8 حرب المعلومات وساحة المعركة المتصلة

د. بريت فان نيكيرك
أستاذ مشارك، جامعة كوازولو ناتال

مقدمة

تمتد الثورة الصناعية الرابعة (4IR) من ثورة المعلومات (الثورة الصناعية الثالثة) مع درجات متزايدة من التكامل بين الأنظمة السيبرانية والفيزيائية والبيولوجية. ومن المتوقع أن تؤثر الثورة الصناعية الرابعة على جميع القطاعات، بما في ذلك طبيعة الصراع (شواب، 2016). تتضمن المفاهيم الأساسية التي تشكل جزءًا من الثورة الصناعية الرابعة على سبيل المثال لا الحصر:

- علم البيانات وتحليلات البيانات الضخمة ، التي غالبًا ما تكون مدفوعة و/ أو مؤتمتة بواسطة الذكاء الاصطناعي والتعلم الآلي؛
- الحوسبة السحابية وتوفير موارد حوسبة يمكن الوصول إليها عن بعد؛
- إنترنت الأشياء (IoT) ، حيث يمكن للأجهزة شديدة الاتصال أن تعمل كمستشعرات وكمحركات لإنتاج كميات كبيرة من المعلومات والترابط السيبراني الفيزيائي؛
- الواقع المعزز، تراكب المعلومات على النظارات أو الخريطة أو الصورة؛
- الأمن السيبراني، بسبب نقاط الضعف التي أُدخِلت عن طريق ربط الأجهزة "غير التقليدية" غير الآمنة بالشبكات.

كانت بعض مفاهيم الحرب الصناعية الرابعة موجودة في الإعداد العسكري بشكل ما، مثل الواقع المعزز المشابه لشاشات العرض التي يتم وضعها على الرأس، ويطوّر مفهوم إنترنت الأشياء الحرب المركزية على الشبكة (أو كما يسميها "واصل 2018، " حرب البيانات" وهو ما أصبح يُعرف باسم "إنترنت الأشياء في ساحة المعركة" "

(IoBT)أو "إنترنت الأشياء العسكرية" (IoMT) (كاستيغليون، شو، نابي، وريكيادي 2017). إنّ تطبيقات إنترنت الأشياء في الجيش تتمتع بالقدرة على دعم القيادة والتحكم (C2) للعمليات متعددة المجالات (MDO) في مجموعة من المجالات (سيفيرز، 2017). وعليه، يمكن اعتبار أن العمليات متعددة المجالات في المستقبل تشتمل على ساحة معركة شديدة الارتباط تؤدي إلى زيادة سطح الهجوم لحرب المعلومات (سينشيوتي، 2017: فان نيكيرك، بريتوريوس، راملوكان وباتريك، 2018). تتم في هذه المقالة دراسة الحرب الإلكترونية في سياق كل من العمليات متعددة المجالات وإنترنت الأشياء في ساحة المعركة (IoBT).

