط في التجسس السيبراني؛ لأنها تأمل في الحصول على المعلومات بدون وطء أرض العدو؛ وهو ما يجعل التجسس السيبراني جذابًا؛ لأنه أقل خطورة من التجسس التقليدي[63]. لذلك ينبغي معرفة أهداف الحماية الأساسية لأمن المعلومات، ومبادئ تصميم الأمان، والقدرة على التفكير بشأن الهجمات والدفاعات من خلال إنشاء منصّات دفاع وهجوم ومناقشة تداعيات القرصنة التي ترعاها الدولة[64].

استطاعت الدول من خلال الهجمات السيبرانية الاستغناء عن بعض الوسائل والأساليب والعمليات النوعية الخطيرة خلف خطوط العدو، أو اختراق منشآته الحيوية والتسلل إليها، والتي من الممكن أن يفقد الجنود فيها أرواحهم؛ إذ أصبح من الممكن القيام بتلك العمليات المؤثرة جدًا،

58 Muhammad Riaz Shad, "Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions," *Policy Perspectives: The Journal of the Institute of Policy Studies*, vol. 15, no. 2 (2018), pp. 41-55.

59 Jan E. Kallberg, Stephen S. Hamilton & Matthew G. Sherburne, "Electronic Warfare in the Suwalki Gap: Facing the Russian 'Accompli Attack'," *Forum/ Electronic Warfare in the Suwalki*, Gap JFQ 97 (2nd Quarter 2020), pp. 30-38.

60 Philip M. Breedlove, "NATO's Next Act: How to Handle Russia and Other Threats," *Foreign Affairs*, vol. 95, no. 4 (2016), pp. 96-105.

61 Ibid.

62 James Shires, "The Cyber Operation Against Qatar News Agency," in: *The 2017 Gulf Crisis,* Mahjoob Zweiri, Mizanur Rahman & Arwa Kamal (eds.), (Singapour: Springer Singapore, 2021), pp. 101-113.

63 Dominik Herrmann, "Cyber Espionage and Cyber Defence," in: Christian Reuter (ed.), *Information Technology for Peace and Security* (Wiesbaden, Germany: Springer Vieweg, 2019), pp. 83-106.

64 Ibid.

والقادرة على تكليف العدوّ فوق طاقته في بيئة آمنة بدون أدنى خطر[65]. وكمثالٍ على ذلك ما قامت به روسيا في آذار/ مارس 2022 حينما نفّذت هجمات سيبرانية شاملة أدّت إلى تعطيل بعض الأنظمة المهمة وتحييدها، واستهدفت المنشآت الحيوية كالمطارات؛ ما تسبب في إضعافها قبيل الزحف عليها من عدّة محاور، وذلك استعدادًا للغزو العسكري الشامل الذي تلا تلك العمليات السيبرانية بغضون أيام قليلة. ولم تقتصر تلك الهجمات السيبرانية على أوكرانيا فقط، بل شملت بعض الدول الأوروبية المعارضة للتدخل الروسي في أوكرانيا[66].

وما زالت تلك الأدوات - مثل استخدام المجال السيبراني الذي لا تكاد تخلو منه مؤسسة عسكرية، سواء أكانت من الفواعل الدولتية أم الفواعل غير الدولتية، ما عدا القلّة القليلة من دول العالم الثالث - محلًا للنقد المستمر كما يرى بعضهم؛ كوفاء لطفي وسنّي ذو الهدى اللذين ذهبا إلى أبعد من ذلك من خلال استخدام مصطلح "الإرهاب السيبراني"[67]، أن استخدام تلك التقنية بالذات ترقى إلى مستوى الجريمة، وذلك لوجود البعد اللاأخلاقي في تلك الممارسات بسبب قيام المخترقين اللاأخلاقيين (Unethical Hacker) بأعمال من الممكن أن يُطلق عليها غير شرعية، مثل طلب الفديات، والتدمير المؤدي إلى خسائر باهظة الثمن. كذلك يشدّد الباحثان على أهمية استخدام كلمة "جريمة" لوصفها؛ لما لها من أثر كبير في البشرية، ولتسببها في الكثير من الأضرار، على المستوى الشخصي، مثل الابتزاز والتهديد، وعلى المستوى الدولي، مثل اختراق الأنظمة بغرض تدميرها أو الحصول على معلوماتها مثل القواعد الصاروخية للجيوش، أو تعطيل أنظمة المطارات المدنية أو العسكرية[68].

4. استخدام الفضاء للأغراض العسكريّة

أثار مصطلح عسكرة الفضاء (SpaceMilitarization) جدلًا واسعًا عندما فكّرت الدول العظمى جديًا في الاستثمار في هذا الجانب؛ لأنّه أصبح جليًا أن التنافس خرج من محدودية إطار الأرض إلى آفاق أوسع وأرحب. وبدأ التنافس الحقيقي في مجال عسكرة الفضاء تحديدًا بعد إطلاق الاتحاد السوفياتي القمر الصناعي الخاص به عام 1957[69]، ولم تلبث الولايات المتحدة الأميركية سوى عام آخر حتّى أطلقت قمرها الصناعي الأول عام 1958، قبل أن يتحول القطبان إلى إطلاق مئات الأقمار الصناعية التي يعتمد عليها الجيشان الأميركي والروسي في

65 Julia E. Sullivan & Dmitriy Kamensky, "How Cyber-Attacks in Ukraine Show the Vulnerability of the US Power Grid," *The Electricity Journal*, vol. 30, no. 3 (2017), pp. 30-35.

66 Siddharth Vikram Philip, "British Airways IT Outage Grounds Planes: Cyber Attack Ruled Out," *Bloomberg*, 26/2/2022, accessed on 25/11/2022, at: https://bloom.bg/3Vv2tCV

67 وفاء لطفي، "الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجًا"، **مجلة كلية الاقتصاد والعلوم السياسية**، مج 23، العدد 1 (كانون الثاني/ يناير 2022)، ص 151-178.

68 سني ذو الهدى، "تهديد الإرهاب السيبراني وإمكانية تطبيق اتفاقية الجرائم السيبرانية"، **التحالف الإسلامي العسكري لمحاربة الإرهاب**، 2020/6/23، شوهد في 2022/11/25، في: https://bit.ly/3Ub9OpY

69 المرجع نفسه.

المنصات والنظم الإلكترونية[70]. يضاف إلى ذلك أن من يكون له السبق في امتلاك التكنولوجيا الفضائية سيكون له أيضًا ميزة التفوق في الحروب المستقبلية.

