Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

P- ISSN: 2070-898X E-ISSN: 2707-9775

أثر الهجمات السيبرانية على العقيدة الجوية الحديثة وأنظمة القيادة والسيطرة

م. د. فراس جمال شاكر محمود الربيعي
جامعة الامام جعفر الصادق (ع) - بغداد - العراق
Firas.alrubaye89@gmail.com

مستخلص البحث:
تناول البحث تأثير الهجمات السيبرانية المتزايدة على العقيدة الجوية الحديثة وأنظمة القيادة والسيطرة، في ظل التحول الكبير نحو الاعتماد على الأنظمة الرقمية والاتصالات الشبكية في إدارة العمليات الجوية. ويوضح البحث كيف أصبحت الهجمات السيبرانية قادرة على تعطيل القدرات الجوية، وإرباك سلسلة القيادة، وإضعاف الوعي الظرفي في بيئة العمليات. كما يناقش البحث نقاط الضعف في البنية الرقمية للقوة الجوية، ويبرز الحاجة إلى تطوير عقيدة سيبرانية جوية تعزّز مرونة الأنظمة وقدرتها على الصمود أمام التهديدات. ويخلص البحث إلى أن دمج الأمن السيبراني داخل العقيدة الجوية يمثل شرطاً أساسياً لتحقيق التفوق الجوي في الحروب الحديثة.

الكلمات المفتاحية: العقيدة الجوية، الحرب السيبرانية، الامن السيبراني، المجال الجوي السيبراني، الهجوم السيبراني.

تاريخ الاستلام ٢٠٢٥/١١/٢٤ تاريخ القبول ٢٠٢٦/٢/١ تاريخ النشر ٢٠٢٦ /٣/١

Cyberattacks Impact on Modern Air Doctrine and Command and Control

Firas Jamal Shaker Mahmood Al-Rubaye
Imam Ja'afar Al-Sadiq University
Firas.alrubaye89@gmail.com

Abstract:
This research examines the impact of the increasing cyberattacks on modern air doctrine and command-and-control systems, in light of the substantial shift toward reliance on digital systems and network-based communications in managing air operations. The study highlights how cyberattacks have become capable of disrupting air capabilities, confusing the chain of command, and weakening situational awareness within the operational environment. It also discusses the vulnerabilities within the digital infrastructure of the air force and underscores the need to develop a cyber-air doctrine that enhances system resilience and strengthens the ability to withstand emerging threats. The research concludes that integrating cybersecurity into air doctrine has become an essential requirement for achieving air superiority in modern warfare.

Key words: Air Doctrine ،Cyber Warfare ،Cybersecurity ،Cyber–Air Domain ،Cyber Attack.

Date Received: 24/11/2025 Date Accepted: 1/2/2026 Date Published 1/3/2026

DOI: https:// doi. Org/***

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

المقدمة:

شهدت العقيدة الجوية الحديثة تحولاً جذرياً خلال العقدين الأخيرين مع تصاعد الاعتماد على النظم الرقمية، والاتصالات المشفرة، والحوسبة السحابية العسكرية، ومنصات الذكاء الاصطناعي في إدارة العمليات الجوية. هذا التحول التكنولوجي الواسع، الذي عزز من دقة الضربات الجوية وفعالية الدعم اللوجستي والعمليات المشتركة، جعل المنظومات الجوية أكثر عرضةً لهجمات سيبرانية معقدة تستهدف مراكز القيادة والسيطرةC2 ، وأنظمة الإنذار المبكر، ومنظومات التحكم بالطائرات المأهولة وغير المأهولة على حدٍّ سواء. تتمثل خطورة الهجمات السيبرانية في كونها هجمات غير مرئية وغير متماثلة، إذ لا تقتصر آثارها على الجبهة العسكرية فقط، بل تمتد لتصيب الاقتصاد الوطني وشبكات الطاقة والاتصالات والبنى الاستراتيجية. وقد كشفت العديد من الحوادث العالمية عن إمكانية استخدام الهجمات السيبرانية لتعطيل طائرات أو أنظمة توجيه دقيقة أو أقمار صناعية عسكرية، الأمر الذي يجعل من السيطرة على الفضاء السيبراني شرطاً أساسياً للسيطرة على الفضاء الجوي. لم تعد التهديدات السيبرانية مجرد أدوات لتعطيل الشبكات أو التشويش على الرادارات، بل أصبحت سلاحاً استراتيجياً يُدار عبر فضاء غير مرئي قادر على شلّ القدرة الجوية، إرباك القرارات، وتضليل القادة في اللحظات الحاسمة. وقد أظهرت عدة صراعات حديثة—منها الحرب الروسية الأوكرانية، والهجمات المتبادلة بين إيران وإسرائيل، والاختراقات التي طالت أنظمة الدفاع الجوي في الشرق الأوسط—أن التفوق الجوي لم يعد يعتمد فقط على الطائرات المتقدمة، بل على متانة البنية السيبرانية التي تديرها وتحميها.

أهمية البحث:

تنبع أهمية هذا البحث من التحولات العميقة التي يشهدها ميدان القوة الجوية في ظل التصاعد المتسارع للهجمات السيبرانية، والتي أصبحت قادرة على التأثير في بنية العقيدة الجوية الحديثة، وتهديد الفاعلية العملياتية لأنظمة القيادة والسيطرة. ومع ازدياد اعتماد القوة الجوية على الأنظمة الرقمية، والذكاء الاصطناعي، والاتصالات المشفرة، أصبح المجال الجوي أكثر ارتباطاً بالفضاء السيبراني، ما يجعل أي اختراق أو هجوم سيبراني قادراً على شل القدرات الجوية أو انتزاع السيطرة من القادة في لحظات حاسمة. وعليه، فإن هذا البحث يسهم في فهم التأثيرات العملياتية والاستراتيجية لهذه الهجمات، ويوضح ضرورة إعادة تشكيل العقيدة الجوية لتتلاءم مع بيئة التهديدات الرقمية الحديثة، ويقدم إطاراً نظرياً يعزز وعي المؤسسات العسكرية بآليات الحماية والتطوير.

إشكالية البحث:

تتمثل الإشكالية الرئيسة للبحث في الآتي:

تتمثل إشكالية البحث في أن تصاعد الهجمات السيبرانية وتحوّل الفضاء السيبراني إلى مجال عملياتي فاعل قد أوجد تهديدات نوعية تمسّ جوهر العقيدة الجوية الحديثة، ولاسيما اعتمادها المتزايد على أنظمة القيادة والسيطرة والاتصالات والاستشعار الرقمية. ويبرز التساؤل حول مدى قدرة هذه العقيدة على التكيّف مع التهديدات السيبرانية، وانعكاس ذلك على فاعلية التفوق الجوي، واستمرارية العمليات الجوية، ومستقبل الردع السيبراني ضمن بيئة الصراع المعاصر؟

وتنبثق من هذه الإشكالية الرئيسة مجموعة تساؤلات فرعية، منها:

ما طبيعة التحول في طبيعة الحروب وأثره على بيئة العمليات الجوية؟

ما نوعية الهجمات السيبرانية والتحديات التقنية للقوات الجوية في الحروب السيبرانية؟

ما طبيعة وتصنيف الهجمات السيبرانية على نظم القيادة والسيطرة العسكرية؟

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

ما هو مستقبل الردع السيبراني الجوي؟

فرضية البحث

تنطلق هذه الدراسة من فرضية مفادها أن تصاعد الهجمات السيبرانية أدى إلى إحداث تحوّل جوهري في العقيدة الجوية الحديثة، من خلال تقويض كفاءة وموثوقية أنظمة القيادة والسيطرة الجوية، الأمر الذي فرض إعادة صياغة مفاهيم التفوق الجوي، واتخاذ القرار، وإدارة العمليات الجوية المشتركة.

أهداف البحث:

١. تحليل طبيعة التحول في أنماط الحروب المعاصرة، ولاسيما الانتقال من الحروب التقليدية إلى الحروب المركّبة والسيبرانية، وبيان انعكاسات هذا التحول على بيئة العمليات الجوية والعقيدة القتالية للقوات الجوية الحديثة.

٢. تحديد نوعية الهجمات السيبرانية التي تستهدف القوات الجوية، مع التركيز على الهجمات الموجّهة ضد أنظمة الطيران العسكري، والاتصالات الجوية، وأنظمة الاستشعار والإنذار المبكر، وبيان التحديات التقنية التي تواجهها القوات الجوية في مواجهتها.

٣. تصنيف وتحليل الهجمات السيبرانية الموجّهة ضد نظم القيادة والسيطرة العسكريةC2 ، وبيان أساليب تنفيذها، ومستويات تأثيرها العملياتي، وانعكاساتها على عملية اتخاذ القرار والسيطرة على العمليات الجوية.

٤. تقييم أثر الهجمات السيبرانية على فاعلية التفوق الجوي والجاهزية القتالية، من خلال دراسة تأثيرها على التنسيق الجوي المشترك، وسلامة سلاسل القيادة، واستمرارية العمليات الجوية في بيئات الصراع الحديثة.

٥. استشراف مستقبل الردع السيبراني الجوي، وتحليل الاتجاهات المستقبلية لتكامل القدرات السيبرانية ضمن العقيدة الجوية، بما يسهم في بناء نماذج ردع جديدة تحافظ على التوازن الاستراتيجي في المجال الجوي–السيبراني.

هيكلية البحث:

تم تقسيم البحث على ثلاث مطالب لإحاطة البحث من الناحية العلمية والأكاديمية وتحقيق الغاية البحثية من معالجة المشكلة والتوصل الى الاستنتاجات والاقتراحات المنطقية وكما يلي:

أولا: المطلب الأول. الإطار النظري والمفاهيمي.

ثالثا: المطلب الثاني. طبيعة وتصنيف الهجمات السيبرانية على نظم القيادة والسيطرة العسكرية.

ثانيا: المطلب الثالث. التحديات التقنية للقوات الجوية في الحروب السيبرانية.

المطلب الأول: الإطار النظري والمفاهيمي .

The Theoretical and Conceptual Framework.

تعتمد القوات الجوية الحديثة في أداء مهامها القتالية والدفاعية على منظومات رقمية متشابكة تضم شبكات الاتصالات، وأنظمة الملاحة والقيادة والسيطرة، والطائرات المقاتلة المجهزة بالذكاء الاصطناعي والطائرات المسيّرة الدرونز، ومراكز التحليل الإلكتروني. هذا الاعتماد الواسع على التكنولوجيا جعلها عرضة لهجمات سيبرانية متطورة يمكن أن تستهدف البنى التحتية للمعلومات، أو تُحدث اختراقاً في شبكات القيادة الجوية، أو تُعطل أنظمة الدفاع الجوي والرادار. ومن هنا أصبح التهديد السيبراني يمثل تحدياً مباشراً لقدرة القوات الجوية على تنفيذ عملياتها بكفاءة وضمان تفوقها العملياتي. أن التحول نحو الذكاء الاصطناعي والطائرات غير المأهولة أوجد تحديات جديدة أمام الأمن الجوي، فهذه الأنظمة المتصلة بشبكات معقدة يمكن أن تكون عرضة للتلاعب أو السيطرة الخارجية إذا

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

لم تُؤمَّن سيبرانياً بشكل محكم. إضافة إلى ذلك، فإن التكامل بين نظم الدفاع الجوي والفضاء السيبراني يجعل أي ثغرة إلكترونية قادرة على تهديد السيادة الجوية للدولة.

