Misan Journal of Political and International Studies
مجلـــة ميسان للدراسات السياسية والدولية
ISSN (Print): 3007-620X , ISSN (Online): 3007-6218

المجلد (1) العدد (1) كانون الأول/ديسمبر2025

Vol. (1) No.,(1) December2025

الردع الاستراتيجي في عصر ما بعد الحقيقة: دراسة تحليلية في الحروب الهجينة

م.م. شيماء محمد ناصر

جامعة بغداد– كلية العلوم السياسية– قسم الدراسات الدولية

shaima.mohammed@copolicy.uobaghdad.edu.iq

orcid=0009-0003-7535-2588

10.65441/umisa.2025.01120

المستخلص

يهدف البحث الى تحليل طبيعة الردع الاستراتيجي في عصر ما بعد الحقيقة من خلال دراسة ديناميات الحروب الهجينة، التي حوّلت ساحة الصراع من القوة العسكرية المباشرة الى الفضاء السيبراني والمعرفي، ويركز البحث على دور الأدوات السيبرانية والمعرفية في تشكيل بيئة ردعية جديدة تستند إلى التأثير في الوعي الجمعي وصناعة القرار بدلاً من استخدام القوة المادية. وتُظهر النماذج التطبيقية، مثل الأزمات الهندية– الباكستانية، والإيرانية– الإسرائيلية، وكوريا الشمالية – كوريا الجنوبية، أن تكامل الأدوات المعرفية والسيبرانية يزيد من فاعلية الردع ويقيد خيارات الخصوم. ويستخلص البحث أن السيطرة على الفضاء السيبراني والمعلومات أصبح محورياً لضبط السلوك الدولي، مع التأكيد على الحاجة الى أطر معيارية وأخلاقية تحمي النظام الدولي من الانزلاق نحو فوضى تهدد الاستقرار الاستراتيجي.

الكلمات المفتاحية: الردع الاستراتيجي، الحرب الهجينة، الردع السيبراني، عصر ما بعد الحقيقة، الردع المعرفي

Strategic Deterrence In The Post-Truth Era: An Analytical Study Of Hybrid Wars

Asst. Lec. Shaymaa mohammed naser

University Of Baghdad – College Of Political Science – Department Of International Studies

shaima.mohammed@copolicy.uobaghdad.edu.iq

orcid=0009-0003-7535-2588

10.65441/umisa.2025.01120

Abstract

This study aims to analyze the nature of strategic deterrence in the post-truth era by examining the dynamics of hybrid warfare, which has shifted the battlefield from direct military force to the cyber and cognitive domains. The research highlights how cyber and cognitive tools contribute to shaping a new deterrence environment that depends on influencing collective perception and decision-making rather than relying solely on physical force.

Through applied case studies—including the India–Pakistan, Iran–Israel, and North–South Korea crises—the study demonstrates that integrating cognitive and cyber capabilities enhances deterrence effectiveness and limits adversaries' strategic options. The findings conclude that control over the cyber and information domains has become essential for regulating international behavior, emphasizing the necessity of developing normative and ethical frameworks to prevent the international system from drifting into instability that threatens strategic security.

Keywords: Strategic Deterrence, Hybrid Warfare, Cyber Deterrence, Post-Truth Era, Cognitive Deterrence

Misan Journal of Political and International Studies
مجلـــة ميسان للدراسات السياسية والدولية
ISSN (Print): 3007-620X , ISSN (Online): 3007-6218
المجلد (1) العدد (1) كانون الأول/ديسمبر2025
Vol. (1) No.,(1) December2025

المقدمة

منذ الحرب الباردة، ارتبط مفهوم الردع بالقدرات النووية والتوازن العسكري بين القوى العظمى، غير أن التطورات التكنولوجية والرقمية في العقود الأخيرة قلبت معادلة الصراع، وأعادت تشكيل أدواته وأساليبه. فلم تُعد المواجهات تُقاس حصراً بالقوة الصلبة، بل امتدت إلى ميادين جديدة مثل الفضاء السيبراني وساحات الإدراك والوعي الجمعي. وفي عصر ما بعد الحقيقة، لم يُعد الهدف من الحرب السيطرة على الأرض، وإنما السيطرة على العقول وتوجيه السلوك، الأمر الذي جعل المعلومات والتقنيات الرقمية أدوات رئيسة في الحروب الهجينة.

تأتي أهمية هذه الدراسة في تحليل العلاقة بين متغيرات عصر ما بعد الحقيقة وتحديات الحرب الهجينة وتأثيرها على الردع الكلاسيكي. وهي تقدم إطاراً استراتيجياً لتعزيز فاعلية الردع من خلال دمج الأدوات السيبرانية والمعرفية لمواجهة المخاطر الأمنية غير التقليدية. وفي ضوء ذلك نعرض في بحثنا هذا التساؤل الرئيس :كيف أدت التحولات الاستراتيجية الناجمة عن الحروب الهجينة واستخدام أدوات التضليل في عصر ما بعد الحقيقة الى قصور الردع الكلاسيكي في تحقيق أهدافه؟ وماهي المكونات والاليات الازمة لصياغة مفهوم الردع المتكامل الذي يستطيع إعادة بناء متطلبات السيطرة والهيمنة في البيئة الدولية الجديدة؟ وينبثق من التساؤل الرئيس الأسئلة الفرعية الاتية:

1 – ماهي التحديات التي يفرضها عصر ما بعد الحقيقة وصعوبة تحديد مسؤولية العدوان على ركائز الردع الكلاسيكي؟
2 – كيف يُسهم المزج بين الردع المعرفي والردع السيبراني– المدعوم بالتضليل الإعلامي والذكاء الاصطناعي وتحليل البيانات الضخمة – في تحقيق الردع المتكامل كنموذج جديد للسيطرة في الحروب الهجينة؟
3 – ماهي الدروس والتحديات الاستراتيجية المستخلصة من النماذج التطبيقية لدول الدراسة (الهند وباكستان، إيران و(إسرائيل)، كوريا الشمالية – كوريا الجنوبية فيما يتعلق بفاعلية الردع السيبراني والمعرفي؟

وتسعى الدراسة لأثبات فرضية مفادها (التكامل الفعال بين القوة العسكرية التقليدية والأدوات السيبرانية والمعرفية يمثل المقاربة القادرة على مواجهة الهجمات الهجينة، والتفوق على الخصم عبر السيطرة على بيئة الادراك والسلوك الاستراتيجي، وهو ما يترجم الى هيمنة استراتيجية جديدة).

وفي ضوء عنوان دراستنا وللوقوف على متطلباتها، تم اتباع المنهج الوصفي – التحليلي لتأصيل المفاهيم الواردة بالبحث، إلى جانب المنهج المقارن لمقارنة الردع التقليدي بالحديث، فيما استخدم منهج دراسة الحالة لتوضيح النماذج التطبيقية. بما يوفّر تحليلاً متكاملاً يجمع بين النظرية والتطبيق.

المطلب الاول: الإطار النظري والمفاهيمي

اولاً: تعريف الردع الكلاسيكي في الفكر الاستراتيجي

يُعد الردع أحد المفاهيم الأساسية في الدراسات الاستراتيجية وألامنية، إذ تطور مفهومه بشكل بارز خلال فترة الحرب الباردة ليصبح أداة رئيسة في مواجهة التهديدات النووية بين القوى العظمى. وتقوم ديناميكية الردع النووي على مفهوم الضربة الثانية، أي قدرة أي من الطرفين على توجيه ضربة نووية مدمرة في حال تعرّضه لهجوم أول، وهو ما يعرف بـ (التدمير المؤكد المتبادل) (Mutual Assured Destruction)، الذي يشكل الأساس في خلق توازن رعب يثني الطرفين عن المبادرة بالتصعيد[1] .

ويُعرّف الردع تقليدياً بأنه القدرة على منع الخصم من تبني سلوك عدائي عبر تهديده بعقوبات أو رد فعل ذات تكلفة عالية أو تأثير مدمر، ما يدفعه إلى إعادة تقييم حساباته الاستراتيجية والتراجع عن التصعيد. وفقًا لتوماس شلينج [2]، فإن الردع هو عملية تواصل استراتيجية تهدف إلى التأثير في سلوك الخصم من خلال التهديد العقلاني والمدروس، بحيث لا يُقصد فعلياً اللجوء إلى استخدام القوة، بل إقناع الخصم بجدية وواقعية التهديد. كما يؤكد أن نجاح الردع يتوقف على ثلاثة عناصر رئيسة: القدرة على تنفيذ التهديد، والمصداقية، والنية الواضحة بعدم التراجع.

ثانيا: مفهوم عصر ما بعد الحقيقة (Post – truth Era)

في العقود الأخيرة، طرأت تحولات نوعية على طبيعة الصراع السياسي والعسكري بفعل ظهور ما يُعرف بـ عصر ما بعد الحقيقة (Post–Truth Era)، ليعبر عن ظاهرة تتراجع فيها أهمية الحقائق الموضوعية أمام التأثير العاطفي والمعتقدات الشخصية في تشكيل الرأي العام. يُعد أول استخدام موثق لهذا المصطلح في مقال كتبه الكاتب الأمريكي Steve Tesich ، بعنوان (A Government of Lies) ونُشر في مجلة (The Nation) في هذا المقال، وصف الكاتب واقعاً اجتماعياً وسياسياً يتسم بتراجع المصداقية، إذ تغلب العواطف والمصالح الشخصية على الحقائق الموضوعية في توجيه السلوك العام، وانتشر التضليل الإعلامي والمعلومات المزيفة كأدوات فعالة في الحروب النفسية والإعلامية، ويرجع ذلك الى سلسلة الفضائح الكبرى مثل (ووترغيت ، وإيران – كونترا) ، التي أدت الى تآكل الثقة في المؤسسات الحكومية والأخبار الرسمية. ونتيجة لذلك، فضل الجمهور الانخراط في حالة إنكار واعٍ للحقائق مستبدلين بها روايات مطمئنة قد لا تسند إلى الحقائق. هذه الظاهرة، كما يؤكد الكاتب، تشكل تهديداً جوهرياً للديمقراطية[3].