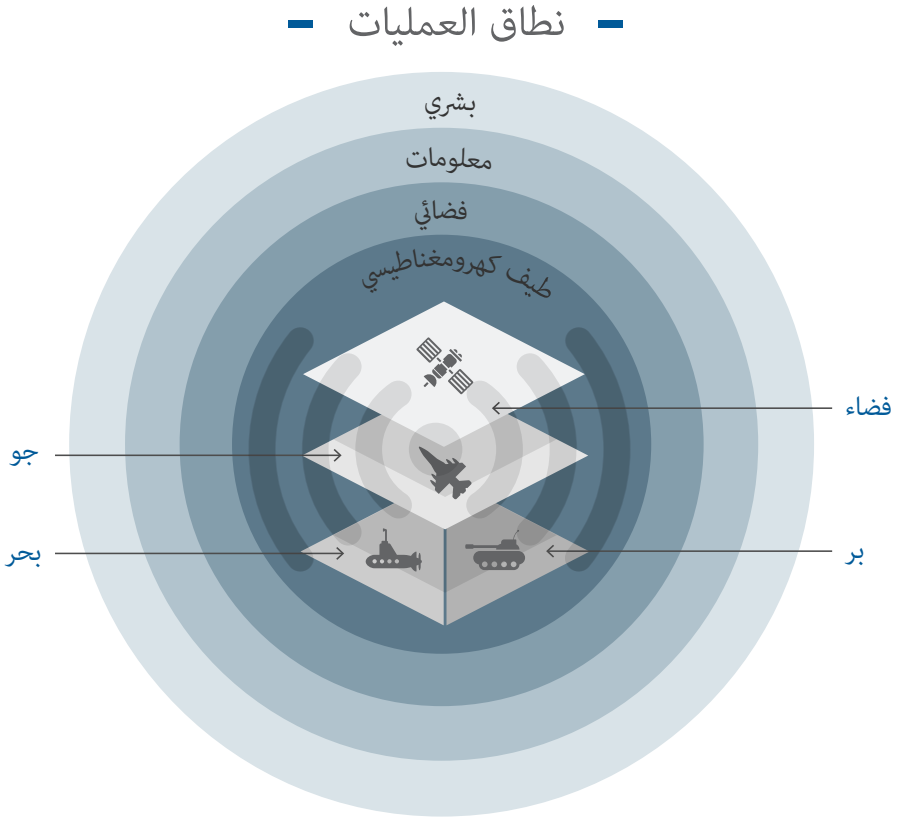
العمليات متعددة المجالات وحرب المعلومات

تشمل المجالات "المادية" التقليدية للعمليات العسكرية الأرض والبحر والجو والفضاء؛ ومع ذلك ، ثمة حاجة متزايدة للسيطرة على الطيف الكهرومغناطيسي (EMS) ، والبيئة السيبرانية، وبيئة المعلومات الأوسع (وين، دورتمانز، تاكور، وروي، 2019). تم وصف نهج العمليات متعددة المجالات بأنه "مفهوم القتال المشترك الذي سيحمل كل القوة النارية والحركية وغير الحركية على حد سواء" لتوفير التفوق عبر ساحة المعركة بطريقة غير مسبوقة (ساوث، 2019).

يوضح الشكل 1 مجالات تشغيلية متعددة: المجالات "المادية" الأربعة موضحة في وسط الشكل؛ عادة ما تكون هذه المجالات متنقلة وتتواصل من خلال وسائط البث على ترددات مختلفة (EMS). يصبح الفضاء الإلكتروني امتدادًا لذلك، حيث يوفر آليات نقل البيانات والمعلومات، مثل بروتوكولات الشبكات. ففي حين يُعتبر مجال المعلومات المعاصر مطابقًا تقريبًا للفضاء السيبراني، فإن بيئة المعلومات أوسع وتتضمن معلومات مطبوعة ومعرفية أيضًا. تدعم كل هذه العناصر العنصر البشري، الذي يشمل عمليات صنع القرار الإستراتيجي والتكتيكي (على سبيل المثال، القيادة والتحكم) لقادة الحرب والقادة ولكنه يمتد على نطاق أوسع ليشمل المجتمع والاقتصاد والسياسة.

> إن احتمال "خداع" الخوارزميات يمثل مصدر قلق خاص لأولئك الذين يحتاجون إلى اتخاذ قرارات القيادة بناءً على البيانات التي تم تحليلها وتقديمها لهم: هل يمكن الوثوق بالمعلومات حول ساحة المعركة؟ على مستوى أكثر تكتيكيًا، هل يمكن لمحطة طيار أو محطة تحكم على سفينة حربية أن تثق في المعلومات التي يتم عرضها؟ إنّ أي تردد أو قرار غير صحيح هو في النهاية هدف حرب المعلومات.

تتألف حرب المعلومات ، في شكلها السابق ، من عمليات يمكن أن تؤثر على المعلومات و/ أو تحميها عبر المجالات المادية والافتراضية والمعرفية (برازولي، 2007، والتز، 1998). تضمنت "ركائز" حرب المعلومات الحرب الإلكترونية (EW)، والعمليات الإلكترونية، والعمليات النفسية (PSYOP) والاستخبارات والحرب المتمركزة حول الشبكة أو حرب البنية التحتية للمعلومات، وحرب القيادة والتحكم (برازولي، 2007)