سيتم بيان اهم المفاهيم الأساسية في هذا البحث لتوضيح الإطار النظري وعلاقتها التكاملية وكما يلي: (احمد، ٢٠٢٢)

أولا: العقيدة الجوية: هي مجموعة المبادئ والمفاهيم والممارسات التي تنظّم كيفية استخدام القوة الجوية لتحقيق الأهداف العسكرية للدولة، من خلال تحديد أساليب التخطيط، وإدارة العمليات، والتكامل مع الأفرع الأخرى للقوات المسلحة. وتشمل العقيدة الجوية الأسس الفكرية التي تُوجّه استخدام الطائرات المأهولة وغير المأهولة، وأنظمة الاستطلاع، والقيادة والسيطرة، والدفاع الجوي، بما يحقق التفوق في المجال الجوي ويضمن فعالية العمليات المشتركة. وتُعد العقيدة إطاراً استراتيجياً يحدد كيفية توظيف القدرات الجوية في السلم والحرب، وتطويرها، وإدارتها ضمن بيئة عملياتية متغيرة تقنياً واستراتيجياً (القوة الجوية الامريكية، ٢٠٢١)

ثانيا: العقيدة السيبرانية الجوية: هي الإطار الفكري والمفاهيمي الذي ينظّم كيفية دمج القدرات السيبرانية مع القوة الجوية بهدف حماية الأنظمة الجوية، وتعزيز فعاليتها العملياتية، وتوسيع نطاق تأثيرها داخل الفضاء السيبراني. وتشمل هذه العقيدة المبادئ التي تحدد كيفية الدفاع والهجوم في الفضاء السيبراني المرتبط بالمنظومات الجوية، بما في ذلك حماية أنظمة القيادة والسيطرة، والطائرات المأهولة وغير المأهولة، والرادارات، والأقمار الصناعية، وشبكات الاتصالات المشفرة. وتسعى العقيدة السيبرانية الجوية إلى توظيف القدرات السيبرانية لحماية التفوق الجوي، وردع الخصوم، ومنع الاختراقات التي قد تشل أو تربك العمليات الجوية. كما تضع أسس التكامل بين العمل الجوي والعمليات السيبرانية، بحيث تُعامل الهجمات السيبرانية باعتبارها جزءًا من بيئة القتال الجوية وليست مجرد تهديد تقني منفصل. (وزارة الدفاع الامريكية، ٢٠٢٠)

ثالثا: المجال الجوي السيبراني: هو الامتداد الرقمي الموازي للمجال الجوي التقليدي، والذي يضم البنية المعلوماتية والاتصالات والبرمجيات التي تتحكم في المنصات الجوية بمختلف أنواعها، بما في ذلك الطائرات المأهولة وغير المأهولة، وأنظمة القيادة والسيطرة، وشبكات الاتصالات العسكرية، والرادارات، والأقمار الصناعية. ويمثل هذا المجال البيئة التي تُنفَّذ فيها العمليات السيبرانية المرتبطة بالقدرات الجوية، سواء كانت عمليات دفاعية أو هجومية أو عمليات دعم استخباري وتشغيلي. ويُعد المجال الجوي السيبراني عنصراً حيوياً للأمن الجوي الحديث، إذ تُدار عبره سلسلة واسعة من المهام: الملاحة الرقمية، الاستطلاع الإلكتروني، نقل البيانات، إدارة المهام الجوية، وتوجيه المنظومات القتالية. كما يشكل ساحة صراع غير مرئية، يمكن عبرها التأثير على كفاءة القوة الجوية، وعرقلة العمليات، أو تعطيل قدرات الردع الجوي للدولة. (الناتو، ٢٠٢١)

رابعا: الأمن السيبراني Cybersecurity. يُعرَّف الأمن السيبراني بأنه مجموعة من السياسات والإجراءات والتقنيات المصممة لحماية الأنظمة الحاسوبية وشبكات الاتصالات والبنى التحتية الرقمية من أي اختراق أو هجوم أو استخدام غير مصرح به. ويهدف إلى الحفاظ على سرية المعلومات وسلامتها وتوافرها Confidentiality, Integrity, Availability. وفي السياق العسكري يعد الأمن السيبراني أحد أركان القوة الدفاعية الحديثة، إذ يسهم في تأمين شبكات القيادة والسيطرة، وأنظمة الطيران، وقواعد البيانات الحساسة، والاتصالات المشفرة، مما يضمن استمرارية العمليات الجوية وحماية المجال المعلوماتي للدولة من التهديدات الخارجية.

خامسا: الهجوم السيبراني Cyber Attack. الهجوم السيبراني هو أي عمل عدائي يتم عبر الفضاء الإلكتروني يهدف إلى إتلاف أو تعطيل أو السيطرة على أنظمة الحواسيب والشبكات أو سرقة البيانات أو التأثير في قرارات أو عمليات الخصم. وتتخذ الهجمات السيبرانية أشكالاً متعددة مثل:

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

(جامعة الدفاع الوطني، ٢٠٢١)

١. الاختراق Hacking للأنظمة والشبكات.
٢. التشويش والتعطيل Denial of Service - DoS على المواقع أو الشبكات.
٣. زرع البرمجيات الخبيثة Malware في الأنظمة الحساسة.
٤. الهندسة الاجتماعية Social Engineering لاختراق العنصر البشري.
٥. في الميدان العسكري، يمكن للهجوم السيبراني أن يؤدي إلى تعطيل أنظمة الدفاع الجوي، أو شل حركة الاتصالات بين الطائرات ومراكز القيادة، أو التلاعب في بيانات الاستطلاع والمراقبة الجوية.

سادسا: الحروب السيبرانية Cyber Warfare. تُعرَّف الحروب السيبرانية بأنها استخدام القدرات التقنية في الفضاء الإلكتروني كوسيلة لتحقيق أهداف عسكرية أو سياسية ضد دولة أخرى، عبر شن هجمات رقمية واسعة النطاق تستهدف البنى التحتية الحيوية أو الأنظمة الدفاعية أو الاقتصادية للخصم. وتتميز الحرب السيبرانية بكونها حرباً غير تقليدية وغير متماثلة، إذ لا تعتمد على الجغرافيا أو القوات الميدانية، بل على القدرات التقنية والاستخبارية. وفي المجال الجوي، تمثل الحرب السيبرانية ميداناً خفياً للتفوق العسكري، حيث يمكن لأي اختراق ناجح أن يغيّر موازين القوة دون مواجهة مباشرة، مثل السيطرة على الطائرات بدون طيار أو تعطيل أنظمة الدفاع الجوي عبر هجوم رقمي دقيق.

سابعا: الفضاء السيبراني Cyberspace. الفضاء السيبراني هو البيئة الافتراضية الناتجة عن الترابط العالمي بين شبكات الحواسيب والاتصالات والأنظمة الرقمية، والتي يتم من خلالها تخزين ومعالجة وتبادل المعلومات. ويُعد الفضاء السيبراني اليوم البُعد الخامس للعمليات العسكرية بعد البر والبحر والجو والفضاء الخارجي، إذ تُدار فيه عمليات استخباراتية وهجومية ودفاعية على مستوى استراتيجي. ويشمل الفضاء السيبراني كل ما يتصل بالشبكات العسكرية وأنظمة الرادار والطائرات المسيرة والمراكز الأرضية، مما يجعله مسرحاً رئيسياً للصراع الحديث الذي يستهدف السيطرة على المعلومات والقدرة على تعطيل الخصم رقمياً.

ثامنا: الأسلحة السيبرانية Cyber Weapons. الأسلحة السيبرانية هي أدوات أو برامج رقمية تُستخدم لتنفيذ هجمات إلكترونية هجومية ضد أهداف محددة بهدف إلحاق الضرر أو تعطيل الأنظمة أو التسلل إليها أو السيطرة عليها. وهي تختلف عن الأسلحة التقليدية بكونها غير مادية وغير مرئية، وتعمل عبر الأكواد البرمجية والفيروسات الخبيثة والبرمجيات التجسسية، وقد تشمل الأسلحة السيبرانية أدوات مثل: (شاريكوف، ٢٠٢١)

١. الفيروسات Viruses وديدان الإنترنت Worms.
٢. برامج التجسس Spyware.
٣. أدوات التحكم عن بُعد Remote Access Tools.
٤. خوارزميات الذكاء الاصطناعي القادرة على استهداف نقاط الضعف في الأنظمة.
٥. في المجال الجوي، تُستخدم هذه الأسلحة لتعطيل أنظمة التوجيه والملاحة، أو اختراق الطائرات غير المأهولة، أو السيطرة على مراكز القيادة الجوية.

العلاقة التكاملية بين المفاهيم السيبرانية والقوات الجوية في الحروب المستقبلية

تشكل المفاهيم السابقة منظومة مترابطة تمثل الإطار النظري لفهم طبيعة التحديات التي تواجه القوات الجوية في عصر الحروب السيبرانية. فالأمن السيبراني يمثل الركيزة الدفاعية التي تضمن سلامة البنى التحتية الرقمية ومنظومات القيادة والسيطرة الجوية، بينما يُعد الهجوم السيبراني الأداة التي يمكن عبرها إضعاف الخصم أو تحييد قدراته الجوية دون اللجوء إلى المواجهة العسكرية المباشرة. أما

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

الحرب السيبرانية فهي الإطار الأشمل الذي يجمع بين الهجوم والدفاع، ويجسّد انتقال الصراع من ميادين القتال المادية إلى فضاء إلكتروني لا تحدهُ الجغرافيا باستخدام عناصر القوة السيبرانية.

