التكنولوجيا التمكينية والأمن الدولي: خلاصة وافية

طبعة 2023

عن المؤلفة

وانتينج هي باحثة مشاركة في برنامج الأمن والتكنولوجيا في معهد الأمم المتحدة لبحوث نزع السلاح. حصلت على درجة الماجستير في الشؤون الدولية من معهد الدراسات العليا للدراسات الدولية والإنمائية في جنيف، ودرجة البكالوريوس في الدبلوماسية من جامعة الشؤون الخارجية الصينية في بكين.

حول معهد الأمم المتحدة لبحوث نزع السلاح

معهد الأمم المتحدة لبحوث نزع السلاح هو معهد مستقل ممول طوعيًا تابع للأمم المتحدة. يعد المعهد أحد المعاهد السياسية القليلة في العالم التي تركز على نزع السلاح، ويعمل على إنشاء المعرفة وتعزيز الحوار والعمل بشأن نزع السلاح والأمن. يقع مقر المعهد في جنيف، ويساعد المجتمع الدولي على تطوير الأفكار العملية والمبتكرة اللازمة لإيجاد حلول للمشكلات الأمنية الحرجة.

ملحوظة

التسميات المستخدمة في هذا المنشور وطريقة تقديم المادة فيه لا تعبر عن أي رأي مهما كان من جانب الأمانة العامة للأمم المتحدة فيما يتعلق بالوضع القانوني لأي بلد، أو إقليم، أو مدينة أو منطقة، أو لسلطاتها، أو فيما يتعلق بتعيين حدودها أو تخومها. الآراء الواردة في هذا المنشور تقع تحت مسؤولية المؤلفة فقط. إنها لا تعكس بالضرورة آراء أو وجهات نظر الأمم المتحدة أو معهد الأمم المتحدة لبحوث نزع السلاح أو موظفيها أو الجهات الراعية لها.

الشكر والتقدير

يشكل الدعم المقدم من الجهات المانحة الرئيسية لمعهد الأمم المتحدة لبحوث نزع السلاح الأساس لجميع أنشطة المعهد. لقد تم تمويل هذا المنشور من قبل الاتحاد الأوروبي في إطار برنامج الأمن والتكنولوجيا التابع لمعهد الأمم المتحدة لبحوث نزع السلاح، والذي تدعمه حكومات جمهورية التشيك وألمانيا وإيطاليا وهولندا وسويسرا والنرويج، بالإضافة إلى شركة مايكروسوفت.

تتقدم المؤلفة بجزيل الشكر للدكتور جياكومو بيرسي باولي على إرشاداته القيمة ومساهماته الثاقبة طوال عملية صياغة المنشور. كما تتوجه بالشكر الخاص إلى إيليا دوران سميث لمساعدتها في البحوث الأساسية. علاوة على ذلك، ترغب المؤلفة في تقديم الشكر إلى جيمس بلاك وسارة جراند كليمنت على مراجعتهما الشاملة وملاحظاتهما البناءة، والتي أثرت العمل النهائي بشكل كبير.

الاقتباس

هي، وانتينج. "التكنولوجيا التمكينية والأمن الدولي: "خلاصة وافية (طبعة 2023)". جنيف، سويسرا: معهد الأمم المتحدة لبحوث نزع السلاح، 2024.

الاختصارات

5G	شبكات الجيل الخامس الخلوية
6G	شبكات الجيل السادس الخلوية
AI	الذكاء الاصطناعي
AIaaS	الذكاء الاصطناعي كخدمة
AR	الواقع المعزز
AWS	خدمات أمازون ويب
CPU	وحدة المعالجة المركزية
CSP	مزود الخدمات السحابية
DOD	وزارة الدفاع (الولايات المتحدة)
EUV	الأشعة فوق البنفسجية القصوى
GNSS	نظام الملاحة العالمي عبر الأقمار الصناعية
GPU	وحدة معالجة الرسوميات
HTS	الموصلات الفائقة عالية الحرارة
IaaS	البنية التحتية كخدمة
ICRC	اللجنة الدولية للصليب الأحمر
ICT	تكنولوجيا المعلومات والاتصالات
IoMT	إنترنت الأشياء العسكرية
IoT	إنترنت الأشياء
ISR	الاستخبارات والمراقبة والاستطلاع
JWCC	القدرة القتالية السحابية المشتركة
LEO	مدار أرضي منخفض
MRI	التصوير بالرنين المغناطيسي
NEMS	الأنظمة الكهروميكانيكية النانوية
nm	نانومتر
NPU	وحدات المعالجة العصبية
PaaS	المنصة كخدمة
PQC	التشفير ما بعد الكمي
QKD	توزيع المفاتيح الكمية
SaaS	البرمجيات كخدمة
SoC	نظام على الشريحة
TPU	وحدة معالجة الموتر
TSMC	شركة تصنيع أشباه الموصلات التايوانية

UAV	مُسيّرة
VR	الواقع الافتراضي

جدول المحتويات

عن المؤلفة 1

حول معهد الأمم المتحدة لبحوث نزع السلاح 1

ملحوظة 1

الشكر والتقدير 1

الاقتباس 1

الاختصارات 2

الموجز التنفيذي 4

1. مقدمة 4

2. الفئة الأولى: المواد المتقدمة 5

2.1 أشباه الموصلات 5

2.2 الموصلات الفائقة 7

2.3 تكنولوجيا النانو 8

3. الفئة الثانية: الأجزاء والمكونات 10

3.1 الرقائق الدقيقة 10

3.2 المستشعرات 12

4. الفئة الثالثة: المعالجة والحوسبة 13

4.1 الحوسبة السحابية 13

4.2 حوسبة الحافة 14

4.3 الحوسبة الكمية 16

5. الفئة الرابعة: البنية التحتية 18

5.1 تكنولوجيا الجيل الخامس والجيل السادس 18

5.2 إنترنت الأشياء 20

5.3 البنية التحتية السحابية 21

5.4 الاتصالات عبر الأقمار الصناعية 22

6. الخلاصة 24

المراجع 26

الموجز التنفيذي

إن التقدم التكنولوجي في مجالات مثل المواد المتقدمة والرقائق الدقيقة والمستشعرات والبنية التحتية للاتصال connectivity infrastructure يمكّن الابتكار في مجالات التكنولوجيا الأخرى، وليس أقلها في مجال تكنولوجيا المعلومات والاتصالات والذكاء الاصطناعي والأنظمة المستقلة. وتساهم هذه التكنولوجيا التمكينية في إعادة تشكيل المشهد الرقمي ولديها تطبيقات محتملة في المجال العسكري. وفي حين تم إحراز تقدم في معالجة الآثار الأمنية لتكنولوجيا المعلومات والاتصالات والذكاء الاصطناعي في إطار مختلف العمليات الحكومية الدولية، فقد تم تخصيص قدر أقل نسبيا من الاهتمام للتكنولوجيا الأساسية التي تسهل أو تقود إلى زيادة تطويرها. ويبرز هذا الأمر الحاجة الملحة إلى دراسةً أكثر شمولاً وعمقاً للتكنولوجيا التمكينية وتأثيراتها المحتملة على الأمن الدولي.

ولمعالجة هذه الفجوة المعرفية، تهدف هذه الخلاصة الوافية إلى تحديد وتحليل أهم التطورات في مجال التكنولوجيا التمكينية، مع التركيز بشكل خاص على تلك التي لا تزال في مراحلها الأولى من التطوير أو التطبيق. وتستكشف الخلاصة الوافية أربع فئات من التكنولوجيا التمكينية، وهي: المواد المتقدمة (أشباه الموصلات والموصلات الفائقة وتكنولوجيا النانو)، والأجزاء والمكونات (الرقائق الدقيقة والمستشعرات)، والمعالجة والحوسبة (الحوسبة السحابية وحوسبة الحافة والحوسبة الكمية)، والبنية التحتية (اتصالات الجيل الخامس 5G والسادس 6G، وإنترنت الأشياء، والبنية التحتية السحابية واتصالات الأقمار الصناعية).

تسلط الخلاصة الوافية الضوء على العديد من الاتجاهات والتطورات الشاملة في مجالات التكنولوجيا قيد الدراسة. ويؤدي الاتجاه الحالي إلى تصغير حجم الأجهزة إلى إنشاء أجهزة صغيرة الحجم وفعالة بشكل متزايد، مما يسهل التكامل الواسع النطاق للتقنيات التمكينية في الأنظمة العسكرية. وتوفر هذه التكنولوجيا تعزيزات كبيرة للقدرات العسكرية والقدرة على تعزيز الجهود الأمنية الدولية. ومع ذلك، تنشأ التحديات من إمكانية زيادة المنافسة التكنولوجية بين الدول ومن مخاطر الأمن السيبراني والثغرات في سلسلة التوريد العالمية المرتبطة بالتكنولوجيا التمكينية. ورغم أن الدور الذي يضطلع به القطاع الخاص بالغ الأهمية، فإن التعاون في مجال التكنولوجيا ذات الاستخدام المزدوج قد يأتي بمخاطر جديدة مثل تعريض المعلومات العسكرية الحساسة للخطر.

ومن ثم فإن الرصد والتحليل المستمر للاتجاهات الناشئة أمر ضروري لإنشاء أطر حوكمة فعالة تحقق التوازن بين الفرص والمخاطر التي تفرضها التكنولوجيا التمكينية.

1. مقدمة

أشباه الموصلات: النقاط البارزة في عام 2023

- تقدم مستمر في إنشاء أشباه الموصلات أقلّ حجمًا وأكثر كفاءة. تسعى الشركات الرائدة في صنع أشباه الموصلات مثل شركة تايوان لصناعة الرقائق و شركة سامسونج بشكل نشط إلى تطوير تكنولوجيا أشباه الموصلات 2 نانومتر من الجيل التالي، والتي من المتوقع أن تزيد سرعات المعالجة بنسبة 10-15 في المائة مقارنة بأشباه الموصلات 3 نانومتر الأكثر تقدمًا حاليًا.
- يظل السيليكون أكثر المواد شبه الموصلة استخدامًا، غير أنه بات يقترب من حدوده الفيزيائية. وتستكشف جهود البحث الجارية مواد أشباه الموصلات الجديدة التي تتمتع بإمكانية تحسين الأداء، بما في ذلك زرنيخيد البورون المكعب والمواد ثنائية الأبعاد.
- سلسلة توريد أشباه الموصلات معرضة للاختلال بسبب طبيعتها المعقدة والمترابطة، مما قد يشكل تحديًا كبيرًا للأمن القومي. ومع ذلك، فإن استكشاف مواد أشباه الموصلات البديلة من الممكن أن يعزز التنوع في سلسلة التوريد العالمية.

تُعدّ التكنولوجيا، بما في ذلك المواد المتقدمة والرقائق الدقيقة والمستشعرات وقوة الحوسبة والبنية التحتية للاتصال، محركاً أساسياً للابتكار إلى الأمام وتطوير القدرات في مجالات التكنولوجيا الأخرى، وليس أقلها في مجال تكنولوجيا المعلومات والاتصالات والذكاء الاصطناعي والأنظمة المستقلة. ويؤدي تطوير التكنولوجيا التمكينية إلى إحداث ثورة في البيئة الرقمية، وتوسيع إمكانيات تطويرها وتطبيقها للأغراض العسكرية.[1] ومع استمرار تقدم هذه التكنولوجيا، أصبح من المهم بشكل متزايد معالجة آثارها على السلام والأمن الدوليين. يعد استكشاف الآفاق باستمرار أمرًا ضروريًا لتسخير فوائد هذه التكنولوجيا مع التخفيف من مخاطرها المحتملة.

ففي تقرير عام 2023 حول "التطورات الحالية في العلوم والتكنولوجيا وتأثيرها المحتمل على الجهود الدولية في مجال الأمن ونزع السلاح"، أكد الأمين العام للأمم المتحدة على المخاوف المستمرة من أن التطورات في العلوم والتكنولوجيا المتصلة بالأمن ونزع السلاح تتجاوز قدرة الأطر المعيارية وأطر الحوكمة على إدارة المخاطر.[2] ولقد حققت العديد من العمليات الحكومية الدولية تقدمًا كبيرًا في معالجة الآثار الأمنية لتكنولوجيا المعلومات والاتصالات والذكاء الاصطناعي، ومع ذلك فقد تم تخصيص قدر أقل نسبيًا من الاهتمام للتكنولوجيات الأساسية التي تمكن أو تدفع المزيد من تطوراتها. يؤكد ذلك الحاجة الملحة إلى إجراء فحص أكثر شمولاً ودقة للتكنولوجيا التمكينية فضلاً عن تأثيراتها المحتملة على الأمن الدولي.

وفي إطار الجهود المبذولة لسد فجوة المعرفة، تهدف هذه الخلاصة الوافية إلى تحديد وتحليل أهم التطورات في مجال التكنولوجيا التمكينية. ويشمل ذلك التكنولوجيا التمكينية التي لا تزال في المراحل الأولى من تطويرها أو تطبيقها ولكن من المتوقع أن يكون لها تأثير مهم على السلام والأمن الدوليين. وتركز هذه الخلاصة الوافية حصريًا على استكشاف التأثيرات من الدرجة الأولى للتكنولوجيا التمكينية على البيئة الرقمية، وخاصة فيما يتعلق بالسلام والأمن الدوليين. ومع ذلك، قد تكون لبعض مجالات التكنولوجيا آثار أوسع نطاقًا تتجاوز ما يشمله هذا التقرير.

تتناول الخلاصة الوافية في الفصول التالية أربع فئات من التكنولوجيا التمكينية، حيث تتضمن الفئة الأولى المواد المتقدمة، مثل أشباه الموصلات والموصلات الفائقة وتكنولوجيا النانو؛ وتبحث الفئة الثانية في الأجزاء والمكونات، بما في ذلك الرقائق الدقيقة والمستشعرات؛ و تشمل الفئة الثالثة المعالجة والحوسبة، أي الحوسبة السحابية وحوسبة الحافة والحوسبة الكمية؛ و تشمل الفئة الرابعة البنية التحتية، من اتصالات الجيل الخامس والسادس، عبر إنترنت الأشياء IoT والبنية التحتية السحابية، إلى اتصالات الأقمار الصناعية. ويقدم كل فصل تحليلاً شاملاً للتكنولوجيا قيد الدراسة، بما في ذلك أحدث التطورات والتطبيقات العسكرية ذات الصلة، يليه تقييم للآثار المحتملة على الأمن الدولي. وتختتم الخلاصة الوافية بفحص شامل للاتجاهات العامة والتطورات في مجال التكنولوجيا التمكينية.

2. الفئة الأولى: المواد المتقدمة

2.1 أشباه الموصلات

*تنتمي **أشباه الموصلات** إلى فئة من المواد تتميز بخصائص التوصيل الكهربائي التي تقع بين خصائص الموصلات (مثل المعادن) والعوازل (مثل الزجاج). يمكن التحكم في التوصيل الكهربائي لأشباه الموصلات وتعديلها، مما يجعلها بمثابة حجر الأساس للأجهزة والمكونات الإلكترونية الحديثة بما في ذلك الصمامات الثنائية والترانزستورات والدوائر المتكاملة.*

لقد أدت الخصائص الكهربائية الفريدة لأشباه الموصلات إلى تحويل مشهد التكنولوجيا، مما أدى إلى تطوير أجهزة وأنظمة إلكترونية أكثر إحكاما وقوة وكفاءة في استخدام الطاقة. وفي صناعة الإلكترونيات، يعد السيليكون المادة شبه الموصلة الأكثر استخدامًا، كما تُستخدم مواد أخرى مثل زرنيخيد الغاليوم والجرمانيوم في التطبيقات المتخصصة. وغالبًا ما توفر رقائق السيليكون الأساس لتصنيع الرقائق الدقيقة وتلعب دورًا أساسيًا في عمل التكنولوجيا الرقمية.

[1] لغرض هذه الخلاصة الوافية، تُعرّف التكنولوجيا التمكينية على أنها التكنولوجيا التي تمّكن أو تدفع الابتكار إلى الأمام، وتطوير القدرات في مجالات التكنولوجيا الأخرى ضمن نطاق العمل الذي يقوم به برنامج الأمن والتكنولوجيا التابع لمعهد الأمم المتحدة لبحوث نزع السلاح الذي يشمل: الأمن السيبراني، والذكاء الاصطناعي، والاستقلالية، فضلاً عن تكامل النظم.

[2] الجمعية العامة للأمم المتحدة (2023).