الشكل 1: مجالات العمليات

يميل الاستخدام الحديث لمصطلح "حرب المعلومات" إلى الإشارة أكثر إلى الجوانب المعرفية، مثل المعلومات المضللة وحملات التأثير، والتي غالبًا ما تكون مدفوعة بوسائل التواصل الاجتماعي والرسائل الفورية (ستينغل، 2019). تركز المناقشات الناشئة على "التقارب" بين الحرب الإلكترونية والإنترنت في ما يعرف بالأنشطة الإلكترونية الكهرومغناطيسية (CEMA) (وزارة الدفاع البريطانية، 2018؛ وزارة الجيش الأمريكية، 2014). ومع ذلك ، يمكن مناقشة تقارب أكبر بين ركائز الحرب العالمية الثانية بشكل خاص بالنظر إلى النجاح

الواضح للمعلومات المنسّقة والعمليات البدنية في أوكرانيا، على الرغم من عدم تحقيق نصر "حاسم (فاليريانو، جنسن، ومانيس، 2008، فان نيكيرك، 2015).

عادةً ما يكون لحرب المعلومات الهجومية أحد عناصر الخمسة التالية: الحرمان أو التحطيم أو التعطيل أو الخداع أو التدمير (ستيرلينغ، 2019) كهدف استراتيجي أو تشغيلي؛ ومع ذلك، اقترح آخرون أيضًا أهدافًا مثل:

- التعطيل ، والإنكار ، والتدمير ، والتلاعب ، والسرقة (هاتشينسون ووارن، 2001)،
- التحطيم والإنكار والفساد والاستغلال (بوردن، 1999، كوب، 2000)،
- المقاطعة والتعديل والتلفيق والاعتراض (بفيلغير وبفيلغير، 2003)

في نهاية المطاف، يتم استهداف صنع القرار البشري على المستويات التكتيكية والتشغيلية والاستراتيجية؛ ومع ذلك ، فإن الصراع من خلال الفضاء الإلكتروني وبيئة المعلومات يستهدف بشكل متزايد اتخاذ القرارات المجتمعية والسياسية والاقتصادية وكذلك العمليات العسكرية أو المشغلين العسكريين. مع التركيز المتزايد على حملات التضليل والتأثير من قبل الجهات الفاعلة الحكومية وغير الحكومية، لا سيما من خلال مواقع "الأخبار" عبر الإنترنت ووسائل التواصل الاجتماعي، تمت إعادة صياغة المزيد من أهداف حرب المعلومات على المستوى الاستراتيجي الأعلى إلى 4 عناصر: الاستبعاد ، التشويه ، صرف الانتباه والترهيب (وايت، 2016). تستهدف مثل هذه الأنواع من العمليات "إرادة" السكان أو السياسيين، وتهدف ، جنبًا إلى جنب مع العناصر الأكثر تركيزًا على العمليات من الحرب العالمية الثانية في ساحة معركة معيّنة، إلى تقليل أو إزالة الدعم الشعبي أو

> يمكن التفكير في أن شبكة الضباب تخدم المستويات التكتيكية والتشغيلية للقيادة والتحكم بينما تخدم الشبكة السحابية المستويات التشغيلية والاستراتيجية للقيادة والتحكم.

السياسي تجاه نزاع أو أهدافه العسكرية.

إنترنت الأشياء وحرب المعلومات

يشير وكاستيغلون، شو، نابيوريكيادي (2017: 6) إلى أن ساحة المعركة قد شهدت "عددًا متزايدًا من أجهزة الاستشعار والحاسوب في كل مكان التي يرتديها الأفراد العسكريون والمدمجة في المعدات العسكرية". أفادت التقارير أن الناتو كان يجري تحقيقات حول الفوائد المحتملة لإنترنت الأشياء للجيش في مجالات مثل الوعي الظرفي والمراقبة والخدمات اللوجستية والتطبيقات الطبية والعمليات الأساسية وإدارة الطاقة (سيفيرز، 2017، ستون، 2018، واصل، 2018). تمتلك إنترنت الأشياء العسكرية/ إنترنت الأشياء في ساحة المعركة أيضًا إمكانات هائلة لدعم القيادة والتحكم في العمليات متعددة المهام من خلال "الدعم اللوجستي للعمليات المشتركة؛

الوعي الظرفي على المستوى التكتيكي، الاستهداف ؛ مراقبة حالة المركبة والجندي ؛ الرعاية الطبية في ساحة المعركة وحتى المراقبة البيئية (سيفيرز، 2017).