أولا: التحول في طبيعة الحروب وأثره على بيئة العمليات الجوية

ان دراسة التحول في طبيعة الحروب واحد من اهم الضرورات الحتمية للتعرف على دلالات الحرب القادمة فضلا عن ذلك لقد غيّر الفضاء السيبراني معادلات الحرب التقليدية وأعاد تشكيل بيئة العمليات الجوية على نحو جذري فالتفوق الجوي لم يعد يُكتسب بالقوة النارية فقط، بل بامتلاك تفوق معلوماتي وتقني يضمن الحماية من الهجمات الرقمية والقدرة على شنها عند الحاجة. ومن ثمّ، فإن فهم التحول في طبيعة الحروب يشكل الأساس الضروري لتحليل التحديات المستقبلية التي ستواجه القوات الجوية في ميادين القتال السيبرانية. بناءا على ذلك تم تقسيم هذا المحور الى الفروع التالية وكما يلي:
(القوة الجوية الامريكية، ٢٠٢٢)

١. **التحول الاستراتيجي في طبيعة الصراع العسكري**. أصبحت بيئة الصراع العسكري في القرن الحادي والعشرين أكثر تعقيدًا وتداخلًا، نتيجة الثورة الرقمية والتكنولوجية التي أعادت تعريف مفهوم الحرب وأدواتها. فقد انتقل العالم من الحروب التقليدية التي تعتمد على القوة المادية إلى حروب رقمية تعتمد على القوة المعلوماتية والسيطرة التقنية وفي ظل هذا التحول، لم تعد الجيوش الحديثة تُقاتل في ميادين الأرض والبحر والجو فحسب، بل انتقلت المعارك إلى الفضاء السيبراني بوصفه بعدًا عملياتيًا جديدًا تتقاطع فيه المعلومات مع القدرات العسكرية. ولأن القوات الجوية هي أكثر فروع القوات المسلحة ارتباطًا بالتكنولوجيا وأنظمة القيادة والسيطرة والاتصال، فقد أصبحت في مقدمة الجبهات المعرضة للهجمات السيبرانية. فكل طائرة حديثة، سواء كانت مأهولة أو غير مأهولة، تعتمد على شبكات رقمية معقدة تربطها بالأقمار الصناعية والمراكز الأرضية ومنظومات التوجيه الذكي، ما يجعلها هدفًا مثاليًا لأي محاولة اختراق أو تشويش إلكتروني. (مارتن، ٢٠٠٩)

٢. **بروز الفضاء السيبراني كامتداد للفضاء الجوي**. لم يعد الفضاء الجوي منفصلًا عن الفضاء السيبراني، بل أصبح كلاهما يشكل بيئة عمليات موحدة تُدار فيها المعارك بشكل متزامن. فأنظمة الملاحة الجوية GPS، والرادارات بعيدة المدى، وأجهزة الاستشعار، والطائرات المسيرة، جميعها تعمل ضمن فضاء معلوماتي مترابط يعتمد على التدفق الآني للبيانات. لقد تحول الفضاء السيبراني إلى ما يمكن وصفه بـ السماء الرقمية، التي تُدار فيها عمليات المراقبة، وتبادل الإشارات، والتوجيه القتالي، وإدارة المهمات الجوية. وفي المقابل، أصبح الفضاء الجوي نفسه عرضة لهجمات إلكترونية يمكن أن تُعطّل شبكات الإنذار المبكر أو تُضلّل أنظمة الدفاع الجوي أو تُسيطر على الطائرات المسيرة عن بعد. هذا التكامل بين المجالين أوجد نمطًا جديدًا من الحروب الجوية السيبرانية، حيث لا تكون المعركة مقتصرة على صواريخ أو مقاتلات، بل تشمل أيضًا البرمجيات والخوارزميات التي تتحكم في الأنظمة الرقمية للعدو أو تدافع عنها (الناتو، ٢٠٢١).

٣. **انعكاسات الثورة التكنولوجية على أداء القوات الجوية**. لقد جعلت الثورة الرقمية من القوات الجوية أحد أكثر الأفرع العسكرية تطورًا من الناحية التقنية، لكنها في الوقت ذاته الأكثر هشاشة أمام الهجمات السيبرانية. فالقوات الجوية الحديثة تعتمد على منظومات متشابكة تُعرف اختصارًا بـ CIS4R القيادة والسيطرة والاتصالات والحواسيب والاستخبارات والمراقبة والاستطلاع. هذه المنظومات هي العمود الفقري للعمليات الجوية، وأي هجوم إلكتروني يستهدفها يمكن أن يؤدي إلى فقدان السيطرة على المجال الجوي بأكمله. ومن أبرز التهديدات التي تواجهها القوات الجوية في هذا الإطار: (الناتو، ٢٠٢٢).

أ. اختراق شبكات القيادة والسيطرة الجوية مما يؤدي إلى تعطيل القرارات العملياتية أو تضليلها.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

ب. الهجمات على أنظمة الطائرات بدون طيار UAVs، سواء بالسيطرة عليها أو بإيقافها عن العمل.
ج. تشويش أنظمة الملاحة والاتصال مما يؤثر في دقة الضربات الجوية أو يربك مسارات الطائرات.
د. استهداف البنى التحتية الأرضية مثل مراكز الاتصالات والرادارات وقواعد البيانات.
ه. إن هذه التحديات تُبرز أن التفوق الجوي لم يعد يُقاس بعدد الطائرات أو مدى الصواريخ، بل بقدرة الدولة على تأمين فضائها الإلكتروني المرتبط بالعمليات الجوية.

٤. **السيادة الجوية في الحروب السيبرانية**. كان مفهوم السيادة الجوية في الماضي يُقاس بقدرة القوات الجوية على السيطرة الميدانية على سماء المعركة ومنع العدو من استخدامها. أما اليوم، فقد تطوّر المفهوم ليشمل السيطرة على المجال المعلوماتي الذي يدير تلك السماء. فالدولة التي تفقد السيطرة على شبكاتها الرقمية أو أنظمة اتصالاتها الجوية لا يمكن أن تدّعي امتلاكها للسيادة الجوية، حتى وإن امتلكت أحدث الطائرات. إذ يمكن لهجوم سيبراني دقيق أن يعطّل أنظمة الرادار أو يشوّه بيانات الأقمار الصناعية أو يقطع الاتصال بين الطيارين ومراكز القيادة، مما يؤدي إلى شلل كامل في القدرة على إدارة العمليات. لذلك أصبحت الحماية السيبرانية جزءًا من معادلة التفوق الجوي، وأحد عناصر الردع في الاستراتيجية الجوية الحديثة. لقد غيّر هذا البعد الجديد موازين القوة، وجعل السيطرة على الفضاء السيبراني شرطًا مسبقًا للسيطرة على الفضاء الجوي (كولن، ٢٠١٢).

٥. **انعكاس الثورة التكنولوجية على أداء القوات الجوية الحديثة.** شهدت القوات الجوية تحولًا عميقًا في بنيتها ووظائفها مع دخول تكنولوجيا المعلومات والاتصالات المتقدمة إلى ميدان الحرب. فأنظمة الطيران الحديثة أصبحت تعتمد على الذكاء الاصطناعي، ونظم القيادة والسيطرة CIS4R، والتشبيك بين الطائرات والمراكز الأرضية والأقمار الصناعية. هذه التقنيات رفعت كفاءة الأداء القتالي، وسرّعت اتخاذ القرار، لكنها في المقابل زادت من حجم التعرض للمخاطر السيبرانية، إذ إن أي اختراق بسيط يمكن أن يُعطّل أنظمة الطيران أو يُضلل مسارات الطائرات أو يُحدث خللاً في توجيه الأسلحة الذكية. كما أن إدخال الطائرات المسيرة والطائرات بدون طيار UAVs فتح الباب أمام استخدامات واسعة في الاستطلاع والهجوم، لكنها أيضًا شكلت تحديًا أمنيًا سيبرانيًا كبيرًا، لأن هذه الأنظمة تعمل عبر روابط بيانات قابلة للاختراق أو التشويش. وبالتالي أصبحت حماية المنظومات الجوية من الهجمات الرقمية جزءًا من الأمن القتالي نفسه (جيمس، ٢٠٢٠).

٦. **الأمن المعلوماتي كعنصر من عناصر القوة الجوية.** أصبح الأمن المعلوماتي في زمن الحروب السيبرانية مكوّنًا أساسيًا من مكونات القوة الجوية. فالبيانات والمعلومات التي تُنقل بين الطائرات وغرف القيادة ومراكز الاستخبارات تمثل عصب العمليات الجوية الحديثة. أي اختراق أو تلاعب بهذه البيانات يؤدي إلى نتائج كارثية على الأداء العملياتي. فالقوة الجوية المعاصرة تعتمد على منظومات رقمية متصلة ببعضها البعض عبر شبكات مشفّرة، تشمل: (محمد ٢٠٢٢)

أ. أنظمة الملاحة الجوية GPS.
ب. أنظمة القيادة والسيطرة CIS4R.
ج. أنظمة الاستهداف الذكي وتحديد الأهداف عبر الأقمار الصناعية.
د. منظومات الطائرات المسيرة UAVs والطائرات الشبحية.
ه. إن اختراق أي من هذه المنظومات يمكن أن يؤدي إلى فقدان الطائرة أو توجيهها بشكل خاطئ أو تعطيل قدرتها على تنفيذ المهمة. ولهذا، فإن أمن المعلومات أصبح لا يقل أهمية عن أمن الطائرات نفسها، وأي ثغرة رقمية تُعد بمثابة نقطة ضعف عملياتية يمكن استغلالها من قبل الخصم.

ثانيا: الهجمات السيبرانية وإعادة تعريف الردع الجوي .

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

P- ISSN: 2070-898X E-ISSN: 2707-9775

كان مفهوم الردع الجوي يقوم على امتلاك الطائرات المتفوقة والأسلحة الدقيقة التي تبعث برسالة قوة إلى الخصم. أما في ظل الحروب السيبرانية، فقد تطوّر الردع ليشمل أيضًا القدرات السيبرانية الهجومية والدفاعية التي تمكّن الدولة من حماية أنظمتها الرقمية، وتهديد الخصم رقميًا في المقابل. فامتلاك قوة جوية سيبرانية أصبح جزءًا من معادلة الردع الشامل، إذ يمكن عبر القدرات الإلكترونية المتقدمة تعطيل رادارات العدو، أو شل مراكز القيادة الجوية، أو اختراق طائراته دون الحاجة إلى مواجهة عسكرية مباشرة. وبالتالي، فإن الردع في عصر الفضاء السيبراني يقوم على مبدأ "من يمتلك السيطرة على المعلومة، يمتلك السيطرة على السماء". إن هذا التحول فرض على الجيوش تطوير عقيدة ردع سيبرانية جوية، تعتمد على مزيج من الدفاع الرقمي المتقدم، والقدرات الهجومية الإلكترونية القادرة على تنفيذ عمليات دقيقة ضد البنى التحتية الجوية المعادية عند الضرورة. (عبد القادر، ٢٠٢٥)

ثالثا: الذكاء الاصطناعي والقيادة الذاتية كجزء من التحدي السيبراني الجوي .