تُعدّ عقدة المعالجة لأشباه الموصلات، والتي يتم قياسها الآن غالبًا بالنانومتر nm،[3] عاملًا حاسمًا في تكنولوجيا أشباه الموصلات، وتسمح عقد المعالجة المخفضة بتجميع المزيد من الترانزستورات على رقيقة واحدة، مما يؤدي غالبًا إلى تحسين الأداء وكفاءة الطاقة. وعلى مر العقود انخفض حجم عقدة أشباه الموصلات بشكل كبير، من القياس الأولي بالميكرومتر μm^4 إلى المستوى الحالي الأكثر تطورًا من تكنولوجيا 3 نانومتر.[5] وتخطط شركة تايوان لتصنيع أشباه الموصلات TSMC، إحدى أكثر شركات تصنيع أشباه الموصلات تقدمًا، لإنتاج أشباه الموصلات 2 نانومتر من الجيل التالي بدءًا من عام 2025. ومن المتوقع أن يؤدي هذا إلى تحقيق سرعات معالجة أعلى بنسبة 10 إلى 15 في المائة من تلك الموجودة في رقائق 3 نانومتر.[6]

القوة الدافعة لتطور عقد المعالجة هي ما أصبح يعرف بقانون مور. وهذه ملاحظة تجريبية من قبل جوردون مور، أحد مؤسسي شركة إنتل، مفادها أن عدد الترانزستورات الموجودة على الرقيقة الدقيقة كان يتضاعف تقريبا كل عامين. وبناء على ذلك، يؤكد هذا القانون أن أداء الحوسبة سوف يستمر في النمو بينما تنخفض تكلفة الحواسيب. وعلى الرغم من أن النظرية ظلت صحيحة إلى حد كبير حتى القرن الحادي والعشرين، فقد بدأ المهندسون في الوصول إلى حدود المواد شبه الموصلة التقليدية ضمن الفهم الحالي لقوانين الفيزياء. ونتيجة لذلك، أعلن بعض المراقبين نهاية قانون مور.[7] تسعى الصناعة الآن إلى إيجاد حلول مبتكرة لتحقيق تحسينات أشباه الموصلات المستقبلية.

بدلاً من السيليكون، تم تحديد مواد أخرى كبدائل محتملة لتلبية الطلب المتزايد على قوة الحوسبة. على سبيل المثال، تقوم أشباه الموصلات المركبة بدمج عناصر متعددة لإنتاج مواد قادرة على التفوق على السيليكون. ومن المتوقع أن تلعب هذه المواد دورًا محوريًا في تطوير التكنولوجيا التوصيلية الجديدة والمركبات ذاتية القيادة.[8] يعتبر زرنيخيد الغاليوم ثاني أكثر المواد شبه الموصلة استخدامًا بعد السيليكون، وهو مركب معروف لتفوق حركية الإلكترونات فيه، مما يؤدي إلى كفاءة أكبر من السيليكون. كما أنه يتميز بقدرة أكبر على تحمل ارتفاع درجة الحرارة. ومع ذلك، فإن الإنتاج واسع النطاق لزرنيخيد الجاليوم سوف يحتاج إلى التغلب على تحديات كبيرة، بما في ذلك الاعتماد على المواد الكيميائية السامة، مما يثير المخاوف بشأن التأثيرات على الصحة العامة والبيئة.[9]

وتستكشف جهود البحث الجارية مواد جديدة تظهر إمكانات كبيرة في تمكين تطوير أجهزة أكثر إحكاما وكفاءة على نحو متزايد. لقد سلطت دراسات حديثة الضوء على فعالية مادة تُعرف باسم زرنيخيد البورون المكعب في معالجة بعض القيود التي تفرضها أشباه الموصلات التقليدية القائمة على السيليكون، مع إمكانية أن تصبح "أفضل مادة أشباه الموصلات التي تم العثور عليها على الإطلاق".[10] وعلى الرغم من خصائصه الواعدة، فإن زرنيخيد البورون المكعب لا يزال في المرحلة التجريبية حاليًا، مما يترك تطبيقاته في العالم الحقيقي غير محددة بالكامل إلى حد الآن. وإلى جانب ذلك، فإن مواد أشباه الموصلات الناشئة الأخرى أيضًا آخذة في الانتعاش شيئًا فشيئًا، بما في ذلك نتريد الغاليوم عالي القدرة، والمواد القائمة على الأنتيمونيد والبيزموثيد، والمواد ثنائية الأبعاد (2D) مثل الغرافين.[11] وتتمتع هذه المواد بخصائص فيزيائية مميزة أثبتت فائدتها في تطبيقات محددة. ومع ذلك، فإن استخدامها على نطاق واسع تعوقه التكاليف وتعقيدات إنتاجها.

سيلعب الابتكار المستمر في المواد شبه الموصلة دورًا محوريًا في الأنظمة العسكرية المستقبلية. تُستخدم أشباه الموصلات في تطبيقات ملموسة في مجموعة من المكونات الأساسية للأجهزة الإلكترونية، بدءًا من المستشعرات والمُشغلات ورقائق الذاكرة إلى الأنظمة الكهروضوئية وأجهزة التحكم الدقيقة.[12] وتشكل أشباه الموصلات هذه العمود الفقري للأجهزة الإلكترونية المتطورة التي تلعب دورًا بارزًا في الأنظمة العسكرية المتطورة، بما في ذلك أجهزة الاتصالات عالية السرعة وأنظمة الرادار والأسلحة الموجهة بدقة. وعلاوة على ذلك، تعمل تكنولوجيا أشباه الموصلات كمحفز للابتكارات التحويلية مثل الذكاء الاصطناعي وإنترنت الأشياء (IoT). ومن ثم فإن ظهور مواد

---

[3] النانومتر الواحد يعادل واحدًا على الألف من الميكرومتر، أو واحدًا على المليار من المتر.

[4] على سبيل المثال، تم إطلاق معالج 4004 من شركة إنتال في عام 1971:
https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html

[5] اعتبارًا من سبتمبر 2023، هناك شركتان فقط في العالم قادرتان على تصنيع أشباه الموصلات بتكنولوجيا 3 نانومتر: شركة تايوان لصناعة الرقائق (https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_3nm) وشركة سامسونج (https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture).

[6] Ryugen, Hideaki (2023).

[7] Arcuri and Shivakumar (2022).

[8] معهد مهندسي الكهرباء والإلكترونيات (بدون تاريخ-أ).

[9] معهد مهندسي الكهرباء والإلكترونيات (بدون تاريخ-ب).

[10] Chandler (2022).

[11] معهد مهندسي الكهرباء والإلكترونيات (بدون تاريخ-ب).

[12] Gargeyas (2022).

أشباه الموصلات الجديدة يحمل في طياته إمكانية تعزيز قدرات الدفاع الوطني، على الرغم من أنه قد يبشر أيضًا بعصر جديد من المنافسة التكنولوجية بين الدول.

علاوة على ذلك، تشكل نقاط الضعف في سلسلة التوريد حاليا تحديا رئيسيا. إن سلسلة توريد أشباه الموصلات عبارة عن شبكة عالمية مترابطة ومعقدة للغاية تتضمن مراحل إنتاج مختلفة وشركات من مناطق مختلفة. وتتميز أيضًا بدرجة عالية من التخصص وتركيز مرافق إنتاج أشباه الموصلات المتقدمة في شرق آسيا، على سبيل المثال. وقد يكون لأي اضطراب في قدرات التصنيع في المنطقة، سواء ناجمًا عن التوترات الجيوسياسية أو الكوارث الطبيعية، تأثير سلبي على توافر أشباه الموصلات وعواقب وخيمة على الأمن القومي. ومع ذلك، فإن تطوير مواد أشباه الموصلات البديلة قد يعيد تشكيل النموذج الحالي وزيادة التنوع في سلسلة التوريد العالمية.

الموصلات الفائقة *مواد يمكنها توصيل الكهرباء دون أي مقاومة أو فقدان للطاقة ويمكنها صد المجالات المغناطيسية عند تبريدها إلى ما دون درجة حرارة حرجة محددة. تتيح هذه الخاصية الفريدة للتيار الكهربائي تدفق التيار الكهربائي في الموصل الفائق دون انقطاع أو فقد للطاقة.*

2.2 الموصلات الفائقة

تتمتع الخصائص الكهرومغناطيسية الاستثنائية للموصلات الفائقة بالقدرة على تعزيز مجالات مختلفة، بما في ذلك الإلكترونيات، والحوسبة الكمية، ونقل الطاقة وتخزينها، وتكنولوجيا التصوير بالرنين المغناطيسي MRI. ومع ذلك، فإن استخدامها العملي محدود في الوقت الحالي بسبب متطلبات درجات الحرارة المنخفضة للغاية، الأمر الذي يستلزم هندسة تبريد باهظة الثمن واستهلاك الطاقة العالية لعملية التبريد. تُظهر معظم مواد الموصلات الفائقة درجات حرارة حرجة تتراوح بين الصفر المطلق و10 كلفن (حوالي -273 إلى -263 درجة مئوية).[13] ونتيجة لذلك، يبقى تطبيق الموصلات الفائقة على نطاق واسع غير عملي في الوقت الراهن.

تركز الأبحاث بشأن الموصلات الفائقة بشكل أساسي على السعي لاكتشاف مواد ذات درجات حرارة حرجة أعلى بكثير. ولقد تم اكتشاف موصلات فائقة عالية الحرارة HTS يمكنها إظهار الموصلية الفائقة في درجات حرارة أعلى من درجات الحرارة التي تتمتع بها المواد التقليدية. وعلى الرغم من تسميتها بـ "عالية الحرارة"، فإن عبارة الموصلات الفائقة عالية الحرارة تشير إلى المواد التي تكون موصلة في درجة حرارة تفوق 77 كلفن (-196.2 درجة مئوية)، وهي نقطة غليان النيتروجين السائل.[14] في السنوات الأخيرة، كان هناك تركيز متزايد في الأوساط العلمية على دفع الحدود إلى أبعد من ذلك من خلال السعي إلى تطوير الموصلية الفائقة في درجة حرارة الغرفة. وفي حين أن هذا البحث لا يزال مستمرًا، لم يتحقق أي تقدم حتى الآن.

قد تؤدي الأبحاث والتطويرات المستقبلية إلى خفض تكاليف التشغيل بشكل فعال وجعل تكنولوجيا الموصلات الفائقة أكثر سهولة في الوصول إليها للتطبيقات العملية. ومن المتوقع أن يكون استخدام الموصلات الفائقة المتقدمة في السياقات العسكرية بمثابة تحول جذري. يمكن استحداث مواد فائقة الموصلية قابلة للتطوير في درجة حرارة الغرفة أن يؤدي إلى ثورة في مجال الإلكترونيات، مما يسمح بتطوير تطبيقات واعدة مثل الرقائق الحاسوبية فائقة السرعة والفعالة في استخدام الطاقة، والاتصالات اللاسلكية ذات النطاق العريض وزمن الانتظار المنخفض، وشبكات الكهرباء عالية الكفاءة.[15] بالإضافة إلى ذلك، يمكن استخدام الموصلات الفائقة لبناء الكيوبتات (الوحدات الأساسية للمعالجات الكمية)، مما يوفر فرصًا واسعة للحوسبة الكمية.[16] يتم حاليا تطوير مواد فائقة الموصلية جديدة لإحداث الكيوبتات تكون قادرة على مقاومة الاضطرابات الخارجية، وهذه سمة يمكن أن تجعل الحواسيب الكمية أكثر موثوقية.[17] ومع ذلك، فإن ظهور الموصلات الفائقة في درجة حرارة الغرفة قد يؤدي إلى تأجيج المنافسة التكنولوجية الجديدة بين الدول، مما قد يؤدي إلى نزاعات دولية بشأن براءات الاختراع ونقل التكنولوجيا والوصول إلى الأسواق.[18]

---

[13] المركز الوطني للكفاءة البحثية (2021). تشير درجة الحرارة الحرجة إلى درجة الحرارة التي تنخفض عندها المقاومة الكهربائية للموصل الفائق إلى الصفر.

[14] Clynes (2023).

[15] Pedram (2023).

[16] للحصول على تحليل مفصل للحوسبة الكمية وأحدث التطورات، راجع القسم 4.3 أدناه.

[17] Feldman (2023).

[18] Roa (2023).

الموصلات الفائقة: النقاط البارزة في عام 2023

- الحاجة إلى درجات حرارة منخفضة للغاية تعوقه حاليًا التطبيق العملي للموصلات الفائقة، مما يتطلب هندسة تبريد مكلفة واستهلاكًا عاليًا للطاقة. وتسعى الجهود العلمية الحثيثة إلى تحقيق الموصلية الفائقة في درجة حرارة الغرفة.
- يعد استحداث الموصلات الفائقة القابلة للتطوير في درجة حرارة الغرفة أمرًا واعدًا لإحداث ثورة في مجال الإلكترونيات، ولكن ظهورها قد يؤدي إلى نزاعات دولية فيما يتعلق بالبراءات ونقل التكنولوجيا والوصول إلى الأسواق.

2.3 تكنولوجيا النانو

*تساهم **تكنولوجيا النانو** في تصميم وتصنيع واستخدام المواد على نطاق النانو، وهو مقياس يمتد من 1 إلى 100 نانومتر (النانومتر الواحد هو جزء من المليار من المتر).*

على المستوى النانوي، تنشأ خصائص فريدة وجديدة في كثير من الأحيان نتيجة للتأثيرات الكمية وسلوك الأسطح.[19] ويمكن الاستفادة من هذه الخصائص في تطبيقات مختلفة، بما في ذلك المواد النانوية والإلكترونيات النانوية. وفي الإلكترونيات الحديثة، يتم تسهيل الاتجاه الحالي لتصغير حجم الأجهزة بشكل كبير من خلال التقدم في أنظمة النانو الكهروميكانيكية NEMS. يمكن استخدام هذه الأنظمة لإنشاء مستشعرات ومشغلات وأجهزة أخرى أصغر حجمًا وأكثر كفاءة ذات تطبيقات مهمة في الاستشعار المتقدم والحوسبة والاتصالات.

في تطبيقات الاستشعار، يتم تطبيق تكنولوجيا النانو في الرصد البيئي لجودة الهواء والمياه وكذلك الكشف عن الملوثات. ويمكن أن يؤدي دمج تكنولوجيا النانو إلى إنتاج مستشعرات أصغر حجمًا وأكثر حساسية للعمليات الميدانية العسكرية، والتي يمكنها، على سبيل المثال، اكتشاف العوامل البيولوجية والكيميائية الخطيرة. وبالمقارنة مع الطرق التقليدية لاكتشاف التهديدات البيولوجية، يمكن للمستشعرات البيولوجية المعتمدة على المواد النانوية تحقيق حساسية ودقة أعلى حتى مع انخفاض حجم العينة ووقت التحضير وتكاليف الاختبار.[20] ويمكن استخدام المستشعرات النانوية لتوفير معلومات في الوقت الحقيقي حول التهديدات المحتملة للعمليات العسكرية، وبالتالي تعزيز الوعي بالأوضاع في ساحة المعركة. كما يمكن أن تكون هذه الحلول مفيدة بنفس القدر لجهود التحقق من نزع السلاح في مجال الأسلحة البيولوجية والكيميائية.

وفي مجال الحوسبة، تمهد تكنولوجيا النانو الطريق أمام الجيل القادم من الحوسبة من خلال تسهيل تطوير المواد النانوية مثل الأنابيب النانوية الكربونية والجرافين والنقاط الكمية. ومع اقتراب تكنولوجيا السيليكون التقليدية من حدودها الفيزيائية، يتزايد الاهتمام بالمواد البديلة والأساليب الجديدة للحوسبة. في السنوات الأخيرة، حدد الباحثون الأنابيب النانوية الكربونية كبديل جذاب لتحل محل السيليكون في تصنيع الترانزستورات.[21] وقد يُسهل استخدام هذه المادة النانوية عالية التوصيل إنشاء تصميمات ترانزستور أصغر حجمًا وأكثر كفاءة، قادرة على التفوق على الترانزستورات القائمة على السيليكون.[22] ومع ذلك، لم يتم بعد إثبات ميزتها في التطبيقات الحقيقية بشكل قاطع.[23] علاوة على ذلك، يمكن للنقاط الكمية (أي البلورات النانوية التي يتم تصنيعها من خلال عملية التصنيع النانوي) أن تحدث ثورة في مجال الحوسبة الكمية. نظرًا لخصائصها الكمية، يمكن استخدام النقاط الكمية ككيوبتات لتشكل الأساس للحواسيب الكمية، مما يتيح بناء آلة عمل قابلة للتطوير وفعالة من حيث التكلفة ومقاومة للأخطاء.[24] ومع ذلك، لا تزال التكنولوجيا في مهدها وهناك العديد من العقبات التقنية والتجارية التي يجب التغلب عليها قبل تحقيق الإنتاج العملي وعلى نطاق واسع للحواسيب الكمية.[25]

---

[19] المكتب الوطني الأمريكي لتنسيق تكنولوجيا النانو (غير مؤرخ).

[20] (Rowland et al. (2016.