يقترح رين وهو (2018) بنية "قتال سحابة- ضباب" بثلاثة طبقات. تشمل فئة "الموارد القتالية" المعدات العسكرية مثل المنصات وأجهزة الاستشعار في المجالات المادية الأربعة التقليدية. يستخدم شينشيوتي (2017) مثالًا لطائرة F-35 تحمل على متنها مستشعرات لجمع المعلومات حول بيئاتها والتهديدات المحتملة؛ بالإضافة إلى مستشعرات داخلية لمراقبة أدائها، وبالتالي يمكن اعتبارها "شيئًا" على الإنترنت، ولكن أيضًا كمجموعة من أجهزة الاستشعار. يعتبر فاليريانو، جنسن، ومانس (2008) أنطائرة F-35 مكافئة لخادم الكمبيوتر. يشير هذا إلى التعقيد المتزايد للأنظمة العسكرية الحديثة، والاعتماد على المعلومات الرقمية، وكمية البيانات التي يمكن إنشاؤها (المتعلقة بالمفاهيم المرتبطة بـ "البيانات الضخمة").

الشكل 2: "أركان" حرب المعلومات

تشتمل الطبقة الثانية من هندسة رين وهوز (2018) على "طبقة ضبابية" للحوسبة والتخزين الموزع المحلي. تتكون الطبقة الثالثة بعد ذلك من الحوسبة السحابية، مع مساحة تخزين أكبر وتتألف من روابط "شبكة ضبابية" متعددة. يمكن التفكير في أن شبكة الضباب تخدم المستويات التكتيكية والتشغيلية للقيادة والتحكم بينما تخدم الشبكة السحابية المستويات التشغيلية والاستراتيجية للقيادة والتحكم.

نظرًا لنطاق العمليات متعددة المجالات، فمن الحكمة توسيع مستشعرات بنية "قتال سحابة- ضباب "لتشمل أجهزة استشعار في المجال الكهرومغناطيسي كجزء من مجموعة الموارد القتالية.

يجب أيضًا توفير المراقبة في المجال السيبراني عبر بنية سحابة قتال للمساعدة في الأمن السيبراني. تم تسجيل حوادث تتعلق بتأثر الوحدات العسكرية و/ أو المعدات العسكرية "المتصلة" بالحوادث الإلكترونية: في عام 2009 تم الإبلاغ عن أن البرمجيات الخبيثة المتنقلة قد أثرت على السفن الحربية والمطار العسكري (بايدج، 2009؛ ويلشر، 2009)، تم استخدام البرمجيات الخبيثة المتنقلة في وحدات مدفعية المسار (فولز، 2016). وثمة الآن مخاوف متزايدة بشأن التهديدات الإلكترونية والكهرومغناطيسية للأقمار الصناعية والأنظمة الفضائية (غارنر، 2020، راجاغوبالان، 2019). تم استخدام أجهزة إنترنت الأشياء التي تم اختراقها لإطلاق هجمات حجب الخدمة الموزعة (DDoS) وكانت من بين أكبر الهجمات التي تم تسجيلها وقت حدوثها (فروهلنغر، 2018).

تشير مثل هذه الحوادث والمخاوف الأوسع المتعلقة بأنظمة المعلومات والأمن إلى المخاطر الكامنة في الأنظمة شديدة الترابط. يوضح فان نيكيرك، بريتوريوس، راملومان، وباتريك (2018) كيف يمكن استخدام حرب المعلومات لاستهداف إنترنت الأشياء والبشر من خلال إنترنت الأشياء الضعيفة. يمكن تطبيق العديد من هذه الهجمات النظرية على السيناريوهات العسكرية، مثل:

- يمكن أن تؤدي البرامج الضارة الماسحة أو برامج الفدية التي تدمر البيانات وبرامج النظام إلى تأثيرات كارثية على الطائرات أو الغواصات المغمورة، على سبيل المثال ؛
- يمكن أن يؤدي حقن رسائل عمليات نفسية في شاشات العرض العلوية للطيارين إلى تشتيت انتباه الطيار وإرباكه من خلال الإشارة إلى أن أنظمة الطائرات معرضة للخطر وتؤثر سلبًا على عملية اتخاذ القرار ذات الأهمية الزمنية.
- تتلاعب الهجمات الإلكترونية بمصفوفات أجهزة الاستشعار (على سبيل المثال، مجموعة السونار أو رادار الدفاع الجوي) بشكل عشوائي لتوفير أهداف خاطئة وإخفاء أهداف فعلية، وبالتالي تشويه منظر ساحة المعركة ؛
- استخدام البرمجيات الخبيثة ووسائل التواصل الاجتماعي على هواتف الأفراد العسكريين لتحديد عمليات الانتشار وبالتالي توليد المعلومات الاستخبارية المتعلقة بالعمليات.