يشكل إدخال الذكاء الاصطناعي AI في المنظومات الجوية الحديثة بُعدًا جديدًا في الحرب السيبرانية. فأنظمة الطيران الذاتي، والطائرات بدون طيار، وأنظمة اتخاذ القرار الآلي، جميعها تعتمد على الخوارزميات والبيانات الضخمة التي يمكن استهدافها أو التلاعب بها. إن الخطر الحقيقي في هذا الجانب لا يتمثل فقط في الهجوم الإلكتروني، بل في الاختراق الخفي للذكاء الاصطناعي نفسه، عبر زرع أكواد خبيثة داخل الأنظمة الذكية يمكن تفعيلها في لحظة حرجة. وهذا يعني أن الحروب المستقبلية قد لا تكون بين طائرات فحسب، بل بين خوارزميات تتنافس على السيطرة على المجال الجوي الرقمي. ولهذا السبب، بدأت الجيوش المتقدمة في إنشاء ما يُعرف بـ "القيادة السيبرانية الجوية"، وهي وحدات متخصصة تتابع التهديدات الإلكترونية التي تستهدف القوات الجوية، وتعمل على تطوير منظومات الذكاء الاصطناعي الآمن والمحصّن ضد الاختراقات. (احمد، ٢٠٢٤)

رابعا: القيادة والسيطرة في بيئة الهجمات السيبرانية الجوية .

تُعد منظومات القيادة والسيطرة Command and Control Systems القلب النابض لأي عملية جوية، فهي تنسّق بين الطيارين والمراكز الأرضية ووحدات الدفاع الجوي والاستطلاع. لكن في بيئة الحرب السيبرانية، أصبح هذا القلب معرضًا لهجمات دقيقة يمكنها أن تُحدث شللًا كاملًا في منظومة القيادة من خلال: (التطورات التكنولوجية، ٢٠٢٣)

١. اعتراض الاتصالات المشفرة.
٢. إدخال بيانات مزيفة إلى أنظمة الرادار.
٣. تنفيذ هجمات "الحرمان من الخدمة" لتعطيل مراكز القيادة.
٤. هذه التهديدات دفعت الدول إلى تطوير ما يُعرف بـ "القيادة والسيطرة السيبرانية المتكاملة"، وهي بنية رقمية جديدة تُدمج فيها إجراءات الأمن السيبراني ضمن كل مرحلة من مراحل التخطيط والتنفيذ الجوي، لضمان الاستمرارية والمرونة في مواجهة الهجمات الرقمية المفاجئة.

يتضح أن الحروب والهجمات السيبرانية أعادت تشكيل جوهر القوة الجوية الحديثة من أساسه، إذ تحولت السماء من ساحة للطائرات إلى ميدان للشبكات الرقمية والأنظمة الذكية. فمن يسيطر على البيانات، يسيطر على الطائرة؛ ومن يسيطر على الطائرة، يسيطر على السماء ولذلك، فإن مفهوم القوة الجوية لم يعد يُختزل في الأسلحة أو الطيارين، بل في القدرة على حماية الفضاء السيبراني الجوي وتوظيفه بفعالية في الصراع العسكري.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

المطلب الثاني: طبيعة وتصنيف الهجمات السيبرانية على نظم القيادة والسيطرة العسكرية .

The Nature and Classification of Cyberattacks on Military Command and Control Systems

تمثل أنظمة القيادة والسيطرة العسكرية Command and Control Systems – C2 العمود الفقري للعمليات الحديثة، إذ تُعدّ الأداة التي تربط بين القيادة العليا والوحدات الميدانية في المستويات العملياتية والتعبوية، وتتيح تبادل الأوامر والمعلومات بصورة آنية ودقيقة. ومع تطور البيئة العملياتية وتحولها إلى بيئة رقمية مترابطة تعتمد على البرمجيات والشبكات، أصبحت هذه الأنظمة عرضة لهجمات سيبرانية متقدمة تستهدف قلب القدرة العسكرية في مراحل التخطيط والتنفيذ.

تنبع خطورة الهجمات السيبرانية على نظم القيادة والسيطرة من كونها لا تهاجم السلاح مباشرة بل تهاجم المعلومة التي توجه السلاح، أي أنها تضرب عقل المؤسسة العسكرية لا أطرافها. فهي قادرة على تعطيل تدفق البيانات، أو تزوير المعلومات الميدانية، أو التشويش على قنوات الاتصال بين القيادة والقوات، مما يؤدي إلى شلل جزئي أو كلي في عملية اتخاذ القرار. (مايكل، ٢٠١٧)

إنّ طبيعة هذه الهجمات تتسم بالتعقيد والتخفي، فهي لا تحتاج إلى وجود مادي في ميدان القتال، بل تُنفذ عبر الفضاء الإلكتروني بوسائل رقمية يمكنها التسلّل إلى الخوادم وأنظمة الاتصالات الحساسة دون أن تُكتشف فورًا. كما أنّ تصنيف هذه الهجمات يختلف بحسب الهدف، والأسلوب، ومستوى التأثير، حيث تشمل أنماطًا تتراوح بين التجسّس الإلكتروني، والتعطيل المؤقت، والتلاعب بالمعلومات، وصولًا إلى الهجمات المدمّرة التي قد تمحو بيانات القيادة بالكامل. وفي ظل تسارع الاعتماد على النظم الذكية في المؤسسات العسكرية، بات من الضروري دراسة طبيعة هذه الهجمات وفهم تصنيفاتها بدقة، لتصميم استراتيجيات دفاعية فعّالة تضمن مرونة واستمرارية أنظمة القيادة والسيطرة في مواجهة أي تهديد سيبراني قد يستهدفها في المستقبل. (مارتن، ٢٠٠٩)

أولا: طبيعة وتصنيف الهجمات السيبرانية

تصنَّف الهجمات السيبرانية التي تستهدف نظم القيادة والسيطرة العسكرية وفق مجموعة من المعايير المتداخلة، تختلف بحسب الهدف الاستراتيجي، وطبيعة التأثير، ومستوى التقنية المستخدمة، ومصدر الهجوم .ويُعدّ هذا التصنيف خطوة أساسية لفهم كيفية حماية البنية التحتية القيادية من التهديدات الرقمية المتزايدة. وتصنف الى ما يلي:

١. هدف الهجوم:

أ. هجمات التجسّس الإلكتروني:Cyber Espionage

تهدف إلى اختراق الأنظمة لجمع معلومات حساسة تتعلق بالخطط العسكرية، مواقع الانتشار، أنظمة الأسلحة، والاتصالات القيادية. وغالبًا ما تُنفَّذ بطريقة خفية على مدى طويل، مما يجعلها الأخطر من حيث التأثير الاستراتيجي لأنها تضرب عنصر السرّية الذي تعتمد عليه القيادة العسكرية. (توماس، ٢٠١٣)

ب. هجمات التعطيل والتشويش:Disruption and Denial

تسعى إلى شلّ قدرة القيادة على التواصل والسيطرة عبر هجمات الحرمان من الخدمة DDoS أو قطع الاتصال بين المراكز الميدانية وغرف التحكم. وقد تُنفَّذ هذه الهجمات تزامنًا مع عمليات عسكرية ميدانية لإرباك سلسلة القيادة وتقليل كفاءة الرد. (مايكل، ٢٠١٤)

ب. هجمات التلاعب بالمعلومات:Manipulation and Deception

تستهدف تغيير أو تزوير البيانات داخل أنظمة القيادة والسيطرة، مثل تعديل مواقع الوحدات أو عرض أهداف وهمية أو أوامر مضلّلة. وهي أخطر الأنواع من حيث التأثير التكتيكي لأنها تؤدي إلى قرارات ميدانية خاطئة قد تسبّب خسائر مباشرة في ساحة القتال. (مؤسسة راند، ٢٠٢١)

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

ج. الهجمات المدمّرة:Destructive Attacks
تهدف إلى تدمير البنية الرقمية كليًا، مثل حذف قواعد البيانات أو تعطيل الخوادم عبر برمجيات مدمّرة Wiper Malware.وغالبًا ما تُستخدم هذه الهجمات في المراحل الأخيرة من النزاع السيبراني لإحداث شلل كامل في القيادة والسيطرة. (ليور، ٢٠١٥)

٢. من حيث طبيعة التأثير التقني: ونبين أهمها كما يلي : (كينيث، ٢٠١٥)

– **هجمات مباشرة :Direct Attacks** . تستهدف الأنظمة العسكرية الحيوية بشكل مباشر كخوادم القيادة، شبكات الاتصالات، الأقمار الصناعية، وأنظمة إدارة العمليات.

– **هجمات غير مباشرة:Indirect Attacks** . تركّز على مزوّدي الخدمات أو البنى التحتية الداعمة مثل شركات الاتصالات أو أنظمة الطاقة لإحداث تأثير غير مباشر على النظام القيادي.

– **هجمات مزدوجة:Combined or Multi-Vector Attacks** . تجمع بين الاختراق التقني والتأثير النفسي أو الإعلامي لتضليل القيادة وخلق فوضى معلوماتية داخل غرف السيطرة.

٣. من حيث مصدر التهديد (روبرت، ٢٠١٩)

– **هجمات ترعاها دول:State-Sponsored Attacks** . تُنفَّذ بواسطة وحدات سيبرانية عسكرية أو استخباراتية منظمة، تسعى إلى تحقيق تفوّق استراتيجي أو توازن ردع رقمي.

– **هجمات من جماعات غير حكومية:Non-State Actors** . تشمل الميليشيات الإلكترونية والجماعات الإرهابية التي تستخدم الفضاء السيبراني كوسيلة لتقويض قدرات الدولة العسكرية.

– **التهديدات الداخلية:Insider Threats** . تنشأ من أفراد داخل المؤسسة، سواء بسبب الإهمال أو القصد، ما يجعلها من أخطر التهديدات لصعوبة اكتشافها مبكرًا.

ثانيا: الطبيعة التقنية والعملياتية للهجمات السيبرانية .

