

نظم السيطرة الإلكترونية العالمية ووسائلها الحديثة للقوات البرية عام 98. إن جذور بداية الحرب الإلكترونية في العالم يعود لما قبل اندلاع الحرب العالمية الأولى، حيث بدأت الاتصالات بين أرجاء العالم المختلفة باستخدام الاتصالات السلكية ثم تبادل المراسلات باستخدام السفن في نقل الرسائل ثم خطوط التلغراف التي كانت هدفاً مهماً للقوات المتحاربة، وبعد ذلك كان التنصت من قبل عمال الإشارة على خطوط المواصلات السلكية على المحادثات ولهذا السبب كان كل جانب يقطع المواصلات الخطية عند عدم الحاجة إليها حتى لا يتداخل عليها الطرف الآخر. 99. كانت أساليب الحرب الإلكترونية تستعمل منذ بداية القرن العشرين وبالأخص عندما استخدمت أجهزة الاتصالات اللاسلكية في الحروب ولكن منذ الحرب العالمية الثانية أصبح موضوع الحرب الإلكترونية محل الاهتمام من حيث المعدات والأساليب. الحرب الإلكترونية في الولايات المتحدة الأمريكية 100. تعتمد القوات البرية للولايات المتحدة الأمريكية (US Army) في الحروب الحديثة على شبكة متكاملة من نظم السيطرة الإلكترونية والقيادة والتحكم، والتي تُعرف اختصاراً بمصطلح C5ISR (القيادة، التحكم، الاتصالات، الكمبيوتر، Cyber، الاستخبارات، المراقبة، والاستطلاع). تهدف هذه المنظومات العالمية إلى تحقيق التفوق المعلوماتي وربط الجندي في الميدان بأعلى مراكز القرار لحظياً. 101. فيما يلي تصنيف شامل لأبرز نظم السيطرة الإلكترونية العالمية ووسائلها الحديثة لدى الجيش الأمريكي: أ. بيئة القيادة التشغيلية الموحدة (COE). تدمج القيادة الأمريكية كافة برمجيات وأنظمة القيادة في بيئة حوسبة موحدة تضمن تدفق البيانات دون انقطاع كالآتي: (1) نظام القيادة والتحكم البري التكتيكي (CPCE) يدمج خرائط أرض المعركة وبيانات الاستخبارات في شاشة عرض موحدة أمام القادة لسرعة اتخاذ القرار. (2) منظومة المبيعات والبيانات التكتيكية المشتركة (JADC2) المشروع الأضخم لربط القوات البرية، البحرية، الجوية، الفضائية، وقوات السابير في شبكة سحابية واحدة عملاقة مدعومة بالذكاء الاصطناعي. ب. وسائل الاتصال والشبكات الميدانية الحديثة. تعتبر الشبكة القتالية العمود الفقري لنقل البيانات المشفرة تحت أي ظرف: (1) شبكة الاتصالات التكتيكية المتكاملة (ITN) تتيح للقادة والمشاة تبادل البيانات والصور ومقاطع الفيديو عبر أجهزة راديو متطورة ومقاومة للتشويش. (2) الأقمار الصناعية ذات المدار المنخفض (LEO) استخدام شبكات الأقمار الصناعية التجارية والعسكرية لتأمين إنترنت فضائي عالي السرعة وبزمن استجابة فائق السرعة للقوات المنتشرة عالمياً. (3) أجهزة الراديو المعرفة برمجياً (SDR) أجهزة لاسلكية قادرة على تغيير الترددات تلقائياً لتفادي الحرب الإلكترونية المعادية. ج. أنظمة إدارة المعارك والمراقبة للمشاة (Tactical Edge). الوسائل التي تمنح الجندي في خط المواجهة وعياً كاملاً بالبيئة المحيطة: (1) نظام Nett Warrior: جهاز لوحي ذكي يرتديه الجندي على صدره، يوضح له مواقع زملائه ومواقع العدو على الخريطة لحظة بلحظة لمنع النيران الصديقة. (2) نظارات الرؤية الاستهدافية المتكاملة (IVAS) نظارات واقع معزز (AR) متطورة تُعرض عليها خرائط ثلاثية أبعاد، ونقاط الأهداف، ورؤية ليلية وحرارية مباشرة أمام عين الجندي. د. وسائل الاستخبارات والحرب الإلكترونية (EW). السيطرة على الطيف الكهرومغناطيسي وحرمان العدو منه: (1) نظام TLS (الأرضي التكتيكي): منظومة متكاملة محمولة على مركبات تكتيكية للتشويش على اتصالات العدو، وراداراته، وطائراته المسيرة، وفي نفس الوقت حماية القوات الصديقة. (2) منظومات الدفاع ضد الطائرات المسيرة (C-UAS): رادارات إلكترونية مدمجة بأسلحة طاقة موجهة (ليزر أو موجات ميكروويف) لإسقاط مسيرات العدو عبر قطع إشارات السيطرة الخاصة بها. هـ. الذكاء الاصطناعي وتحليل البيانات الضخمة. مشروع لينكس (Project Linx) ومشروع غايا (Project Gaia): استخدام الخوارزميات لتحليل آلاف الساعات من تصوير الطائرات المسيرة وبيانات الرادارات، وتحديد الأهداف العسكرية تلقائياً وتنبيه القادة إليها خلال ثوانٍ معدودة. الحرب الإلكترونية في روسيا الاتحادية 102. تعتمد القوات البرية الروسية على شبكة متكاملة ومتطورة للحرب والسيطرة الإلكترونية (EW)، تستهدف شل قدرات العدو الاستخباراتية وتعطيل اتصالاته وراداراته وطائراته المسيرة في الوقت الفعلي، مستخدمة منظومات متنقلة فائقة القدرة مثل "كراسوخا-4" وريبلنت-1. 