يوضح الجدول 1 تهديدات "حرب المعلومات العامة" المحتملة ذات الصلة ببنية إنترنت الأشياء في ساحة المعركة السحابية.

الجدول 1: تهديدات حرب المعلومات على إنترنت الأشياء العسكرية

تهديدات مجال هندسة السحابة الضبابية
المستوى 3: التدمير المادي للسحابة للبنية التحتية للشبكة السحابية
هجمات حجب الخدمة الموزعة (DDoS) السيبرانية لزيادة التحميل على الشبكة السحابية
اختراق الشبكة لسرقة المعلومات
اختراق الشبكة للتلاعب بالمعلومات
اختراق الشبكة لتدمير المعلومات

المستوى 2: شبكة الضباب التدمير المادي للبنية التحتية لشبكة الضباب
التشويش الكهرومغناطيسي على أجهزة الاستقبال اللاسلكية بشبكة الضباب
هجمات حجب الخدمة الموزعة (DDoS) السيبرانية لزيادة التحميل على شبكة الضباب
اختراق الشبكة لسرقة المعلومات
اختراق الشبكة للتلاعب بالمعلومات
اختراق الشبكة لتدمير المعلومات

المستوى 1: التدمير المادي للمورد القتالي لأجهزة الاستشعار/ المعدات
التشويش الكهرومغناطيسي على الوصلات اللاسلكية بين الأجهزة
الطاقة الموجهة لتدمير الأجهزة الإلكترونية
البرامج الضارة السيبرانية على الأجهزة لتتبع الوحدات
البرامج الضارة لتقليل أداء المعدات
اختراق النظام لمعالجة معلومات المستشعر
إرسال رسائل العمليات النفسية المعرفية إلى الأجهزة

بشكل عام ، قد يؤدي إنترنت الأشياء في ساحة المعركة إلى ازدحام طيف الكهرومغناطيسي وشبكة بسبب زيادة عدد الإشارات الكهرومغناطيسية وكمية البيانات التي يتم نقلها. وهذا بدوره قد يزيد من قابلية التعرض لهجمات الحرب الإلكترونية وهجمات هجمات حجب الخدمة الموزعة(DDoS) حيث يمكن أن تقدم كل إشارة نفسها على أنها "ضوضاء" لبعضها البعض، وسيؤدي التشويش إلى زيادة مستوى "الضوضاء" هذا لتقليل فعالية روابط الاتصال أو تعطيلها. بطريقة مماثلة، كلما اقتربت كمية البيانات من "عتبة" الشبكة، كلما كانت أكثر عرضة للفيضان والارتباك من قبل حركة المرور الضارة.

> نظرًا لنطاق العمليات متعددة المجالات، فمن الحكمة توسيع مستشعرات بنية "قتال سحابة- ضباب "لتشمل أجهزة استشعار في المجال الكهرومغناطيسي كجزء من مجموعة الموارد القتالية.

من المحتمل أن يساهم إنترنت الأشياء في ساحة المعركة (IoBT) إلى "التقارب" بين الإنترنت والحرب الإلكترونية وجهاز العمليات النفسية على المستوى التكتيكي؛ يناقش فان نيكيرك وبريتوريوس وراملاكان وباتريك (2018) بعض جوانب هذا التقارب في سياق عام. ذكر أعلاه إمكانية استخدام الإنترنت لحقن رسالة عمليات نفسية لاستهداف الطيارين؛ كذلك، يمكن استخدام الحرب الإلكترونية "للتغلب" على الاتصالات اللاسلكية لنقل رسائل عمليات نفسية إلى الأفراد. يمكن اعتبار هذا التقارب كنموذج متعدد الطبقات لحرب المعلومات حيث تستهدف الحرب الإلكترونية الطبقة المادية للشبكة، وتستهدف السيبرانية الطبقات والبروتوكولات الأعلى ، وخيار الحمولة للمكوِّن السيبراني هو توزيع رسائل عمليات نفسية.