تتميّز الهجمات السيبرانية على نظم القيادة والسيطرة العسكرية بكونها هجينة ومعقدة، فهي تجمع بين العناصر التقنية الصرفة والعناصر العملياتية الميدانية، بحيث تستهدف البنية التحتية الرقمية من جهة، والمنظومة القيادية والاتصالية من جهة أخرى. ويمكن تحديد أبرز السمات التقنية والعملياتية لهذه الهجمات في النقاط الآتية:

– **الطابع الشبكي المترابط :** وهي أنظمة القيادة والسيطرة تعتمد على شبكات متعددة المستويات استراتيجية، عملياتية، تكتيكية؛ لذلك يمكن لاختراقٍ واحد في نقطة اتصال فرعية أن يمتدّ إلى النظام المركزي عبر قنوات الربط، وهو ما*يُعرف بـ* سلسلة العدوى السيبرانية. (بيتر، ٢٠١٤)

– **الاعتماد على الذكاء الاصطناعي والتحليل الآلي:**طوّرت الجهات المهاجمة أدوات هجومية تستخدم الذكاء الاصطناعي لتعلّم أنماط السلوك داخل الشبكة وتعديل أسلوب الهجوم تلقائيًا، مما يقلّل من إمكانية اكتشافها في الوقت المناسب. (الناتو، ٢٠٢٠)

– **الاندماج مع الحرب الإلكترونية:Electronic Warfare Integration** في الحروب الحديثة، لم يعد الهجوم السيبراني منفصلًا عن التشويش الراداري أو الحرب الإلكترونية، بل يُنفَّذان بالتزامن لزيادة فعالية التشويش وتعطيل الاتصالات العسكرية. (مارتن، ٢٠١٦)

– **استهداف الثقة والمعلومة:Targeting Trust** ولا تقتصر هذه الهجمات على سرقة أو تدمير البيانات، بل تستهدف تقويض *ثقة القادة بالمعلومات المستلمة* من الأنظمة، مما يؤدي إلى تعطيل اتخاذ القرار أو اللجوء إلى أوامر يدوية أقل كفاءة. (مارتن، ٢٠٠٩)

– **تعدد طبقات الهجوم:** تبدأ الهجمات غالبًا من الطبقة البرمجية Software Layer عبر إدخال شيفرات خبيثة، ثم تنتقل إلى الطبقة الشبكية Network Layer لتدمير البنية التحتية، وفي النهاية تصل

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

إلى طبقة البيانات التشغيلية Operational Data التي تتحكم بحركة القوات والمعلومات الميدانية. (هيرب، ٢٠١٩)

– **الاستمرارية وصعوبة الاكتشاف**: بعض الهجمات تبقى كامنة داخل النظام لأشهر دون أن تُكتشف، وتُفعّل في لحظة حرجة مثل وقت العمليات أو المناورات، ما يجعلها أشبه بـ "قنابل منطقية رقمية" تنتظر الأمر للتنفيذ. (مايكل، ٢٠٢٢)

المطلب الثالث: التحديات التقنية للقوات الجوية في الحروب السيبرانية .

Technical Challenges of Air Forces in Cyber Warfare

تمثل الحروب السيبرانية أحد أبرز ملامح الصراع العسكري الحديث، إذ انتقل التهديد من ساحة المعركة التقليدية إلى فضاءٍ غير مرئي تتحكم فيه البيانات والشبكات. وفي ظل هذا التحول، أصبحت القوات الجوية في مقدمة المستهدفين لما تمتلكه من أنظمة رقمية معقدة تشكل العمود الفقري لعملياتها. ومن هنا تبرز أهمية دراسة التحديات المستقبلية للقوات الجوية في الحروب السيبرانية لفهم طبيعة المخاطر، وتحديد آليات المواجهة وبناء استراتيجيات تضمن التفوق في بيئة القتال الحديثة وكما يلي: (جين، ٢٠٢٣)

أولا: التحديات التقنية في بيئة الحرب السيبرانية الجوية

تواجه القوات الجوية في العالم مجموعة متصاعدة من التحديات التقنية المعقدة نتيجة الاعتماد الكبير على التكنولوجيا الرقمية في إدارة وتنفيذ العمليات الجوية. فكل طائرة مقاتلة حديثة تحتوي على آلاف الأنظمة الإلكترونية المترابطة، وكل شبكة قيادة وسيطرة تعتمد على اتصالات مؤمنة ومعالجات رقمية فائقة الحساسية. ومن أبرز التحديات التقنية التي تواجهها القوات الجوية في ميدان الهجمات السيبرانية ما يلي: (محمد، ٢٠٢٢)

– **تعقيد الأنظمة المترابطة Interconnected Systems**. إن تشابك الأنظمة بين الطائرات، والأقمار الصناعية، ومراكز القيادة، يخلق ثغرات يمكن للخصم استغلالها لاختراق الشبكة بأكملها. فالهجوم على نقطة واحدة في النظام قد يؤدي إلى انهيار متسلسل في المنظومات الجوية كافة.

– **ضعف أمن البرمجيات العسكرية.** تعتمد معظم المنظومات الجوية على برمجيات معقدة يتم تطويرها عبر عقود وشركات مختلفة. هذا التنوع في المصدر يؤدي أحيانًا إلى وجود ثغرات برمجية غير مكتشفة يمكن استغلالها في تنفيذ هجمات سيبرانية دقيقة تؤدي إلى تعطيل مهام الطيران أو فقدان السيطرة.

– **الاعتماد على الذكاء الاصطناعي والبيانات الضخمة**. إن استخدام تقنيات الذكاء الاصطناعي في الطائرات دون طيار وأنظمة الدفاع الجوي يوفر مرونة كبيرة في إدارة المعركة، لكنه في الوقت ذاته يُدخل القوات الجوية في دائرة جديدة من المخاطر تتعلق بإمكانية اختراق الخوارزميات أو التلاعب بالبيانات التدريبية، مما يهدد دقة القرار الآلي في القتال.

– **التهديدات الكامنة في سلسلة التوريد Supply Chain.** تعتمد القوات الجوية على مكونات إلكترونية وبرمجيات يتم تصنيعها عالميًا، وغالبًا ما تتضمن هذه السلسلة مورّدين من دول متعددة. هذه البيئة المعقدة تزيد من خطر زرع برمجيات خبيثة أو أبواب خلفية داخل المكونات الإلكترونية منذ مرحلة الإنتاج، مما يجعل الهجوم السيبراني يبدأ قبل دخول المنظومة الخدمة الفعلية.

ثانيا: التحديات في إدارة الهجمات السيبرانية الجوية .

ان تحليل طبيعة التحديات المستقبلية التي ستواجه القوات الجوية في ظل تصاعد الحروب السيبرانية امرا في غاية الأهمية، لذلك يمكن استعراض أبرز أشكال التهديدات الإلكترونية المحتملة، وتقييم مدى استعداد القوات الجوية لمواجهتها. كما يسعى البحث إلى تسليط الضوء على سبل تعزيز الدفاعات

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

السيبرانية الجوية من خلال تطوير الاستراتيجيات، وبناء القدرات التقنية والبشرية، وتكامل العقيدة العسكرية مع الأمن السيبراني كجزء لا يتجزأ من منظومة القوة الوطنية الشاملة.

إن التحديات المستقبلية للقوات الجوية في هذا الميدان لا تقتصر على التهديدات التقنية فقط، بل تمتد إلى البعد الاستراتيجي والتنظيمي والبشري، حيث تواجه القوات الجوية صعوبة في مواكبة التطور السريع في تقنيات الحرب السيبرانية، وفي بناء كوادر متخصصة تمتلك الخبرة التقنية والعسكرية الكافية للتعامل مع بيئة عمليات إلكترونية معقدة. كما أن غياب الأطر القانونية الدولية المنظمة لاستخدام القوة في الفضاء السيبراني يزيد من غموض المشهد ويضاعف المخاطر المستقبلية. (الناتو، ٢٠٢١)

تواجه القوات الجوية تحديات واسعة تتعلق بتنسيق العمليات بين الفضاءين الجوي والسيبراني، وضمان استمرارية المهام القتالية في بيئة تتعرض لهجمات إلكترونية معادية. من أبرز هذه التحديات: (مايكل، ٢٠١٧)

- **صعوبة التكامل بين العمليات الجوية والسيبرانية**. في الوقت الذي تُدار فيه العمليات الجوية بسرعة ودقة عالية، تحتاج العمليات السيبرانية إلى وقت للتحليل والكشف والتعامل مع التهديدات، مما يخلق فجوة زمنية خطيرة بين الفعل ورد الفعل في ساحة المعركة.
- **استهداف شبكات القيادة والسيطرة** C2. تُعد مراكز القيادة الجوية من أكثر الأهداف حساسية في أي حرب سيبرانية. إذ إن تعطيلها يؤدي إلى شل حركة الطائرات والمراقبة الجوية، ويجبر القادة على اتخاذ قرارات عشوائية أو غير دقيقة.
- **الاختراق النفسي والإلكتروني في آن واحد**. تعتمد الجيوش الحديثة على ثقة الطيارين والمشغلين في الأنظمة الذكية. لكن الهجمات السيبرانية يمكن أن تُحدث ارتباكًا نفسيًا وعملياتيًا لدى الأطقم الجوية، عندما يشكون في مصداقية شاشاتهم أو أنظمتهم.
- **تحديات التدريب والجاهزية.** إعداد طيارين وضباط لديهم وعي سيبراني عالٍ أصبح ضرورة حتمية. فالحروب الحديثة لا تدار فقط من قمرة القيادة، بل من وحدات متخصصة في الدفاع الإلكتروني والهجوم الرقمي الجوي. لكن تدريب هذه الكوادر يتطلب استثمارات ضخمة ومناهج متقدمة.
- **ضعف حماية الأنظمة الإلكترونية للطائرات الحديثة**. تعتمد الطائرات المقاتلة على شبكات رقمية للتحكم والملاحة والتسليح، مما يجعلها عرضة لاختراق أنظمة التشغيل أو التشويش على البيانات الملاحية. فمجرد دخول برمجية خبيثة Malware إلى منظومة الطائرة قد يؤدي إلى تعطيلها أثناء المهمة أو تحويل مسارها.
- **تهديدات الأقمار الصناعية وأنظمة الملاحة GPS Spoofing**. تعتمد القوات الجوية بشكل واسع على الأقمار الصناعية لتحديد المواقع والتوجيه ويمكن للهجمات السيبرانية أن تضلل إشارات GPS وتجعل الطائرات تتجه نحو أهداف خاطئة أو مناطق خطر.
- **استهداف أنظمة الطائرات دون طيار UAVs.** يمكن للخصوم الإلكترونيين اعتراض الاتصالات بين الطائرة المشغَّلة والقاعدة الأرضية، أو حتى اختطاف الطائرة إلكترونيًا وتوجيهها ضد أهداف صديقة.
- **ضعف تأمين البيانات الحساسة في شبكات الصيانة والدعم الفني**. الأنظمة التي تتعامل مع الصيانة أو تسجيل بيانات الطيران قد تُستغل للوصول إلى البنية الأساسية للقوات الجوية عبر "الهندسة الاجتماعية" أو اختراق الشبكات الخلفية. أدت الحروب السيبرانية إلى إعادة صياغة المفاهيم العسكرية التقليدية، وامتد تأثيرها ليشمل جوهر العقيدة الجوية التي تقوم عليها الجيوش الحديثة. فمع تصاعد الاعتماد على الأنظمة الرقمية والذكاء الاصطناعي في العمليات الجوية، أصبح الفضاء السيبراني

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨
P- ISSN: 2070-898X E-ISSN: 2707-9775

ساحة موازية تحدد النصر أو الهزيمة قبل اندلاع المعارك. ومن ثمّ، فإن دراسة أثر الحروب السيبرانية على مستقبل العقيدة الجوية تمثل خطوة أساسية لفهم التحول في فلسفة القوة الجوية وأساليب الردع والسيطرة في القرن الحادي والعشرين.