[21] Fadelli (2023).

[22] (Basheer et al. (2022.

[23] Fadelli (2023).

[24] Hecht (2022).

[25] للحصول على تحليل مفصل للحوسبة الكمية وأحدث التطورات، راجع القسم 4.3 أدناه.

علاوة على ذلك، يمكن لتكنولوجيا النانو تسهيل الاتصالات المتقدمة للعمليات العسكرية، وتقديم فوائد متعددة بما في ذلك انخفاض استهلاك الطاقة، وأجهزة الاتصالات المصغرة، وتعزيز التوصيلية. وفي أنظمة الاتصالات اللاسلكية، يؤدي تطوير تكنولوجيا النانو إلى إنتاج مستشعرات لاسلكية أصغر وأرخص وأقل استهلاكًا للطاقة وأكثر كفاءة ويجعل شبكات الجيل الخامس ممكنة.[26] ويمكن أيضًا استخدام المواد النانوية لإنشاء هوائيات عالية الكفاءة تسمح بتحسين كفاءة الإشارة وموثوقيتها. على سبيل المثال، قام الباحثون بتطوير هوائيات نانوية الحجم لتمكين نقل البيانات بسرعة الضوء بين معالجات ذات نواة مختلفة مع القليل من الخسارة.[27]

رغم أن تكنولوجيا النانو تنطوي على إمكانات كبيرة لتعزيز أنظمة المعلومات والاتصالات العسكرية، فإن تطويرها ونشرها ينطويان أيضًا على بعض المخاطر، حيث أشارت الدراسات إلى أن الجسيمات النانوية يمكن أن تنطوي على مجموعة واسعة من السّمّية والمخاطر البيئية، مما يشكل تهديدات كبيرة لصحة الإنسان والرفاهة البيئية.[28] يسمح حجم وتركيب الجسيمات النانوية لها باختراق الحواجز الفسيولوجية للكائنات الحية ويمكنهما التسبب في تفاعلات بيولوجية ضارة في جسم الإنسان (على سبيل المثال، التهاب الرئة وأمراض القلب).[29] ويمكن للمواد النانوية المنتجة من خلال عمليات التصنيع أن تدخل البيئة من خلال إطلاقات متعمدة أو عرضية. وبمجرد ترسبها في التربة، فإنها تستطيع تلويث الأرض ثم الانتقال إلى أنظمة المياه.[30]

تكنولوجيا النانو: النقاط البارزة في عام 2023

- يؤدي التقدم المستمر في تكنولوجيا النانو بشكل مستمر إلى تحسين وتقدم الاستشعار والحوسبة والاتصالات، حيث إن المواد النانوية مثل أنابيب الكربون النانوية و النقاط الكمية لديها القدرة على قيادة الجيل القادم من الحوسبة، بما في ذلك مجال الحوسبة الكمية الناشئ. ومع ذلك، لا تزال هناك تحديات أمام تحقيق إنتاجها العملي وعلى نطاق واسع.
- توفر تكنولوجيا النانو فوائد محتملة لأنظمة المعلومات والاتصالات العسكرية، ولكنها تشكل أيضًا مخاطر. وتشير البحوث إلى أن الجسيمات النانوية قد تكون سامة وخطيرة على البيئة، مما يشكل تهديدات كبيرة لصحة الإنسان والرفاهية البيئية.

3. الفئة الثانية: الأجزاء والمكونات

3.1 الرقائق الدقيقة

__الرقائق الدقيقة__ أو الرقائق، والمعروفة أيضًا باسم الدوائر المتكاملة، هي مجموعات مدمجة من المكونات الإلكترونية المصغرة بما في ذلك الترانزستورات والديودات والمقاومات المثبتة على قطعة مسطحة صغيرة من مادة أشباه الموصلات، وعادة ما تكون عبارة عن رقاقة سيليكون.

لا يمكن المبالغة في أهمية تكنولوجيا الرقائق الدقيقة. إنها تشكل حجر الأساس للإلكترونيات الحديثة وأنظمة الحوسبة، حيث تمكن من صنع أجهزة ليست فقط أصغر حجمًا، ولكنها أيضًا أكثر قوة وفعالية من حيث التكلفة والكفاءة في استخدام الطاقة من تلك المصنوعة من مكونات منفصلة. يمكن للرقائق الدقيقة أداء وظائف مهمة مختلفة، بما في ذلك معالجة المعلومات وتخزين البيانات وتنفيذ التعليمات، ويمكن استخدامها كرقائق ذاكرة ووحدات معالجة مركزية CPUs ووحدات معالجة الرسوم GPUs).

تتطور الرقائق الدقيقة باستمرار، حيث يتم التقدم في مواد أشباه الموصلات مما يؤدي إلى إنشاء وظائف جديدة وأداء أعلى بتكاليف أقل.[31] وكما تم توضيحه أعلاه، تواصل صناعة أشباه الموصلات دفع حدود التصغير لتطوير الترانزستورات ذات عقد معالجة أصغر. ويسمح

[26] حمزة وجعفر (2022).
[27] Kullock et al. (2020).
[28] Kumah et al. (2023).
[29] المرجع نفسه.
[30] Ray, Paresh et al. (2009).
[31] للحصول على تحليل مفصل لتكنولوجيا أشباه الموصلات وأحدث التطورات، راجع القسم 2.1 أعلاه.

الحجم المصغر بتجميع عدد أكبر من الترانزستورات على رقيقة واحدة صغيرة، مما يؤدي إلى زيادة قوة المعالجة وكفاءة الطاقة. ومع ذلك، وبما أن تكنولوجيا أشباه الموصلات الحالية القائمة على السيليكون تقترب تدريجيًا من حدودها الفيزيائية، يتم البحث عن مواد وأساليب بديلة لضمان النمو المستمر والتحول في تكنولوجيا الرقائق الدقيقة.

يتم أيضًا تعزيز الابتكار في هذا المجال من خلال تحسين تصميم الرقائق. وقد تم طرح طرق بديلة لتصميم الرقائق مثل "أنظمة متعددة الرقائق" و"التصميم القائم على الرقائق المنفصلة".[32] وعلى عكس الرقائق التقليدية أحادية الكتلة، تتكون بنية الرقائق متعددة المكعبات من مجموعة من الرقائق المتخصصة مثل الذاكرة ووحدات المعالجة المركزية التي يمكن ربطها لإنشاء حزمة نظام على رقيقة SoC معقدة ومتكاملة. ويُعتقد أن تصميم الرقائق المبتكر قادر على دعم التعلم الآلي للذكاء الاصطناعي على نطاق واسع، وتعزيز إنتاجية السيليكون وتقليل النفايات في عملية تصنيع الرقائق.[33] تم تصميم الأنظمة على الرقائق SoC المخصصة من قبل شركات مثل آبل وغوغل/ألفبت Google/Alphabet وخدمات أمازون ويب AWS لتحسين أداء الرقائق لتطبيقات وأعباء عمل محددة - وهذا ما يُعرف باسم نهج "السيليكون المخصص".[34]

يجري تصميم رقائق دقيقة متخصصة لتمكين تطبيقات تكنولوجية أخرى مثل تكنولوجيا الجيل الخامس والذكاء الاصطناعي. وتتطلب توصيلية الجيل الخامس تطوير رقائق دقيقة متقدمة يمكنها تلبية متطلبات السرعة العالية وزمن الانتظار المنخفض للتكنولوجيا. وتعتمد قدرات الذكاء الاصطناعي أيضًا إلى حد كبير على قوة معالجة الرقائق الدقيقة المتخصصة مثل وحدات معالجة الموتر TPUs ووحدات المعالجة العصبية NPUs. يمكن أن تكون رقائق الذكاء الاصطناعي المتطورة أسرع بعشرات الآلاف من المرات وأكثر كفاءة من الرقائق ذات الاستخدام العام مثل وحدات المعالجة المركزية.[35]

علاوة على ذلك، تقوم تكنولوجيا الطباعة الحجرية فوق البنفسجية القصوى EUV حاليًا بدور مهم في تصنيع الرقائق الدقيقة الأكثر تقدمًا في العالم. فإنها تسهل إنشاء مكونات فائقة الصغر ودقيقة للغاية على رقائق السيليكون وتساهم في التصغير المستمر للرقائق الدقيقة. ولزيادة عملية التصغير، وضع الباحثون طريقة أكثر تعقيدًا، تُعرف باسم الطباعة الحجرية فوق البنفسجية ذات الفتحة العددية العالية، لتحقيق الإنتاج الضخم لتكنولوجيا العقدة 2 نانومتر من الجيل التالي.[36] ومن المتوقع أن تدخل أنظمة التصنيع الجديدة مرحلة التشغيل الكامل بحلول عام 2025.[37] وبالإضافة إلى ذلك، تستمر طرق التغليف المتقدمة أيضًا في تعزيز أداء الرقائق الدقيقة وكفاءة الطاقة، ولا سيما تقنيات التكديس والتغليف ثلاثية الأبعاد 3D التي تدمج رقائق متعددة في بنية ثلاثية الأبعاد.[38]

ستستمر التطورات الجديدة في تكنولوجيا الرقائق الدقيقة في تشكيل المشهد التكنولوجي في السنوات القادمة، وستكون لها آثار كبيرة على الأمن الدولي. إن الدور المنتشر للأنظمة الإلكترونية في الحرب الحديثة يعني أن تحسين أداء الرقائق الدقيقة يمكن أن يفيد جوانب مختلفة من العمليات العسكرية. وتشمل هذه العمليات زيادة دقة وفعالية الأسلحة المتقدمة، وتعزيز قدرات الاستخبارات والمراقبة والاستطلاع، وتحسين أنظمة الاتصالات، وتسهيل دمج الذكاء الاصطناعي والاستقلالية في الأنظمة العسكرية. ومع ذلك، فإن هذه التكنولوجيا تنطوي أيضًا على تحديات أمنية جديدة. وتعتبر سلسلة توريد الرقائق الدقيقة عالمية ومعقدة للغاية، بدءًا من تصميم الرقائق وتصنيعها إلى التعبئة والتغليف والاختبار والتوزيع. وغالبًا ما تتركز أحدث التكنولوجيا والقدرات التصنيعية في مناطق معينة، مما قد يؤدي إلى نقاط ضعف محتملة في سلسلة التوريد. على سبيل المثال، تعد شركة أ آس آم آل ASML في هولندا حاليًا الشركة الوحيدة التي تمتلك القدرة على تصنيع آلات الطباعة الحجرية فوق البنفسجية المستخدمة في الإنتاج واسع النطاق لأكثر الرقائق الدقيقة تقدمًا في العالم.[39]

وهناك تحد آخر يتعلق بالطبيعة المزدوجة لاستخدام التكنولوجيا وانتشارها المحتمل، حيث يمكن أن تقع الرقائق الدقيقة المستخدمة في التطبيقات المدنية، مثل الهواتف الذكية والحواسيب المحمولة، خارج نطاق لوائح مراقبة الصادرات، وبالتالي يمكن استغلالها لأغراض عسكرية أو دمجها في الأنظمة العسكرية.[40] وهناك أيضًا مخاوف تتعلق بالأمن السيبراني مرتبطة باستخدام الرقائق الدقيقة. فمن الصعب اكتشاف نقاط الضعف في الأجهزة نظرًا لتعقيد بنية الدائرة المتكاملة. ويمكن إخفاء التعديلات الفيزيائية بشكل فعال بين المجموعة الواسعة

[32] MIT Technology Review Insights (2023).
[33] المرجع نفسه.
[34] Shilov (2023).
[35] Khan and Mann (2020).
[36] IBM (2023).
[37] ASML (n.d.).
[38] Moore (2022).
[39] ASML (n.d.).
[40] Gilchrist (2023).

من المكونات والوظائف الصالحة والبقاء غير مكتشفة لفترة طويلة.[41] وبالمقارنة بقضايا البرمجيات، فإن إصلاح عيوب الأجهزة غالبًا ما يكون أكثر صعوبة وتكلفة، وهو ما يفتح نافذة ضعف ويعرض الأنظمة الرقمية الأوسع للخطر.[42]

الرقائق الدقيقة: النقاط البارزة في عام 2023

- تستمر التطورات في تكنولوجيا أشباه الموصلات في تحسين أداء ووظائف الرقائق الدقيقة بتكاليف أقل من خلال التصغير. ومن شأن استكشاف المواد والأساليب البديلة لأشباه الموصلات أن يعزز القدرة على دعم نمو وتحول تكنولوجيا الرقائق الدقيقة.
- يتحقق التقدم في هذا المجال أيضًا من خلال تحسين تصميم الرقائق وتقنيات الإنتاج. وتقدم تصميمات الرقائق المبتكرة، مثل "الأنظمة المتعددة المكعبات"، أنظمة رقائق متكاملة ومعقدة ويمكنها دعم التعلم الآلي للذكاء الاصطناعي على نطاق واسع. يهدف التطوير المستمر للطباعة الحجرية فوق البنفسجية ذات الفتحة العددية العالية إلى تمكين الإنتاج الضخم لتكنولوجيا العقدة 2 نانومتر من الجيل التالي بحلول عام 2025.
- على الرغم من الفوائد المحتملة لتحسين أداء الرقائق الدقيقة في العمليات العسكرية، فإن التحديات تشمل نقاط الضعف في سلسلة التوريد، والطبيعة المزدوجة لاستخدام التكنولوجيا، ومخاوف الأمن السيبراني.

3.2 المستشعرات

المستشعرات *أجهزة مصممة لاكتشاف الخصائص الفيزيائية والظروف البيئية ومن ثم تحويل هذه المعلومات إلى إشارات مخرجات.*

تتمتع المستشعرات، التي تشمل مستشعرات الحركة ومستشعرات القرب والمستشعرات الحيوية ومستشعرات الصور، من بين أنواع أخرى، بمجموعة واسعة من التطبيقات والوظائف. ولقد أصبحت هذه العناصر لا غنى عنها في كل جانب تقريبًا من جوانب الأنظمة العسكرية، بدءًا من المركبات الأرضية والسفن والمُسَيَّرات إلى الصواريخ والأقمار الصناعية. ولهذا السبب فإن التقدم في تكنولوجيا الاستشعار يلعب دورًا حاسمًا في تحديث القدرات الدفاعية، مع القدرة على تعزيز فعالية العمليات العسكرية بشكل عام. ويمكن لتطبيقات الاستشعار المتقدمة أن تمكن القوات العسكرية بجمع البيانات بشكل أكثر دقة وفي الوقت المناسب، وتعزيز الوعي بالأوضاع والحماية في ساحة المعركة، وتحسين دقة الاستهداف واكتشاف التهديدات، وتسهيل اتخاذ القرار في البيئات التشغيلية الدينامية.

لقد ظهرت العديد من التطورات في مجال تكنولوجيا الاستشعار للأغراض العسكرية، حيث يمثل دمج المستشعرات أحد المجالات الرئيسية للابتكار. وتسعى القوات المسلحة بشكل متزايد إلى الجمع بين مصادر استشعار متعددة للحصول على معلومات أكثر دقة وشاملة عن ساحة المعركة. وتقوم أنظمة المستشعرات المتعددة بدمج وتحليل البيانات من أنواع مختلفة من المستشعرات (على سبيل المثال، المستشعرات الصوتية والرادارية والكهربائية الضوئية وتحت الحمراء)، مما يعزز الوعي بالأوضاع situational awareness إلى مستوى يتجاوز ما يمكن تحقيقه عادة من خلال تحليل هذه المصادر بشكل فردي. وفي المركبات العسكرية الأرضية، توفر تكنولوجيا دمج المستشعرات للطاقم أو القائد رؤية شاملة بزاوية 360 درجة لمحيطه وتسهل تبادل المعلومات مع الأنظمة الأخرى.[43]

يستغل الاستشعار الكمي الحساسية الكامنة في الحالات الكمية للاضطرابات، مما لا يسمح فقط بإجراء قياسات أكثر دقة وحساسية، بل يفتح أيضًا إمكانية قياس الظواهر التي لم تكن قابلة للقياس من قبل.[44] وبإمكان الاستشعار الكمي أن يحول القدرات العسكرية. على سبيل المثال، قام الباحثون بتطوير مستشعرات كمية قادرة على اكتشاف الأشياء المخفية خلف الجدران والحواجز الأخرى، وهو ما يمكن أن يساعد في التطبيقات العسكرية مثل الاستطلاع.[45] وبالإضافة إلى ذلك، فإن تكنولوجيا الاستشعار الكمي قد تُحسّن دقة أنظمة الملاحة بالقصور الذاتي

[41] Levine and Pipikaite (2019).
[42] Giles (2019).
[43] Eshel (2022).
[44] van Amerongen (2021).
[45] برنامج التكنولوجيا الكمية الوطنية في المملكة المتحدة (بدون تاريخ).

inertial navigation systems المستخدمة في السفن والغواصات والطائرات. ومن شأن ذلك أن يعزز بشكل كبير قدرات تحديد المواقع والملاحة في البيئات التي لا تتوفر فيها خدمة النظام العالمي لسواتل الملاحة GNSS.[46]

يتم دمج المستشعرات بشكل متزايد مع تقنيات الذكاء الاصطناعي لتوفير جمع وتحليل البيانات الذكية، وبالتالي تحسين كفاءة عملية صنع القرار العسكري. وتستخدم أنظمة الرادار المعرفي قدرات التعلم الآلي للتكيف مع التغيرات في البيئة أو في سلوك الخصم.[47] وبالإضافة إلى ذلك، تم تطوير مستشعرات حيوية يمكن ارتداؤها لمراقبة العلامات الحيوية للجنود في الوقت الفعلي (على سبيل المثال، معدل ضربات القلب، ودرجة حرارة الجسم والترطيب)، بالإضافة إلى الحالة العقلية بما في ذلك مستويات التعب والتوتر. وسيكون دمج الذكاء الاصطناعي في الأنظمة المستقبلية أمرًا حاسمًا في تسريع عملية غربلة وتفسير البيانات التي يتم جمعها من الأجهزة القابلة للارتداء التي يرتديها الجنود.[48] ومن الممكن أن يساعد هذا التطور الجديد القادة في اتخاذ القرارات العسكرية ويؤدي إلى تحسين أداء الأفراد العسكريين.