ويشمل استخدام الفضاء للأغراض العسكرية، أو عسكرة الفضاء، العديد من الأسلحة المصممة خصّيصًا للعمل في بيئة فضائية، وهي صواريخ الطائرات المقاتلة المضادة للأقمار الصناعية الأرضية، والأسلحة المدارية الحاملة للمركبات المضادة للأقمار الصناعية ويُطلق عليها الأقمار الصناعية الانتحارية، وقد صُمّمت بغرض تدمير الأقمار الصناعية للدول المعادية ذات المدافع الليزرية المخصّصة لمهمات تدمير الأهداف الأرضية وضربها[71]، والأقمار الصناعية التي تستطيع حمل الرؤوس النووية، وتُسمّى كذلك أقمار القصف المداري وتمتاز بخاصيّة تدمير المنشآت الحيويّة والأهداف الأرضية ذات الطابع الاستراتيجي، والمركبات الفضائية المُصممَة لغرض مهمات الاستخبارات والاستطلاع والتعرّف إلى الأقمار الصناعية الأخرى، وتلك المركبات تُسمّى غير المأهولة لعدم وجود العنصر البشري بها؛ إذ يجري التحكم بها عن بعد[72]، وأنظمة الخداع والتشويش على الأقمار الصناعية، إضافة إلى الطائرات بدون طيار، وهي كذلك مسلّحة بمدافع ليزرية مضادة للأقمار الصناعية.

وتتولّى المنصّات الفضائية الاهتمام بمنظومات توجيه الصواريخ عبر الأقمار الصناعية وأقمار الاتصالات. وقد وصل عدد الأقمار الصناعية المُطلقة في الفضاء منذ بدء الثورة الفضائية ما يقارب 6542 حتّى تاريخ 1 كانون الثاني/ يناير 2021[73]. تدور حول الأرض الأقمار متعددة المهمات، وتوفر الصور والمعلومات والخدمات الضرورية للحياة المدنية والعسكرية والعلمية والاقتصادية. ومع تزايد أهمية الأقمار الصناعية، زاد القلق العالمي بشأن كيفية الحفاظ عليها وتأمينها، خصوصًا بعد ظهور رغبة سوفياتية وأميركية بشأن تدمير الأقمار الصناعية للدول الأخرى المعادية في وقت مبكّر[74]، تقريبًا في بداية الستينيات من القرن العشرين، بغرض منع الطرف المعادي من المعلومات الاستخباراتية والتجسس والصور المهمّة والاتصالات عبر الأقمار الصناعية. وإذا ما جرى تدمير الأقمار الصناعية التي تعتمد عليها الدول، فإنّ الجيوش ستفقد العنصر الاستخباراتي الذي يتيح لها التخطيط المسبق، وسيترتّب على ذلك الضبابيّة وعدم اليقين الذي يؤدّي إلى الفوضى وعدم التنسيق وفقدان الاتصال وغياب المعلومات، وستتحوّل الجيوش إلى جيوش تقليدية غير قادرة على التنبؤ الصحيح والتخطيط السليم[75]. وقد استطاعت مراكز البحوث

70 Harvey M. Sapolsky & Jeremy Shapiro, "Casualties, Technology, and America's Future Wars," *The US Army War College Quarterly: Parameters*, vol. 26, no. 2 (1996).

71 Michael Krepon & Julia Thompson (eds.), *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations* (Monterey, CA: Naval Postgraduate School/ Center on Contemporary Conflict, 2013).

72 جاد، ص 28-30.

73 Robert Preston et al., *Space Weapons Earth Wars* (Santa Monica, CA: RAND Corporation, 2002), pp. 101-107.

تنبغي الإشارة هنا إلى أنّ هذه الرقم تقريبي، وليس دقيقًا، لثلاثة أسباب: أولًا، العدد قد زاد بسبب مضي عام تقريبًا على آخر إحصائية، ثانيًا، بسبب الإقبال المستمر والتطور التكنولوجي المتسارع، ثالثًا، عدم الإفصاح عن إطلاق بعض الأقمار الصناعية العسكرية من أجل السريّة.

74 Ibid., pp. 32-36.

75 Krepon & Thompson, pp. 77-78.

والتطوير الأميركية تطوير الأسلحة المضادة للأقمار الصناعية، مثل (Anti-Satellite Weapons, ASAT) التي أُطلقت في الفضاء عام 1958، وهي مرحلة أولية من برنامج تطوير تكنولوجي لسلاح الجو الأميركي، مشتملةً على التجربة التي تهدف إلى تطوير قدرة الصاروخ الباليستي المضاد للأقمار الصناعية، والذي يمكن أن يُحمل جوًا على قاذفات (B-47)،ويحتوي على شحنة نووية أُطلق عليه اسم (WS-199 Bord Orion)[76].

5. الذكاء الاصطناعي والروبوتات العسكرية

إن الذكاء الاصطناعي – ببساطة – هو تهيئة حافظة الآلة (Memory)، وتحفيزها، وتغذيتها بكميات هائلة من المعلومات (Big Data) عن طريق آلية تعليم الآلة (Machine Learning)، بحيث تتلقّى المعلومات وتخزّنها بطريقة معينة، وتسترجعها عند الطلب (Retreat)، كما يجري تعليمها كيفية التصرف إذا ما حدث أمر ما؛ بمعنى كيفية الرد على حدث معيّن طبقًا للتجارب السابقة بما يتناسب مع محاكاة العقل البشري والتصرف بنفس الطريقة والأسلوب، إضافة إلى الكثير من الإجراءات التي تتكيّف الآلة على التعامل معها بوساطة أفضل التجارب التي جرى التوصل إليها من خلال الأحداث المتعددة؛ وهذا يعطي الآلة إمكانية وضع الفرضيات وعمل الحسابات بناءً على تجارب سابقة، ومن ثمّ تسهيل مهمة اتخاذ القرار من قبل القادة وأصحاب العلاقة[77].