رغم أن مصطلح (ما بعد الحقيقة) ظهر لأول مرة في أوائل التسعينيات، لكن استخدامه لم يشهد انتشاراً واسعاً وتحول إلى ظاهرة سياسية وثقافية بارزة إلا في العقد الثاني من القرن الحادي والعشرين، لا سيما عقب أحداث محورية مثل الانتخابات الرئاسية الأمريكية عام 2016 واستفتاء خروج بريطانيا من الاتحاد الأوربي(Brexit) وقد بلغ هذا المفهوم ذروته في العام نفسه، حين اختار قاموس أكسفورد مصطلح " Post–Truth " ليكون كلمة العام، معرفًا إياه بأنه يشير إلى "الظروف التي تصبح فيها الحقائق الموضوعية أقل تأثيرًا في تشكيل الرأي العام من المناشدات العاطفية والمعتقدات الشخصية"[4] .

وانطلاقاً من هذا التعريف، تناول عدد من الباحثين هذه الظاهرة من زوايا متعددة، أبرزهم **(d'Ancona Matthew)** في كتابه Post–Truth: The New War on Truth and How to Fight Back ، الذي أوضح كيف هيمنت السرديات العاطفية على المشهد السياسي المعاصر، مع تراجع الثقة في المؤسسات الإعلامية والتعليمية وانعكاس ذلك على الحملات الانتخابية. ومن منظور فلسفي واجتماعي، بحث **McIntyre (Lee)**جذور انتشار المعلومات المضللة وتراجع مكانة الحقيقة في الثقافة الحديثة، لافتًا إلى دور التعقيدات الرقمية في إضعاف قدرة الجمهور على التمييز بين الحقيقة والزيف[5]. وفي سياق نقدي، طرحت **(Michiko Kakutani)** قراءة نقدية لانهيار مفهوم الحقيقة في الخطاب السياسي والإعلامي المعاصر، مؤكدة أن جذور هذه الأزمة تعود جزئياً إلى الإرث الفكري لما بعد الحداثة الذي روّج لفكرة نسبية الحقيقة وتقويض الموضوعية. تربط الكاتبة بين هذا الأساس الفلسفي وصعود خطاب (ألحقائق البديلة)، إذ تحوّل الكذب إلى أداة سياسية منهجية، ووجد بيئة خصبة في ظل فوضى الإعلام الرقمي وفقاعات التصفية التي تعزل الأفراد داخل أنماط معلوماتية تؤكد قناعاتهم المسبقة[6].

استنادًا إلى ما تقدم، يتضح أن (عصر ما بعد الحقيقة) كإطار تحليلي لفهم التحولات التي أحدثتها البيئة الرقمية في السياسة والإعلام والثقافة، إذ تراجعت سلطة الحقائق الموثقة لصالح العاطفة والمعتقدات الشخصية، ما أفسح المجال أمام توظيف الأخبار المضللة والتلاعب بالمعلومات كأدوات للحروب الهجينة. وبهذا يمكن تعريفه بأنه (مرحلة **تاريخية تُقاس فيه المعلومة بقدرتها على التأثير لا بمدى صحتها، مما يجعل الوعي الجمعي أداة وهدفاً في آن واحد، فيتحول الوعي الجمعي إلى ساحة صراع استراتيجي).**

ثالثاً: الحرب الهجينة – المفهوم والخصائص

مع تطور بيئة الصراعات في القرن الحادي والعشرين، باتت الحروب تأخذ أشكالًا جديدة تتجاوز النزاعات المسلحة التقليدية، ومن أبرزها الحرب الهجينة(Hybrid Warfare) ، التي تُعد من الظواهر المعقدة والمتعددة الأبعاد في النزاعات الحديثة. عرفها(Frank Hovman) في كتابه Conflict In The 21st Century: The Rise of Hybrid Wars على أنها (**استراتيجية تجمع بين التكتيكات العسكرية التقليدية وغير التقليدية، واداة للفاعلين الدوليين وغير الدوليين)**[7].

Misan Journal of Political and International Studies
مجلـــة ميسان للدراسات السياسية والدولية
ISSN (Print): 3007-620X , ISSN (Online): 3007-6218
المجلد (1) العدد (1) كانون الأول/ديسمبر2025
Vol. (1) No.,(1) December2025

وتتميّز هذه الحرب بجملة من الخصائص التي تجعلها أكثر تعقيداً وخطورة مقارنة بأشكال الحرب التقليدية وكما موضح في الشكل رقم (١) تشمل الدمج بين الوسائل النظامية وغير النظامية، تعدد أدوات التأثير، الوكلاء بالنيابة، الضبابية والإنكار، الاستنزاف التدريجي، استخدام الفضاء السيبراني، المرونة والتكيف، واستغلال المنطقة الرمادية[8] .

الشكل رقم (١) يوضح خصائص الحرب الهجينة

الشكل من اعداد الباحثة

المطلب الثاني: الأبعاد الجديدة لمفهوم الردع في سياق الحروب الهجينة وعصر ما بعد الحقيقة

اولاً: التحول في مفهوم الردع الاستراتيجي

شهد مفهوم الردع تحوّلات جوهرية في العقود الأخيرة، مدفوعاً بالتغيرات الهيكلية التي طالت طبيعة الفواعل الدولية، وأنماط الحروب، وبيئة الصراع الإستراتيجية. فعلى خلاف ما كان عليه خلال الحرب الباردة، حين تمحور الردع حول التهديد باستخدام القوة النووية أو العسكرية التقليدية لضمان الاستقرار الاستراتيجي، اتجه المفهوم اليوم نحو مقاربات أكثر تكاملًا، تستوعب تعقيدات البيئة الأمنية الحديثة التي تتداخل فيها الأبعاد العسكرية، المعلوماتية، السيبرانية، والاقتصادية.

1 - التحول من الردع الكلاسيكي إلى الردع المتكامل

اعتمد الردع التقليدي على منطق التهديد بالعقاب المؤكد، إذ بُني على أساس التوازن الاستراتيجي بين القوى الكبرى، خصوصاً في ظل الثنائية القطبية. غير أن تصاعد الحروب الهجينة، التي تدمج بين الوسائل النظامية وغير النظامية، كشف عن محدودية هذا النموذج.

في هذا السياق، برز مفهوم (الردع المتكاملIntegrated Deterrence) ، الذي تبنته الولايات المتحدة الامريكية رسمياً في استراتيجية الدفاع الوطني، لا سيما في ظل التحولات الجيوسياسية المتسارعة وتصاعد حدة التهديدات الهجينة متعددة الأبعاد. ويعكس هذا المفهوم نهجاً شمولياً يسعى إلى دمج الأدوات العسكرية وغير العسكرية، التقليدية وغير التقليدية، الوطنية والمتعددة الأطراف، من أجل بناء بيئة أمنية تمنع الخصوم من التفكير في سلوك عدائي، عبر التأثير في نواياهم الاستراتيجية وليس فقط قدراتهم العملياتية. وبهذا يتجاوز الردع المركب النموذج التقليدي القائم على العقوبة أو الإنكار، ليتجه نحو هندسة بيئة الردع الشاملة، اعتمادًا على أدوات متزامنة ومتشابكة تؤسس لاستجابة استراتيجية متعددة الجبهات[9].

تتبع أهمية التحول نحو الردع المتكامل من إدراك متزايد لدى صانعي القرار بأن البيئة الأمنية المعاصرة أصبحت أكثر تعقيداً، مع تصاعد التهديدات التي تصدر عن فواعل دولية وغير دولية تتبنى تكتيكات هجينة تمزج بين القوة الصلبة والناعمة. تستهدف هذه التهديدات في الغالب الإدراك بقدر ما تستهدف البنية المادية أو القدرات العسكرية للخصم.

وقد أكد تقرير صادر عن مؤسسة (RAND) أن أحد أعمدة فعالية الردع المتكامل يكمن في بناء معادلة ردع غير خطية تدمج بين الردع الصلب والردع المعرفي، بهذا يصبح الردع المتكامل ليس خيارًا تكتيكاً فحسب، بل ضرورة استراتيجية لإعادة بناء توازن الردع في عالم يتسم بالتشابك وتعدد مصادر التهديد[10].

2 - الحرب المعرفية والردع: تحوّل في مفاهيم السيطرة والهيمنة الإستراتيجية

برزت الحرب المعرفية (Cognitive Warfare)، من بين أخطر مخرجات الحرب الهجينة، كإحدى أدوات الصراع الأكثر تعقيداً وتأثيراً، إذ لم تُعد تستهدف القدرات العسكرية أو البنى التحتية للدول فحسب، بل أصبح **العقل البشري ذاته ميداناً للمعركة**.

وفقًا للتقرير الصادر عن(Innovation Hub) التابع لحلف شمال الأطلسي (الناتو) عرف الحرب المعرفية بأنها (عمليات منظمة تهدف إلى استهداف العمليات المعرفية لصناع القرار، من خلال استخدام تقنيات متقدمة تشمل المعلومات المضللة، والتلاعب الإعلامي، والهجمات السيبرانية، لخلق بيئة من التشويش والارتباك، ما يؤدي إلى تقويض قدرة الخصم على اتخاذ قرارات سليمة وفعالة).