بالإضافة إلى تعزيز القدرات العسكرية، فإن التقدم في تكنولوجيا الاستشعار يقدم فرصًا جديدة لتحقيق السلام والأمن الدوليين. يمكن أن تساعد تكنولوجيا الاستشعار عن بعد في مراقبة النزاعات المسلحة المستمرة والالتزام باتفاقيات السلام.[49] ويساهم استخدام المستشعرات المتقدمة أيضًا في تعزيز كفاءة اكتشاف المواد الخطرة، مثل العوامل الكيميائية والبيولوجية، الموجودة في البيئة. وتستطيع هذه التطبيقات تسهيل الكشف المبكر عن التهديدات، مما يتيح الاستجابة السريعة واتخاذ تدابير التخفيف، كما تتمتع بالقدرة على تعزيز أنظمة التحقق من نزع السلاح.

ومع ذلك، فإن استخدام المستشعرات يطرح أيضًا مجموعة فريدة من التحديات التي يجب معالجتها. تعتمد المستشعرات، وخاصة تلك التي تشارك في تبادل البيانات عبر أنظمة مختلفة، إلى حد كبير على الشبكات وبالتالي فهي عرضة للهجمات الإلكترونية. وقد تحاول الجهات الخبيثة تعطيل أنظمة الاستشعار أو التلاعب بها، مما يعرض سلامة البيانات للخطر ويؤدي إلى اتخاذ قرارات خاطئة. ومع تقدم التكنولوجيا، تكتسب المستشعرات القدرة على إنتاج كميات أكبر من البيانات في الأنظمة، وهو ما قد يؤدي إلى فترات تأخير كبيرة ويؤثر على جودة البيانات.[50] وقد يؤدي ذاك إلى إعاقة عملية اتخاذ القرار العسكري ما لم يتم تحسين بنية الشبكة. وأخيرا، ومن خلال جمع وتخزين المعلومات المتعلقة بالعسكريين والمدنيين على حد سواء، فإن تطبيقات الاستشعار قد تثير مخاوف مشروعة بشأن الخصوصية الشخصية وممارسات المراقبة.

المستشعرات: النقاط البارزة في عام 2023

- يوفر دمج المستشعرات، الذي يدمج البيانات من مصادر متنوعة (على سبيل المثال، المستشعرات الصوتية والرادارية وذات الأشعة تحت الحمراء)، وعيًا شاملاً بساحة المعركة.
- يبشر الاستشعار الكمي بنتائج إيجابية في التطبيقات العسكرية من خلال الاستفادة من حساسية الحالات الكمية للاضطرابات، مما يتيح قياسات أكثر دقة، وكشف الأشياء خلف الحواجز، وتحسين أنظمة الملاحة بالقصور الذاتي inertial navigation systems في البيئات التي لا تتوفر فيها خدمة النظام العالمي لسواتل الملاحة GNSS. ويؤدي دمج المستشعرات مع تقنيات الذكاء الاصطناعي إلى تعزيز جمع البيانات وتحليلها، مما يُحسن عملية اتخاذ القرار العسكري.
- يمكن أن تساهم تكنولوجيا الاستشعار المتقدمة في جهود الأمن الدولية من خلال المساعدة في مراقبة الصراعات المسلحة المستمرة والالتزام باتفاقيات السلام، فضلاً عن الكشف المبكر عن المواد الخطرة. ومع ذلك، فمن الضروري معالجة مخاوف الأمن السيبراني والتحديات الأخرى، بما في ذلك فترات تأخير محتملة نتيجة لزيادة حجم البيانات.

[46] Coggins et al. (بدون تاريخ).
[47] مختبر العلوم والتكنولوجيا الدفاعية في المملكة المتحدة (2022).
[48] Hamblen (2023).
[49] Avtar et al. (2021).
[50] Macri (2022).

4. الفئة الثالثة: المعالجة والحوسبة

4.1 الحوسبة السحابية

*تسهل **الحوسبة السحابية** وصول المستخدم إلى موارد الحوسبة دون الحاجة إلى صيانة البنية التحتية المحلية، فهي توفر المرونة لتوسيع نطاق الموارد مع تغير المتطلبات.*

تعمل الحوسبة السحابية بدعم من مكونات الأجهزة والبرمجيات المتكاملة للبنية التحتية السحابية.[51] في السنوات الأخيرة، عملت قدرات الحوسبة السحابية كمحفز للابتكار عبر مجموعة متنوعة من التطبيقات، بما في ذلك تحليلات البيانات الضخمة، والتعلم الآلي، والحوسبة بدون خادم، والواقع المعزز AR، والواقع الافتراضي VR والعديد من التكنولوجيا المتطورة الأخرى. وتتيح المنصات المستندة إلى السحابة الآن الاستعانة بمصادر خارجية للذكاء الاصطناعي كخدمة AIaaS، مما يسهل الوصول على نطاق واسع إلى القدرات التحويلية للذكاء الاصطناعي.[52] علاوة على ذلك، ظهرت التكنولوجيا السحابية الأصلية كنهج جديد لبناء واختبار ونشر وإدارة التطبيقات في بيئات الحوسبة السحابية، مما يوفر فوائد زيادة الكفاءة وخفض التكاليف وقابلية التوسع.[53]

تتمتع الحوسبة السحابية بالقدرة على تعزيز الابتكار في القطاع العسكري، وعلى وجه التحديد، فإن الاستفادة من تكنولوجيا الحوسبة السحابية يمكن أن تساعد في تسريع عمليات تصميم وتطوير واختبار البرمجيات للأنظمة العسكرية.[54] ويمكن أن يؤدي ذلك إلى تعزيز القدرات في التطبيقات العسكرية المتنوعة، بدءًا من الذكاء الاصطناعي والتعلم الآلي إلى تحديث البرمجيات والأمن السيبراني.[55] في التدريب العسكري، يمكن للمنصات المستندة إلى السحابة أن توفر للأفراد إمكانية الوصول إلى بيئات تدريب واقعية وغامرة بفضل التكنولوجيا الناشئة مثل الواقع الافتراضي أو الواقع المعزز. فمنذ سبتمبر 2022، تعاون الجيش البريطاني مع شركة خاصة لتطوير وتوسيع نطاق محاكاة غامرة موزعة على السحابة للحرب البرية والتي تم تصميمها لتسهيل التدريب الجماعي واسع النطاق للمستخدمين الفعليين والافتراضيين في مواقع مختلفة.[56] علاوة على ذلك، توفر الحوسبة السحابية قوة الحوسبة عالية السرعة الضرورية للتعامل مع معالجة البيانات واسعة النطاق في العمليات العسكرية. ونظرًا لتعقيد وحجم البيانات العسكرية، فإن التكنولوجيا السحابية تمكّن من نشر الأدوات التي تساعد القوات المسلحة في تحليل البيانات بشكل أكثر فعالية، مما يسمح لها باتقاء التهديدات التي تتطور بسرعة مع الحفاظ على أمنها.[57]

ومع ذلك، فإن التكنولوجيا السحابية تنطوي على تهديدات وتحديات محتملة. يثير دمج الحوسبة السحابية في العمليات العسكرية مخاوف بشأن أمن البيانات، وخاصة عندما يتعلق الأمر بمقدمي خدمات سحابية تابعين لجهات خارجية.[58] وبالإضافة إلى ذلك، يمكن للمشكلات التوصيلية، مثل ارتفاع زمن الانتظار في البيئات النائية أو الصعبة، أن تؤثر على موثوقية الخدمات المستندة إلى السحابة، وبالتالي يكون لها تأثير على الكفاءة التشغيلية واتخاذ القرارات في الوقت الفعلي. وأخيرا، قد تصبح المنافسة العالمية المتزايدة في مجال تكنولوجيا الحوسبة السحابية بمثابة حافز محتمل لزيادة التوتر الدولي، حيث إن الدول تسعى إلى تشديد ضوابط التصدير على تكنولوجيا الحوسبة السحابية المتقدمة بما يتماشى مع مصالحها الأمنية الوطنية.[59]

---

[51] للحصول على تحليل مفصل للبنية التحتية السحابية وأحدث التطورات، راجع القسم 5.3 أدناه.

[52] Marr (2023).

[53] جوجل (بدون تاريخ) وأمازون على الإنترنت (بدون تاريخ)

[54] Microsoft (2023).

[55] US Department of Defense (2023).

[56] Hadean (2022).

[57] Microsoft (2023).

[58] لمزيد من التحليل لقضايا أمن البيانات المرتبطة بالتكنولوجيا السحابية، راجع القسم 5.3 أدناه.

[59] Hayashi and McKinnon (2023).

الحوسبة السحابية: النقاط البارزة في عام 2023

- تستمر الحوسبة السحابية في تعزيز الابتكار عبر مجموعة من التطبيقات المتطورة، بما في ذلك تحليلات البيانات الضخمة، والتعلم الآلي، والحوسبة بدون خادم serverless computing، والواقع المعزز والواقع الافتراضي. وتسمح المنصات المستندة إلى السحابة حاليًا بالاستعانة بمصادر خارجية في مجال الذكاء الاصطناعي كخدمة (AIaaS)، وتسهيل وصول الجميع إلى قدرات الذكاء الاصطناعي التحويلية.
- في القطاع العسكري، يمكن للتكنولوجيا السحابية أن تسهل بيئات تدريبية واقعية وغامرة، وذلك بفضل التكنولوجيا الناشئة مثل الواقع الافتراضي أو الواقع المعزز. وتوفر الحوسبة السحابية أيضًا قوة الحوسبة عالية السرعة باعتبارها بالغة الأهمية للتعامل مع معالجة البيانات واسعة النطاق في العمليات العسكرية. ومع ذلك، فإن المشكلات التوصيلية، مثل زمن الانتظار المرتفع في البيئات البعيدة، قد تؤثر على موثوقية الخدمات المستندة إلى السحابة.

4.2 حوسبة الحافة

*تستخدم **حوسبة الحافة** نموذج الحوسبة الموزعة الذي ينقل تخزين البيانات والحوسبة إلى أقرب مصدر البيانات أو "حافة" الشبكة، بدلاً من الاعتماد على نظام مركزي قائم على السحابة.*

في حوسبة الحافة Edge computing، تتم معالجة البيانات على جهاز أو خادم محلي يقع على "حافة" الشبكة. وعندما تتطلب البيانات المعالجة في مركز البيانات السحابي المركزي، يتم نقل المعلومات الهامة فقط.[60] ونتيجة لذلك، تعمل حوسبة الحافة على تقليل زمن الانتظار وتعزيز قوة الحوسبة من خلال تخزين البيانات ومعالجتها محليًا وتخفيف الاختناقات المحتملة في الشبكات السحابية ومراكز البيانات. وتكتسب هذه المزايا أهمية خاصة بالنسبة لأجهزة الحافة التي تتطلب معالجة في الوقت الفعلي، كما هو واضح في التطبيقات مثل إنترنت الأشياء والمركبات ذاتية القيادة والواقع المعزز.

يتمتع تطوير حوسبة الحافة بالقدرة على تحويل الطريقة التي يعمل بها القطاع العسكري، وتعزيز قدرات الاتصالات ومعالجة البيانات واتخاذ القرار.[61] ويتيح نشر حوسبة الحافة في الميدان تبادل البيانات بشكل فوري بين القوات المتصلة داخل نفس شبكة الحافة، مما يسهل الاتصال والتنسيق في الوقت الفعلي. كما أنه يعمل على جلب الموارد الحسابية إلى الحافة التكتيكية للعمليات العسكرية ويقلل الاعتماد على مراكز البيانات السحابية. يمكن تحليل مجموعات البيانات الكبيرة من الميدان، مثل بيانات المستشعرات وتدفقات الفيديو للمراقبة والاستطلاع، محليًا في مواقع الحافة، مما يؤدي إلى تسريع زمن الاستجابة وتحسين الوعي بالأوضاع. وبناءً على ذلك، فإن اعتماد بنية الحافة في ساحة المعركة يمكن أن يعزز تطبيقات إنترنت الأشياء العسكرية IoMT ويسمح للأفراد العسكريين بالرد بسرعة على المواقف الخطيرة المحتملة.[62]

تضمن حوسبة الحافة توفر موارد البيانات والحوسبة في المواقع البعيدة مع التوصيلية المتقطعة بالإنترنت وحتى في البيئات التشغيلية القاسية. ويمكن أن تعمل تحليلات الذكاء الاصطناعي المتقدمة بشكل فعال على منصات الحافة عندما تكون غير متصلة بالإنترنت تمامًا في بيئات قاسية، مما يمكّن دعم المهام الحرجة مثل عمليات البحث والإنقاذ.[63] ومع ذلك، فإن تطبيقات الذكاء الاصطناعي المستخدمة على أجهزة الحافة العسكرية مثل المُسَيَّرات والأقمار الصناعية والمركبات الأرضية تواجه في كثير من الأحيان قيودًا، وقد تكون أدنى من النماذج الحديثة بسبب القيود المفروضة على سرعة المعالجة والذاكرة العاملة والطاقة.[64] وعلاوة على ذلك، قدمت خدمات أمازون ويب مؤخرًا "سنوبلايد لخدمات أمزون ويب" AWS Snowblade، وهو منتج جديد للحوسبة التطورية تم تصميمه خصيصًا للعقد الذي أبرمته

[60] مايكروسوفت أزور (بدون تاريخ).
[61] Lee et al. (بدون تاريخ).
[62] Cameron (2018).
[63] Thomas (2021).
[64] Miller and Lohn (2023).

مع وزارة الدفاع الأمريكية والمسمى "القدرة السحابية القتالية المشتركة" JWCC.[65] تتيح سنوبلايد لخدمات أمزون على الإنترنت للمستخدمين العسكريين للقدرة السحابية القتالية المشتركة JWCC تشغيل العمليات في مواقع الحافة التي قد تكون عرضة لدرجات حرارة أو اهتزازات أو صدمات شديدة.

ومع ذلك، فإن حوسبة الحافة تفرض تحديات أمنية معينة للتطبيقات العسكرية. وقد يعمل إطار عمل الحوسبة الموزعة distributed computing framework على زيادة مساحة الهجوم، مما يوفر المزيد من نقاط النهاية للهجمات السيبرانية. وتتعرض حوسبة الحافة لمجموعة من تهديدات الأمن السيبراني، بما في ذلك هجمات رفض الخدمة Denial-of-Service، وهجمات القنوات الجانبية، وهجمات حقن البرامج الضارة، وهجمات المصادقة والتفويض.[66] وقد تتعرض مرافق حوسبة الحافة أيضًا إلى الأضرار المادية، مما يؤدي إلى انقطاعات وانتهاكات للبيانات في شبكات الحافة.[67] ولمعالجة هذه الثغرات، يتم بذل جهود مستمرة لتعزيز التدابير الأمنية لأنظمة حوسبة الحافة. على سبيل المثال، أدرجت أجهزة الحافة لسنوبلايد لخدمات أمزون على الإنترنت AWS Snowblade تكنولوجيا تشفير متقدمة لضمان أمن البيانات ومنع الوصول غير المصرح به من الخصوم المحتملين.[68]

حوسبة الحافة: النقاط البارزة في عام 2023

- حوسبة الحافة قادرة على تحويل العمليات العسكرية، وتعزيز قدرات الاتصالات ومعالجة البيانات واتخاذ القرار. علاوة على ذلك، في البيئات البعيدة أو القاسية، تلعب حوسبة الحافة دورًا حاسمًا في تأمين البيانات وتوفير الموارد الحسابية اللازمة.
- تُمكّن منصات الحافة تحليلات الذكاء الاصطناعي من العمل بكفاءة دون اتصال بالإنترنت في البيئات الصعبة، مما يدعم المهام الحرجة مثل عمليات البحث والإنقاذ. ويُمكن أن تؤثر القيود المتعلقة بسرعة المعالجة والذاكرة والطاقة على تطبيقات الذكاء الاصطناعي في أجهزة التي تمنح التفوق العسكري.
- تشمل التحديات الأمنية المستمرة في مجال حوسبة التفوق العسكري المساحة المتوسعة للهجمات الإلكترونية والتعرض للأضرار المادية. ويجري حاليًا تنفيذ الجهود الجارية لتعزيز تدابير الأمن، مثل التشفير المتقدم في خدمات أمزون على الإنترنت.