ثالثا: التحديات المستقبلية على العقيدة الجوية . وتشمل مجموعة من التحديات وكما يلي:
(سينغر، ٢٠١٤)

١. **تعطيل منظومات القيادة والسيطرة خلال العمليات الجوية**. أي هجوم سيبراني ناجح قد يؤدي إلى شل حركة الطائرات في الجو نتيجة فقدان الاتصال أو التشويش على الإشارات الرقمية.

٢. **تأخير في اتخاذ القرار العملياتي**. في ظل هجوم إلكتروني، قد تحتاج الفرق الفنية إلى وقت للكشف والمعالجة، مما يؤخر القرارات الحاسمة في المعركة.

٣. **التشويش على شبكات الاتصال التكتيكية Tactical Data Links**. مثل شبكات Link-١٦ التي تُستخدم في التنسيق بين الطائرات، مما يؤدي إلى فقدان التناغم العملياتي بين الأسراب الجوية.

٤. **تضليل نظم الإنذار المبكر والرادارات**. يمكن للهجمات السيبرانية أن تُدخل بيانات زائفة أو تعطل الرادارات، فيُعتقد بوجود أهداف وهمية، أو لا تُكتشف الطائرات المعادية في الوقت المناسب.

٥. **صعوبة التنسيق بين القوات الجوية والقوات السيبرانية.** تتطلب الحروب الحديثة تكاملًا فوريًا بين المجالين الجوي والسيبراني، إلا أن الاختلاف في العقيدة والتخصص يعقد عملية التنسيق الفعال.

رابعا: التحديات المستقبلية الاستراتيجية على العقيدة الجوية في الحروب السيبرانية.
وتشمل مجموعة من التحديات وكما يلي: (كولن، ٢٠١٢)

- **غياب عقيدة جوية سيبرانية متكاملة**. العديد من القوات الجوية لم تُدمج بعد الأمن السيبراني ضمن عقيدتها القتالية، مما يخلق فجوة بين الواقع الميداني والمفاهيم النظرية.
- **سباق التسلح السيبراني بين القوى الكبرى.** تنخرط الدول الكبرى في تطوير أسلحة سيبرانية هجومية قادرة على تعطيل طائرات أو مراكز قيادة، مما يزيد من هشاشة الأمن الجوي للدول الصغيرة.
- **صعوبة الردع في الفضاء السيبراني**. من الصعب تحديد مصدر الهجوم السيبراني بدقة، مما يجعل الرد العسكري التقليدي معقدًا من الناحية القانونية والسياسية.
- **تكاليف ضخمة لتأمين الأنظمة الجوية**. تحديث الأنظمة القديمة وتطوير حلول حماية رقمية للطائرات المكلفة جدًا، خاصة في ظل محدودية الموارد في بعض الدول.
- **تزايد الاعتماد على القطاع المدني في تكنولوجيا الطيران.** الشركات المدنية الخاصة التي تطور أنظمة الاتصالات والطائرات المسيرة قد لا تلتزم بنفس معايير الحماية العسكرية، مما يوسع دائرة المخاطر.

خامسا: التحديات المستقبلية المتوقعة . وتشمل مجموعة من التحديات وكما يلي:

- ظهور أسلحة سيبرانية مخصصة للطائرات الذكية والطائرات الشبحية.
- استهداف الذكاء الاصطناعي العسكري عبر "تسميم البيانات" Data Poisoning.
- توسع استخدام الاتصالات الكمية مما يتطلب جيوشًا جاهزة لحقبة ما بعد التشفير التقليدي.
- اندماج الفضاءين الفضائي والسيبراني في العمليات الجوية المستقبلية.
- تصاعد تهديدات "الحرب الهجينة" التي تمزج بين الهجوم السيبراني والتشويش الكهرومغناطيسي.
- مستقبل الردع السيبراني الجوي ضمن اليات المواجهة

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

P- ISSN: 2070-898X E-ISSN: 2707-9775

في المستقبل القريب، سيصبح مفهوم الردع الجوي متكاملًا مع الردع السيبراني، بحيث تعتمد الدول على قدرات رقمية متقدمة لشل أنظمة الدفاع الجوي للعدو أو تعطيل قدراته الإلكترونية قبل اندلاع أي مواجهة، ان الردع السيبراني الجوي سيعتمد على ثلاث ركائز أساسية: (المعهد الدولي، ٢٠٢٤)

١. القدرة على الحماية الذاتية الرقمية.
٢. القدرة على تنفيذ هجمات دقيقة ومخفية.
٣. القدرة على التعافي السريع بعد أي هجوم.

وبذلك، ستكون السيادة الجوية في المستقبل مرهونة بالسيادة السيبرانية، إذ لن تتحقق السيطرة على السماء دون السيطرة على فضائها الإلكتروني السيبراني أولًا. إن بناء تفوق جوي مستقبلي مرهون ببناء قوة سيبرانية جوية متقدمة قادرة على مواجهة التهديدات الرقمية، وامتلاك أدوات الهجوم والدفاع في آن واحد، لضمان السيادة الجوية في بيئة عملياتية لا تعرف الحدود بين الواقع والفضاء الإلكتروني.

الخاتمة:

أن الهجمات السيبرانية قد أحدثت تحولًا جذريًا في طبيعة العمليات الجوية، وأعادت تعريف مفهوم القوة الجوية والسيادة في الجو أذ لم يعد التفوق الجوي يعتمد فقط على الطائرات المقاتلة أو الصواريخ الدقيقة، بل أصبح مرتبطًا بشكل مباشر بالقدرة على حماية الأنظمة الرقمية، وتأمين شبكات القيادة والسيطرة، والتحكم بالبيانات والمعلومات في الوقت الحقيقي. أن القوات الجوية تواجه تحديات متعددة، تشمل التحديات التقنية، العملياتية، الاستراتيجية الأمر الذي يفرض على الدول تطوير عقيدة جوية متكاملة تتضمن الأمن السيبراني كركيزة أساسية لضمان التفوق والاستمرارية في الحروب المستقبلية.

لقد تحوّلت العقيدة الجوية من منظومة تقليدية تعتمد على القوة النارية والتكنولوجيا الصلبة إلى عقيدة شبكية معلوماتية مترابطة، ترتكز على تدفق البيانات، ومرونة الأنظمة الرقمية، والتكامل بين منصات الذكاء الاصطناعي وشبكات القيادة والسيطرة. وقد أدى هذا التحول إلى رفع مستوى الأداء العملياتي بشكل لم يسبق له مثيل، لكنه في المقابل فتح الباب أمام تهديدات سيبرانية تستهدف العصب الحيوي للقوة الجوية: أنظمة الاتصال، والاستشعار، والملاحة، والتخطيط، والتوجيه، والتحكم. وعليه، يتضح أن حماية العقيدة الجوية من الهجمات السيبرانية أصبحت ضرورة استراتيجية لا تقل أهمية عن تطوير الطائرات أو تعزيز قدرات الدفاع الجوي. كما أصبح من المهم تبني عقيدة سيبرانية جوية واضحة، تقوم على الدمج الفعّال بين الدفاع الجوي التقليدي والعمليات السيبرانية، وبناء قدرات استجابة مرنة، وتعزيز الردع السيبراني، وتطوير أنظمة ذكاء اصطناعي مقاومة للهجمات الخداعية.

الاستنتاجات:

– العقيدة الجوية الحديثة أصبحت عقيدة رقمية بامتياز يتضح أن التحول نحو الأنظمة الرقمية والذكاء الاصطناعي والاتصالات الشبكية جعل القوة الجوية أكثر فاعلية، لكنه في الوقت نفسه رفع مستوى هشاشتها أمام الهجمات السيبرانية، مما فرض إعادة تعريف شاملة لمفاهيم السيطرة الجوية والجاهزية القتالية.

– الهجمات السيبرانية أصبحت قادرة على إحداث تأثيرات عملياتية تعادل أو تتجاوز الضربات الجوية التقليدية فاختراق أنظمة القيادة والسيطرة أو تعطيل الملاحة الجوية أو تضليل البيانات يمكن أن يشلّ العمليات الجوية بالكامل من دون إطلاق رصاصة واحدة، ويقلب ميزان القوة في ساحة المعركة. كما ان التفوق الجوي أصبح معتمدًا على الأمن الرقمي وان السيطرة على الطائرات والمنظومات تعتمد اليوم على حماية الشبكات والأنظمة من الهجمات السيبرانية. وبذلك فأن الهجمات السيبرانية تزيد من هشاشة القوة الجوية بذلك فأن أي ثغرة في أنظمة الطائرات أو شبكات القيادة والسيطرة تهدد الاستراتيجية الجوية الوطنية.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

– العقيدة الجوية المستقبلية تتطلب دمج الذكاء الاصطناعي والأمن السيبراني لتكون القوات الجوية قادرة على مواجهة التحديات الرقمية والهجومية المتطورة.

– في هذا السياق، يصبح الفضاء السيبراني ساحة العمليات الجديدة التي تدور فيها المنافسة بين القوى الجوية العالمية، حيث تتقاطع المعلومات والاستخبارات والقدرات التقنية في معركة من نوع مختلف، لا تعتمد على التفوق العددي أو الناري، بل على القدرة على السيطرة على المعلومات وتأمينها واستخدامها كسلاح. ومن هنا تبرز الأسلحة السيبرانية كعامل حاسم في المعارك المستقبلية، إذ يمكنها تعطيل طائرة، أو شل شبكة دفاع جوي، أو تضليل منظومة رادارية بكود واحد فقط، مما يجعلها أكثر تأثيراً من كثير من الوسائل القتالية التقليدية.

– لقد أصبح التكامل بين هذه المفاهيم ضرورة استراتيجية لتأمين التفوق الجوي. فالقوة الجوية الحديثة لا يمكن أن تحقق السيطرة الجوية المطلقة ما لم تمتلك قدرة سيبرانية دفاعية وهجومية متقدمة، قادرة على حماية أنظمتها الرقمية من جهة، وتهديد البنى التحتية المعلوماتية للخصوم من جهة أخرى. وبالتالي، فإن مستقبل الحروب الجوية سيتحدد بدرجة اندماج الأمن السيبراني في بنية القوة الجوية، وبمدى جاهزيتها لخوض معارك إلكترونية متعددة الأبعاد في فضاء لا يُرى، لكنه يحسم نتائج الحروب قبل أن تبدأ في السماء.

-تُظهر المعطيات أن مستقبل القوات الجوية سيتحدد بمدى قدرتها على التكيّف مع بيئة الحرب السيبرانية، التي تمزج بين القوة الصلبة والتقنية الذكية. فالتحديات التقنية والعملياتية تتطلب تبني استراتيجيات وطنية شاملة تدمج الأمن السيبراني في كل جزئية من منظومة القوة الجوية. غياب العقيدة السيبرانية الجوية يعرض الدول لتهديدات قد تؤدي إلى فقدان السيطرة الجوية في الساعات الأولى من أي صراع إذ يمكن لهجمات سيبرانية منسقة إسقاط شبكات القيادة، وشل منظومات الملاحة، وتعطيل المهام، مما يترك الدولة في حالة عمى عملياتي كامل.