ثمة جانب آخر يجب مراعاته وهو الخوارزميات التي يتم تنفيذها لتحليل البيانات وتشغيل المعدات العسكرية. نظرًا لكمية البيانات التي تنتجها المعدات الحديثة، فإنّه من المستحيل على البشر تحليلها بالكامل، وثمة حاجة إلى درجة من الأتمتة، يتم تنفيذها عادةً باستخدام الذكاء الاصطناعي. ومع ذلك، كانت هناك حالات توضح أن المدخلات المعدلة أدت إلى توفير الذكاء الاصطناعي لتصنيف غير صحيح (فيلد، 2017، ليموس، 2021). غالبًا ما يتم تنفيذ التقنيات الجديدة دون مراعاة الأمان، ولا يختلف الأمر مع الذكاء الاصطناعي. في المجال الأكاديمي، ثمة زيادة حادة في كمية الأبحاث التي تحقق في الهجمات على أنظمة الذكاء الاصطناعي بما في ذلك الهجمات العدائية للحث على مخرجات غير صحيحة، بالإضافة إلى تسمم البيانات (المعروف أيضًا باسم تسمم النموذج) الذي يفسد بيانات التدريب لإنتاج نموذج معيب (قسطنطين ، 2021 ؛ ليموس ، 2021). إن احتمال "خداع" الخوارزميات يمثل مصدر قلق خاص لأولئك الذين يحتاجون إلى اتخاذ قرارات القيادة بناءً على البيانات التي تم تحليلها وتقديمها لهم: هل يمكن الوثوق بالمعلومات حول ساحة المعركة؟ على مستوى أكثر تكتيكيًا، هل يمكن لمحطة طيار أو محطة تحكم على سفينة حربية أن تثق في المعلومات التي يتم عرضها؟ إنّ أي تردد أو قرار غير صحيح هو في النهاية هدف حرب المعلومات.

الخاتمة

تشمل العمليات متعددة المجالات جميع البيئات المادية ويمكن أن تمتد إلى المجالات الكهرومغناطيسية والسيبرانية أيضًا. يوفر إنترنت ساحة المعركة آلية لتحقيق عمليات متعددة المجالات من خلال أجهزة استشعار مدمجة توفر صورة مشتركة لبيئة (بيئات) التشغيل. ومع ذلك، فقد نُظر إلى إنترنت الأشياء بشكل عام على أنها عرضة للتسوية، ويمكن أن تؤدي ساحة المعركة شديدة الارتباط إلى زيادة سطح الهجوم لحرب المعلومات عبر المجالات المادية والكهرومغناطيسية والإلكترونية والمعرفية. يمكن أن تستهدف الهجمات البنية التحتية المادية والإشارات وبروتوكولات الشبكة والخوارزميات والبيانات وعلم النفس البشري.

المراجع

بوردن، أ. (1999). ما هي حرب المعلومات؟ مجلة القوة الجوية والفضائية، 2 نوفمبر. تم الوصول إليه في 2 يوليو 2009 من : http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html.

برازول ، إم إس (2007). الآفاق المستقبلية لحرب المعلومات والعمليات النفسية على وجه الخصوص. في L. le Roux، رؤية جيش جنوب إفريقيا 2020 (ص 217 - 232). بريتوريا: معهد الدراسات الأمنية.

Cenciotti، D. (2017) Cybersecurity In the Sky: Internet of Things قدرات تجعل الطائرات أكثر عرضة للتهديدات السيبرانية أكثر من أي وقت مضى ، الطيران ، 20 يونيو. تم الوصول إليه في 26 سبتمبر 2021 من https://theaviationist.com/2017/06/20/cybersecurity-in-the-sky-internet-of-things-capabilities-to-make-aircraft-more-exposed-to-cyber-threats - أكثر مما سبق./

كونستانتين ، إل (2021) كيف يهاجم تسمم البيانات نماذج التعلم الآلي الفاسدة ، CSO Online، 12 أبريل. تم الوصول إليه في 5 أكتوبر 2021 من https://www.csoonline.com/article/3613932/how-data-poisoning-attacks-corrupt-machine-learning-models.html.