4.3 الحوسبة الكمية[69]

الحوسبة الكمية *مجال ناشئ يستفيد من مبادئ ميكانيكا الكمية لمعالجة مشكلات معقدة تتجاوز قدرات الحواسيب العادية.*

ترجع إمكانية تفوق الحواسيب الكمية على الحواسيب العادية إلى ظواهر كمية فريدة، ولا سيما التراكب والتشابك، حيث يمكن للكيوبتات quantum bits (البتات الكمية)، وهي الوحدات الأساسية للمعلومات في الحوسبة الكمية، أن توجد في وقت واحد في حالات متعددة (0 و1) بسبب التراكب. وعندما تتشابك الكيوبتات، تصبح حالة الكيوبت (qubit) الواحد مرتبطة بشكل مباشر بحالة كيوبت الآخر، بغض

[65] AWS (2023).
[66] (Xiao et al. 2019).
[67] مركز التميز التعاوني للدفاع الإلكتروني التابع لمنظمة حلف شمال الأطلسي (2022).
[68] Konkel (2023).
[69] سيقدم تقرير قادم من معهد الأمم المتحدة لبحوث نزع السلاح بعنوان "الأمن الدولي في عصر الكمية" العالم الجديد: دليل تمهيدي"، تحليلاً إضافيًا لمجال الحوسبة الكمية وآثارها المتعلقة بالأمن الدولي.

النظر عن المسافة المادية بينهما. يمكن الاستفادة من التشابك الكمي لتحقيق زيادات كبيرة في سرعة الحوسبة، مما يمكّن الحواسيب الكمية من إجراء حسابات محددة بكفاءة أكبر من نظيراتها العادية.

لقد شهد مجال الحوسبة الكمية تقدمًا كبيرًا، وقد استثمرت شركات خاصة بما فيها آي بي آم وغوغل/ألفبت ومايكروسوفت بشكل كبير في البحث والتطوير المتعلق بالحواسيب الكمية العملية. على سبيل المثال، قامت شركة آي بي آم بزيادة عدد الكيوبتات على الرقيقة الواحدة بشكل مطرد. وفي ديسمبر 2023، كشفت شركة آي بي آم عن معالج كوندور Condor، الذي يحتوي على 1121 كيوبت، وهو تقدم ملحوظ عن معالج أوسبري Osprey السابق الذي يحتوي على 433 كيوبت.[70] وفي الوقت نفسه، قدمت الشركة معالج هيرون Heron، وهو أعلى معالج كمي أداءً حتى الآن، والمزود بـ 133 كيوبت عالية الجودة.[71] ومن الجدير بالذكر أن معالجات هيرون Heron لديها القدرة على الاتصال مباشرة بمعالجات هيرون الأخرى، مما يسهل إمكانية توسيع نطاق الحواسيب الكمية.[72]

ومع ذلك، وفي خضم هذه التطورات، لا يزال هذا المجال يواجه تحديات كبيرة يتعين معالجتها. ومن بين القضايا الرئيسية المعروفة ما يسمى بظاهرة فقدان التماسك decoherence، وهي ظاهرة كمية تنتج عن العزل غير الكافي لكيوبت فيزيائي عن بيئته، وهو ما قد يؤدي إلى إدخال الضوضاء في الحسابات. ومن ثم أصبح التغلب على مشكلة فقدان التماسك وتصحيح الأخطاء الكمية أمرًا بالغ الأهمية.[73] وبالإضافة إلى ذلك، وعلى الرغم من أن الأدلة الرياضية تشير إلى مزايا كمية مقارنة بالنماذج العادية، فأن الأدلة التجريبية لا تزال غير متوفرة بسبب عدم توفر الحواسيب الكمية التي تحتوي على عدد كافٍ من الكيوبتات.[74] على سبيل المثال، قدر الباحثون أن فك تشفير أحدث التكنولوجيا في ثماني ساعات سيتطلب 20 مليون كيوبت.[75]

وفي حين أن التطبيقات العملية للحوسبة الكمية لا تزال تلوح في الأفق، فإن التطورات المستقبلية المحتملة تحمل في طياتها آثارًا عميقة على الممارسات العسكرية والأمن الدولي، حيث تتمتع الحوسبة الكمية بالقدرة على إحداث ثورة في مجالات تكنولوجية متنوعة، وخاصة في تعزيز الذكاء الاصطناعي والتعلم الآلي. وغالبًا ما يعتمد نجاح خوارزميات التعلم الآلي العادية على بارامترات واسعة النطاق وبيانات تدريب كبيرة. وعلى النقيض من ذلك، يمكن للتعلم الآلي الكمي أن يقلل من العدد المطلوب من البارامترات والبيانات عن طريق الاستفادة من الحالات المتنوعة المتاحة للجسيمات الكمية.[76] لقد أظهرت الأبحاث التجريبية أن الشبكات الهجينة، التي تجمع بين ميزات كل من الحواسيب العادية والكمية، يمكن أن تحقق تدريبًا أفضل لنماذج التعلم الآلي.[77] وقد تؤدي هذه التطورات إلى تحويل تطبيقات الذكاء الاصطناعي العسكرية المستقبلية، وخاصة في تطوير أنظمة الأسلحة المستقلة القاتلة والأكثر دقة.[78]

علاوة على ذلك، يمكن للحوسبة الكمية إعادة تشكيل مشهد الأمن السيبراني، من خلال تقديم التحديات والفرص في الوقت نفسه. وتتمتع الحواسيب الكمية بالقدرة على حل بعض المشكلات الرياضية بشكل أسرع بكثير من الحواسيب العادية، مما قد يعرض للخطر أمن بعض الخوارزميات التشفيرية المستخدمة بشكل شائع (على سبيل المثال، مخططات التشفير RSA وECC). تم تطوير خوارزميات كمية قادرة على فك تشفير الاتصالات الرقمية، ولا سيما خوارزمية شور، حيث يمكن تنفيذها بمجرد توفر الحواسيب الكمية العملية.[79] ويؤدي هذا إلى ظهور ثغرات جديدة في الأمن السيبراني ويمكن أن يؤدي إلى هجمات من نوع "احصد الآن وفكّ التشفير لاحقًا" HNDL، حيث تستحوذ الجهات الخبيثة على بيانات مشفرة وحساسة الآن بقصد فك تشفيرها لاحقًا بعد الاختراقات المحتملة في تكنولوجيا فك التشفير. ويمكن أن تؤدي مثل هذه الهجمات إلى إثارة مخاوف تتعلق بالأمن القومي، مما يسمح للخصوم بالوصول إلى معلومات عسكرية حساسة.[80] وردًا على التهديدات الكمية المحتملة، تُبذل جهود مستمرة لتطوير التشفير ما بعد الكمي post-quantum cryptography. ويتضمن ذلك إنشاء أنظمة تشفير قادرة على الصمود في وجه الهجمات المستقبلية التي تشنها الحواسيب الكمية. كما توفر التكنولوجيا الكمية الناشئة، مثل

[70] Gambetta (2023).
[71] المرجع نفسه.
[72] Brooks (2023a).
[73] Lidar (2023).
[74] Brooks (2023b).
[75] المرجع نفسه.
[76] المرجع نفسه.
[77] Xu (2023).
[78] US Congressional Research Service (2023).
[79] van Amerongen (2021).
[80] US Congressional Research Service (2023).

توزيع المفاتيح الكمية (Quantum Key Distribution)[81] وتوليد الأرقام العشوائية الكمية (Quantum Random Number Generation)[82] فرصًا لتعزيز آليات التشفير وتأمين الاتصالات.

الحوسبة الكمية: النقاط البارزة في عام 2023

- لقد تم تحقيق تقدم كبير في الحوسبة الكمية. على سبيل المثال، تقوم شركة آي بي آم بزيادة عدد الكيوبتات على رقيقة واحدة بشكل مستمر، وقد وصلت إلى نقطة مهمة مع طرح معالج كوندور بسعة 1121 كيوبت في عام 2023. وفي الوقت نفسه، أطلقت الشركة معالج هيرون Heron الذي يتمتع بالقدرة على الاتصال مباشرة بمعالجات هيرون الأخرى، مما قد يسهل تعزيز قابلية التوسع.
- وقد أظهرت الأبحاث التجريبية أن الشبكات الهجينة، التي تجمع بين الحواسيب العادية والكمية، يمكنها تحقيق تدريب أفضل لنماذج التعلم الآلي. ويحمل هذا التطور آثارًا عميقة على تطبيقات الذكاء الاصطناعي العسكرية، خاصة فيما يتعلق بتطوير أنظمة الأسلحة القاتلة ذاتية التحكم الأكثر دقة.
- ومع ذلك، فإن تطوير الحوسبة الكمية يطرح تحديات كبيرة في مجال الأمن السيبراني والمعلوماتي، ولا سيما خطر هجمات "احصد الآن وفك التشفير لاحقًا " Harvest Now Decrypt Later، نظرًا لاحتمال اختراق الحواسيب الكمية العملية لخوارزميات التشفير المستخدمة على نطاق واسع. ونتيجة لذلك، هناك جهود مستمرة لتطوير التشفير ما بعد الكمي استجابة للتهديدات الكمية الناشئة.

5. الفئة الرابعة: البنية التحتية

5.1 تكنولوجيا الجيل الخامس والجيل السادس

تمثل تكنولوجيا الجيل الخامس معيارًا لشبكات الهاتف المحمول، والتي توفر اتصالات النطاق العريض المتقدمة التي تتفوق على سابقاتها، مثل 4G LTE. تشير تكنولوجيا الجيل السادس إلى التطوير المستمر لتكنولوجيا الهاتف الخلوي من الجيل السادس المصممة لتجاوز تقنية الجيل الخامس، وتوفير قدرات شبكية أكثر تقدمًا.

يتميز الجيل الحالي من البنية التحتية التوصيلية بالتقدم الكبير في تكنولوجيا الاتصالات اللاسلكية، ولا سيما التنفيذ واسع النطاق لشبكات الجيل الخامس (5G) الخلوية. تتمتع تكنولوجيا الجيل الخامس بمزايا مختلفة مقارنة بالتقنيات السابقة، وذلك بفضل الميزات الجديدة مثل تقطيع الشبكة والقدرة على العمل على طيف الموجات المليمترية mmWave، وهو نطاق عالي التردد من الطيف الراديوي في نطاق 30-300 جيجاهرتز.[83] تعمل تكنولوجيا الجيل الخامس 5G على رفع مستوى التوصيلية بشكل كبير من خلال توفير سرعات أكبر وتقليل زمن الانتظار وتعزيز موثوقية الشبكة ودعم الاتصال المتزامن لعدد أكبر من الأجهزة. ولهذه القدرات المبتكرة التي تتمتع بها تكنولوجيا الجيل الخامس دور أساسي في تلبية المتطلبات المتزايدة للابتكارات التكنولوجية، وخاصة في التطبيقات القائمة على إنترنت الأشياء، مما يتيح ربط المزيد من الأجهزة والأشياء بالشبكات.

يمكن لتكنولوجيا الجيل الخامس أن تفتح آفاقًا هائلة للتطبيقات العسكرية التحويلية، وتسهل تحسين الاتصالات والنقل السريع للبيانات وقدرات اتخاذ القرار في الوقت الفعلي على ساحة المعركة. وتتمتع هذه الأنظمة بقدرة توصيلية عالية السرعة ومنخفضة زمن الانتظار، مما يمكنها من دعم الوظائف العسكرية الحرجة، بدءًا من الاتصالات والخدمات اللوجستية إلى الاستخبارات والمراقبة والاستطلاع، فضلاً عن القيادة والتحكم. وقد أبرزت الأبحاث الحديثة ثلاثة تطبيقات عسكرية ملموسة أصبحت ممكنة بفضل تنفيذ تكنولوجيا الجيل الخامس، وهي: تتبع

[81] NATO (2022).
[82] (Argillander et al. 2023).
[83] (Gerwig and Goss. 2023).

العناصر والمعدات باستخدام العلامات الذكية لتحسين العمليات؛ والاستفادة من شبكات الجيل الخامس عالية النطاق في نقل البيانات لمجموعات بيانات الاستشعار الكبيرة؛ واستخدام اتصالات الجيل الخامس عن بعد للقيادة والتحكم لتعزيز التنسيق متعدد الجنسيات.[84] ولاستخدام تتبع العلامات الذكية في الشحنات عبر شبكة الجيل الخامس أيضًا آفاق واعدة في تعزيز جهود ضبط الأسلحة من خلال التخفيف المحتمل من المخاطر المرتبطة بتحويل الأسلحة والذخيرة التقليدية. علاوة على ذلك، يمكن أن تعمل تكنولوجيا الجيل الخامس كمحفز قوي للتطبيقات المتطورة للذكاء الاصطناعي وإنترنت الأشياء في المجال العسكري، مما يمهد الطريق لتعزيز القدرات. ويمكن لشبكات الجيل الخامس عالية السرعة تسهيل دمج الذكاء الاصطناعي من أجل معالجة فعالة لكميات هائلة من بيانات الاستشعار في ساحة المعركة. على سبيل المثال، من الممكن نقل إشارات الخصم في الوقت الفعلي من خلال شبكة الجيل الخامس الآمنة لمزيد من التحليل باستخدام خوارزميات معالجة الإشارات المتقدمة.[85]

ومع ذلك، فإن دمج تكنولوجيا الجيل الخامس يطرح مخاطر جديدة، خاصة في مجال الأمن السيبراني، فمع الارتفاع الكبير في أحجام البيانات والأجهزة المترابطة في شبكات الجيل الخامس، يمكن تضخيم نقاط الضعف الأمنية المحتملة، مما يوفر للجهات الخبيثة فرصًا متزايدة للاستغلال والتعطيل. كما أن خصائص تكنولوجيا الجيل الخامس، بما في ذلك الواجهات البينية المفتوحة وطبيعتها المستندة إلى السحابة، تُحدث أيضًا تهديدات أمنية إضافية، مما يؤدي إلى توسيع نطاق التهديدات لعمليات نشر تكنولوجيا الجيل الخامس.[86] وقد تظهر مجموعة متنوعة من تهديدات الأمن السيبراني عبر أنظمة الجيل الخامس الفرعية المتعددة، والتي تمتد من معدات مستخدمي الجيل الخامس وشبكة الوصول اللاسلكي RAN إلى الشبكة الأساسية والخدمات السحابية وحوسبة الحافة متعددة الوصول multi-access edge computing، من بين المكونات المهمة الأخرى.[87]

يجري حاليًا تطوير شبكات الجيل السادس للهاتف الخلوي، وهي تحمل وعودًا أعظم من التطورات الحالية التي شهدتها تكنولوجيا الجيل الخامس. ومن المتوقع أن تحقق المزيد من التحسينات في السرعة وزمن الانتظار والتوصيلية، فضلاً عن القدرة على تمكين مجموعة أوسع من التطبيقات التكنولوجية الجديدة. وبالمقارنة مع الأجيال السابقة من شبكات الاتصالات، فإن البحث والتطوير في مجال الجيل السادس يركز بشكل أكبر على تحقيق تغطية شاملة للشبكة "على الأرض وفي البحر وفي الجو والفضاء"، من خلال الجمع بين شبكات الهاتف الخلوي الأرضية والمنصات الجوية والأقمار الصناعية.[88] وينبغي أن توفر هذه البنية المتكاملة لشبكة الأقمار الصناعية الأرضية إمكانات كبيرة لضمان تغطية الإنترنت العالمية وتوفير دعم الاتصالات في كل مكان لإنترنت الأشياء.[89] ومن المتوقع أن يبدأ طرح تكنولوجيا الجيل السادس بحلول عام 2030 تقريبًا.[90]

تكنولوجيا الجيل الخامس والجيل السادس: النقاط البارزة في عام 2023

- يفتح التقدم الحالي في تكنولوجيا الجيل الخامس المجال أمام إمكانات تحويلية في التطبيقات العسكرية، مما يدعم الاتصالات المعززة والنقل السريع للبيانات واتخاذ القرارات في الوقت الفعلي في ساحة المعركة. ويمكن لتكنولوجيا الجيل الخامس أيضًا تسهيل دمج التطبيقات المتطورة للذكاء الاصطناعي وإنترنت الأشياء، وبالتالي تعزيز القدرات العسكرية.
- ومع ذلك، فإن إدخال تكنولوجيا الجيل الخامس يضخم نقاط الضعف المحتملة للأمن السيبراني بسبب زيادة أحجام البيانات والأجهزة المترابطة. كما أن الواجهات المفتوحة وطبيعتها المستندة إلى السحابة تخلق أيضًا مشهد تهديدات واسعة النطاق لنشر تكنولوجيا الجيل الخامس.
- تركز أعمال البحث والتطوير الجارية لشبكات الجيل السادس الخلوية على تحقيق التغطية الشاملة عبر البر والبحر والجو والفضاء من خلال شبكة أقمار صناعية أرضية متكاملة، ومن المتوقع أن يتم إطلاقها بحلول عام 2030.