التوصيات:

أمام هذه التحديات، بات لزامًا على الدول وضع استراتيجيات جوية سيبرانية مستقبلية تضمن القدرة على الدفاع والهجوم في الفضاء الإلكتروني بشكل متكامل مع العمليات الجوية التقليدية. ومن هنا نبين المقترحات وكما يلي:

– تعزيز دمج الأمن السيبراني داخل العقيدة الجوية وينبغي إعادة صياغة العقيدة الجوية بحيث تتضمن مبادئ واضحة للدفاع والهجوم السيبراني، وإطاراً متكاملاً يربط بين العمليات الجوية والفضاء السيبراني، بدلاً من التعامل معه كعنصر تقني منفصل.

– تطوير بنية سيبرانية مرنة Cyber Resilience لمنظومات القيادة والسيطرة من الضروري إنشاء بنى تحتية رقمية مقاومة للاختراق، تمتلك القدرة على التعافي السريع بعد الهجمات، وتستمر في تقديم الحد الأدنى من القدرات العملياتية أثناء الهجوم.

– بناء قوة سيبرانية جوية متخصصة وهي وحدات مكرّسة لحماية المجال السيبراني للقوات الجوية، تشرف على أمن الشبكات والأنظمة الإلكترونية الخاصة بالطيران، وتعمل على تنفيذ عمليات هجومية ضد أهداف سيبرانية معادية عند الحاجة.

– إنشاء وحدات متخصصة في الدفاع السيبراني الجوي لتكون قادرة على حماية الشبكات، ومراقبة الهجمات، والرد بسرعة على التهديدات.

– تعزيز التدريب والوعي السيبراني للكوادر الجوية لضمان جاهزية الطيارين والمشغلين للتعامل مع الهجمات الرقمية أثناء المهمات الجوية.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

– تحديث الأنظمة الرقمية والطائرات بشكل دوري لضمان حماية البرمجيات والمعدات من الثغرات والهجمات المحتملة.

– تطوير شراكات دولية لتبادل المعلومات التقنية بهدف تعزيز الردع السيبراني والاستفادة من التجارب العالمية في حماية المجال الجوي.

– الاستثمار في الذكاء الاصطناعي الآمن لتطبيق نظم اتخاذ القرار الآلي في الطائرات بدون طيار وأنظمة الدفاع الجوي دون تعرضها للاختراق أو التلاعب.

التمويل

لم يتلق هذا البحث أي تمويل محدد من أي جهة مانحة في القطاعات العامة أو التجارية أو غير الربحية.

تضارب المصالح

يُعلن المؤلفون عدم وجود أي تضارب في المصالح فيما يتعلق بنشر هذه الورقة البحثية .

شكر وتقدير

يتقدم المؤلفون بجزيل الشكر للمؤسسة على دعمها المعنوي طوال فترة هذا البحث. لقد كان لتشجيعها وتوجيهها دورٌ بالغ الأهمية في إنجاز هذا البحث.

المصادر باللغة العربية:

– أحمد محمود، *الأمن السيبراني والطائرات الذكية في العمليات الجوية الحديثة* القاهرة: دار الفكر العسكري، ٢٠٢٢، ٥٥–٧٢.

– التكامل بين الفضاءين الجوي والسيبراني في العمليات المستقبلية." مجلة الأمن والدفاع العربي، ٢٠٢٣.

– التطورات التكنولوجية في سلاح الجو وتحديات الحرب الإلكترونية." مجلة الدراسات الاستراتيجية والعسكرية، العدد ١٥، ٢٠٢٣. ص٥.

– محمد عبد الله العتيبي، *الأمن السيبراني العسكري وحماية المنظومات القتالية الحديثة* الرياض: مركز الدراسات الاستراتيجية والدفاعية، ٢٠٢٢، ٤٥–٦٠

– عبد القادر بوغازي، الردع السيبراني: مقاربة للطبيعة، الفواعل وقيود القانون الدولي، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد ١٠، العدد ١ يونيو ٢٠٢٥: ٨٥٥–٨٦٩.

– أحمد محمود، الذكاء الاصطناعي والأمن السيبراني في المنظومات العسكرية الحديثة، مجلة العلوم العسكرية العربية، المجلد ١٢، العدد ٣ ٢٠٢٤: ١١٢–١٢٨.

– محمد عبد الله العتيبي، الأمن السيبراني العسكري وحماية المنظومات القتالية الحديثة الرياض: مركز الدراسات الاستراتيجية والدفاعية، ٢٠٢٢، ٧٧–١٠١.

– جامعة الدفاع الوطني .(NDU) دمج العمليات السيبرانية والجوية: رؤى عقائدية .واشنطن العاصمة: مطبعة جامعة الدفاع الوطني، ٢٠٢١.

– بافيل شاريكوف .مستقبل العمليات السيبرانية الجوية والفضائية .موجز أبحاث مؤسسةRAND ، ٢٠٢١.

– مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي .(CCDCOE) قابلية التشغيل البيني بين المجالين الجوي والسيبراني في عمليات الناتو .تالين: منشوراتCCDCOE ، ٢٠٢٢.

– القوات الجوية الأمريكية .مفهوم التشغيل المستقبلي للقوات الجوية: رؤية للقوات الجوية في عام ٢٠٣٥ .واشنطن العاصمة: وزارة القوات الجوية، ٢٠٢٢.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

P- ISSN: 2070-898X E-ISSN: 2707-9775

– جينز ديفنس ويكلي. "التهديدات السيبرانية الناشئة ضد القوات الجوية وأنظمة الدفاع الجوي." جينز ديفنس ويكلي، ٢٠٢٣.
– بي. دبليو. سينغر، وألان فريدمان .الأمن السيبراني والحرب السيبرانية: ما الذي ينبغي للجميع معرفته؟ نيويورك: مطبعة جامعة أكسفورد، ٢٠١٤.
– المعهد الدولي للدراسات الاستراتيجية .(IISS) التوازن العسكري ٢٠٢٤ .لندنIISS :، ٢٠٢٤.
– وزارة الدفاع الأمريكية، العمليات في الفضاء السيبراني وتكامل القوة الجوية المشتركة .واشنطن العاصمة: هيئة الأركان المشتركة، ٢٠٢٠، ص٧.
– القوات الجوية للولايات المتحدة، منشور عقيدة القوات الجوية رقم ١: القوات الجوية .واشنطن العاصمة: وزارة القوات الجوية، ٢٠٢١، ص١٢.
– القوات الجوية للولايات المتحدة، منشور عقيدة القوات الجوية رقم ١: القوات الجوية .واشنطن العاصمة: وزارة القوات الجوية، ٢٠٢١، ص١٢.
– وزارة الدفاع الأمريكية، العمليات في الفضاء السيبراني وتكامل القوة الجوية المشتركة .واشنطن العاصمة: هيئة الأركان المشتركة، ٢٠٢٠، ص٧.
– مركز التميز للدفاع السيبراني التعاوني التابع للناتو، تكامل المجالين السيبراني والجوي: مفاهيم ناشئة في القوة الجوية .تالينCCDCOE :، ٢٠٢١، ص١٥.
– جامعة الدفاع الوطني .(NDU) دمج العمليات السيبرانية والجوية: رؤى عقائدية .واشنطن العاصمة: مطبعة جامعة الدفاع الوطني، ٢٠٢١، ص٥.
– بافيل شاريكوف .مستقبل العمليات السيبرانية الجوية والفضائية .موجز أبحاثRAND ، ٢٠٢١، ص١٣.
– القوات الجوية الأمريكية .مفهوم التشغيل المستقبلي للقوات الجوية: رؤية للقوات الجوية في عام ٢٠٣٥ .واشنطن العاصمة: وزارة القوات الجوية، ٢٠٢٢، ص١٨.
– مارتن سي. ليبيكي، الردع السيبراني والحرب السيبرانية .سانتا مونيكا، كاليفورنيا: مؤسسة RAND، ٢٠٠٩، ص١٥–٣٠؛ كولن إس. غراي، القوة الجوية لتحقيق الأثر الاستراتيجي .قاعدة ماكسويل الجوية، ألاباما: مطبعة جامعة سلاح الجو، ٢٠١٢، ص٤٥–٦٠.
– مركز التميز للدفاع السيبراني التعاوني(CCDCOE) ، الدفاع السيبراني والقوة الجوية: التداعيات الاستراتيجية .تالين: الناتوCCDCOE ، ٢٠٢١، ص٣٥–٥٠؛ مارتن سي. ليبيكي، الردع السيبراني والحرب السيبرانية .سانتا مونيكا، كاليفورنيا: مؤسسةRAND ، ٢٠٠٩، ص٤٢–٥٥.
– مركز التميز للدفاع السيبراني التعاوني التابع للناتو .(CCDCOE) قابلية التشغيل البيني بين المجالين الجوي والسيبراني في عمليات الناتو .تالين: منشوراتCCDCOE ، ٢٠٢٢، ص١٩.
– كولن إس. غراي، القوة الجوية لتحقيق الأثر الاستراتيجي .قاعدة ماكسويل الجوية، ألاباما: مطبعة جامعة سلاح الجو، ٢٠١٢، ص١١٥–١٢٨؛ مارتن سي. ليبيكي، الردع السيبراني والحرب السيبرانية .سانتا مونيكا، كاليفورنيا: مؤسسةRAND ، ٢٠٠٩، ص٦٠–٧٢.
– جيمس أ. لويس، الأمن السيبراني والقوة الجوية: التهديدات الناشئة للطيران العسكري .واشنطن العاصمة: مركز الدراسات الاستراتيجية والدولية، ٢٠٢٠، ص٢٨–٤٤؛ مركز التميز للدفاع السيبراني التعاوني(CCDCOE) ، الدفاع السيبراني والقوة الجوية: التداعيات الاستراتيجية .تالين: الناتو CCDCOE، ٢٠٢١، ص٥١–٦٦.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