وقد وُظِّف الذكاء الاصطناعي في الاستخدامات العسكرية المتعددة بعد النجاح منقطع النظير الذي حققه في الاستخدامات المدنية من خلال اعتماد التكنولوجيا بما يتناسب مع الاستخدامات ذات الصلة[78]. مثلًا، عندما تصوّر المستشعرات في الأقمار الصناعية موقعًا عسكريًا أو منشأة عسكرية معينة، يجري تحويل تلك الصور إلى أنظمة الذكاء الاصطناعي المرتبطة بالأقمار الصناعية، بحيث تقوم تلك المنظومات الذكية بتحليل الصور، ومعرفة نوع الطائرات الموجودة، ونوع المدرج المُستخدَم، سواء كان مدنيًا أم عسكريًا، ونوعية الصواريخ الأرضية سواء كانت مسيّرة أم لا، وكيفية التعامل مع تلك الطائرات والأسلحة والوقت المستغرق للوصول إليها والكثير من التفاصيل ذات الصلة، في سبيل إعطاء أفضل الحلول للتعامل مع الموقف[79]. وبذلك تمنح جميع تلك المعلومات صورةً واضحة لصاحب القرار لاتخاذ القرار الأفضل بناءً على الموقف نفسه. ومن المهم هنا التأكيد أنّ منظومات الذكاء الاصطناعي لا تتخذ القرار بالنيابة عن البشر، ولكنها تعطي القراءات الصحيحة للأوضاع المختلفة بطريقة دقيقة وتحليل صائب يضمنان تقليل الأخطاء والمخاطر المحتملة، في سبيل منح أفضل الخيارات والحلول لمتخذي القرار. وفي نهاية المطاف، يجري اتخاذ القرار بوساطة البشر وليس الآلة[80].

76 Ibid.

77 Ibid.

78 عبد القادر محمود محمد الأقرع، "الروبوتات العسكرية في الحروب المستقبلية ومدى خضوعها لأحكام القانون الدولي الإنساني"، **المجلة القانونية**، مج 8، العدد 3 (تشرين الثاني/ نوفمبر 2020)، ص 957-960، 899-966.

79 Khade Gaurav & Gerard Mies, "Military Robots of The Present and The Future," *ACADEMIA Accelerating the World's Research*, vol. 9, no. 1 (2010), pp. 125-137.

80 Ibid.

أما فيما يخص الروبوت العسكري، فهو أداة تقوم ببعض الواجبات بدل البشر للمحافظة على سلامة العنصر البشري في الحروب؛ إذ يقوم مصممو الروبوتات العسكرية ببرمجتها لتقوم بوظائفها من خلال التحكم عن بعد بوساطة ما[81]. فمثلًا، تُستخدَم الروبوتات العسكرية لتطهير أرض المعركة من الألغام والمتفجرات، ولاستكشاف المباني المُحتمَل وجود العدو فيها في حروب الشوارع أو حروب المدن، وكذلك حروب المباني التي تعتبر من أخطر حروب المواجهة. كما تُستخدَم الروبوتات على الحدود بوصفها أسلحة موجهة عالية الدقة لمنع التسلل، ويجري التحكم بها عن بعد في غرف العمليات ومراكز القيادة والسيطرة على بعد عشرات أو مئات الكيلومترات من الحدود، بحيث لم يعد من الضروري وجود الجنود على نحو دائم على الحدود في ظل الروبوتات المتطورة تكنولوجيًا، خصوصًا تلك المزودة بكاميرات عالية الاستبانة[82].

وقد يصبح الأمر أكثر إثارة عند المواءمة بين الذكاء الاصطناعي والروبوت العسكري، وهو ما جرى فعلًا؛ إذ أصبح بمقدور الذكاء الاصطناعي توجيه الروبوت العسكري للقيام بواجبات يجري تحديدها وبرمجتها سلفًا، كما أصبح بمقدور الروبوت التعامل مع الأحداث المحيطة به بدقة ومرونة عاليتين. ويصبح الروبوت حينئذٍ أداةً لتنفيذ الأعمال الموكلة إليه من الذكاء الاصطناعي من دون تدخل البشر؛ وهذا التطور التكنولوجي واعد وقد يُحدِث ثورةً جديدة في التطور التكنولوجي[83]، غير أن بعض العلماء أبدوا قلقهم من احتمال خروج الروبوتات عن السيطرة في أرض المعارك؛ لأنها ليس لديها إحساس أو مشاعر، ولا تعرف الفرق بين المدنيين والعسكريين؛ ما قد يتسبب بكوارث إنسانية. فالروبوتات العسكرية في أرض المعركة ستُجهّز بأسلحة آلية أوتوماتيكية أو نصف أتوماتيكية، وتصبح أداة قتل لا يمكن ردعها في حال حدوث خطأ ما[84].

وبالرغم من ذلك، ستستمر الجيوش في تطوير الروبوتات لأغراضها الخاصة كلما دعت الحاجة إلى ذلك، مثل التعامل مع الألغام. كما أن التطور التكنولوجي يتيح للمطورين والمصممين بناء أنظمة جديدة لمزيد من المهمات، وستكون المركبات الأرضية غير المأهولة ذات قيمة كبيرة لمثل هذه الأغراض؛ لأنها قادرة على إدارة العديد من المهمات بكفاءة عالية[85]. ولا تقتصر أدوار الروبوتات على المهمات القتالية فقط، بالرغم من مخاطرها الكثيرة؛ إذ إن الروبوت لا يفرّق بين الرجل والمرأة أو الطفل والحجر؛ إذ يطلق النار على من يظهر أمامه، بل تخطتها إلى آفاق أرحب، فقد تُستخدَم أيضًا لدعم المسعفين ومقدمي الخدمات الطبية التي تتصف وظائفهم بالخطورة، خصوصًا في ساحات المعارك. فعلى سبيل المثال، الروبوت "بلودهاوند" (Bloodhound) تتجلى مهمته في البحث عن الجنود الجرحى في ميادين القتال،

81 الأقرع، ص 957-960.

82 المرجع نفسه.

83 Gabriel Hallevy, *When Robots Kill: Artificial Intelligence Under Criminal Law* (Lebanon/ New Hampshire: Northeastern University Press, 2013).

84 Ibid.

85 Gaurav & Mies.

وإجراء العلاجات البسيطة، مثل فحص الوظائف الحيوية وإعطاء المسكّنات[86]. والروبوت "ميدبوتس" (Medbots) المصمم خصيصًا لنقل الجنود الجرحى وسحبهم إلى الأماكن الآمنة والبعيدة عن خطوط التماس، وإجراء عمليات جراحية داخل السيارات المدرّعة والمجهزة لتلك العمليات. والجدير بالذكر أن وكالة مشاريع البحوث الدفاعية المتقدمة (DARPA) أنفقت أكثر من 12 مليون دولار من خلال مراكز بحوثها بهدف تقليل المخاطر على الجنود والعمل على الأنظمة الجراحية الروبوتية. ومن ثمّ، فإن الاحتمالات لاستخدامها في غضون العشرة إلى الخمسة عشر عامًا القادمة وارد الحدوث[87].