[84] Lee et al. (2023).
[85] Tucker (2022).
[86] Śliwa and Suchański (2022).
[87] NATO CCDCOE (2022).
[88] Chen et al. (2023).
[89] Tirmizi et al. (2022).
[90] Kharpal (2023) and Chen et al. (2023).

5.2 إنترنت الأشياء

*يربط **إنترنت الأشياء IoT** شبكة واسعة من الأجهزة المادية والأجهزة والمركبات والأشياء الأخرى المتكاملة مع المستشعرات والبرمجيات وتوصيلية الشبكة، مما يسهل جمع البيانات وتبادلها بين الأجهزة والأنظمة. ومن خلال تمكين هذه الأجهزة من التواصل والتعاون مع بعضها البعض عبر الإنترنت أو شبكات الاتصالات الأخرى، فإن إنترنت الأشياء يخلق نظامًا بيئيًا مترابطًا يمكن مراقبته والتحكم فيه عن بعد.*

تتشابك التطورات الأخيرة في مجال إنترنت الأشياء (IoT) مع الابتكارات التكنولوجية في مجالات أخرى، ولا سيما حوسبة الحافة، وشبكات الجيل الخامس، ودمج الذكاء الاصطناعي.[91] لقد أدى ظهور حوسبة الحافة إلى تعزيز نهج أكثر محلية لمعالجة البيانات وتخزينها، مما أدى إلى تقليل زمن الانتظار بشكل فعال وتعزيز قدرات المعالجة في الوقت الفعلي لأجهزة إنترنت الأشياء.[92] وفي الوقت نفسه، ساهم طرح شبكات الجيل الخامس أيضًا في تسريع تطوير إنترنت الأشياء من خلال توفير سرعات أعلى لنقل البيانات وزمن انتقال أقل وزيادة سعة الشبكة.[93] علاوة على ذلك، فإن دمج تقنيات الذكاء الاصطناعي، وتحديدًا التعلم الآلي، يمكن أن يدعم التحليل والتفسير في الوقت الفعلي لكمية كبيرة من البيانات التي تولدها تطبيقات إنترنت الأشياء، مما يؤدي إلى اتخاذ قرارات أكثر كفاءة والأتمتة.

تتم الاستفادة بشكل متزايد من تكنولوجيا إنترنت الأشياء في الأنظمة العسكرية لتحسين العمليات وتعزيز الكفاءة، مما يسهّل التحول نحو مشهد عسكري أكثر اتصالاً واعتمادًا على البيانات. ويمكن أن يستخدم إنترنت الأشياء العسكرية (IoMT) مجموعة متنوعة من المستشعرات المنتشرة عبر مختلف المجالات، بهدف تحقيق الوعي الشامل بالأوضاع والسيطرة الفعالة في بيئات الصراع المعقدة والمتنوعة.[94] كما يمكن أن يرفع دمج شبكات الاستشعار والأنظمة غير المأهولة في إطار إنترنت الأشياء العسكرية بشكل كبير من قدرات المراقبة والاستطلاع، مما يمكن القوات العسكرية من تتبع بيئة ساحة المعركة، وإدارة المعدات والمركبات، ومراقبة الظروف الصحية للجنود.[95] ويمكن أن تعزز الاستفادة من تكنولوجيا إنترنت الأشياء/إنترنت الأشياء العسكرية دقة الاستهداف وتقلل من خطر وقوع إصابات بين المدنيين أثناء العمليات العسكرية، حيث يمكن للمستشعرات المدمجة داخل شبكة إنترنت الأشياء/إنترنت الأشياء العسكرية توجيه الأسلحة بشكل أكثر دقة إلى هدفها المقصود.[96]

علاوة على ذلك، أدت التطورات في تكنولوجيا إنترنت الأشياء/إنترنت الأشياء العسكرية أيضًا إلى تحسين أنظمة الاتصالات العسكرية بشكل كبير، حيث يسهل إنترنت الأشياء تبادل البيانات والتوصيلية بشكل سلس، وبالتالي يعزز التعاون بين القوات المشتركة وقوات التحالف وعبر المجالات المختلفة.[97] وعلاوة على ذلك، فإن دمج بروتوكولات الاتصالات الآمنة واستخدام التشفير والتوقيعات الرقمية في الأنظمة التي تدعم إنترنت الأشياء يمكن أن يحمي قنوات الاتصالات بشكل فعال، ويضمن سرية المعلومات العسكرية الحساسة وسلامتها وتوافرها.[98] ومع ذلك، فبدون وجود بروتوكولات اتصالات قوية، فإن الاعتماد واسع النطاق لتكنولوجيا إنترنت الأشياء يمكن أن يؤدي إلى إدخال تهديدات أمنية سيبرانية كبيرة للأنظمة العسكرية المترابطة. تقدم شبكات إنترنت الأشياء العسكرية (IoMT) مساحة هجوم كبير تشتمل على أجهزة إنترنت الأشياء العسكرية IoMT، وقنوات الاتصال التي تربط هذه الأجهزة، وتطبيقات الواجهة الخلفية الخاصة بإنترنت الأشياء العسكرية IoMT، بالإضافة إلى تخزين البيانات الخلفية.[99] وقد تمتد آثار العمليات السيبرانية التي تنطوي على أجهزة إنترنت الأشياء إلى ما هو أبعد من الأنظمة العسكرية، مما قد يتسبب في حدوث اضطرابات عشوائية في الأنظمة المتصلة الأخرى، بما في ذلك المرافق الطبية والمؤسسات التعليمية وغيرها من الشبكات الحساسة.[100]

---

[91] Coughlin (2023).

[92] للحصول على تحليل مفصل لحوسبة الحافة وأحدث التطورات، انظر القسم 4.2 أعلاه.

[93] للحصول على تحليل مفصل لشبكات الهاتف الخلوي من الجيل الخامس وأحدث التطورات، راجع القسم 5.1 أعلاه.

[94] Withrington (2023).

[95] Khawaja (2023).

[96] Douglass (2022).

[97] Breaking Defense (2023).

[98] Kannan et al. (2023).

[99] Withrington (2023).

[100] Renals (2021).

إنترنت الأشياء: النقاط البارزة في عام 2023

- يتم تطبيق تكنولوجيا إنترنت الأشياء بشكل متزايد في الأنظمة العسكرية لتحسين العمليات (المعروفة باسم إنترنت الأشياء العسكرية). يستخدم إنترنت الأشياء العسكرية مجموعة متنوعة من المستشعرات عبر المجالات من أجل الوعي الشامل بالأوضاع والسيطرة عليه. ويمكن للمستشعرات المدمجة في شبكة إنترنت الأشياء/إنترنت الأشياء العسكرية أيضًا تعزيز دقة الاستهداف في العمليات العسكرية، مع إمكانية تقليل مخاطر وقوع إصابات بين المدنيين.
- ومع ذلك، ففي غياب بروتوكولات اتصالات قوية، فإن الاعتماد واسع النطاق لإنترنت الأشياء في الأنظمة العسكرية قد يؤدي إلى مخاطر تتعلق بالأمن السيبراني. وتُحدث شبكات إنترنت الأشياء العسكرية مساحة هجوم كبيرة مع آثار محتملة تتجاوز الأنظمة العسكرية، مما يؤثر على القطاعات الحيوية الأخرى بما في ذلك المرافق الطبية والمؤسسات التعليمية وغيرها من الشبكات الحساسة.

5.3 البنية التحتية السحابية

*تتكون **البنية التحتية السحابية** من مكونات الأجهزة والبرمجيات الأساسية لتقديم الخدمات السحابية عبر الإنترنت. ويتضمن ذلك الأجهزة مثل الخوادم ووسائل التخزين ومكونات الشبكات ومراكز البيانات، بالإضافة إلى البرمجيات مثل برمجيات المحاكاة الافتراضية.*

توفر البنية التحتية السحابية الأساس الذي يتم بناء خدمات الحوسبة السحابية عليه وتقديمها.[101] شهدت الخدمات السحابية توسعًا في السنوات الأخيرة، حيث تلعب الشركات الخاصة دورًا حاسمًا كمقدمي خدمات سحابية (Cloud Service Providers). يشمل مقدمو الخدمات السحابية الرئيسيين: خدمات أمازون ويب AWS، ومايكروسوفت أزور Microsoft Azure، ومنصة جوجل السحابية Google Cloud، وحوسبة أوراكل السحابية Oracle Cloud، وسحابة علي بابا Alibaba Cloud. وتقدم هذه الشركات مجموعة متنوعة من الخدمات السحابية، والتي يمكن تصنيفها في ثلاث فئات رئيسية: البنية التحتية كخدمة IaaS، والمنصة كخدمة PaaS، والبرمجيات كخدمة SaaS. يواصل مقدمو الخدمات السحابية توسيع نطاق تغطية البنية التحتية السحابية الخاصة بهم بسرعة في جميع أنحاء العالم، وإنشاء حضور لهم في كل قارة.[102]

تتم الاستفادة بشكل متزايد من التكنولوجيا السحابية لتعزيز الكفاءة التشغيلية وإدارة البيانات في الإعدادات العسكرية. ولم تكتف القوات العسكرية بتطوير البنية التحتية السحابية الداخلية الخاصة بها، بل تعتمد أيضًا قدرات وخدمات السحابة التجارية من مقدمي خدمات الاتصالات الخاصة. على سبيل المثال، في ديسمبر 2022، منحت وزارة الدفاع الأمريكية عقودًا لأربعة من مزودي خدمات الاتصالات الرائدين (AWS وGoogle وMicrosoft وOracle) لدعم قدرة السحابة الحربية المشتركة التابعة لوزارة الدفاع.[103] وتتيح البنية التحتية السحابية للقوات العسكرية تخزين وإدارة كميات كبيرة من البيانات العسكرية، بدءًا من بيانات الاستخبارات والمراقبة والاستطلاع إلى المعلومات اللوجستية وغيرها من البيانات ذات الأهمية البالغة للمهام، حيث يمكن أن يسهل ذلك التواصلَ والتنسيقَ بين الأفراد والوحدات العسكرية من مواقع مختلفة.

يعد ضمان أمن البيانات أحد الاعتبارات الأساسية في نشر التكنولوجيا السحابية ضمن السياقات العسكرية، حيث غالبًا ما توفر البنية التحتية السحابية أمنًا معززًا للمعلومات الحساسة، من خلال التشفير القوي وإدارة الهوية والوصول، وغير ذلك من ميزات الأمن المتقدمة. ومن الجدير بالذكر أن الخطوة الاستباقية التي اتخذتها الحكومة الأوكرانية لنقل جزء كبير من بياناتها الهامة إلى السحابة أدت إلى رفع جاهزية

[101] للحصول على تحليل مفصل للحوسبة السحابية وأحدث التطورات، راجع القسم 4.1 أعلاه.
[102] خريطة عالمية للبنية التحتية السحابية عبر ثمانية من كبار مزودي الخدمات السحابية: https://www.cloudinfrastructuremap.com/
[103] وزارة الدفاع الأمريكية (2022).

البلاد لمقاومة الهجمات الإلكترونية غير المسبوقة.[104] وتواصل الحكومات ومقدمو خدمات الاتصالات تعزيز التدابير الأمنية للبنية التحتية السحابية الخاصة بها، بما في ذلك اعتماد نهج الثقة الصفرية zero-trust في بيئات الحوسبة السحابية.[105]

ومع ذلك، تظل البيئات السحابية، مثل غيرها من المنصات الرقمية، عرضة للمخاطر والثغرات الإلكترونية المحتملة. وقد يؤدي نقل البيانات الحساسة إلى أنظمة السحابة إلى زيادة المخاوف الأمنية، كما يتضح من حوادث أمن السحابة السابقة. ففي فبراير 2023، تم الكشف عن عدد كبير من رسائل البريد الإلكتروني العسكرية الحساسة بسبب خادم بريد إلكتروني تم إعداده بشكل غير صحيح على منصة السحابة الحكومية لمايكروسوفت أزور.[106] وعلى الرغم من أن الاستفادة من خدمات السحابة التجارية من كبار مزودي خدمات الاتصالات توفر مزايا بروتوكولات الأمن القوية والتركيزات العالية من الخبرة، فإنها تنطوي أيضًا على إمكانية وقوع حوادث تؤثر على البنية التحتية السحابية لهؤلاء المزودين والتي قد تكون لها تأثيرات واسعة النطاق.[107] وعلاوة على ذلك، سلطت اللجنة الدولية للصليب الأحمر الضوء على الانخراط المتزايد للمدنيين في العمليات الرقمية أثناء النزاعات المسلحة، مما قد يؤدي إلى زيادة استخدام البنية التحتية المدنية، بما في ذلك البنية التحتية السحابية، للأغراض العسكرية.[108] ويشكل هذا الاتجاه خطرًا متزايدًا على المدنيين والبنية التحتية المدنية، مما يقوض مبدأ التمييز المدعوم عالميا.[109]

البنية التحتية السحابية: النقاط البارزة في عام 2023

- تعتمد القوات العسكرية بشكل متزايد على البنية التحتية السحابية لتعزيز الكفاءة التشغيلية وإدارة البيانات. ففي حين يتم تنفيذ تدابير أمنية متقدمة، مثل التشفير القوي، فإن دمج بيئات السحابة في الإعدادات العسكرية يظل عرضة للمخاطر السيبرانية، كما يتضح من الحوادث الماضية.
- بالإضافة إلى ذلك، سلطت اللجنة الدولية للصليب الأحمر الضوء على الانخراط المدني المتزايد في العمليات الرقمية أثناء النزاعات المسلحة، مما قد يؤدي إلى زيادة استخدام البنية التحتية المدنية، بما في ذلك البنية التحتية السحابية، للأغراض العسكرية. ويؤدي ذلك إلى زيادة خطر استهداف المدنيين والبنية التحتية المدنية، مما يقوض مبدأ التمييز.

5.4 الاتصالات عبر الأقمار الصناعية

*تتضمن **الاتصالات عبر الأقمار الصناعية** استخدام الأقمار الصناعية لإنشاء روابط اتصال بين مواقع مختلفة على الأرض.*

تلعب أنظمة الاتصالات عبر الأقمار الصناعية دورًا حاسمًا في ضمان تغطية الإنترنت العالمية وسد الفجوة الرقمية وزيادة قدرة البنية التحتية للتوصيلية على الصمود، خاصة في المناطق التي تكون فيها شبكات الاتصالات الأرضية التقليدية محدودة أو غير متاحة. وتشكل تكنولوجيا الأقمار الصناعية جزءًا لا يتجزأ من العمليات العسكرية، كما أن التقدم المستمر في هذا المجال يواصل دفع الابتكار في قطاع الدفاع. ومن المتوقع أن يؤدي الارتفاع الحالي في نشر مجموعات الأقمار الصناعية ذات المدار الأرضي المنخفض Low Earth Orbit إلى زيادة كبيرة في عدد الأقمار الصناعية التي تدور حول الأرض. ومقارنة مع الأقمار الصناعية التقليدية المتزامنة مع الأرض، فإن مجموعات كبيرة من الأقمار الصناعية الأصغر حجمًا في المدار الأرضي المنخفض قادرة على تقليل زمن الانتظار بشكل كبير، وزيادة سعة النطاق الترددي، وتوفير تغطية عالمية متسقة. وتتولى الكيانات الخاصة بشكل أساسي زمام المبادرة في تطوير الأقمار الصناعية ذات

[104] Lewis (2023).
[105] وزارة الدفاع الأمريكية (2023).
[106] Martin et al. (2023).
[107] Maurer and Hinck (2020).
[108] اللجنة الدولية للصليب الأحمر (2023).
[109] المرجع نفسه.