فيلد ، إم. (2017) الكتابة على الجدران على لافتات التوقف يمكن أن تخدع السيارات بدون سائق لدفعها بشكل خطير ، التلغراف ، 7 أغسطس. تم الوصول إليه في 5 أكتوبر 2021 من https://www.telegraph.co.uk/technology/2017/08/07/graffiti-road-signs-could-trick-driverless-cars-driving-dangerously/.

Fruhlinger، J. (2018) شرح الروبوتات في Mirai: كيف أن المحتالين المراهقين وكاميرات الدوائر التلفزيونية المغلقة كادوا يتسببون في تدمير الإنترنت، CSO Online، 9 مارس. تم الوصول إليه في 29 سبتمبر 2021 من https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-bopped-down-the-internet.html .

Garner، T. (2020) لماذا يجب إعطاء الأولوية للأمن السيبراني عبر الأقمار الصناعية في New Frontier، NextGov، 1 مايو. تم الوصول إليه في 10 سبتمبر 2021 من https://www.nextgov.com/ideas/2020/05/w/

الأمن السيبراني للأقمار الصناعية يجب أن يكون ذا أولوية الحدود الجديدة / 164977./

هاتشينسون ، و. ، ووارن ، م. (2001). حرب المعلومات: هجوم الشركات والدفاع في عالم رقمي. أكسفورد وأوكلاند: بتروورث هاينمان.

كوب ، سي (2000). نموذج أساسي من Infowar ، الأنظمة: الحوسبة الشهرية للمؤسسات ، سيدني : Auscom Publishing، 46-55.

ليموس ، ر. (2021). توقع زيادة الهجمات على أنظمة الذكاء الاصطناعي ، القراءة المظلمة ، 27 أبريل. تم الوصول إليه في 5 أكتوبر 2021 من https://www.darkreading.com/vulnerabilities---threats/advanced-threats/expect-an-increase-in-attacks-on-ai-systems/d/d-id/1340833

Page، L. (2009). لا تزال شبكات وزارة الدفاع تعاني من البرامج الضارة بعد أسبوعين ، السجل ، 20 يناير. تم الوصول إليه في 10 سبتمبر 2021 من https://www.theregister.com/2009/01/20/mod_malware_still_going_strong/.

Pfleeger، P. ، Pfleeger، and S. (2003). الأمن في الحوسبة ، الإصدار الثالث. نهر السرج العلوي ، نيو جيرسي: برنتيس هول.

Rajagopalan، R.P. (2019) الحرب الإلكترونية والسيبرانية في الفضاء الخارجي ، معهد الأمم المتحدة لبحوث نزع السلاح. تم الوصول إليه في 10 سبتمبر 2021 من https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf.

شواب ، ك. (2016) ، الثورة الصناعية الرابعة: ماذا تعني ، كيف تستجيب ، المنتدى الاقتصادي العالمي ، 14 يناير. تم الوصول إليه في 25 سبتمبر 2021 من https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

Seffers، G. I. (2017) الناتو يدرس تطبيقات إنترنت الأشياء العسكرية ، الإشارة ، 1 مارس. تم الوصول إليه في 25 سبتمبر 2021 من https://www.afcea.org/content/Article-nato-studying-military-iot-applications.

ساوث، ت. (2019). يشرح جنرال الجيش هذا من فئة 3 نجوم ما تعنيه العمليات متعددة المجالات بالنسبة لك ، وقت الجيش ، 11 أغسطس. تم الوصول إليه في 25 سبتمبر 2021 من https://www.armytimes.com/news/your-army/2019/08/11/this-3-star-army-general-explains-what-multi-domain-operations-mean-for-أنت./

ستينجل ، ر. (2019) حروب المعلومات: كيف خسرنا المعركة العالمية ضد المعلومات المضللة وما يمكننا القيام به حيال ذلك. لندن: كتب الأطلسي.

ستيرلينغ ب. تم الوصول إليه في 24 سبتمبر 2021 من https://www.wired.com/beyond-the-beyond/2019/04/deny-degrade-disrupt-deceive-destroy/.