وعلى غرار الروبوتات الأرضية، يطوّر الجيش الأميركي أجهزة روبوتية لاستخدامها في البحر والسفن السطحية غير المأهولة (USV) والمركبات غير المأهولة على الأرض[88]. وقد استثمرت البحرية الأميركية مبالغ كبيرة في تطوير القوارب الآلية التي تعمل على الاستكشاف والتواصل مع السفن الكبرى التي تحتوي على مراكز قيادة وسيطرة. وأخيرًا، يعتقد الخبراء أن الفضاء يمكن أن يكون ساحةَ معركةٍ وتحديًا جديدًا إذا تطورت منطقة الصراع فيه، فيجب تزويده بأجهزة غير مأهولة، حيث سيكون إرسال البشر والإمدادات الضرورية والأكسجين مكلفًا للغاية[89].

86 Ibid.

87 Ibid.

88 Ibid.

89 أولى المركبات من دون طيار للاستخدام في الفضاء هي قيد التطوير والتجارب المستمرة، وإحدى هذه السفن الفضائية هي طائرة (بوينغ X-37) التي يجري العمل عليها حاليًا، ينظر: Ibid.

ثالثًا: أثر التطور التكنولوجي للقوة العسكرية في الدول الصغرى

1. مفهوم الدول الصغرى

إنّ الدول الصغرى (Small States) في مفهوم النظام الدولي هي الدول ذات المساحات الصغيرة، ولا تتمتّع بعمق استراتيجي قادر على حمايتها من أطماع الدول المجاورة. وبالرغم من أنّها دول ذات سيادة، فإنها تحتوي على عدد قليل جدًا من السكان[90]. ولذا تسعى إلى تعويض نقطة الضعف في المحافظة على المقدرات والمكتسبات باللجوء إلى امتلاك المنظومات العسكرية الاستراتيجية المتطورة، بحيث يكون تسليحها أو ترسانتها العسكرية أقوى من تسليح الدول المجاورة لها، أو على مستوى الإقليم، لضمان قوة الردع الكافية في حال حاولت بعض الدول المجاورة، سواءً كانت فرادى أو تكتلات، من الاستفادة من تلك الثغرة خصوصًا مع غياب العمق الاستراتيجي من خلال شن عمليات عسكرية لتنفيذ مخططات توسعية بغرض الحصول على مقدرات تلك الدول ومكتسباتها، أو من أجل فرض سياسة الأمر الواقع تمهيدًا لمفاوضات تسفر عن المحافظة على وضع معيّن، أو تقديم تنازلات من الدول المُعتدى عليها[91].

وفي هذا السياق، يضرب إبراهيم اسعيدي مثالًا عن تطور العلاقات العسكرية على نحو تدريجي

90 بلخيرات حوسين، "استراتيجيات الدول الصغرى في مواجهة القوى الكبرى"، *المعهد المصري للدراسات* (30 نيسان/ أبريل 2018)، شوهد في 2022/11/25، في: https://cutt.us/ITWDb

91 المرجع نفسه.

بين الولايات المتحدة بوصفها دولة كبرى ودولة قطر بوصفها دولة صغرى. وقد ساعد على ذلك الوضع الجيوسياسي من جهة، والتهديدات الأمنية وعدم وضوح المشهد في الشرق الأوسط من جهة أخرى. فالولايات المتحدة تعتبر الشراكة الدفاعية مع قطر والحصول على موطئ قدم في المنطقة من خلال الوجود في قاعدة العديد العسكرية من أبجديات سياساتها. أما بالنسبة إلى دولة قطر، فهي ترى في هذه الشراكة تحقيق مكسب يتمثل في مواجهة التهديدات الخارجية والاستفادة من التمارين المشتركة في ظل قدراتها العسكرية. كما يرى سعيدي أن هذه الشراكة الثنائية ذات المصالح المتبادلة التي أثرت إدارة الأزمات والصراع في المنطقة، لها أربعة أعمدة: اتفاقية الدفاع الثنائية، واستخدام الأميركيين قاعدة العديد، ومبيعات الأسلحة المستمرة، وتعزيز الاتصالات العسكرية. وبالرغم من ذلك، فإن هذه العلاقة لا تمثّل ضمانًا أميركيًا لدولة قطر[92] من الناحية القانونية.

لذلك تلجأ بعض الدول الصغرى إلى إقامة علاقات ثنائية مع بعض الدول الكبرى ذات النفوذ والهيمنة في بعض الأقاليم، أو الدول ذات الثقل السياسي أو الاقتصادي، بغرض الاستفادة من الدعم المباشر أو غير المباشر، سواء كان ماديًا، كالمساعدات، أو معنويًا، كالمساندة أمام المنظمات الدولية، مثل الأمم المتحدة، أو صندوق النقد الدولي، أو الجهات الأخرى ذات الصلة.

كما تلجأ بعض الدول الصغرى، خصوصًا تلك التي لا تمتلك عمقًا استراتيجيًا ومحاطة ببعض الدول ذات الأطماع، إلى عقد تحالفات عسكرية واتفاقيات دفاع مشترك لردع المخاطر المحتملة[93]. وهذا السياق يتفق مع "نظرية الدول الصغرى"، في محاولة سد ذلك النقص بطريقة معينة بما يضمن سلامة حدود تلك الدول ومقدراتها ومكتسباتها من أطماع الدول الكبرى وبطشها[94].

وبهذا، لم يعد حجم الدول مقياسًا لقوّتها العسكرية أو ضعفها في مفهوم الحروب الحديثة؛ حيث إنّ الدول الصغرى من الممكن أن تستغل صِغَرَ حجمها تعزيزًا لقوتها وتأمينًا لحدودها البريّة والبحريّة والجويّة، خصوصًا إذا امتلكت التسليح المتطوّر والمنظومات الاستراتيجية الحديثة التي من شأنها كبح جماح العدو مهما كَبُرَ حجمه[95]، ومن الممكن أن تنفّذ العمليات النوعية التي قد تحدث دمارًا هائلًا في صفوفه من دون المخاطرة بأرواح الجنود أو استهلاك الموارد. فإسرائيل، مثلًا، مساحتها صغيرة وليس لديها عمق استراتيجي ومحاطة بدول عربية ذات ثقل عسكري، ولكنها ما زالت قادرة على حماية كيانها، وهذا يدلّ على قوة مراكز الثقل لديها[96]. ويُعزى هذا التفوّق

92 Brahim Saidy, "Qatari-US Military Relations: Context, Evolution and Prospects," *Contemporary Arab Affairs*, vol. 10, no. 2 (2017), pp. 286-299.