المدار الأرضي المنخفض، بما في ذلك ستارلنك Starlink التابع لشركة سبايسآكس SpaceX، ووان ويب OneWeb، وبروجكت كويبر Project Kuiper التابع لأمزون.[110]

يمكن للقوات العسكرية الاستفادة من التوصيلية المحسنة التي توفرها أنظمة الأقمار الصناعية ذات المدار الأرضي المنخفض لتمكين نقل البيانات في الوقت الفعلي، وتحسين الدقة والكفاءة في العمليات العسكرية. وكما لوحظ في الصراع بين روسيا وأوكرانيا، لعبت مجموعة أقمار ستارلنك التابعة لشركة سبايسآكس دورًا حاسمًا في تسهيل الاتصالات الحرجة للأغراض المدنية والعسكرية في أوكرانيا، بما في ذلك النشر على المُسَيَّرات للمراقبة والاستطلاع.[111] وإلى جانب تطبيقات الدفاع، تتمتع مجموعات الأقمار الصناعية ذات المدار الأرضي المنخفض أيضًا بالقدرة على سد الفجوة الرقمية العالمية، من خلال توفير الإنترنت عالي السرعة في المناطق النائية أو الريفية حيث يكون من الصعب نشر البنية التحتية الأرضية التقليدية.[112]

إن دمج التكنولوجيا الكمية من بين الابتكارات البارزة الأخرى في مجال الاتصالات عبر الأقمار الصناعية، حيث يمكن لنظام توزيع المفاتيح الكمية (QKD) تأمين الاتصالات عبر الأقمار الصناعية من خلال تطبيق مبادئ الميكانيكا الكمية لإنشاء مفاتيح التشفير وتبادلها بين طرفين. ففي سبتمبر 2022، أعلنت وكالة الفضاء الأوروبية عن تعاونها مع المفوضية الأوروبية وأكثر من 20 شركة فضاء أوروبية لتقديم أول نظام توزيع المفاتيح الكمية قائم على الفضاء في المنطقة، والمعروف باسم القمر الصناعي إيجل-1 (Eagle-1).[113] وسوف يمهد هذا النظام التوصيلي المعتمد على الأقمار الصناعية الطريق أمام شبكة فائقة الأمن في أوروبا. وفي الوقت نفسه، تواصل بعض الدول بما فيها الصين[114] وسنغافورة[115] تطوير تكنولوجيا توزيع المفاتيح الكمية لتعزيز الأمن في الاتصالات عبر الأقمار الصناعية.

في حين تفتح تكنولوجيا الأقمار الصناعية إمكانيات واسعة للاتصال العالمي والاتصالات الآمنة، فإنها تثير أيضًا مجموعة من المخاوف الأمنية. ويتعلق أحد التحديات بقابلية أنظمة الأقمار الصناعية للتعرض للتهديدات السيبرانية وانتهاكات البيانات المحتملة. الاتصالات عبر الأقمار الصناعية ضرورية لنقل المعلومات الحساسة ذات الأهمية للعمليات العسكرية، حيث يمكن أن يؤدي أي اختراق للأنظمة إلى نقاط ضعف استراتيجية كبيرة. لقد أصبحت أنظمة الاتصالات العسكرية عبر الأقمار الصناعية أهدافًا للهجمات الإلكترونية، مما يؤدي إلى انقطاعات واضطرابات في الخدمات الحيوية.[116] ويمكن أن يثير نشر الأقمار الصناعية في المدار، وخاصة العدد الكبير من أقمار المدار الأرضي المنخفض، أيضًا مخاطر أمنية مثل تلك المتعلقة بحركة المرور الفضائية وزيادة الحطام الفضائي، مما يشكل تهديدًا لأمن الفضاء واستدامته.[117] وعلاوة على ذلك، ونظرًا للدور المحوري الذي تقوم به الكيانات الخاصة في مجال الاتصالات عبر الأقمار الصناعية، فإن القوات العسكرية ستواصل الاستفادة من التكنولوجيا التجارية لصالحها. ومع ذلك، فإن الاعتماد على الجهات التجارية لتوفير البنية التحتية للاتصالات الحيوية أثناء النزاعات قد أبرز المخاطر المحتملة الناشئة عن الاختلافات في الحوافز ومبادئ التشغيل وآليات المساءلة بين الكيانات الخاصة والعامة.[118]

[110] Borowitz (2022).
[111] Jayanti (2023).
[112] Marquina (2022).
[113] وكالة الفضاء الأوروبية (2022).
[114] Laursen (2022).
[115] SpeQtral (2022).
[116] Menn (2023).
[117] Mukherjee (2021).
[118] Jayanti (2023).

الاتصالات عبر الأقمار الصناعية: النقاط البارزة في عام 2023

- تشمل الابتكارات المهمة في مجال الاتصالات عبر الأقمار الصناعية زيادة كبيرة في مجموعات أقمار المدار الأرضي المنخفض LEO، بقيادة كيانات خاصة مثل ستارلنك Starlink التابع لشركة سبايساكس SpaceX، فهي لا تساعد فقط على تحسين التوصيلية العالمية ولكنها تقوم أيضًا بدور حيوي في العمليات العسكرية من خلال تسهيل الاتصالات الحرجة أثناء الصراعات. علاوة على ذلك، فإن دمج تكنولوجيا توزيع المفاتيح الكمية في أنظمة الأقمار الصناعية يمهد الطريق لتحقيق اتصالات أكثر أمانًا.
- ومع ذلك، يمكن أن تشكل الاتصالات عبر الأقمار الصناعية أيضًا تحديات أمنية، بما في ذلك نقاط الضعف بالنسبة للتهديدات السيبرانية والمخاوف بشأن حطام الفضاء. وبالإضافة إلى ذلك، ومع استمرار استفادة القوات العسكرية من تقنيات الأقمار الصناعية التجارية، فمن الأهمية بمكان تسليط الضوء على المخاطر المحتملة التي تتعلق بالاختلافات في الحوافز ومبادئ التشغيل وآليات المساءلة بين الكيانات العامة والخاصة.

6. الخلاصة

في مختلف مجالات التكنولوجيا التي تمت مناقشتها في هذه الوثيقة، ظهرت العديد من الاتجاهات والتطورات الشاملة. وعلى وجه الخصوص، فإن عملية التصغير المستمرة تُعد اتجاهًا مستمرًا في تكنولوجيا الأجهزة، مما يؤدي إلى إنشاء أجهزة صغيرة الحجم وفعالة بشكل متزايد. وقد لعبت الإنجازات الأخيرة في مجال مواد أشباه الموصلات وتكنولوجيا النانو والرقائق الدقيقة والمستشعرات أدوارًا محورية في دفع هذه النقلة التحويلية، حيث يساهم هذا الاتجاه في تسهيل الاعتماد واسع النطاق للتقنيات التمكينية في الأسلحة والأنظمة العسكرية وفي تحديث المعدات العسكرية.

ومن شأن تسخير التكنولوجيا التمكينية أن يرفع من القدرات العسكرية المختلفة بشكل ملحوظ. تشمل هذه القدرات تحسين الوعي بالأوضاع وتبسيط القيادة والسيطرة وتسريع نقل البيانات ومعالجتها وزيادة دقة الأسلحة المتقدمة. ومن الجدير بالذكر أن بعض التكنولوجيا التمكينية، مثل الرقائق الدقيقة، والحوسبة السحابية والحوسبة الكمية تعمل كمحفزات للابتكار في التطبيقات العسكرية، كما أنها تسهل دمج التكنولوجيا التحويلية مثل الذكاء الاصطناعي وقدرات التعلم الآلي، مما يضخم إمكانات التقدم في العمليات العسكرية. وعلاوة على ذلك، تتمتع التكنولوجيا التمكينية بالقدرة على تعزيز جهود الأمن الدولي من خلال تعزيز آليات التحقق من نزع السلاح ورصد الصراعات. ويمكن تحقيق ذلك، على سبيل المثال، من خلال استخدام مستشعرات متقدمة للكشف عن العوامل الكيميائية والبيولوجية في البيئة، فضلاً عن مراقبة الامتثال لاتفاقيات السلام.

ومع ذلك، فإن التطورات الأخيرة في التكنولوجيا التمكينية تنشئ أيضًا مخاطر وتحديات كبيرة؛ ففي حين أن الابتكارات في تكنولوجيا الحوسبة السحابية وتوزيع المفاتيح الكمية يمكن أن تعزز أمن الاتصالات وتخزين المعلومات ومعالجة البيانات، فإن نشر التكنولوجيات التمكينية على نطاق واسع يؤدي إلى زيادة التعرض لمخاطر الأمن السيبراني، كما يمكن أن يؤدي هذا التوسع في المشهد التكنولوجي إلى توسيع نطاق الهجوم، مما يفرض تحديات متزايدة في حماية الأنظمة العسكرية من التهديدات السيبرانية المحتملة. فبإمكان الحوسبة الكمية، على وجه الخصوص، تعطيل بروتوكولات ومعايير التشفير المستخدمة على نطاق واسع بفضل قدراتها المتوقعة على فك الشفرات.

علاوة على ذلك، فإن السعي إلى تحقيق الابتكارات المتطورة في مجال التكنولوجيا التمكينية من شأنه أن يُصعّد التوترات الدولية وتأجيج المنافسة التكنولوجية بين الدول. فقد تسعى الدول إلى فرض ضوابط صارمة على تصدير التكنولوجيا المتقدمة بما يتماشى مع مصالح أمنها الوطني. وكذلك، تشكل نقاط الضعف في سلسلة التوريد تحديًا كبيرًا في مجال التكنولوجيا التمكينية. فإن سلسلة التوريد لمكونات الأجهزة، مثل الرقائق الدقيقة، عبارة عن شبكة عالمية ومعقدة للغاية، مع تركيز كبير للتخصص في الإنتاج في مناطق معينة من العالم، فأي انقطاع في قدرات التصنيع في هذه المناطق، سواء كان ناجمًا عن التوترات الجيوسياسية أو الكوارث الطبيعية، قد يؤثر سلبًا على توافر التكنولوجيا وتكون له آثار على الأمن الدولي.

وأخيرا، فإن التطورات في العديد من مجالات التكنولوجيا تؤكد الدور الحاسم الذي يلعبه القطاع الخاص، حيث إن الشركات الخاصة تُعد محرك التقدم والابتكار في مجموعة متنوعة من التطبيقات التكنولوجية، بما في ذلك تكنولوجيا الحوسبة السحابية، والاتصالات عبر الأقمار الصناعية، والحوسبة الكمية. فقد بدأت القوات العسكرية منذ فترة طويلة تتعاون مع كيانات خاصة للاستفادة من أحدث التكنولوجيا، لكن

هذه المشاركة ليست خالية من المخاطر، فالحوادث التي تؤثر على البنية التحتية للشركات الخاصة قد يكون لها آثار واسعة النطاق، مع خطر تعرض المعلومات العسكرية الحساسة للخطر. وقد يؤدي الاعتماد على الجهات الفاعلة الخاصة أيضًا إلى مخاطر محتملة ناجمة عن الاختلافات في الحوافز ومبادئ التشغيل وآليات المساءلة بين الكيانات الخاصة والعامة.

سوف تظل التطورات في مجال التكنولوجيا التمكينية ذات آثار كبيرة على الممارسات العسكرية والأمن الدولي، ويتطلب ذلك مواصلة استكشاف آفاق الاتجاهات الجديدة والناشئة، فضلاً عن مزيد من فحص أطر الحوكمة المحتملة لاستغلال الفرص مع التخفيف من المخاطر. وفي مشاريع البحث المستقبلية، سيواصل المعهد تحديد وفحص التكنولوجيا الجديدة والناشئة، فضلاً عن التطبيقات الجديدة للتكنولوجيات الأكثر رسوخًا، وتقديم توصيات سياسية موجهة نحو العمل من أجل إدارة فئات التكنولوجيا المختلفة بشكل فعال.

المراجع

Amazon Web Services (AWS). 2023. "Announcing AWS Snowblade for U.S. Department of Defense JWCC Customers". 6 June. As of 6 December 2023: https://aws.amazon.com/about-aws/whats-new/2023/06/aws-snowblade-us-defense-jwcc-customers/

—.n.d. "What is cloud native?". As of 6 December 2023: https://aws.amazon.com/what-is/cloud-native/

Arcuri, Gregory and Sujai Shivakumar. 2022. "Moore's Law and Its Practical Implications". Center for Strategic & International Studies. 18 October. As of 6 December 2023: https://www.csis.org/analysis/moores-law-and-its-practical-implications

Argillander, Joakim et al. 2023. "Quantum Random Number Generation Based on a Perovskite Light Emitting Diode". *Communications Physics* 6, 157. As of 6 December 2023: https://doi.org/10.1038/s42005-023-01280-3

ASML. n.d. "EUV Lithography Systems". As of 6 December 2023: https://www.asml.com/en/products/euv-lithography-systems

Avtar, Ram et al. 2021. "Remote Sensing for International Peace and Security: Its Role and Implications". *Remote Sensing* 13, 3: 439. As of 6 December 2023: https://doi.org/10.3390/rs13030439

Basheer, Taha et al. 2022. "Nanotechnology and Computer Science: Trends and Advances". *Memories - Materials, Devices, Circuits and Systems* 2, October. As of 6 December 2023: https://doi.org/10.1016/j.memori.2022.100011

Borowitz, Mariel. 2022. "The Military Use of Small Satellites in Orbit". French Institute of International Relations. 4 March. As of 6 December 2023: https://www.ifri.org/sites/default/files/atoms/files/m._borowitz_military_use_small_satellites_in_orbit_03.2022.pdf

Breaking Defense. 2023. "When We Talk about What Will Enable JADC2, We're Really Talking about the Internet of Warfighting Things". 22 March. As of 6 December 2023: https://breakingdefense.com/2023/03/when-we-talk-about-what-will-enable-jadc2-were-really-talking-about-the-internet-of-warfighting-things/

Brooks, Michael. 2023a. "What's Next for Quantum Computing". MIT Technology Review. 6 January. As of 6 December 2023: https://www.technologyreview.com/2023/01/06/1066317/whats-next-for-quantum-computing/

Brooks, Michael. 2023b. "Quantum Computers: What are They Good For?". Nature. 24 May. As of 6 December 2023: https://www.nature.com/articles/d41586-023-01692-9

Cameron, Lori. 2018. "Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT". IEEE Computer Society. 1 March. As of 6 December 2023: https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt

Chandler, David L. 2022. "The Best Semiconductor of Them All?". MIT News. 21 July. As of 6 December 2023: https://news.mit.edu/2022/best-semiconductor-them-all-0721

Chen, Zhi et al. 2023. "Experts' Take on 6G Technology". China Daily. 7 August. As of 6 December 2023: https://www.chinadaily.com.cn/a/202308/07/WS64d01ddca31035260b81a8d3_1.html

Clynes, Tom. 2023. "5 Big Ideas for High-Temperature Superconductors". IEEE Spectrum. 18 September. As of 6 December 2023: https://spectrum.ieee.org/high-temperature-superconductors

Coggins, Kevin et al. n.d. "Quantum Sensing: A New Approach to Maintaining PNT in GPS-Denied Environments". US Naval Institute. As of 6 December 2023: https://www.usni.org/magazines/proceedings/sponsored/quantum-sensing-new-approach-maintaining-pnt-gps-denied

Coughlin, Tom. 2023. "9 IoT Trends to Keep an Eye on in 2023 and Beyond". TechTarget. 12 July. As of 6 December 2023: https://www.techtarget.com/iotagenda/opinion/IoT-trends-to-keep-an-eye-on

Douglass, Robert. 2022. "Introduction: IoT for Defense and National Security". In IoT for Defense and National Security (eds R. Douglass, K. Gremban, A. Swami and S. Gerali). As of 6 December 2023: https://doi.org/10.1002/9781119892199.fmatter

Eshel, Tamir. 2022. "Sensor Fusion for Land Combat Vehicles". European Security & Defence. 26 April. As of 6 December 2023: https://euro-sd.com/2022/04/articles/exclusive/25763/sensor-fusion-for-land-combat-vehicles/

European Space Agency (ESA). 2022. "Quantum Encryption to Boost European Autonomy". 22 September. As of 6 December 2023: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Quantum_encryption_to_boost_European_autonomy

Fadelli, Ingrid. 2023. "Researchers Demonstrate Scaling of Aligned Carbon Nanotube Transistors to below Sub-10 nm Nodes". Phys.org. 27 July. As of 3 January 2024: https://phys.org/news/2023-07-scaling-aligned-carbon-nanotube-transistors.html

Feldman, Andrey. 2023. "New Superconductor Could Lead to Quantum Computing Breakthrough". Advanced Science News. 18 July. As of 6 December 2023: https://www.advancedsciencenews.com/new-superconductor-could-lead-to-quantum-computing-breakthrough/