وتقوم الحرب المعرفية وفقاً للتقرير على استخدام تقنيات متقدمة – مثل الذكاء الاصطناعي، البيانات الضخمة، علم النفس العصبي، والتحكم بالإعلام – من أجل التأثير على طريقة تفكير الأفراد والمجتمعات، وزعزعة إدراكهم للواقع، وإضعاف ثقتهم بالمؤسسات، وإرباك عملية اتخاذ القرار. كما تسعى إلى **اختراق البُنى المعرفية للمجتمعات** واستهداف (مراكز الجاذبية الإدراكية)، لا من خلال الحرب المباشرة، بل عبر أدوات ناعمة وغير مرئية، لكنها فعالة.[11]

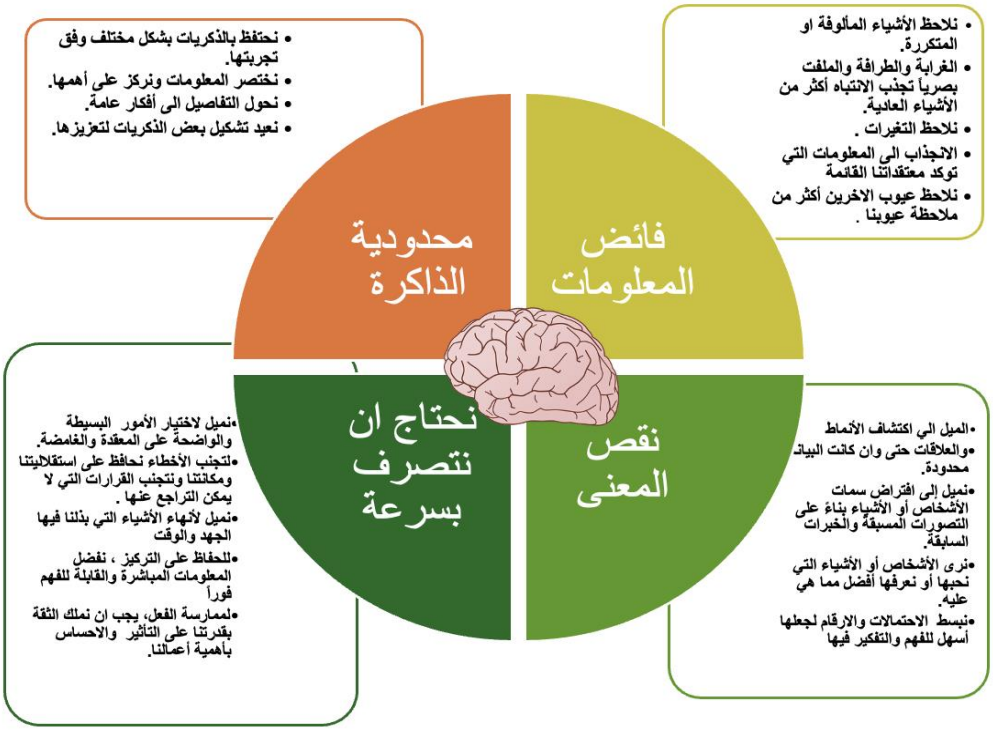
وتزداد خطورة هذا النوع من الحروب كما ذكر التقرير عندما يُقترن بتطور ما يُعرف بـ (الأسلحة العصبية Neuro-Weapons)، وهي أدوات متقدمة تستخدم علوم الأعصاب لاستهداف الإدراك البشري، والتحكم في العاطفة والانتباه والقرار، ما يجعل من الإنسان سلاحًا بحد ذاته. ويؤكد التقرير أن هذه الأسلحة تُعيد رسم طبيعة الحرب، وتجعل من إدارة الادراك معركة مستمرة لا تخضع لمنطق (الهدنة) أو (السلام)، لأنها تجري في وعي الإنسان دون أن يشعر[12] .

تشكل **التحيزات المعرفية** إحدى أهم نقاط الضعف التي تُستغل في الحرب المعرفية، إذ يعتمد العقل البشري على اختصارات ذهنية لمعالجة المعلومات واتخاذ قرارات سريعة، ما يفتح المجال واسعًا أمام التلاعب والإرباك. تبين خريطة (التحيّزات المعرفية*Cognitive Bisa Codex*)

Misan Journal of Political and International Studies
مجلـــة ميسان للدراسات السياسية والدولية
ISSN (Print): 3007-620X , ISSN (Online): 3007-6218
المجلد (1) العدد (1) كانون الأول/ديسمبر2025
Vol. (1) No.,(1) December2025

(الشكل رقم ٢)، كيف أن الدماغ عرضة لما يزيد عن 180 نوعاً من التحيزات، تُصنف ضمن أربع فئات رئيسة: فائض المعلومات، نقص المعنى، الحاجة للتصرف بسرعة، ومحدودية الذاكرة. يستغل الفاعلون هذه التحيزات عبر الاعلام والخوارزميات والتقنيات السلوكية لإعادة تشكيل الإدراك وصناعة واقع بديل، مما يجعل حماية الادراك مهمة استراتيجية تضاهي أهمية الدفاع العسكري[13].

الشكل رقم (2) خريطة التحيزات المعرفية



الشكل من اعداد الباحثة وفقاً للمصدر : Innovation Hub. *Cognitive Warfare*. Paris: NATO, 2020

في ظل هذا التحوّل العميق في طبيعة الصراع، لم يعد الردع التقليدي – القائم على التهديد باستخدام القوة الصلبة – كافيًا لمواجهة التحديات غير المادية التي تفرضها الحرب الإدراكية. فالصراع لم يعد يدور فقط حول توازن القوة العسكرية، بل أصبح يتمحور حول السيطرة على الإدراك والمعرفة والتأثير على وعي الخصم وسلوك المجتمع.

ومن هنا، يبرز الردع المعرفي (Cognitive Deterrence) كأحد الأدوات الاستراتيجية الفعالة الذي يُشير إلى (قدرة الدولة أو الفاعل الاستراتيجي في تشكيل إدراك الخصم للمخاطر والتكاليف المحتملة لأي تصرف عدائي، من خلال السيطرة والتحكم في المعلومات وبث رسائل استراتيجية مدروسة تهدف إلى زرع الشك وعدم اليقين في وعي وصورة الخصم الذاتية، بطريقة تجعله يتوقع عواقب سلبية لأي تصرف عدائي ما يؤدي إلى تعديل سلوكه وقراراته قبل وقوع أي تصعيد فعلي [14]، ما يوفر هامشاً أوسع للتهدئة والحوار. ويُعد الردع المعرفي ركيزة أساس في البيئة الأمنية الحالية التي تتسم بالتعقيد والتشابك بين الأبعاد السياسية والإعلامية والتقنية.

3 – الردع السيبراني

أ. مفهوم الردع السيبراني

أصبحت العلاقة بين الحرب السيبرانية واستراتيجية الردع محور اهتمام الباحثين في الدراسات الأمنية الحديثة، إذ يسعى الباحثون إلى إعادة تفسير مبادئ الردع الكلاسيكي وتكييفها لتتناسب مع خصوصيات الفضاء السيبراني، بهدف منع أو تقليل الهجمات الإلكترونية على الأصول الحيوية للدول. وفي هذا الإطار، يوضح (Joseph Nye) أن الردع السيبراني ليس مجرد تهديد بالعقاب، بل هو عملية إدراكية تهدف إلى جعل الخصم يقدّر أن تكاليف الهجوم المحتملة تفوق المنافع المرجوة.

ويشير Nyeإلى أن هناك أربع آليات رئيسة لتحقيق الردع والسيطرة على السلوك العدائي في الفضاء السيبراني[15] :

1. التهديد بالعقوبة :(Threat of Punishment) إذ يواجه الخصم تهديداً بعقوبات موجعة في حال قيامه بالهجوم.
2. الحرمان عبر الدفاع :(Denial by Defense) أي بناء قدرات دفاعية متينة تحول دون تحقيق أهداف الهجوم وتجعلها غير مجدية.
3. التشابك :(Entanglement) وجود مصالح اقتصادية أو سياسية متبادلة تجعل أي هجوم مكلفاً على الخصم نفسه.
4. الأعراف أو المحرمات المعيارية :(Normative Taboos) ترسيخ قواعد دولية وأعراف تمنع أو تقيّد استخدام القدرات السيبرانية في أفعال عدائية.

وبهذا الطرح، يتجاوز الردع السيبراني النموذج التقليدي القائم على القوة العسكرية فقط، ليصبح إطاراً متعدد الأبعاد يجمع بين القوة النفسية، الدفاعية، السياسية، والأخلاقية، ما يعكس الطبيعة المعقدة والمتغيرة للفضاء السيبراني، ويمنح صانعي السياسات أدوات أكثر مرونة وفاعلية للتصدي للتهديدات الرقمية الحديثة.

ب. تعريف الفضاء السيبراني

يُمثل الفضاء السيبراني (Cyberspace) ساحة مركزية للصراع غير التقليدي بين الدول والجهات الفاعلة من غير الدول في الحروب الهجينة. وقد عُرّف بأنه (المجال غير المادي الناتج عن الربط بين الشبكات الرقمية وأنظمة المعلومات والاتصالات، والذي يُمكّن من إنشاء ومعالجة وتبادل المعلومات عبر البنى التحتية الإلكترونية). ووفقًا لـ الاستراتيجية السيبرانية الوطنية الأميركية يُعد الفضاء السيبراني بُعدًا عملياتي خامساً إلى جانب البر، والبحر، والجو، والفضاء، تُمارس فيه الدول والمنظمات أنشطة دفاعية وهجومية لتحقيق مكاسب استراتيجية غير تقليدية[16].

في سياق الحروب الحديثة، تتطلب دراسة الردع التعرض الى الهجمات السيبرانية التي تستخدم كوسيلة استراتيجية لتعطيل الوعي الجمعي وإرباك عملية اتخاذ القرار لدى الخصم، من خلال سلسلة أفعال عدائية منسقة تُنفذ عبر الفضاء الإلكتروني بهدف تعطيل أو تدمير أو التلاعب بأنظمة الحاسوب، وشبكات الاتصالات، والبيانات الحساسة، سواء أكانت مدنية أو عسكرية. وتُدمج هذه الهجمات في إطار أوسع يُعرف بالـ تهديدات الهجينة(Hybrid Threats) ، التي تمزج بين الوسائل العسكرية وغير العسكرية– مثل الحرب السيبرانية، والمعلوماتية، والدعاية— بهدف زعزعة استقرار الخصم دون الانخراط في مواجهة مسلحة مباشرة، مع إضعاف ثقته بالمؤسسات وإرباك آليات صنع القرار لديه.