103. أبرز المنظومات والوسائل الحديثة. أ. كراسوخا-4 (Krasukha-4). نظام متنقل مخصص لقمع أقمار التجسس، الرادارات الأرضية، وأنظمة الإنذار والتحكم المبكر المحمولة جواً (أواكس)، عبر إنشاء تشويش راداري مكثف يعطل الصواريخ الموجهة بدقة. ب. ريبيلنت-1 (Repellent-1). منظومة متخصصة في رصد وكشف الطائرات المسيرة (الدرونز) ومطاردة ترددات تشغيلها وقطع ارتباطها بمشغليها عبر تشويش واسع النطاق يمتد لمسافات مؤثرة. ج. موسكو-1 (Moscow-1). محطة استطلاع إلكتروني وإدارة متكاملة؛ تقوم بمسح المجال الجوي وتصنيف الأهداف المعادية حسب خطورتها، ثم توزع البيانات تلقائياً على وسائل الدفاع الجوي وأنظمة التشويش الميدانية. د. منظومات التحكم الآلي الذكية. أدخلت روسيا مؤخراً أنظمة تحكم آلي ميدانية مرتبطة بالذكاء الاصطناعي لتحليل

كثافة هجمات المسيرات (مثل طائرات FPV) والتعامل معها وقمعها أوتوماتيكياً في زمن الحقيقي (Real-time). هـ. بريزيدنت-أس (President-S). نظام إخماد بصري وإلكتروني يُثبت على الآليات والمركبات العسكرية لحمايتها من الصواريخ المضادة الموجهة حرارياً أو برادارياً عبر إضلائها وصرفها عن أهدافها. الحرب الإلكترونية في جمهورية الصين الشعبية 104. تبني القوات البرية لجيش التحرير الشعبي الصيني (PLAGF) استراتيجية متطورة تُعرف عقائدياً باسم "الحرب الذكية والمعلوماتية (Intelligentized & Informatised Warfare)، والتي تهدف إلى دمج شبكات القيادة والسيطرة وأنظمة التداخل الكهرومغناطيسي لفرض السيادة الرقمية" بالكامل في ساحة المعركة. 105. تعتمد الصين في هذا المجال على مفهوم عملياتي موحد يسمى "حرب الشبكات الإلكترونية المتكاملة" (Integrated Network Electronic Warfare – INEW)، وهو الدمج الكامل بين الهجمات السيبرانية، وتدمير النظم الإلكترونية، والتشويش والتعمية الكهرومغناطيسية. 106. أبرز وسائل ونظم السيطرة الإلكترونية الحديثة للقوات البرية الصينية تتلخص في المحاور التالية : أ. عقيدة حرب الشبكات الإلكترونية المتكاملة (INEW). تركز هذه العقيدة على شل قدرة العدو على القيادة والسيطرة عبر الهجوم المتزامن على برمجياته (سيبرانياً) وأجهزته وراداراته (كهرومغناطيسياً). يتم تنسيق هذه العمليات عبر لواء الأسلحة المشتركة (Combined Arms Brigades) بدعم مركزي مباشر . ب. منظومات الحرب الإلكترونية الأرضية والمتحركة . تمتلك القوات البرية ترسانة من محطات الرصد والتشويش المتحركة على شاحنات عسكرية مخصصة للتحرك السريع مع القوات المدرعة: (1) منظومة CHL-906 . محطة متطورة جداً تعمل كمنظومة "رصد سلبي وهجومي" في آن واحد، قادرة على كشف رادارات العدو وتصنيف انبعاثاتها من مسافات تصل إلى 600 كيلومتر وحماية الرادارات الصديقة من الاستهداف. (2) منظومات تتبع سلاسل البيانات . (Data-Link Jamming) مثل المنظومات المشابهة لـ RCT195B، والمخصصة لقطع الاتصال بين الطائرات والمسيّرات المعادية ومراكز القيادة الأرضية عبر التشويش على الإشارات الرقمية المعقدة. ج. السيطرة عبر إنترنت الأشياء العسكري (IoMT) والذكاء الاصطناعي . تحولت شبكات السيطرة الصينية إلى جيل مؤتمت بالكامل يعتمد على إنترنت الأشياء العسكري (IoMT) ودمج خوارزميات الذكاء الاصطناعي. يتيح هذا النظام لآلاف الوحدات غير المأهولة (مثل "الذئاب الروبوتية" والمسيّرات) تبادل البيانات الفورية وتحديد الأهداف دون تدخل بشري مباشر، مما يحقق ما يسميه الخبراء "الشفافية أحادية الجانب" (رؤية العدو بوضوح مع البقاء في حالة تخفٍّ كامل . د. رادارات الحوسبة المتقدمة والذكاء الاصطناعي . طورت الصين رادارات مدعومة بالذكاء الاصطناعي قادرة على مواجهة وسائل التشويش المعادية حيث تقوم بتحليل الطيف الكهرومغناطيسي فوراً وبسرعات فائقة للتفريق بين الإشارات الحقيقية وإشارات الخداع الإلكتروني، مما يضمن تدفقاً سلساً لبيانات القيادة والسيطرة. [1] هـ. الدمج بين الدفاع الجوي والسيطرة الإلكترونية . تتميز النظم الحديثة مثل FB-10A (منظومات الدفاع الجوي قصيرة المدى المتنقلة) بتصميم يعتمد على هندسة معيارية تربط الرادارات، ووحدات حساب الإحداثيات، ومراكز التحكم بالنيران إلكترونياً، مما يسمح لها بالعمل بشكل مستقل أو كجزء من شبكة دفاع جوي وطني متكاملة لمواجهة أسراب المسيّرات وصواريخ كروز.