93 Ibid.

94 Christine Ingebritsen, Iver Neumann & Sieglinde Gsthl (eds.), *Small States in International Relations* (Washington DC: University of Washington Press, 2012), pp. 300-340.

95 صبري مقلد إسماعيل، "مخاطر تسببها الفجوة الرقمية: ثورة المعلومات وحروب المستقبل المحتملة"، **آفاق المستقبل**، العدد 15 (تموز/ يوليو-آب/ أغسطس-أيلول/ سبتمبر 2012)، ص 40-44.

96 Ralph Sanders, "An Israeli Military Innovation: UAVs," *JFQ/* National Defense University (Winter 2002-03), pp. 114-118.

العسكري إلى التطوّر التكنولوجي في التسليح من خلال المنظومات الاستراتيجية، مثل منظومات (C4ISR)، والقبّة الحديدية والصواريخ الموجّهة، والطائرات المسيرة[97].

وهذا يعطي انطباعًا بأن هيكلة القوات المسلحة وحجمها في الحروب المستقبلية سيعتمدان على الأسلحة النوعية الذكية ذات الكفاءة والمرونة (Efficiency & Resilience) العالية، التي يساعد في تحقيقها التطور التكنولوجي، أكثر من الاعتماد على العدد والعتاد اللذين ليسا بالضرورة مصدرَي قوّة. بل على العكس، أثبتت التجربة البريطانية أنّ الأسلحة والقوى البشرية الضخمة تتطلب جهدًا مضاعفًا في التدريب المستمر والصيانة والإدامة، إضافة إلى تراكم الأعباء المالية والإدارية والعملياتية[98]. وعلى الرغم من ذلك، لا يمكن القول إن التطور التكنولوجي هو الحل السحري للعديد من المشكلات والتحديات، بقدر ما هو عنصر فعال يساعد على تقليل المخاطر واستشراف التحديات مثل منظومات الاستشعار عن بعد، والذكاء الاصطناعي، التي تعطي الوقت الكافي للتحليل الدقيق، وذلك لمعرفة أسلحة العدو وتسهيل عملية صنع القرار للقادة بشأن كيفية التعامل معها، تحقيقًا لنظرية "الكفاءة وليس العدد" (Quality Not Quantity)[99].

97 Gil Baram & Isaac Ben-Israel, "The Academic Reserve: Israel's Fast Track to High-Tech Success," *Israel Studies Review,* vol. 34, no. 2 (Autumn 2019), pp. 75-91.

98 Ibid.

99 Daniel S. Hoadley & Nathan J. Lucas, "Artificial Intelligence and National Security," *Congressional Research Service,* R45178, Version 10 Updated (November 10, 2020).

وفي ضوء التغييرات التي طرأت على هياكل القوات المسلحة للدول سواء الكبرى أو الصغرى وسياساتها التسليحية بسبب التطور التكنولوجي والأسلحة الذكية، فإن الاستراتيجية العسكرية وخطط الحرب ينبغي أن تتغير بما يتناسب مع الطرق والأساليب الجديدة للحروب الحديثة[100]؛ إذ إن الحروب الحديثة تبدأ باستطلاع إمكانات العدو وتسليحه ومنظوماته الاستراتيجية وإعداد جيشه، تمهيدًا لاستهداف البنى التحتية بغرض تدميرها أو إضعافها، ثم شن الحروب السيبرانية بهدف تدمير المنظومات الاستراتيجية والأسلحة ذات الثقل العسكري، لغاية الوصول إلى سيناريوهات تناسب الهدف المراد تحقيقه، سواءً كان احتلالًا، أو الحصول على تنازلات، أو الاستحواذ على شيء معيّن؛ لذلك قد لا ترقى الاستراتيجية العسكرية وخطط الحرب إلى القتل والتدمير، بل قد تكون حربًا من نوع آخر تؤدي إلى الأهداف نفسها، مثل تضييق الخناق على الدول المستهدفة بغرض الاستسلام أو التنازلات عن بعض المواضيع ذات الصلة[101].

2. تغيير سياسات التسلّح واستراتيجياته للدول الصغرى: إسرائيل نموذجًا

لطالما كان غياب العمق الاستراتيجي لإسرائيل هاجسًا يؤرق قادتها وجنرالاتها طوال العقود الستة الماضية، خصوصًا أن هناك أحداثًا أثبتت أن خاصرة ذلك الكيان هشة وعرضة للانهيار في أي وقت، لا سيما في حال كانت هناك وقفة صارمة

100 Ibid.

101 Ibid.

وعمل عسكري احترافي من الدول العربية المحيطة بإسرائيل، مثل حرب 1948، والعدوان الثلاثي 1956، والنكسة 1967، وحرب تشرين الأول/ أكتوبر 1973، بغض النظر عن نتائج تلك الحروب؛ لأن الكيان الصهيوني يعلم يقينًا أن معظم الشعوب العربية لا تعترف بإسرائيل بصفتها دولة حسب عقيدتيها الدينية والعسكرية[102]. لذلك تعيش إسرائيل في بيئة تهديد وجودي دائم في المقام الأول، وتواجه تهديدات متنوعة إثر إحاطتها بدول معادية علانية، أو يحتمل أن تكون معادية، كالفواعل الدولتية أو الفواعل غير الدولتية.

يضاف إلى ذلك أنها دولة صغيرة ذات عمق استراتيجي ضئيل، يبلغ عرضها 85 ميلًا (137 كيلومترًا) عند أوسع نقطة لها، و9 أميال (14 كيلومترًا) في أضيقها (استنادًا إلى حدود إسرائيل قبل عام 1967)، ويبلغ عدد سكانها اليهود 6.5 ملايين. وقد ظلّ هذا الوضع الجيوستراتيجي موجودًا منذ عام 1947؛ ما أدّى لاحقًا إلى توجيه سياسة الأمن القومي الإسرائيلي إلى السعي وراء التفوق التكنولوجي العسكري وصناعة الدفاع المحلية[103].