وتتنوع أنماط الحروب السيبرانية لتشمل ثلاث فئات رئيسة :الحروب منخفضة الشدة، التي تتجسد في أنشطة مثل التجسس الرقمي، والاختراقات، وحملات التضليل النفسي؛ والحروب متوسطة الشدة، التي ترتبط غالباً بالأعمال العسكرية التقليدية وتستهدف البنى التحتية الحيوية أو أنظمة القيادة والسيطرة؛ والحروب عالية الشدة، التي تمثل سيناريوهات محتملة قد تؤدي، في حال وقوعها، إلى شلل شامل للبنى التحتية الرقمية والمادية على حد سواء[17]. وتُستخدم هذه الأنماط عبر تقنيات متعددة تشمل الاختراق الإلكتروني(Hacking) ، والهجمات الموزعة لحرمان الخدمة (DDoS)، والبرمجيات الخبيثة(Malware) ، والتصيد الإلكتروني(Phishing) ، فضلاً عن أساليب متقدمة تستهدف الثغرات التقنية والبشرية على السواء، بهدف تسريب المعلومات أو حجبها وإثارة حالة من عدم اليقين.

Misan Journal of Political and International Studies
مجلـــة ميسان للدراسات السياسية والدولية
ISSN (Print): 3007-620X , ISSN (Online): 3007-6218
المجلد (1) العدد (1) كانون الأول/ديسمبر2025
Vol. (1) No.,(1) December2025

وقد أكد تقرير صادر عن مركز الدفاع السيبراني التابع لحلف الناتو أن التهديدات السيبرانية لم تُعد محصورة في النطاق التقني، بل تحولت إلى أداة لإحداث تأثيرات نفسية ومعرفية طويلة الأمد تستهدف كفاءة الأنظمة السياسية والاجتماعية[18] وبذلك، يغدو الفضاء السيبراني ليس فقط ميدانًا تقنياً للمواجهة، بل منصة استراتيجية لإعادة تشكيل الإدراك الجمعي والتأثير في السلوك السياسي والاجتماعي للخصم، ضمن بنية متكاملة للردع في بيئة ما بعد الحقيقة.

ثانياً: أدوات الردع المعرفي والسيبراني

يمثل الردع الإدراكي والمعرفي أحد أبرز مكونات الحروب الحديثة، إذ يُستخدم للتأثير في وعي الخصم وتشكيل تصوراته ومواقفه من خلال أدوات غير تقليدية تستهدف البنية النفسية والمعلوماتية.. ويمكن تحديد أبرز هذه الأدوات كما يلي:

1 – الإعلام والتضليل المعلوماتي Media & Disinformation

تُستخدم وسائل الإعلام التقليدية ومنصات التواصل الاجتماعي كأدوات مركزية في توجيه الرأي العام والتأثير على الإدراك الجمعي. إذ تُنشر عبرها حملات منظمة من المعلومات المضللة التي تهدف إلى خلق سرديات بديلة للواقع، مما يؤدي إلى زعزعة الثقة بالمؤسسات، وإضعاف معنويات المجتمعات. التدخل الروسي في الانتخابات الأمريكية عام 2016، يُعد من أبرز الأمثلة على توظيف وسائل التواصل الاجتماعي لنشر أخبار مضللة أثرت في تصورات الناخبين وسلوكهم السياسي، إذ استُغلت هذه الوسائل وخوارزمياتها لخلق بيئات معلوماتية مغلقة (Echo Chambers)، تعزز التصورات المسبقة وتُضعف التمييز بين الحقيقة والتضليل. يشير Thomas Rid الى أن هذه (الإجراءات النشطة) تشمل أيضًا التلاعب بالمؤسسات السياسية وزرع الفتنة واختراق الأنظمة السيبرانية، وتُعد أداة ردع معرفي تهدف إلى تشويش المعرفة وتقويض صنع القرار[19].

إلى جانب ذلك، تم توظيف المؤثرين الرقميين (Digital Influencers) كجزء من المنظومة الإعلامية المتكاملة التي اعتمدتها (وكالة أبحاث الإنترنت الروسيةIRA)، إذ أشار تقرير لجنة الاستخبارات في مجلس الشيوخ الأمريكي، ان الوكالة قامت بتوظيف مؤثرين رقميين أو نشطاء، ودفعهم – أحيانًا دون علمهم – لنشر رسائل أو تنظيم فعاليات تتماشى مع أهداف الحملة الروسية. وقد صنّف التقرير هؤلاء الأفراد إلى ثلاث فئات رئيسة: المستغلون دون وعي، (Useful Idiots) الذين يُستغلون دون إدراك لخدمة المصالح الروسية، و Fellow) (Travelersالمتعاطفون أيديولوجيًا مع المواقف الروسية، وعملاء التحريض(Agent Provocateurs) الذين يتم استقطابهم للقيام بأعمال غير قانونية أو سرية لصالح روسيا. ويؤكد التقرير أن هذا الأسلوب منح عمليات التأثير الروسية مصداقية أكبر، وساعد على توسيع نطاق وصولها للجمهور المستهدف، من خلال واجهات بشرية إذ يُستخدمون لنشر رسائل سياسية واستراتيجية بطرق تبدو عفوية وغير مباشرة[20].

وفي سياق مشابه، وظّفت حملة الرئيس الفلبيني (Rodrigo Duterte) مجموعة من المؤثرين المحليين على منصات مثل يوتيوب وفيسبوك، بهدف مهاجمة الصحفيين المستقلين، وتعزيز صورته أمام الرأي العام من خلال إنتاج محتوى منسق يُظهره بمظهر القائد القوي والحازم، ويُهمّش الأصوات الناقدة لرئاسته، وهو ما يعكس توظيفًا استراتيجيًا للتأثير الرقمي في توجيه الرأي العام المحلي[21].

2– الذكاء الاصطناعي وتحليل البيانات الضخمة(AI & Big Data Analytics)

تُعد تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة من الركائز الأساس في منظومة الردع المعرفي لما يتيح من قدرة فائقة على تحليل السلوك الرقمي وفهم ديناميات التفاعل على المنصات الإلكترونية. وبالاستفادة من خوارزميات التعلم الآلي والنماذج التنبؤية، يمكن تصميم حملات دعائية موجهة بدقة لاستهداف فئات بعينها، بما يعزز فاعلية التأثير على الرأي العام. وقد تجلّى هذا الدور بوضوح خلال (انتخابات الرئاسة الامريكية عام 2016) لعبت شركة (Cambridge Analytica) دوراً محورياً في حملة الرئيس الامريكي (دونالد ترامب) من خلال استغلال البيانات الشخصية لمستخدمي وسائل التواصل الاجتماعي، وبالأخص فيسبوك بشكل غير قانوني لجمع وتحليل الملفات النفسية للمواطنين. استخدمت الشركة نموذج (Big Five) لتحليل السمات الشخصية للمستخدمين بناءً على بياناتهم وسلوكياتهم على الإنترنت، مما مكنها من إنشاء

ملفات نفسية دقيقة (psychographic profiles) لكل فرد وبالاعتماد على هذه الملفات، طورت حملة ترامب استراتيجيات تسويقية وسياسية مخصصة تستهدف الناخبين برسائل مصممة خصيصاً لتحفيز مشاعرهم والتأثير على قراراتهم الانتخابية. وقد أسهم هذا النهج في استقطاب فئات محددة من الناخبين بطريقة فعالة، مما أحدث تحولًا نوعياً في كيفية إدارة الحملات الانتخابية وأثار جدلاً واسعاً حول أخلاقيات استخدام البيانات الشخصية في السياسة[22] .

كما كشفت أبحاث حديثة وجود بوتات اجتماعية متطورة (sleeper social bots) وهي بوتات مدعومة بـ(Chat GPT) تتمتع بقدرة عالية على التخفّي داخل شبكات التواصل الاجتماعي والتفاعل مع المستخدمين بطريقة مشابهة للبشر، ما يجعلها أدوات مؤثرة في نشر التضليل دون اكتشاف سريع. وقد أظهرت تجربة فعلية أن الطلاب المشاركين لم يستطيعوا التمييز بين هذه (bots) والبشر أثناء نقاش حول اقتراح انتخابي وهمي، مما يؤكد خطورتها كأدوات تضليل سياسي متطورة[23].

من جهة أخرى، بينت دراسة نُشرت في مجلة (Nature Human Behavior) أن نماذج اللغة الكبيرة مثل (GPT-4) تمتلك قدرة إقناعية قد تفوق البشر في النقاشات السياسية، إذ يتم تفصيل خطاب هذه النماذج وفقاً لخصائص الجمهور مثل العمر والجنس والانتماء السياسي، مما يمنح الرسائل تأثيرًا نفسيًا عميقًا يتجاوز التوقعات التقليدية[24] .

المطلب الثالث: النماذج التطبيقية

في هذا المطلب، سيتم تناول النماذج التطبيقية للحروب الهجينة، والتي جرى اختيارها استناداً إلى معايير منهجية تهدف الى ابراز التنوع الجغرافي والاستراتيجي في بؤر التوتر العالمية وتشمل هذه النماذج (الهند – باكستان، كوريا الشمالية، إيران – إسرائيل)، لما تمثله من حالات بارزة في توظيف أدوات الحرب المعرفية والسيبرانية. فهي تغطي جنوب آسيا وشرق آسيا والشرق الأوسط، بما يعكس اختلاف السياقات والبيئات السياسية التي تُختبر فيها ديناميات الردع في عصر ما بعد الحقيقة. أما من حيث الحدود الزمانية، فيركز البحث على الفترة الممتدة بين **2025–2010**، وهي مرحلة شهدت بروزاً متزايداً للحروب الهجينة وتوسعاً في استخدام الأدوات المعرفية والسيبرانية في الصراعات الدولية، الأمر الذي يجعلها مجالاً خصباً للتحليل والمقارنة، كما هو موضح أدناه:

اولاً: نماذج الحروب المعرفية

1 . الصراع الهندي – الباكستاني

تُعد حالة الصراع بين **الهند وباكستان** بين عامي 2019 و2025 نموذجًا واضحًا لهذا التحول النوعي في ميدان الحرب المعرفية. ففي عام 2019، شهد الصراع الهندي – الباكستاني تصعيدًا ملحوظًا عقب حادثة (بولواما) وردها العسكري في (بالاكوت)، إذ استخدمت الهند حملات معلوماتية مكثفة استهدفت تشكيل إدراك داخلي وخارجي يعزز من موقفها الاستراتيجي. اعتمدت (نيودلهي) على وسائل إعلام تقليدية ومنصات رقمية لنشر سرديات تحاول بها تصوير قدراتها العسكرية بصورة تفوق الواقع، مع إلحاق رسائل نفسية تهدف إلى زعزعة استقرار الرأي العام الباكستاني وتعزيز الوحدة الوطنية الهندية، تمثل في صياغة خطاب موحّد يظهر الهند كقوة تحمي سيادتها بكل عزم، وفي الوقت ذاته يشكك في قدرة باكستان على تحمل تكاليف تصعيد أكبر. وقد أسهم هذا الخطاب، إلى جانب تدخلات سيبرانية وحملات معلوماتية منظمة، في تقويض قدرة القيادة الباكستانية على اتخاذ قرار تصعيدي رغم أنها تمتلك السلاح النووي، من جانبها، ردت باكستان بحملات مضادة على الفضاء السيبراني، لكنها واجهت تحديات في التنسيق المؤسسي والفجوات التقنية التي حدّت من تأثير حملاتها المعرفية[25].