P- ISSN: 2070-898X E-ISSN: 2707-9775

– مايكل ن. شميت (محرر)، دليل تالين ٢,٠ بشأن القانون الدولي المطبق على العمليات السيبرانية . كامبريدج: مطبعة جامعة كامبريدج، ٢٠١٧، ص٣١٠–٣٢٥؛ مارتن سي. ليبيكي، الردع السيبراني والحرب السيبرانية .سانتا مونيكا، كاليفورنيا: مؤسسةRAND ، ٢٠٠٩، ص٦٦–٨٠.
– مارتن سي. ليبيكي، الردع السيبراني والحرب السيبرانية .سانتا مونيكا، كاليفورنيا: مؤسسة RAND، ٢٠٠٩، ص٤٥–٥٨؛ مايكل ن. شميت (محرر)، دليل تالين ٢,٠ بشأن القانون الدولي المطبق على العمليات السيبرانية .كامبريدج: مطبعة جامعة كامبريدج، ٢٠١٧، ص٢٩٨–٣٠٩.
– توماس ريد، الحرب السيبرانية لن تقع .مطبعة جامعة أكسفورد، ٢٠١٣، ص٤٥–٤٦.
– مايكل وارنر، "الأمن السيبراني وشبكات القيادة في البنتاغون." مجلة القوة المشتركة (Joint Force Quarterly)، العدد ٧٥، ٢٠١٤، ص٢٧–٣١.
– مؤسسةRAND ، العمليات السيبرانية العسكرية والمرونة في ساحة المعركة الرقمية .سانتا مونيكا، ٢٠٢١، ص٣٣–٣٥.
– ليور تابانسكي وإسحاق بن إسرائيل، الأمن السيبراني في إسرائيل .سبرنغر، ٢٠١٥، ص٥٧–٥٩.
– كينيث غيرز، "الجهات الفاعلة غير الحكومية في عمليات الفضاء السيبراني." تقرير مركز التميز للدفاع السيبراني التعاوني للناتو، ٢٠١٥، ص٦–١٠.
– روبرت تشيسني ودانييل سيترون، "التزييف العميق: تحدٍ وشيك للخصوصية والديمقراطية والأمن القومي." مجلة كاليفورنيا للقانون، المجلد ١٠٧، العدد ٦، ٢٠١٩، ص١٧٦٨–١٧٧٢.
– بيتر دبليو. سينغر وألان فريدمان، الأمن السيبراني والحرب السيبرانية: ما الذي ينبغي للجميع معرفته؟ مطبعة جامعة أكسفورد، ٢٠١٤، ص١٠٧–١١٠.
– مركز التميز للدفاع السيبراني التعاوني(CCDCOE) ، الذكاء الاصطناعي ومستقبل الدفاع السيبراني .تالين، ٢٠٢٠، ص٢٢–٢٥.
– مارتن سي. ليبيكي، الفضاء السيبراني في السلم والحرب .مطبعة المعهد البحري، ٢٠١٦، ص١٤٣–١٤٧.
– مارتن سي. ليبيكي، الردع السيبراني والحرب السيبرانية .سانتا مونيكا، كاليفورنيا: مؤسسة RAND، ٢٠٠٩، ص٥٢–٦٣.
– هيرب لين، "حول دور الثقة في العمليات السيبرانية العسكرية." مجلة الأمن السيبراني، المجلد ٥، العدد ٣، ٢٠١٩، ص٨–١٢.
– مايكل وارنر، صعود الصراع السيبراني .مطبعة جامعة جورجتاون، ٢٠٢٢، ص٦٤–٦٨.
– جينز ديفنس ويكلي، "التهديدات السيبرانية الناشئة ضد القوات الجوية وأنظمة الدفاع الجوي." جينز ديفنس ويكلي، ٢٠٢٣، ص٢٨.
– مركز التميز للدفاع السيبراني التعاوني(CCDCOE) ، الدفاع السيبراني والقوة الجوية: التداعيات الاستراتيجية .تالين: الناتوCCDCOE ، ٢٠٢١، ص٤٢–٥٨.
– مايكل ن. شميت (محرر)، دليل تالين ٢,٠ بشأن القانون الدولي المطبق على العمليات السيبرانية . كامبريدج: مطبعة جامعة كامبريدج، ٢٠١٧، ص٣–١٠.
– بي. دبليو. سينغر وألان فريدمان، الأمن السيبراني والحرب السيبرانية: ما الذي ينبغي للجميع معرفته؟ نيويورك: مطبعة جامعة أكسفورد، ٢٠١٤، ص٣.
– كولن إس. غراي، القوة الجوية لتحقيق الأثر الاستراتيجي .قاعدة ماكسويل الجوية، ألاباما: مطبعة جامعة سلاح الجو، ٢٠١٢، ص٨٣–٩٩.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108
P- ISSN: 2070-898X E-ISSN: 2707-9775

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

– جيمس أ. لويس، الأمن السيبراني والقوة الجوية: التهديدات الناشئة للطيران العسكري .واشنطن العاصمة: مركز الدراسات الاستراتيجية والدولية، ٢٠٢٠، ص٢٢–٣٥.
– المعهد الدولي للدراسات الاستراتيجية(IISS) ، التوازن العسكري ٢٠٢٤ .لندنIISS :، ٢٠٢٤، ص١٨.

Sources

– National Defense University NDU. Integrating Cyber and Air Operations: Doctrinal Perspectives. Washington, D.C.: NDU Press, 2021.
– Sharikov, Pavel. The Future of Air and Space Cyber Operations. RAND Research Brief, 2021.
– NATO Cooperative Cyber Defense Centre of Excellence CCDCOE. Air and Cyber Interoperability in NATO Operations. Tallinn: CCDCOE Publications, 2022
– U.S. Air Force. Air Force Future Operating Concept: A View of the Air Force in 2035. Washington, D.C.: Department of the Air Force, 2022.
– Jane's Defense Weekly. "Emerging Cyber Threats to Air Forces and Air Defense Systems." Jane's Defense Weekly, 2023
– Singer, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know? New York: Oxford University Press, 2014
– International Institute for Strategic Studies IISS. The Military Balance 2024. London: IISS, 2024
– Department of Defense, Cyberspace Operations and Joint Air Power Integration Washington, D.C.: Joint Chiefs of Staff, 2020, 7
– United States Air Force, *Air Force Doctrine Publication 1: The Air Force* Washington, D.C.: Department of the Air Force, 2021, 12
– United States Air Force, *Air Force Doctrine Publication 1: The Air Force* Washington, D.C.: Department of the Air Force, 2021, p12.
– Department of Defense, *Cyberspace Operations and Joint Air Power Integration* Washington, D.C.: Joint Chiefs of Staff, 2020, p 7.
– NATO Cooperative Cyber Defense Centre of Excellence, *Cyber and Air Domain Integration: Emerging Concepts in Air Power* Tallinn: CCDCOE, 2021, p15.
– National Defense University NDU. Integrating Cyber and Air Operations: Doctrinal Perspectives. Washington, D.C.: NDU Press, 2021. ، p5.
– Sharikov, Pavel. The Future of Air and Space Cyber Operations. RAND Research Brief, 2021 ،P13.
– U.S. Air Force. Air Force Future Operating Concept: A View of the Air Force in 2035. Washington, D.C.: Department of the Air Force, 2022. ، P18.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:88-108

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد : ٢٣ العدد: ٩٣ ص: ٨٨- ١٠٨

P- ISSN: 2070-898X E-ISSN: 2707-9775

– Martin C. Libicki, *Cyberdeterrence and Cyberwar* Santa Monica, CA: RAND Corporation, 2009, 15–30; Colin S. Gray, *Air Power for Strategic Effect* Maxwell Air Force Base, AL: Air University Press, 2012, 45–60.
– NATO Cooperative Cyber Defense Centre of Excellence CCDCOE, *Cyber Defense and Air Power: Strategic Implications* Tallinn: NATO CCDCOE, 2021, 35–50; Martin C. Libicki, *Cyberdeterrence and Cyberwar* Santa Monica, CA: RAND Corporation, 2009, 42–55.
– NATO Cooperative Cyber Defense Centre of Excellence CCDCOE. Air and Cyber Interoperability in NATO Operations. Tallinn: CCDCOE Publications, 2022.p19.
– Colin S. Gray, *Air Power for Strategic Effect* Maxwell Air Force Base, AL: Air University Press, 2012, 115–128; Martin C. Libicki, *Cyberdeterrence and Cyberwar* Santa Monica, CA: RAND Corporation, 2009, 60–72.
– James A. Lewis, *Cybersecurity and Air Power: Emerging Threats to Military Aviation* Washington, DC: Center for Strategic and International Studies, 2020, 28–44; NATO Cooperative Cyber Defense Centre of Excellence CCDCOE, *Cyber Defense and Air Power: Strategic Implications* Tallinn: NATO CCDCOE, 2021, 51–66.
– Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Cambridge: Cambridge University Press, 2017, 310–325; Martin C. Libicki, *Cyberdeterrence and Cyberwar* Santa Monica, CA: RAND Corporation, 2009, 66–80.
– Martin C. Libicki, *Cyberdeterrence and Cyberwar* Santa Monica, CA: RAND Corporation, 2009, 45–58; Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Cambridge: Cambridge University Press, 2017, 298–309.
– Thomas Rid, *Cyber War Will Not Take Place* Oxford University Press, 2013, pp 45–46.
– Michael Warner, "Cybersecurity and the Pentagon's Command Networks," *Joint Force Quarterly*, no. 75 2014: pp 27–31.
– RAND Corporation, *Military Cyber Operations and Resilience in the Digital Battlespace* Santa Monica, 2021, pp 33–35.
– Lior Tabansky and Isaac Ben-Israel, *Cybersecurity in Israel* Springer, 2015, 57–59.
– Kenneth Geers, "Non-State Actors in Cyberspace Operations," *NATO Cooperative Cyber Defense Centre of Excellence Report* 2015, pp 6–10.

– Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 2019: 1768–1772.
– Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* Oxford University Press, 2014, pp107–110.
– NATO Cooperative Cyber Defense Centre of Excellence, *AI and the Future of Cyber Defense* Tallinn, 2020, 22–25.
– Martin C. Libicki, *Cyberspace in Peace and War* Naval Institute Press, 2016, 143–147.
– Martin C. Libicki, *Cyberdetetterance* and Cyberwar Santa Monica, CA: RAND cooperation, 2009, 52-63.
– Herb Lin, "On the Role of Trust in Military Cyber Operations," *Journal of Cybersecurity* 5, no. 3 2019: pp 8–12.
– Michael Warner, *The Rise of Cyber Conflict* Georgetown University Press, 2022, 64–68.
– Jane's Defense Weekly. "Emerging Cyber Threats to Air Forces and Air Defense Systems." Jane's Defense Weekly, 2023 ، P28.
– NATO Cooperative Cyber Defense Centre of Excellence CCDCOE, Cyber Defense and Air Power: Strategic Implications Tallinn: NATO CCDCOE, 2021, 42–58.
– Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Cambridge: Cambridge University Press, 2017, 3–10.
– Singer, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press, 2014.p3.
– Colin S. Gray, Air Power for Strategic Effect Maxwell Air Force Base, AL: Air University Press, 2012, 83–99.
– James A. Lewis, Cybersecurity and Air Power: Emerging Threats to Military Aviation Washington, DC: Center for Strategic and International Studies, 2020, 22–35.
– International Institute for Strategic Studies IISS. The Military Balance 2024. London: IISS, 2024. ، p18.