كما تستند استراتيجية الدفاع الإسرائيلية إلى ثلاث ركائز تاريخية أساسية: (أ) الردع، بما في ذلك الردع النووي؛ (ب) الإنذار (الاستراتيجي والتكتيكي) المبكر؛ و(ج) اتخاذ القرار العسكري السريع الذي يؤدي إلى نصر حاسم في ساحة المعركة. ومن ثمّ، ينبغي أن تكون التكنولوجيا المبتكرة في سياق المتطلبات الأساسية. ولذا يرى ديما أدامسكي أنّ مقاربة إسرائيل للأمن هي من منطلق ثقافة الإسرائيليين الاستراتيجية التي تأثرت بـ "عقلية الحصار المهووسة"، و"السعي وراء المطلق"[104]. ونتيجةً لذلك، حافظت السياسة الأمنية الإسرائيلية على "التفوق التكنولوجي على منافسيها"[105].

على سبيل المثال، في بداية ثمانينيات القرن العشرين، عكف المخططون والاستراتيجيون الإسرائيليون على تنفيذ سياسة "الحصول على أحدث تكنولوجيا للمعركة المتكاملة، والحصول على أكثر الأسلحة الممكنة تقدمًا"، مثل دبابات "الميركافا" الإسرائيلية الصنع، والطائرات الأميركية المقاتلة الحديثة، وطائرات الإنذار المبكر، والصواريخ الحرارية المسيرة[106]. كما عكفت إسرائيل على تكييف سياساتها الاستراتيجية بما يتناسب مع ملء فراغ غياب العمق الاستراتيجي، من خلال امتلاك المنظومات والأسلحة الاستراتيجية اللتين لا تمتلكهما دول الجوار؛ وقد ساهمت الولايات المتحدة في ذلك من خلال بيع المنظومات والأسلحة المؤثرة، بحيث لا تستطيع الدول العربية امتلاك أسلحة أو

102 Alyson J.K. Bailes, Jean-Marc Rickli & Baldur Thorhallsson, *Small States: Survival and Strategy* (Milton Park; Abingdon; Oxon/ New York: Routledge, 2014), pp. 26-45.

103 Bitzinger.

104 Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, Calif.: Stanford University Press, 2010), pp. 200-248.

105 Ibid.

106 Ibid.

منظومات مشابهة[107]. وهذا النهج الذي تتبعه الولايات المتحدة يمنح إسرائيل التفوق العسكري القادر على فرض السيطرة والهيمنة، سواء الجوية أو البرية أو البحرية أو الإلكترونية أو الفضائية. ولعل التوسع الاستيطاني من خلال بناء المستوطنات في دولة الكيان الصهيوني خير دليل على تعزيز العمق الاستراتيجي وتوسيعه، وكذلك القبة الحديدية التي تعمل بصفتها درعًا يحمي تل أبيب من الهجمات الصاروخية الموجّهة من منظمة "حماس" والفصائل الفلسطينية المقاتلة الأخرى[108].

لذا كان الإسرائيليون سباقين في هذا المجال؛ إذ عملوا بجدّ على أنظمة الطائرات المسيّرة في مرحلة مبكّرة بذريعة مكافحة الإرهاب المتمثّل في منظمة "حماس" حسب زعمهم، حيث تقوم الطائرات المسيّرة المزوّدة بصواريخ "بايثون" (Python) جو - جو بمقاومة الصواريخ الباليستية[109]. وجادل المخططون بأن القدرة على العمل بارتفاعات عالية لأيام تكاد تكون محصنة ضد هجوم الصواريخ الأرضية، وبدؤوا كذلك في تصميم طائرة (HA-10)، وهي طائرة شبحية مسيّرة طويلة التحمل[110].

خاتمة

من خلال تسليط الضوء على التطور التكنولوجي في الحروب الحديثة، بيّنا في هذه الدراسة أن مفهوم الحروب قد تأثر بالتطور التكنولوجي الذي أحدث عليه تغييرًا جذريًا من خلال الأنظمة الحديثة والمنظومات الاستراتيجية التي حافظت على الوقت والجهد، والأهم من ذلك، على أرواح الجنود، علمًا أن الأضرار التي تستطيع إحداثها في صفوف العدوّ لا تقل ضراوةً عن القتل والتدمير في الحروب القديمة، مثل الحرب الإلكترونية، وأنظمة المراقبة والاستطلاع، والأمن السيبراني، وأنظمة الهجوم الإلكتروني، وأنظمة الدفاع الإلكتروني، والاستشعار عن بعد، واستخدام المجال الكهرومغناطيسي، التي تستطيع كبح جماح العدو وردعه، وأحيانًا القيام بعمليات هجوم نوعية قادرة على تعطيل أنظمة التسليح المعادية وتحييدها أو تدميرها. كما استطاع البحث من خلال الاستشهاد ببعض الأمثلة، إثبات فرضية أنّه ليس بالضرورة أن الدول الصغرى ما زالت الحلقة الأضعف في سلسلة الصراعات مع الدول الكبرى، خصوصًا إذا كانت الدول الصغرى تمتلك المنظومات الاستراتيجية المطوّرة تكنولوجيًا.

---

107 Raphael D. Marcus, "Military Innovation and Tactical Adaptation in the Israel–Hizballah conflict: The institutionalization of Lesson-learning in the IDF," *Journal of Strategic Studies*, vol. 38, no. 4 (2015), pp. 500-528.

108 وائل عبد الحكيم محمد ربيع، "سياسات الاستيطان الإسرائيلية بعد حرب 1967"، **مجلة بحوث الشرق الأوسط**، مج 10، العدد 74 (نيسان/ أبريل 2022)، ص 61-84.

109 Vivek Kapur, *Stealth Technology and its Effect on Aerial Warfare*, Idsa Monograph Series, no. 33 (New Delhi: Institute for Defence Studies & Analyses, 2014), pp. 64-102.

110 Sanders.

بيد أنهم لم يوفّقوا في صنعها؛ لأن الدعم الأميركي لمثل هذا المشروع لم يستمر، أو أن التمويل المطلوب يستغرق وقتًا طويلًا. كما اعتبرت الولايات المتحدة أن استخدام الطائرات المسيّرة في مرحلة التعزيز قد يكون تحديًا فنيًا ومكلفًا جدًا. ينظر: Ibid.

عطفًا على كل الأمثلة والتجارب السابقة والدروس المستفادة والأدلة والبراهين والتحليلات المذكورة، نجد أنّ القفزة التكنولوجية في الجيوش الحديثة تتجلى في الأدوات والأسلحة التي ستُستخدم في في حروب المستقبل، خصوصًا أن التطور المهول والتسارع المستمر يلقي بظلاله على العالم أجمع، ويفرض على الدول واقعًا جديدًا ينبغي استخدامه لمواكبة سباق التسلح التكنولوجي الذي يشهده العالم حاليًا، وكذلك لمعرفة الثغرات والتهديدات المستقبلية المحتملة وكيفية التعامل معها.