بحلول عام 2025، تطور الصراع إلى مستوى متقدم من **الحرب المعرفية**، بعد هجوم (باهالغام)، نفذت الهند ما يُسمى بـ (عملية السندور) التي شملت تنفيذ ضربة محدودة جنباً إلى جنب مع حملة سيبرانية واستراتيجية استهدفت السردية الدولية حول باكستان كداعم للإرهاب. بالمقابل، ردت باكستان بـ(عملية بنيان المرصوص) التي وظفت وسائل إعلامية رقمية ودبلوماسية تنطوي على رواية المظلومية واتهام الهند بالنزعة التوسعية. هذا

التكامل بين إنشاء سرديات مؤثرة ومعززة بالخطاب السيبراني والدبلوماسي أدى إلى تثبيط أي توجّه باكستاني للتصعيد العسكري، مما يؤكد أن الردع المدعوم بالإدراك المعرفي قد يتفوق على الرد التقليدي فاعلية[26].

ويُعد هذا التطور في الأدوات والأساليب بين 2019 و2025 مؤشرًا واضحًا على تحول الردع الاستراتيجي إلى ميدان **الحروب المعرفية**، إذ أصبحت السيطرة على الإدراك العام وتهيئة السردية الوطنية والدولية عاملًا حاسمًا في الصراع بين الدولتين.

2 . استراتيجية كوريا الشمالية الحرب النووية – المعرفية وحرب النفايات

تمثل كوريا الشمالية نموذجاً متقدماً للهجمات المعرفية من خلال ما يُعرف بـ (استراتيجية الحرب النووية–المعرفية) "Nuclear–Cognitive Warfare"وهي مقاربة تتخطى حدود الردع النووي التقليدي لتدمج بين أدوات القسر النووي ووسائل التأثير الإدراكي والنفسي على الخصوم. وتستهدف هذه الاستراتيجية وكما موضح في الجدول رقم (١) ثلاث دوائر رئيسة: (1) الرأي العام عبر صناعة الخوف والقلق من (نية) وقدرات نووية متضّخمة؛ (2) تماسك تحالف كوريا الجنوبية–الولايات المتحدة الامريكية عبر زعزعة الثقة بالردع الممتد الأميركي؛ (3) صناع القرار النووي لتعطيل آليات اتخاذ القرار أو إبطائها وإرباكها في لحظات الضغط. بهذه المقاربة تسعى كوريا الشمالية إلى تأخير القرارات غير المرغوبة لديها، أو حرفها، أو شلّها مؤقتًا[27].

جدول رقم (١) خصائص استراتيجية الحرب النووية –المعرفية

الفئة المستهدفة	نقاط الضعف	نوع الهجوم	هدف الهجوم
الرأي العام	**سهولة الوصول إلى المعلومات النووية، ثغرات في المعتقدات والقيم**	**التلاعب بالمعلومات، السرديات**	**إثارة الخوف والقلق**
الأطراف الرئيسة في تحالف كوريا الجنوبية–الولايات المتحدة (الحكومة أو الجيش)	**المعلومات غير المتكافئة والمصالح المتعارضة، السياسات النووية المتضاربة.**	**السرديات، التلاعب بالمعلومات**	**زعزعة تماسك التحالف**
صناع القرار النووي	**ضيق الوقت، الأعباء السياسية والاجتماعية.**	**تعطيل عملية اتخاذ القرار النووي**	**تعطيل عمليات اتخاذ القرار النووي**

الجدول من اعداد الباحثة وفقا للمصدر: Sohn, Hanbyeol, and Changwoo Kang. "North Korea's Nuclear–Cognitive Warfare Strategy."

لقد طبّقت كوريا الشمالية استراتيجيتها في الحرب النووية–المعرفية من خلال عدد من الإجراءات العملية التي تهدف إلى زرع الخوف والقلق لدى الجمهور وصناع القرار في كوريا الجنوبية والولايات المتحدة الامريكية. فقد زعمت في اذار 2022، عن إطلاق ناجح لصاروخ باليستي عابر للقارات من طراز (Hwasong–17)، لكن وزارة الدفاع الكورية الجنوبية أوضحت أن الصاروخ كان في الواقع من طراز (Hwasong–15)، فيما بدا أنه خداع يهدف إلى إرباك المجتمع الدولي[28] . في تشرين الاول 2022 أعلنت أنها أطلقت صاروخ كروز استراتيجي بالقرب من المياه قبالة (أولسان)، على الرغم من نفي السلطات الكورية الجنوبية لهذه الادعاءات[29].

الى جانب زراعة الخوف لدى الجمهور، تسعى كوريا الشمالية إلى **إضعاف تماسك تحالف كوريا الجنوبية–الولايات المتحدة** الامريكية واستغلال نقاط الضعف في سياسات الردع النووي لكلا البلدين لتقويض الثقة المتبادلة. تركز (بيونغ يانغ) على الردع الممتد، إذ تُغرس الشكوك لدى الحكومة والجيش والجمهور بشأن استعداد الولايات المتحدة لاستخدام الأسلحة النووية والتزاماتها في حالات الطوارئ. فعلى سبيل المثال، وصفت (كيم يو جونغ) إعلان واشنطن 2023 بأنه "تصريح متهور"، بينما شبهت صحيفة Tongil Sinbo التزام أمريكا بـ "منديل يمكن التخلص منه في أوقات الأزمات". كما تسعى كوريا الشمالية لاستغلال الغموض الاستراتيجي في السياسات النووية الأمريكية لنشر عدم الثقة وإثارة الانقسامات داخل التحالف[30] .

في الوقت نفسه، تهدف كوريا الشمالية إلى تعطيل عمليات صنع القرار النووي من خلال نشر المعلومات المضللة والإغراق الإعلامي، مما يستهلك وقت وموارد سيول وواشنطن. كما تعمل على خلق تصورات تهديد متباينة بين الحليفين، إذ تركز كوريا الجنوبية على الصواريخ التكتيكية قصيرة المدى، بينما تهتم الولايات المتحدة بالصواريخ العابرة للقارات، ما يضعف التنسيق بينهما. فضلاً عن ذلك، تستغل كوريا الشمالية الأعباء السياسية والدولية المحتملة لاستخدام الأسلحة النووية الأمريكية لتثبيط ردود الفعل المباشرة، مع تصوير الولايات المتحدة على أنها غير موثوقة، مما يعزز الشكوك لدى سيول بشأن تماسك التحالف.

من زاوية أخرى، استخدمت كوريا الشمالية (حرب النفايات) نموذجاً عملياً للحرب المعرفية والهجينة التي تعتمد على أدوات غير تقليدية للتأثير في البيئة الإدراكية للخصم. فقد لجأت بيونغ يانغ إلى إطلاق بالونات محمّلة بالنفايات نحو أراضي كوريا الجنوبية كرد فعل على إرسال منشورات مناهضة للنظام الكوري الشمالي من قبل نشطاء في الجنوب، وهذه البالونات تحتوي على نفايات منزلية مثل السجائر، الاكياس البلاستيكية وغيرها من القمامة. تهدف هذه العمليات إلى إرباك صانعي القرار وإحداث إرهاق إعلامي ومؤسساتي وتلوث بيئي، ما يعكس كيفية استخدام الفاعلين لوسائل رمزية وبسيطة لتحقيق أهداف استراتيجية دون اللجوء إلى المواجهة العسكرية المباشرة[31].

تمثل هذه النماذج دليلاً واضحاً على أن **الردع المعرفي** لم يعد مجرد أداة تكميلية، بل أصبح **ركيزة أساس في بنية الحروب الهجينة الحديثة** .

ثانياً: نماذج الحروب السيبرانية

1 – الصراع السيبراني الإيراني – الإسرائيلي

يُعَدّ هجوم ((Stuxnet الذي استهدف منشأة نطنز النووية في إيران سنة 2010 محطة مفصلية في تاريخ الهجمات السيبرانية، إذ شكّل أول حالة موثّقة يُسفر فيها هجوم إلكتروني عن أضرار مادية مباشرة خارج بيئة الاختبار. فقد صُمّم البرنامج الخبيث لاختراق أنظمة التحكم الصناعي وإتلاف أجهزة الطرد المركزي، في الوقت الذي قدّم فيه قرارات مضللة للمشغلين تُظهر أن الأجهزة تعمل بشكل طبيعي. هدفت الولايات المتحدة الامريكية، بالتعاون مع (إسرائيل) وفق ما تشير إليه تقارير عديدة، إلى إضعاف البرنامج النووي الإيراني من دون اللجوء إلى ضربة جوية أو عمليات خاصة. وقد أثار هذا الهجوم نقاشاً واسعاً بين الخبراء وصنّاع القرار حول انعكاساته الاستراتيجية، باعتباره سابقة توضح كيف يُمكن للقدرات السيبرانية أن تُستخدم كأداة مكمّلة للخيارات التقليدية في تقويض البنى التحتية الحساسة، الأمر الذي فتح الباب أمام مرحلة جديدة في التفكير بالردع والأمن الدولي.[32]