Stone، A. (2018) يمكن أن تكون الإجابة على المشكلات اللوجستية في ساحة المعركة هي إنترنت الأشياء C4ISRnet ، 12 أكتوبر. تم الوصول إليه في 25 سبتمبر 2021 من https://www.c4isrnet.com/it-networks/2018/10/12/the-answer-to-battlefield-logistics-problems-could-be-iot/.

وزارة الدفاع البريطانية. (2018) الأنشطة السيبرانية والكهرومغناطيسية ، مذكرة العقيدة المشتركة 18/1. تم الوصول إليه في 24 سبتمبر 2021 من https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf.

وزارة الجيش الأمريكية. (2014) الأنشطة الكهرومغناطيسية السيبرانية ، FM3-38. تم الوصول إليه في 24 سبتمبر 2021 من https://irp.fas.org/doddir/army/fm3-38.pdf.

فاليريانو ، بي ، جنسن ، بي ، ومانيس ، آر سي ، (2018) إستراتيجية الإنترنت: الطابع المتطور للقوة والإكراه. أكسفورد: مطبعة جامعة أكسفورد.

van Niekerk، B. (2015) "Information Warfare in the 2013-2014 Ukraine Crisis"، in: Richet، J. (ed.)، Cybersecurity Policies and Strategies for Cyberfare Prevention. هيرشي ، بنسلفانيا: آي جي آي جلوبال ، ص 307-339.

van Niekerk، B.، Pretorius، B.، Ramluckan، T.، and Patrick، H. (2018) "The Impact of IoT on Information Warfare"، in: Fields، Z. (ed.)، Handbook of

Research on Information والأمن السيبراني في الثورة الصناعية الرابعة ، Hershey، PA: IGI، pp. 141-164.

Volz، D. (2016) قراصنة روس تعقبوا وحدات مدفعية أوكرانية باستخدام غرسة أندرويد: تقرير ، رويترز ، 22 ديسمبر. تم الوصول إليه في 29 سبتمبر 2021 من https://www.reuters.com/article/us-cyber-ukraine-idUSKBN14B0CU.

والتز ، إي (1998). حرب المعلومات: المبادئ والعمليات. بوسطن ولندن.Artech House

Wassel، P. (2018) 3 Military Applications of Internet of Things ، Augmate، 27 April.تم الوصول إليه في 25 سبتمبر 2021 من

https://www.augmate.io/3-military-applications-of-the-internet-of-things/.

Ween، A.، Dortmans، P.، Thakur، N.، and Rowe، C. (2019) تأطير الحرب الإلكترونية: منظور محلل ، مجلة نمذجة الدفاع والمحاكاة: التطبيقات ، المنهجية ، التكنولوجيا 16 (3) ، 335– 345.

White، J. (2016) Dismiss، Distort، and Dismay: Continuity and Change in Russian Disin Information، Policy Brief 2017/13، Institute for European Studies.تم الوصول إليه في 25 سبتمبر 2021 من
https://www.ies.be/node/3689.

ويلشر ، ك. (2009). طائرات مقاتلة فرنسية أسقطت بسبب فيروس الكمبيوتر ، التلغراف ، 7 فبراير. تم الوصول إليه في 26 سبتمبر 2021 من
http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

د. بريت فان نيكيرك أستاذ محاضر كبير في جامعة كوازولو ناتال، ويشغل منصب رئيس الاتحاد الدولي لفريق عمل معالجة المعلومات حول تكنولوجيا المعلومات والاتصالات في السلام والحرب، ورئيس التحرير المشارك للمجلة الدولية للحرب السيبرانية والإرهاب. يمتلك سنوات عديدة من الخبرة في مجال المعلومات/ الأمن السيبراني في كل من الأوساط الأكاديمية والصناعية، وقد ساهم في معايير أمن معلومات المنظمة الدولية للمقاييس/اللجنة الكهرتقنية الدولية (ISO / IEC) ومجموعات العمل الدولية. له أكثر من 70 منشورًا وعرضًا تقديميًا باسمه. تخرج بدرجة الدكتوراه التي تتركزعلى عمليات المعلومات وحماية البنية التحتية الحيوية في عام 2012. وهو حاصل أيضًا على ماجستير في الهندسة الإلكترونية واصبح مدير أمن المعلومات المعتمد (CISM).