ومن ثمّ، نجد أن بوصلة الحروب الحديثة تُشير إلى مستقبل حروب تكنولوجية ذكية قد لا يكون الهدف منها القتال في ساحات المعارك، بقدر ما تكون حروب ذات أهداف استراتيجية تُدار من خلف الشاشات، أو حروب عن بعد، وهو ما يسمّى حديثًا بـ "الحروب بدون جنود"، أو "الحروب بدون أرض معركة". ولذا ستكون دول العالم بعامّة، والدول الصغرى بخاصّة، مرغمةً على التكيف مع أوضاع الحروب الحديثة في المستقبل، وستكون الدول الصغرى تحت ضغط أكبر بصفتها الأكثر حاجةً في ظل هذا الصراع المستمر والمتغيّر.

وأخيرًا، وتماشيًا مع "نظرية الدول الصغرى"، بيّنا أنّ الدول الصغرى، بصفتها دولًا تنتهج العقيدة العسكرية الدفاعية، تبذل جهدًا مضاعفًا لمواكبة التطور التكنولوجي، وذلك بسدّ فجوة صغر المساحة وغياب العمق الاستراتيجي بالحصول على أسلحة متطورة ومنظومات استراتيجية قادرة على ردع الأطماع وتحييد الأسلحة المتطورة التي تمتلكها الدول الكبرى.

المراجع

العربية

إسماعيل، صبري مقلد. "مخاطر تسببها الفجوة الرقمية: ثورة المعلومات وحروب المستقبل المحتملة". **آفاق المستقبل**. العدد 15 (تموز/ يوليو-آب/ أغسطس-أيلول/ سبتمبر 2012).

الأقرع، عبد القادر محمود محمد. "الروبوتات العسكرية في الحروب المستقبلية ومدى خضوعها لأحكام القانون الدولي الإنساني". **المجلة القانونية**. مج 8، العدد 3 (تشرين الثاني/ نوفمبر 2020).

حوسين، بلخيرات. "استراتيجيات الدول الصغرى في مواجهة القوى الكبرى". المعهد المصري للدراسات. 2018/4/30. شوهد في 2022/11/25. في: https://cutt.us/ITWDb

دريسي، حنان. "الثورة في الشؤون العسكرية وتداعياتها على السياسات الدفاعية للدول". **المجلة الجزائرية للدراسات السياسية**. مج 8، العدد 2 (2021).

ربيع، وائل عبد الحكيم محمد. "سياسات الاستيطان الإسرائيلية بعد حرب 1967". **مجلة بحوث الشرق الأوسط**. مج 10، العدد 74 (نيسان/ أبريل 2022).

زاد، زلمي خليل وجون وايت (محرران). **الدور المتغير للمعلومات في الحرب**. سلسلة **دراسات عالمية**. العدد 53. أبوظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2004.

الزيديين، نواف موسى مسلم. "مدى مشروعية الحرب الوقائية على أفغانستان والعراق في القانون الدولي". **مجلة كلية الشريعة والقانون بتفهنا الأشراف - دقهلية**. العدد 23، ج 4 (2021).

عامر، مصباح. **نظرية العلاقات المدنية العسكرية: الحالات التطبيقية في التحليل الاستراتيجي**. القاهرة: دار الكتاب الحديث، 2018.

ـــــــــــــــ. **تطور علم الاستراتيجية**. القاهرة: دار الكتاب الحديث، 2017.

عبد العزيز، سارة. "الحرب السيبرانية: التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية". مجلة **اتجاهات الأحداث**. العدد 20 (2017).

عبد الكاظم، رياض مهدي وآلاء طالب خلف. "المعلوماتية والحروب الحديثة: دراسة حالة الحرب الأمريكية على العراق عام 2003". **مجلة واسط للعلوم الإنسانية**. مج 11، العدد 30 (2015).

علواني، علي. "دور أنظمة القيادة والسيطرة في الحروب الحديثة: مستقبل أنظمة القيادة والسيطرة". **درع الوطن**. العدد 480 (2021).

علي، عمران عمر. "الصراع والتعاون في العلاقات الدولية: الإسهامات النظرية للنقاش بين الواقعية الجديدة وبين الليبرالية الجديدة". **مجلة العلوم الإنسانية لجامعة زاخو**. مج 8، العدد 4 (كانون الأول/ ديسمبر 2020).

العمار، منعم صاحي وعلي محمد امنيف الرفيعي. "المتغيرات المؤثرة في استخدام الولايات المتحدة الأمريكية للقوة الناعمة بعد أحداث 11 أيلول 2011". **قضايا سياسية**. العدد 42 (2015).

قبلان، قاسم وأحمد عاقل. "تحليل وكشف البرمجيات الخبيثة في أنظمة التشغيل للهواتف الذكية دراسة حالة نظام التشغيل (أندرويد)". **مجلة جامعة تشرين للبحوث والدراسات العلمية**. مج 39، العدد 3 (2017).

كاظم، محمد كريم وبراء عبد القادر وحيد. "التطور التكنولوجي والحرب". **مجلة دراسات دولية**. العدد 45 (2010).

لطفي، وفاء. "الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجًا". **مجلة كلية الاقتصاد والعلوم السياسية**. مج 23، العدد 1 (كانون الثاني/ يناير 2022).

معلا، بشرى وهيثم الرضوان وعلاء محفوض. "دراسة تحليلية لتأثير أنواع هجوم التشويش على أداء شبكات Ad Hoc". **مجلة جامعة تشرين**. مج 41، العدد 5 (2019).

الأجنبية

Acton, James M. "Debating Conventional Prompt Global Strike." *Carnegie Endowment for International Peace* (October 2013).

Adamsky, Dima. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel.* Stanford, Calif.: Stanford University Press, 2010.

of Archaeological Site Damage in The Syrian Civil War." *PLOS ONE*. vol. 12, no. 11 (2017).

Chin, Warren. "Technology, War and the State: Past, Present and Future." *International Affairs*. vol. 95, no. 4 (2019).

Clausewitz, Carl von. *On War*. Michael Howard & Peter Paret (Trans.) Oxford & New York: Oxford University Press, [1976] 2006.

Creveld, Martin van. "Modern Conventional Warfare: An Overview." *Hebrew University, Jerusalem* (2004).

Dawson, Linda. *War in Space: The Science and Technology Behind Our Next Theater of Conflict*. Cham: Springer-Praxis Books, 2018.