بلغ الصراع السيبراني ذروته في عام **2025**، عندما تعرّضت شبكات الاتصالات الإسرائيلية لاختراق واسع النطاق، وتعطّل البث التلفزيوني الرسمي الإيراني، ما اضطر السلطات إلى إخلاء مقرات قناتي 12 و14. في الوقت نفسه، شلّت الهجمات السيبرانية بنك(سبه) الحكومي في طهران، وأعلنت مجموعة تُعرف باسم "**العصفور المفترس** "مسؤوليتها عن تدمير البيانات بالكامل. كما شهدت هذه المرحلة نشاطًا متزايدًا لمجموعات(الهاكتفيزم)، إذ نفذت نحو 170 مجموعة إسرائيلية حوالي 1,345 هجومًا، في مقابل 55 مجموعة هاجمت إيران بواقع 155 عملية. ومن أبرز هذه الكيانات" و"**Mr. Hamza**، و"TEAM FEARLESS "، وArabian Ghosts "، التي ركّزت هجماتها على البنية التحتية المالية والإعلامية، مما أضاف بعدًا نفسيًا وإدراكيًا للصراع الرقمي.[33]

3- الهجمات السيبرانية الروسية على أوكرانيا

منذ عام 2014، شهدت أوكرانيا تصاعدًا ملحوظًا في الهجمات السيبرانية التي استهدفت بنيتها التحتية الحيوية، إذ لعبت مجموعات متعددة تابعة للاستخبارات العسكرية الروسية (GRU) أدوارًا رئيسة في هذا السياق. في عام 2015، نفذت مجموعة (Sandworm) المعروفة أيضًا بوحدة 74455 ضمن (GRU) سلسلة من الهجمات السيبرانية على شركات الكهرباء الأوكرانية، مستخدمة برمجيات خبيثة متخصصة مثل (Kill disk ، Blackenergy3)، مما أدى إلى انقطاع التيار الكهربائي عن مئات الآلاف من المستهلكين وتعطيل أنظمة التحكم الصناعية (SCADA) لفترات طويلة. في ديسمبر 2016، استُخدمت برمجية أكثر تطورًا تسمى (Crash override) في هجوم على محطة فرعية كهربائية أوكرانية، معززة بقدرات تحليلية واستهدافية متقدمة تعتمد على بروتوكولOPC ، ما مثّل تطوراً نوعياً في أساليب الهجوم السيبراني الروسي[34] من جهة أخرى، وابتداءً من عام 2020 وما بعده، تركزت الهجمات على وحدة أخرى من GRU تُعرف بوحدة **29155**، التي استخدمت أدوات متقدمة مثل (**Whisper Gate**، و**Raspberry Robin**، و**Saint Bot**)، مستهدفة مؤسسات في أكثر من عشرين دولة، بما فيها أوكرانيا ودول حلف شمال الأطلسي، بغرض التجسس والتخريب. يعكس هذا التطور تعدد وحدات الاستخبارات الروسية وتنوع استراتيجياتها، ما يجعل التهديد السيبراني مستمرًا ومتعدد الأبعاد، ويؤكد الحاجة إلى تعزيز القدرات الدفاعية والتنسيق الدولي لمواجهته[35] .

يتضح من العرض السابق أن كلا البعدين – المعرفي والسيبراني – يشتركان في بعض الأدوات والفضاءات، إلا أنهما يختلفان من حيث نطاق الاستهداف والنتائج المرجوة. ولتوضيح هذه الفوارق بصورة منهجية، يبين الجدول رقم (٢) مقارنة بين الحرب السيبرانية والحرب الإدراكية.

جدول رقم (٢) أوجه الاختلاف بين الحرب السيبرانية والحرب المعرفية/ الادراكية

البعد	Cognitive Warfare (الحرب المعرفية/ الادراكية)	Cyber Warfare (الحرب السيبرانية)
النطاق	**العقل البشري والإدراك (المعتقدات، السلوك، اتخاذ القرار)**	الفضاء السيبراني (الشبكات، الأنظمة، البنية التحتية الرقمية)
الهدف	**التأثير على العقول، تشكيل السرديات، زعزعة الثقة، التحكم بالوعي**	تعطيل الأنظمة، سرقة أو تدمير البيانات إضعاف البنية التحتية
الأدوات	**التضليل الإعلامي، الأخبار الكاذبة، الحرب النفسية، الدعاية ، استغلال مواقع التواصل الاجتماعي.**	فيروسات، برمجيات خبيثة، هجمات DDoSاختراقات، تجسس تقني
المخرجات	**تغيير القناعات، فقدان الثقة بالمؤسسات، شلل القرار السياسي والمجتمعي.**	توقف خدمات، فقدان بيانات، خسائر اقتصادية وتقنية
المستهدف	**الإنسان كفرد ومجتمع**	الأنظمة التقنية والدولار الرقمي
العلاقة	**معركة على العقل)وغالباً تستخدم الفضاء السيبراني كأداة)**	معركة على الآلة

الجدول من اعداد الباحثة

ومن خلال هذا التمييز يمكن القول إن الردع الإدراكي يمثل مرحلة أكثر تعقيداً من الردع السيبراني، لأنه يتجاوز الآلة ليصل إلى الإنسان ذاته، الأمر الذي يجعل أدواته أكثر تأثيراً واستدامة على المدى البعيد.

المطلب الرابع: تحديات الردع المعرفي والسيبراني

يواجه الردع السيبراني والمعرفي مجموعة من العقبات المعقدة التي تحد من فعاليته، سواء على مستوى التطبيق العملي أو التأثير النفسي على الأطراف المستهدفة. ومن اهم هذه التحديات كالاتي:

أولاً: تحديات الردع السيبراني

يمكن اجمال تحديات الردع السيبراني بالآتي[36]:

1. مشكلة الإسناد: يُعدّ تحديد الفاعل المسؤول عن الهجمات السيبرانية من أكبر التحديات التي تواجه الردع السيبراني. طالما الجهات المهاجمة لم تعلن مسؤوليتها رسمياً، كما يمكن لأي طرف، مثل الجماعات الإرهابية، الادعاء بالمسؤولية، مما يضعف من منطق الردع.
2. تعدد الفاعلين: الفضاء السيبراني لا يقتصر على الدول، إذ تنشط فيه الجماعات الإرهابية والمنظمات الاجرامية والنشطاء السياسيين، ما يجعل فرض الردع التقليدي صعباً، خصوصاً عند استهداف بنى تحتية حساسة عبر (وكلاء) لا ينتمون رسمياً لدولة معينة.
3. غياب الإطار القانوني والأعراف الدولية: تشكل القوانين الدولية الحالية تحدياً أمام الردع السيبراني، إذ يجرم القانون الدولي العدوان العسكري لكنه لا يحدد بوضوح متى يُعد الهجوم السيبراني عدواناً، مما يترك مساحات رمادية تعقد شرعية الرد وتضعف بناء استراتيجية فعّالة.
4. تجنب الرد بالانتقام أو الرد المضاد: تمثل طبيعة الهجمات السيبرانية غير المتوقعة وطول المدة الزمنية بين الهجوم والرد تحدياً في تطبيق الرد، فقد يبدو الرد تعسفياً او غير مرتبط بالحادث الأصلي. وفي بعض الحالات النادرة، قد تختار الدول الامتناع عن الرد لتجنب التصعيد.
5. وضوح الرسائل والانذارات للخصم: نجاح الردع يعتمد على قدرة الدولة على توصيل نواياها وقدرتها للخصم بوضوح، غير ان الطبيعية الخفية للهجمات السيبرانية تجعل من الصعب تفسير هذه الرسائل، وقد يؤدي سوء الفهم او تجاهلها الى تصعيد غير مقصود. ولذلك توصيل الرسائل بوضوح عنصرا اساسياً لضمان فاعلية الردع السيبراني.

ثانياً: تحديات الردع المعرفي

1. صعوبة قياس الادراك البشري: غياب أدوات دقيقة لقياس مستوى الخوف، القناعة، أو الثقة لدى الخصم، مما يجعل التنبؤ بالاستجابات العقلية والسلوكية أمرا معقداً.
2. التباين الثقافي والقيمي: إن التباين في البنى الثقافية والقيمية بين المجتمعات ينعكس على كيفية استقبال الرسائل الردعية؛ فبينما قد تُدرك في سياق ما كأداة ردع فعّالة، يمكن أن تُفسَّر في سياق اخر بوصفها مجرد دعاية أو تهديداً بلا جدوى.[37]
3. فجوة القدرات بين الدول: تفاوت القدرات التقنية والمعرفية يجعل بعض الدول غير قادرة على الردع الفعال مقارنة بالدول المتقدمة.
4. تسارع تدفق المعلومات في عصر ما بعد الحقيقة: انتشار المعلومات المضللة والتلاعب بالسرديات يُضعف من قدرة الدولة على ترسيخ خطاب ردعي مستدام[38].
5. البعد الأخلاقي: استخدام تقنيات التأثير والمعرفة المضللة يحقق أهداف الردع لكنه يقوّض الثقة المجتمعية ويهدد الاستقرار السياسي، ويزداد التعقيد مع دخول الذكاء الاصطناعي في توجيه السلوك الجمعي.

الخاتمة:

بعد اكمال محاور البحث من الناحيتين النظرية ودراسة بعض النماذج العملية عن الحروب الهجينة، يمكن لنا وضع هذه الخاتمة التي سنقسمها الى قسمين أحدهما يهتم بالنتائج والاستنتاج، والثاني يقدم عدد من التوصيات للوقوف بصورة مختصره عن مضامينه ومخرجاته النظرية والعملية، وذلك من خلال الاتي:

اولاً: النتائج والاستنتاجات

تمثل الحروب الهجينة نقطة تحول أساسية **في طبيعة ومنطق الردع الاستراتيجي**، إذ لم يُعد الاسناد إلى القوة العسكرية الصلبة كافياً لضبط سلوك الخصوم داخل بيئة دولية مضطربة تتسم بضبابية المعلومات وتعدد الفواعل وسرعة التطورات التكنولوجية. فقد انتقل الردع من الاعتماد على التهديد العسكري المباشر إلى **مزيج متداخل من الأدوات السيبرانية والمعرفية**، في انعكاس مباشر للتغيرات البنيوية التي أصابت طبيعة الصراع الدولي في **عصر ما بعد الحقيقة**.