Gambetta, Jay. 2023. "The Hardware and Software for the Era of Quantum Utility is Here". IBM. 4 December. As of 11 January: https://www.ibm.com/quantum/blog/quantum-roadmap-2033

Gargeyas, Arjun. 2022. "The Role of Semiconductors in Military and Defence Technology". *Defence and Diplomacy Journal* 11, 2 (January–March). As of 6 December 2023: https://capsindia.org/wp-content/uploads/2022/07/DD-Journal-January-March-2022-Arjun-Gargeyas.pdf

Gerwig, Kate and Michaela Goss. 2023. "The Essential 5G Glossary of Key Terms and Phrases". TechTarget. 19 October. As of 6 December 2023: https://www.techtarget.com/searchnetworking/feature/The-essential-5G-glossary-of-key-terms-and-phrases

Gilchrist, Karen. 2023. "How U.S. Microchips are Fueling Russia's Military – Despite Sanctions". CNBC. 7 August. As of 6 December 2023: https://www.cnbc.com/2023/08/07/how-us-microchips-are-fueling-russias-military-despite-sanctions.html

Giles, Martin. 2019. "Cybersecurity Flaws in Chips are Still Taking Too Long to Fix". MIT Technology Review. 3 June. As of 6 December 2023: https://www.technologyreview.com/2019/06/03/135108/cybersecurity-flaws-in-chips-are-taking-too-long-to-fix/

Google. n.d. "What is Cloud Native?". As of 6 December 2023: https://cloud.google.com/learn/what-is-cloud-native

Hadean. 2022. "Hadean Awarded British Army Contract to Build Simulation Pathfinder". 14 July. As of 6 December 2023: https://hadean.com/news/hadean-awarded-british-army-contract-to-build-simulation-pathfinder/

Hamblen, Matt. 2023. "Stephanie Brown on Sensors Worn by Soldiers for Their Vital Data". Fierce Electronics. 6 June. As of 6 December 2023: https://www.fierceelectronics.com/sensors/tesla-recalls-2-million-cars-software-update-provide-visual-and-audible-alerts

Hamza, Ekhlas Kadum and Shahad Nafea Jaafar. 2022. "Nanotechnology Application for Wireless Communication System". In *Nanotechnology for Electronic Applications. Materials Horizons: From Nature to Nanomaterials*. Springer, Singapore. As of 6 December 2023: https://doi.org/10.1007/978-981-16-6022-1_6

Hayashi, Yuka and John D. McKinnon. 2023. "U.S. Looks to Restrict China's Access to Cloud Computing to Protect Advanced Technology". 4 July. As of 6 December 2023: https://www.wsj.com/articles/u-s-looks-to-restrict-chinas-access-to-cloud-computing-to-protect-advanced-technology-f771613

Hecht, Jeff. 2022. "Nanomaterials Pave the Way for the Next Computing Generation". Nature. 10 August. As of 6 December 2023: https://www.nature.com/articles/d41586-022-02147-3

IBM. 2023. "Why We Need EUV Lithography for the Future of Chips". 26 June. As of 6 December 2023: https://research.ibm.com/blog/what-is-euv-lithography

Institute of Electrical and Electronics Engineers (IEEE). n.d.-a. "Future of Semiconductor Performance". As of 6 December 2023: https://irds.ieee.org/topics/future-of-semiconductor-performance

—.n.d.-b. "Semiconductor Materials". As of 6 December 2023: https://irds.ieee.org/topics/semiconductor-materials

Intel. n.d. "The Story of the Intel® 4004". As of 6 December 2023: https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html

Jayanti, Amritha. 2023. "Starlink and the Russia–Ukraine War: A Case of Commercial Technology and Public Purpose?". Analysis & Opinions, Belfer Center for Science and International Affairs, Harvard Kennedy School. 9 March. As of 6 December 2023: https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose

Kannan, B. Maruthu et al. 2023. "Secure Communication in IoT-enabled Embedded Systems for Military Applications Using Encryption," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, pp. 1385–1389. As of 6 December 2023: https://doi.org/10.1109/ICECAA58104.2023.10212400

Khan, Saif M. and Alexander Mann. 2020. "AI Chips: What They Are and Why They Matter". Center for Security and Emerging Technology. April. As of 6 December 2023: https://cset.georgetown.edu/publication/ai-chips-what-they-are-and-why-they-matter/

Kharpal, Arjun. 2023. "Next-gen Mobile Internet – 6G – will Launch in 2030, Telecom Bosses Say, Even as 5G Adoption Remains Low". CNBC. 7 March. As of 6 December 2023: https://www.cnbc.com/2023/03/08/what-is-6g-and-when-will-it-launch-telco-execs-predict.html

Khawaja, Saleem. 2023. "How Military Uses of the IoT for Defence Applications are Expanding". Army Technology. 28 March. As of 6 December 2023: https://www.army-technology.com/sponsored/how-military-uses-of-the-iot-for-defence-applications-are-expanding/

Konkel, Frank. 2023. "AWS Unveils Edge Device for Defense Customers in Most Extreme Environments". Nextgov/FCW. 8 June. As of 6 December 2023: https://www.nextgov.com/digital-government/2023/06/aws-unveils-edge-device-defense-customers-most-extreme-environments/387302/

Kullock, René et al. 2020. "Electrically-driven Yagi-Uda Antennas for Light". *Nature Communications* 11, 115. As of 6 December 2023: https://doi.org/10.1038/s41467-019-14011-6

Kumah, Elizabeth Adjoa et al. 2023. "Human and Environmental Impacts of Nanoparticles: A Scoping Review of the Current Literature". *BMC Public Health* 23, 1059. As of 6 December 2023: https://doi.org/10.1186/s12889-023-15958-4

Laursen, Lucas. 2022. "As China's Quantum-Encrypting Satellites Shrink, Their Networking Abilities Grow". IEEE Spectrum. 25 August. As of 6 December 2023: https://spectrum.ieee.org/satellite-qkd-china

Lee, Ki et al. n.d. "Decentralized Decision Making at the Tactical Edge". Booz Allen. As of 6 January 2024: https://www.boozallen.com/s/insight/blog/decentralized-decision-making-at-the-tactical-edge.html

Lee, Mary et al. 2023. "Opportunities and Risks of 5G Military Use in Europe". Santa Monica, CA: RAND Corporation. As of 6 December 2023: https://www.rand.org/pubs/research_reports/RRA1351-2.html

Lee, Sukbae et al. 2023a. "The First Room-Temperature Ambient-Pressure Superconductor". arXiv. 22 July. As of 6 December 2023: https://arxiv.org/abs/2307.12008

—. 2023b. "Superconductor Pb10−xCux(PO4)6O Showing Levitation at Room Temperature and Atmospheric Pressure and Mechanism". arXiv. 22 July. As of 6 December 2023: https://arxiv.org/abs/2307.12037

Levine, Edlyn V. and Algirde Pipikaite. 2019. "Hardware is a Cybersecurity Risk. Here's What We Need to Know". World Economic Forum. 19 December. As of 6 December 2023: https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/

Lewis, James Andrew. 2023. "Accelerating Federal Cloud Adoption for Modernization and Security". Center for Strategic & International Studies (CSIS). 28 July. As of 6 December 2023: https://www.csis.org/analysis/accelerating-federal-cloud-adoption-modernization-and-security

Lidar, Daniel. 2023. "A Scientist Explains an Approaching Milestone Marking the Arrival of Quantum Computers". Phys.org. 20 November. As of 6 December 2023: https://phys.org/news/2023-11-scientist-approaching-milestone-quantum.html

Macri, Kate. 2022. "Army is Modernizing Sensors for Data-Driven Decision-Making". GovCIO Media & Research. 4 March. As of 6 December 2023: https://governmentciomedia.com/army-modernizing-sensors-data-driven-decision-making

Marquina, Claudia. 2022. "How Low-Earth Orbit Satellite Technology Can Connect the Unconnected". 18 February. As of 6 December 2023: https://www.weforum.org/agenda/2022/02/explainer-how-low-earth-orbit-satellite-technology-can-connect-the-unconnected/

Marr, Bernard. 2023. "The 10 Biggest Cloud Computing Trends In 2024 Everyone Must Be Ready For Now". Forbes. 9 October. As of 6 December 2023: https://www.forbes.com/sites/bernardmarr/2023/10/09/the-10-biggest-cloud-computing-trends-in-2024-everyone-must-be-ready-for-now/?sh=7ab779e66d67

Martin, Peter et al. 2023. "Pentagon and Microsoft Are Investigating Leak of Military Emails". Bloomberg. 22 February. As of 6 December 2023: https://www.bloomberg.com/news/articles/2023-02-22/pentagon-and-microsoft-investigating-leak-of-military-emails

Maurer, Tim and Garrett Hinck. 2020. "Cloud Security: A Primer for Policymakers". Carnegie Endowment for International Peace. August. As of 6 December 2023: https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf

Menn, Joseph. 2023. "Cyberattack Knocks Out Satellite Communications for Russian Military". *Washington Post*. 30 June. As of 6 December 2023: https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/

Microsoft. 2023. "BAE Systems and Microsoft Join Forces to Equip Defence Programmes with Innovative Cloud Technology". 14 April. As of 6 December 2023: https://news.microsoft.com/en-gb/2023/04/14/bae-systems-and-microsoft-join-forces-to-equip-defence-programmes-with-innovative-cloud-technology/

Microsoft Azure. n.d. "What is Edge Computing?" As of 6 December 2023: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-edge-computing

Miller, Kyle and Andrew Lohn. 2023. "Onboard AI: Constraints and Limitations". Center for Security and Emerging Technology (CSET). August. As of 6 January 2024: https://cset.georgetown.edu/publication/onboard-ai-constraints-and-limitations/

MIT Technology Review Insights. 2023. "Multi-die Systems Define the Future of Semiconductors". 31 March. As of 6 December 2023: https://wp.technologyreview.com/wp-content/uploads/2023/03/Synopsys-Report-v6.pdf

Moore, Samuel K. 2022. "3 Ways 3D Chip Tech Is Upending Computing". IEEE Spectrum. 16 March. As of 6 December 2023: https://spectrum.ieee.org/amd-3d-stacking-intel-graphcore

Mukherjee, Supantha. 2021. "Should We be Worried about Space Debris? Scientists Explain". World Economic Forum. 24 November. As of 6 December 2023: https://www.weforum.org/agenda/2021/11/space-debris-satellite-international-space-station/

National Centre of Competence in Research (NCCR). 2021. "Superconductivity, High Critical Temperature Found in 2D Semimetal Tungsten Nitride". Phys.org. 5 May. As of 6 December 2023: https://phys.org/news/2021-05-superconductivity-high-critical-temperature-2d.html

NATO. 2022. "Using Quantum Technologies to Make Communications Secure". 27 September. As of 6 December 2023: https://www.nato.int/cps/en/natohq/news_207634.htm

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2022. "Military Movement: Risks from 5G Networks". Research Report. As of 6 December 2023: https://ccdcoe.org/uploads/2022/06/Report_Military-Movement-Risks-from-5G-Networks.pdf

Pedram, Massoud. 2023. "Room-Temperature Superconductors Could Revolutionize Electronics – An Electrical Engineer Explains the Materials' Potential". The Conversation. 28 March. As of 6 December 2023: https://theconversation.com/room-temperature-superconductors-could-revolutionize-electronics-an-electrical-engineer-explains-the-materials-potential-201849

Ray, Paresh et al. 2009. "Toxicity and Environmental Risks of Nanomaterials: Challenges and Future Needs". *Journal of Environmental Science and Health,* Part C, 27:1, 1–35. As of 6 December 2023: https://doi.org/10.1080/10590500802708267

Renals, Pete. 2021. "Future Developments in Military Cyber Operations and Their Impact on the Risk of Civilian Harm". ICRC Humanitarian Law & Policy. 24 June. As of 6 December 2023: https://blogs.icrc.org/law-and-policy/2021/06/24/future-military-cyber-operations/

Roa, Carlos. 2023. "Have We Created the Philosopher's Stone? Policymakers Should Care about Room-Temperature Superconductors". *National Interest*. 2 August. As of 6 December 2023: https://nationalinterest.org/feature/have-we-created-philosopher%E2%80%99s-stone-policymakers-should-care-about-room-temperature

Rowland, Clare E. et al. 2016. "Nanomaterial-Based Sensors for the Detection of Biological Threat Agents". *Materials Today*, 19, 8, October. As of 6 December 2023: https://doi.org/10.1016/j.mattod.2016.02.018

Ryugen, Hideaki. 2023. "TSMC to Make Cutting-edge 2-nm Chips at New Plant in Southern Taiwan". *Nikkei Asia*. 10 August. As of 6 December 2023: https://asia.nikkei.com/Business/Tech/Semiconductors/TSMC-to-make-cutting-edge-2-nm-chips-at-new-plant-in-southern-Taiwan

Samsung. 2022. "Samsung Begins Chip Production Using 3nm Process Technology with GAA Architecture". As of 6 December 2023: https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture

SpeQtral. 2022. "SpeQtral Announces SpeQtral-1 Quantum Satellite Mission for Ultra-Secure Communications". 9 February. As of 6 December 2023: https://speqtralquantum.com/newsroom/speqtral-announces-speqtral-1-quantum-satellite-mission-for-ultra-secure-communications

Shilov, Anton. 2023. "The Golden Age of Custom Silicon Draws Near". EE Times. 26 July. As of 6 December 2023: https://www.eetimes.com/the-golden-age-of-custom-silicon-draws-near/

Śliwa, Joanna and Marek Suchański. 2022. "Security Threats and Countermeasures in Military 5G Systems," 2022 24th International Microwave and Radar Conference (MIKON), Gdansk, Poland, pp. 1-6. As of 6 December 2023: https://doi.org/10.23919/MIKON54314.2022.9924818

Taiwan Semiconductor Manufacturing Company (TSMC). n.d. "3nm Technology". As of 6 December 2023: https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_3nm

Thomas, Arthur. 2021. "AI at the Tactical Edge for Search & Rescue Operations". Microsoft. 22 June. As of 6 December 2023: https://www.microsoft.com/en-us/industry/blog/government/2021/06/22/ai-at-the-tactical-edge-for-search-rescue-operations/

Tirmizi, Syed Bilal Raza et al. 2022. "Hybrid Satellite–Terrestrial Networks toward 6G: Key Technologies and Open Issues". Sensors 22, no. 21: 8544. https://doi.org/10.3390/s22218544

Tucker, Patrick. 2022. "How Will the Military Use 5G? A New Drone Experiment Offers Clues". Defense One. 28 September. As of 6 December 2023: https://www.defenseone.com/technology/2022/09/how-will-military-use-5g-new-drone-experiment-offers-clues/377745/

UK Defence Science and Technology Laboratory. 2022. "Sensing: Defence Science and Technology Capability". 31 March. As of 6 December 2023: https://www.gov.uk/guidance/sensing-defence-science-and-technology-capability

UK National Quantum Technologies Programme. n.d. "Look Around Corners with the Quantum Periscope". As of 6 December 2023: https://uknqt.ukri.org/wp-content/uploads/2021/10/Look-Around-Corners-With-The-Quantum-Periscope.pdf

United Nations General Assembly (UNGA). 2023. "Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts". UN document A/78/268, 1 August.

US Congressional Research Service. 2023. "Defense Primer: Quantum Technology". 25 October. As of 6 December 2023: https://crsreports.congress.gov/product/pdf/IF/IF11836

US Department of Defense. 2022. "Department of Defense Announces Joint Warfighting Cloud Capability Procurement". 7 December. As of 6 December 2023: https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/

—. 2023. "DOD Makes Headway on Cloud Computing". 29 March. As of 6 December 2023: https://www.defense.gov/News/News-Stories/Article/Article/3345260/dod-makes-headway-on-cloud-computing/

US National Nanotechnology Coordination Office. n.d. "What Is So Special about "Nano"?". As of 6 December 2023: https://www.nano.gov/about-nanotechnology/what-is-so-special-about-nano

van Amerongen, Michiel. 2021. "Quantum Technologies in Defence & Security". NATO Review. 3 June. As of 6 December 2023: https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html

Withrington, Claire. 2023. "The Internet of Military Things". The Cove. 24 August. As of 6 December 2023: https://cove.army.gov.au/article/internet-military-things

Xiao, Yinhao et al. 2019. "Edge Computing Security: State of the Art and Challenges," in *Proceedings of the IEEE* 107, n8, pp. 1608–1631, August. As of 6 December 2023: https://doi,org/10.1109/JPROC.2019.2918437

Xu, Tammy. 2023. "Better Machine-Learning Models with Quantum Computers". IEEE Spectrum. 15 November. As of 6 December 2023: https://spectrum.ieee.org/quantum-machine-learning-terra-quanta