Diaconu, Mihaela. "Technological Innovation: Concept, Process, Typology and Implications in the Economy." *Theoretical and Applied Economics*. vol. XVIII, no. 10 (2011).

Dougherty, James E. & Robert L. Pfaltzgraff. *Contending Theories of International Relations: A Comprehensive Survey*. 3rd ed. New York: Longman, 2001.

Gaurav, Khade & Gerard Mies. "Military Robots of The Present and The Future." *ACADEMIA Accelerating*

Ananthan, Subramaniam. "The Elements of National Power and its Relevance to National Security." *Zulfaqar Journal of Defence Management. Social Science & Humanities*. Special Issue: "Social Sciences and Humanities in the 4th Industrial Revolution Issues." (2020).

Bailes, Alyson J.K., Jean-Marc Rickli & Baldur Thorhallsson. *Small States, Survival and Strategy*. Milton Park; Abingdon; Oxon/ New York: Routledge, 2014.

Baram, Gil & Isaac Ben-Israel. "The Academic Reserve: Israel's Fast Track to High-Tech Success." *Israel Studies Review*. vol. 34, no. 2 (Autumn 2019).

Bearden, Tom E. "Scalar Electromagnetic Weapons and Their Terrorist Use." *World Affairs: The Journal of International*. vol. 9, no. 4 (2005).

Bitzinger, Richard A. "Military-technological Innovation in Small States: The cases of Israel and Singapore." *Journal of Strategic Studies*. vol. 44, no. 6 (2021).

Breedlove, Philip M. "NATO's Next Act: How to Handle Russia and Other Threats." *Foreign Affairs*. vol. 95, no. 4 (2016).

Casana, Jesse & Elise Jakoby Laugier. "Satellite Imagery-Based Monitoring

University of Washington Press/ University of Iceland Press, 2006.

Ingebritsen, Christine, Iver Neumann & Sieglinde Gsthl (eds.). *Small States in International Relations.* Washington DC: University of Washington Press, 2012.

Kallberg, Jan E., Stephen S. Hamilton & Matthew G. Sherburne. "Electronic Warfare in the Suwalki Gap: Facing the Russian 'Accompli Attack'." *Forum/ Electronic Warfare in the Suwalki*, Gap JFQ 97 (2nd Quarter 2020).

Kapur, Vivek. *Stealth Technology and its Effect on Aerial Warfare*. Idsa Monograph Series. no. 33. New Delhi: Institute for Defence Studies & Analyses, 2014.

Krepon, Michael & Julia Thompson (eds.). *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations.* Monterey, CA: Naval Postgraduate School/ Center on Contemporary Conflict, 2013.

Marcus, Raphael D. "Military Innovation and Tactical Adaptation in the Israel–Hizballah conflict: the Institutionalization of Lesson-learning in the IDF." *Journal of Strategic Studies*. vol. 38, no. 4 (2015).

Smith, Patrick. "Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy." *American the World's Research*. vol. 9, no. 1 (2010).

Grilo, Antonio et al. "Electronic Protection and Routing Optimization of MANETs Operating in An Electronic Warfare Environment." *Ad Hoc Networks*. vol. 5, no. 7 (September 2007).

Hallevy, Gabriel. *When Robots Kill: Artificial Intelligence Under Criminal Law.* Lebanon/ New Hampshire: Northeastern University Press, 2013.

Handler, Stephenie Gosnell. "New Cyber Face of Battle: Developing A Legal Approach to Accommodate Emerging Trends in Warfare." *Stanford Journal of International Law*. vol. 48, no. 1 (2012).

Hoadley, Daniel S. & Nathan J. Lucas. "Artificial Intelligence and National Security." *Congressional Research Service*. R45178. Version 10 Updated (November 10, 2020).

Hofstetter, Jeremy & Adam Wojciechowski. "Electromagnetic Spectrum Survivability in Large-Scale Combat Operations." *Infantry* (Winter 2020–2021).

Ingebritsen, Christine et al. (eds.). *Small States in International Relations*. Series: New Directions in Scandinavian Studies. Seattle:

War College Quarterly: Parameters. vol. 40, no. 1 (2010).

Sengupta, Shubhashis & K. M. Annervaz. "Multi-Site Data Distribution for Disaster Recovery: A Planning Framework." *Future Generation Computer Systems*. vol. 41 (December 2014).

Shad, Muhammad Riaz. "Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions." *Policy Perspectives: The Journal of the Institute of Policy Studies*. vol. 15, no. 2 (2018).

Smeltz, Dina, Stepan Goncharov & Lily Wojtowicz. "US and Russia: Insecurity and Mistrust Shape Mutual Perceptions." *Chicago Council on Global Affairs* (November 2016).

Sullivan, Julia E. & Dmitriy Kamensky. "How Cyber-Attacks in Ukraine Show the Vulnerability of the US Power Grid." *The Electricity Journal*. vol. 30, no. 3 (2017).

Sutherland, Daniel E. *A Savage Conflict: The Decisive Role of Guerrillas in the American Civil War*. Chapel Hill: University of North Carolina Press, 2006.

Zweiri, Mahjoob, Mizanur Rahman & Arwa Kamal (eds.). *The 2017 Gulf Crisis*. Singapour: Springer Singapore, 2021.

Security Project - Perspective (April 2020).

Preston, Robert et al. *Space Weapons Earth Wars*. Santa Monica. CA: RAND Corporation, 2002.

Qureshi, Waseem Ahmad, "Fourth- and Fifth-Generation Warfare: Technology and Perceptions," *San Diego International Law Journal*, vol. 21, no. 1 (Fall 2019).

Reuter, Christian (ed.). *Information Technology for Peace and Security*. Wiesbaden, Germany: Springer Vieweg, 2019.

Saidy, Brahim "Qatari-US Military Relations: Context, Evolution and Prospects." *Contemporary Arab Affairs*. vol. 10, no. 2 (2017).

Sanders, Ralph. "An Israeli Military Innovation: UAVs." *JFQ*/ National Defense University (Winter 2002-03).

Sapolsky, Harvey M. & Jeremy Shapiro. "Casualties, Technology, and America's Future Wars." *The US Army War College Quarterly: Parameters*, vol. 26, no. 2 (1996).

Schroeder, Richard E. *The Foundation of the CIA: Harry Truman, the Missouri Gang, and the Origins of the Cold War*. Columbia, Missouri: University of Missouri Press, 2017.

Schuurman, Bart. "Clausewitz and the 'New Wars' Scholars." *The US Army*