خلال الحرب الباردة، ارتكز الردع على منطق مغاير تماماً، فقد قامت معادلته على **(توازن الرعب النووي)**، إذ كانت القوة التدميرية والقدرة على إيقاع عقاب ساحق بالخصم تمثل الضمانة لمنع التصعيد. وكانت الإشارات الردعية آنذاك واضحة ومباشرة: مناورات عسكرية، سباقات تسلح، تجارب نووية، وحسابات دقيقة متصلة بقدرة الضربة الثانية. بعبارة أخرى، كان الردع الكلاسيكي **عسكرياً – مادياً** يستند إلى (إظهار العقوبة المحتملة).

أما في عصر ما بعد الحقيقة والحروب الهجينة، فقد تحول مركز الثقل إلى (الوعي **الجمعي والفضاء السيبراني)** بوصفه ساحة الصراع الحقيقية. ولم تُعد المعلومات تُقاس بصدقها، بل بقدرتها على التأثير في الإدراك وصناعة القرار لدى الخصم. وهنا يظهر التمايز بين **الردع السيبراني**، الذي يستهدف الأنظمة التقنية بالتعطيل أو الإتلاف أو استنزاف الموارد، و**الردع المعرفي** الذي يركز على الإنسان كفرد وجماعة عبر تغيير القناعات وزرع الشك وشلّ القدرة على اتخاذ القرار. وغالباً ما يعمل الفضاء السيبراني كأداة ناقلة للأثر المعرفي.

هذا التراكب الجديد يمنح الردع مرونة وفورية تتفوق على الأطر التقليدية المبنية على تهديدات صريحة وثابتة، ويُبرز أهمية السيطرة على الفضاء السيبراني والتدفق المعلوماتية والتأثير في الرأي العام كعوامل أساس للردع المعاصر. ولتوضيح الفروقات بصورة منهجية، يعرض **الجدول رقم (٣)** مقارنة بين الردع الكلاسيكي والحديث وفق أبعاد: الهدف الرئيس، أساس الردع، الأداة، طبيعة الرسالة، الفاعلين، بيئة الصراع، زمن الفعل والتأثير، فضلاً عن قابلية **القياس والإسناد**، إذ يتسم الردع الكلاسيكي بوضوح أكبر، بينما يتسم الحديث بالغموض وصعوبة تحديد الفاعل أو قياس أثره بدقة.

وتؤكد **النماذج التطبيقية** التي تناولتها الدراسة على واقعية هذا التحول. ففي الأزمة الهندية–الباكستانية (2019–2025)، لم يكن امتلاك السلاح النووي هو العامل الحاسم في منع التصعيد، بل كان لتكامل الحرب المعرفية والسيبرانية دور جوهري في تقييد خيارات إسلام آباد. فقد ركّزت نيودلهي على التأثير في إدراك باكستان من خلال حملات إعلامية موجهة، وتوظيف مراكز الفكر للتأثير في الرأي الدولي، وتنفيذ هجمات سيبرانية عطّلت البنية التحتية الرقمية. هذه الإجراءات مجتمعة أضعفت ثقة الخصم بقدراته وحدّت من رغبته في التصعيد العسكري. وبالمثل، قدّمت كوريا الشمالية نموذجًا لـ **(الردع المعرفي– النووي)**، إذ لم تكتف بامتلاك قدرات نووية، بل وظّفت أدوات معرفية تستهدف ثلاثة مستويات: الرأي العام عبر تضخيم إنجازاتها النووية وإثارة المخاوف، التحالفات الدولية عبر زرع الشك في جدوى الردع الأمريكي الممتد، وصنّاع القرار عبر تكتيكات الإغراق المعلوماتي والتضليل الاستراتيجي. وبذلك لم يعد التحكم في القدرات وحده كافياً، بل أصبح التحكم في صورة القدرات وأثرها المعرفي جزءًا من معادلة الردع.

أما الحالة الإيرانية– الإسرائيلية، فقد أبرزت كيف يمكن للأداة السيبرانية أن تتحول إلى أداة ردعية ممتدة الأثر. فمنذ هجوم (Stuxnet 2010) وحتى موجة الهجمات المتبادلة في 2025، لم يقتصر الهدف على تعطيل البنية التحتية، بل تعدّاه إلى **زعزعة الثقة المجتمعية وإضعاف الرواية الوطنية** .وتكشف المقارنة بين هذه الحالة والهجمات الروسية على البنية التحتية الأوكرانية عن أن الهجمات السيبرانية لم تُعد مجرد وسيلة للتجسس أو المضايقة، بل قادرة على إحداث **أضرار مادية مباشرة** في شبكات الكهرباء ومحطات الطاقة والاتصالات، ما يجعلها أداة استراتيجية ذات أثر مزدوج: مادي ومعرفي.

ومع ذلك، تكشف النتائج ايضاً عن حدود وتحديات معقدة ينبغي التعامل معها بجدية. فعلى المستوى المنهجي، يصعب قياس فعالية الردع الادراكي– السيبراني بدقة بسبب طبيعته غير الملموسة واعتماده على متغيرات نفسية واجتماعية يصعب إخضاعها لمقاييس كمية صارمة. كما أن إشكالية **الإسناد** تمثل عائقاً رئيس، إذ تتيح للفاعلين إمكانية إنكار مسؤوليتهم عن الهجمات، مما يفتح الباب أمام أخطاء في التقدير أو تصعيد غير مقبول. وفي المقابل، يرتبط الردع المعرفي بإشكالية أخرى تتمثل في تباين فاعلية السرديات تبعاً لاختلاف البيئات الثقافية والسياسية، فما قد ينجح في جنوب آسيا قد لا يكون مؤثراً في الشرق الأوسط أو أوروبا الشرقية، وهو ما يحدّ من إمكانية تعميم نتائجه بشكل مطلق.

أما على المستوى الأخلاقي، فتبدو التحديات أكثر حدة، إذ يثير البعد السيبراني إشكالية التناسب ومشروعية استهداف البنى التحتية المدنية والمجتمعات بأكملها عبر الوسائل الرقمية، وهو ما يتعارض مع مبادئ القانون الدولي الإنساني، في حين يطرح البعد المعرفي معضلة مشروعية التلاعب بالوعي الجمعي من خلال صناعة سرديات مضللة أو استخدام تقنيات متقدمة مثل التزييف العميق والذكاء الاصطناعي التوليدي، التي تسمح بتحليل البيانات والتلاعب بالمشاعر وتوجيه السلوك الجمعي على نحو يقوّض الثقة المجتمعية ويهدد الشرعية السياسية والاستقرار الداخلي، كما يهدد حقوق الانسان ومبادئ الديمقراطية. ويُخشي هنا أن تتحول أدوات الردع الادراكي– السيبراني إلى وسائل ابتزاز سياسي أو حرب نفسية مستدامة، بما يتجاوز حدود الردع المشروع إلى مستويات من التلاعب بالإنسان ذاته. ومن ثمّ، فإن التحدي الرئيس لا يكمن فقط في تطوير أدوات فعّالة للردع الإدراكي–السيبراني، بل في صياغة أطر معيارية وأخلاقية تضمن استخدامه ضمن حدود تحافظ على استقرار النظام الدولي وتمنع انزلاقه إلى حالة من الفوضى المعرفية الشاملة.

جدول رقم (3) مقارنة بين الردع الكلاسيكي والردع الحديث

العنصر	الردع الكلاسيكي	الردع الحديث
الهدف الرئيس	منع الخصم من اتخاذ قرار هجومي عبر التهديد باستخدام القوة العسكرية	منع الخصم من اتخاذ قرار هجومي عبر مزيج من القوة الصلبة العسكرية (والقوة الناعمة)الإعلام الإدراك، المعلومات)
أساس الردع	الخوف من الرد الانتقامي أو العقوبة (الضربة النووية)	خلق بيئة من الغموض والتشويش على الإدراك إلى جانب التهديد باستخدام القوة التقليدية
الأداة الأساس	الأسلحة التقليدية والنووية، التهديد المباشر	القوة العسكرية +الإعلام +الفضاء السيبراني الذكاء الاصطناعي +التضليل المعلوماتي
طبيعة الرسالة الردعية	واضحة وصريحة (إذا هاجمت سأرد بعنف)	مزيج من الرسائل المباشرة وغير المباشرة، تُبنى عبر السرديات والخداع والتضليل المعلوماتي
الفاعلون الرئيسيون	الدول ذات القدرات النووية الكبرى	الدول+ الفاعلون من غير الدول+ الذكاء الاصطناعي
بيئة الصراع	بيئة مادية (البر، البحر، الجو)	بيئة + غير مادية (الفضاء المعلوماتي الإدراك العام+ الواقع الرقمي)
زمن الفعل والتأثير	فوري ومباشر	تدريجي، تراكمي، طويل الأمد
الإسناد	واضح ومباشر– الفاعل معلوم (دولة وجيش وقدرات مرئية)	غامض وصعب – قابلية الإنكار، فاعلون متعددون

الجدول من اعداد الباحثة

ثانياً: التوصيات:

1. تبني عقيدة الردع المتكامل من قبل مؤسسات الأمن القومي، من خلال إدماج الردع السيبراني والمعرفي بوصفهما امتداداً لا يتجزأ من القوة العسكرية التقليدية، بما يعزز مرونة الاستجابة ويحقق تكاملاً فعالاً في منظومة الردع الشامل.
2. تعزيز الوعي الاستراتيجي الدولي لدى صانعي القرار من خلال تفعيل الدبلوماسية السيبرانية والاعلام الموجه كأدوات رئيسة لإدارة السرد الدولي في عصر ما بعد الحقيقة، بما يُسهم في كسب الشرعية الدولية للردود الوطنية وتقويض جهود الخصم في التضليل والتأثير على الرأي العام. كما يُعد بناء قدرات الردع الاعلامي أولوية في مواجهة الحروب المعرفية، استناداً إلى حالة الصراع الهندي–الباكستاني (2019–2025) التي بينت أن الحملات المضللة قادرة على إعادة تشكيل الإدراك العام وإضعاف خيارات الخصم، فيما أظهرت التجربة أن سرعة التصحيح وتوحيد الرسائل الإعلامية تعكس قدرة الدولة على حماية سرديتها الوطنية وترسيخ الردع المعرفي.
3. كشف هجوم Stuxnetعلى إيران والهجمات الروسية على البنية التحتية الأوكرانية هشاشة الأنظمة الصناعية الحيوية، ما يؤكد ضرورة تعزيز الأمن السيبراني لهذه الأنظمة عبر تحديثها المستمر، اعتماد التحليلات السلوكية للكشف المبكر عن الأنشطة غير الاعتيادية، وتفعيل آليات استجابة سريعة ومرنة.
4. ضرورة تطوير إطار قانوني متكامل على المستوين الدولي والوطني، يهدف الى تحديد قواعد الاشتباك في الفضاءين السيبراني والمعرفي، وتصنيف الهجمات ذات الطبيعة المعلوماتية أو السيبرانية ضمن أعمال العدوان وفق معايير محددة، بما يُسهم في تسهيل تحديد المسؤولية وتعزيز المساءلة القانونية للدول أو الجهات الفاعلة من غير الدول المنخرطة في هذا النوع من الصراعات.
5. تعزيز استخدام الذكاء الاصطناعي في الأنظمة الاستخباراتية لتعزيز دقة وسرعة تحديد مصدر الهجمات السيبرانية والمعرفية. كما يجب دمج هذه التقنية ضمن إطار قانوني واخلاقي لضمان موثوقية النتائج، مع تعزيز التعاون الدولي وتبادل المعلومات لدعم الاستدلال والتحقق الفعال.

---

(1) Shaymaa Mohammed Naser. "The Global Strategic Balance in the Middle East: A Study in the strategic Triangle (United states of America–Russia–China)." Master's thesis, Al-Nahrain University, College of Political Science, 2022,p17-18.

(2) Thomas Schelling. The Strategy of Conflict. Translated by Nuzhat Tayeb and Akram Hamdan. Beirut: Arab Scientific Publishers in collaboration with Al Jazeera Center for Studies, 2009, p 210-217.

(3) Steve Tesich, "A Government of Lies." The Nation 254, no. 1, January 1992, p12-14. https://www.prrac.org/projects/fair_housing_commission/los_angeles/AndPoorGetPoorer-TheNation.01.96.pdf?utm_source=chatgpt.com (accessed: 13 July 2025)

(4) Oxford English Dictionary. 2016."Word of the Year 2016: Post-truth." November ,2016. https://languages.oup.com/word-of-the-year/2016/ (accessed 13 July 2025)

(5) Lee Mcintyre. post-Truth, Cambridge: The MIT Press essential knowledge, 2018,p17-20.

(6) Kakutani Michiko. The Death of Truth Notes on Falsehood in the Age of Trump, New York: Tim Duggan Books, 2018, p12.

(7) Frank Hovman. Conflict in the 21st Century: The Rise of Hybrid Wars, Virginia: Potomac Institute for policy studies, 2007, p 28-29. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

(8) Saad Ubaid Al-Saidi, Ali Hindol Al-Shammari. "Modern Wars and Their Impact on Foreign Policy Objectives: Reflections on Supreme Goals as a Model", Al-Mahad Journal, no. 16 March 2024, p197; Andrew Radden. Hybrid Warfare in the Baltic Region: Threats and Possible Responses, California: RAND Corporation, 2017, p 5.

(9) U.S Department of Defense. National Defense Strategy 2022, 27 October 2022, p8-9. (accessed : 13 July 2025) https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf

(10) Mazarr Michael J. Integrated deterrence as a defense planning concept, Santa Monica: Rand Corporation, 2024, p1-8. https://www.rand.org/pubs/perspectives/PEA2263-1.html (accessed: 13 July 2025)

(11) Innovation Hub. Cognitive Warfare, Paris: NATO, 2020, p 8-12. https://innovationhub-act.org/wp-content/uploads/2023/12/20210122_CW-Final.pdf(accessed: 13 July 2025)

(12) Ibid.

(13) Ibid.

(14) Eric Ouellet, Madeleine D'Agata, and Keith Stewart. Deterrence in the 21st Century: Statecraft in the Information Age, Calgary: University of Calgary Press, 2024, p 23-26 . https://library.oapen.org/bitstream/id/a53f81e2-2ded-46d2-8042-c9e87ce34f43/9781773854045_OA.pdf (accessed: 14 July 2025)

(15) Joseph Nye S. Jr. "Deterrence and Dissuasion in Cyberspace.", International Security 41, no. 3 January 2017, p 54-62. https://doi.org/10.1162/ISEC_a_00266

(16) The White House. National Cybersecurity Strategy. March 1, 2023, p3-5. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf(accessed: 14 July 2025)

(17) Israa Shareef Al-Kaeud. "The Cyber Influence of the National Security of the Active Countries (United States of America as a Model", Political Science Journal, no. 64 , December 2022, p5-6 .

(18) A. Ertan et al. Cyber Threats and NATO 2030: Horizon Scanning and Analysis, Tallinn: NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) , 2020, p 10-45. https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis/ . (accessed: 29 July 2025)

(19) Thomas Rid. Active measures: the secret history of disinformation and political warfare. New York: Farrar, Straus and Giroux, 2020, p4-11. https://profilebooks.com/wp-content/uploads/wpallimport/files/PDFs/9781788160759_preview.pdf (accessed: 29 July 2025)

(20) U.S. Senate Select Committee on Intelligence. Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media. 116th Congress, 1st Session. Washington, D.C.: U.S. Government Publishing Office, 2020, p 20-21. https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf(accessed: 30 July 2025)

(21) Ong Jonathan Corpus, Cabbuag Samuel. “Pseudonymous Influencers and Horny 'Alts' in the Philippines: Media Manipulation Beyond Fake News”, The Journal of Socio-Technical Critique 2, no 2, January 2022, p 13-18. https://scholarworks.umass.edu/entities/publication/38871dc6-f552-481c-8c7e-7544e3e23361 (accessed: 30 July 2025)

(22) David Ingram, Trumb Consultants Harvested Data From 50 million Facebooke Users Reuters . 17 March 2018. https://www.reuters.com/article/technology/trump-consultants-harvested-data-from-50-million-facebook-users-reports-idUSKCN1GT02U/ (accessed:31 July 2025)

(23) Jaiv Doshi et al. “Sleeper Social Bots: A New Generation of AI Disinformation Bots Are Already a Political Threat” arXiv , 2024,p 4-18 . https://doi.org/10.48550/arXiv.2408.12603.(accessed: 31 July 2025)

(24) Francesco Salvi et al. “On the Conversational Persuasiveness of GPT-4” ,Nature Human Behavior 9 , May 2025, p1645-1653 . https://doi.org/10.1038/s41562-025-02194-6 . (accessed: 2 August 2025)

(25) Minahil Shawal Afridi. “India's Strategic Information Warfare: Challenges and Policy Options For Pakistan”, NDU Journal 38, no.1, March2024, P77-93. https://ndujournal.ndu.edu.pk/site/article/view/184 (Accessed: 2 August 2025)

(26) Dilawar Singh. “Cognitive Warfare in the India-Pakistan Conflict: The Invisible Battlefield of 2025”, International Business Times. 20 May 2025. https://www.ibtimes.co.in/cognitive-warfare-india-pakistan-conflict-invisible-battlefield-2025-883425 (Accessed: 2 August 2025)

(27) Hanbyeol Sohn, Kang Changwoo. North Korea’s Nuclear-Cognitive Warfare Strategy, 38 North, April 14, 2025. https://www.38north.org/2025/04/north-koreas-nuclear-cognitive-warfare-strategy/.(accessed: 2 August 2025)

(28) Vann H ,Van Diepen, North Korea Showcases Two Types of ICBMs In November 2022 Tests, 38 North, 2 December 2022. https://www.38north.org/2022/12/north-korea-showcases-two-types-of-icbms-in-november-2022-tests/ (accessed: 2 August 2025)

(29) Kyodo News, North Korea Vows 'Overwhelming' Military Steps to Counter Drills, 7 November, 2022, https://english.kyodonews.net/articles/-/37488 (Accessed: 4 August 2025)

(30) Hanbyeol Sohn, Kang Changwoo, op cit.

(31) Emad Salah Abulrazzaq ,Ali Abdulrazzaq Shanshool. “environmental war in the korean peninsula:waste balloons as a model” ,Political Issues 79, December 2024, p718. DOI:10.58298/792024750 .

(32) LTC Marco De Falco, Stuxnet Facts Reports, Tallinn: NATO cooperative cyber defense center of excellence (CCDCOE) ,2012. https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf?utm_source=chatgpt.com (accessed: 4 August 2025)

(33) NSFOCUS , The Hacktivist Cyber Attacks In the Iran- Israel Conflict, 26 June2025. https://nsfocusglobal.com/the-hacktivist-cyber-attacks-in-the-iran-israel-conflict/

(34) Dragos Inc. CRASHOVERRIDE: Analyzing the Threat to Electric Grid Operations. June 2017, p10-12. https://nsarchive.gwu.edu/sites/default/files/documents/3869008/Dragos-CRASHOVERRIDE-Analyzing-the-Threat-to.pdf. (accessed: 6 August 2025)

(35) Cybersecurity and Infrastructure Security Agency (CISA), Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure, 5 September2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a. (accessed: 6 August 2025)

(36) Raghda Al-Bah. "Cyber Deterrence: The Concept, dilemmas and Requirements", Journal of Political Science and Law, no. 1, February 2017, p 62-63.

(37) NATO Allied Command Transformation, Cognitive Warfare: Strengthening and Defending the Mind, April 5, 2024. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/ (accessed: 10 August 2025)

(38) Rand Waltzman. Emerging Cognitive Threats, Arlington: Irregular Warfare Center, 25 May 2025, p3-4. https://irregularwarfarecenter.org/wp-content/uploads/P27_Emerging_Cognitive_Threats.pdf (accessed: 10 August 2025)