Security Policy Papers
أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp
ورقة تحليل سياسات أمنية

أثر التقنيات الناشئة في الأمن الصناعي

The Effect of Emerging Technologies on Industrial Security

المخرجات الرئيسة:

- تسهم التقنيات الناشئة في دفع عجلة تطور الأمن الصناعي، عبر توفير أنظمة مراقبة متكيفة مع المتغيرات البيئية والتهديدات الأمنية، مع إمكانية تطويرها إلى نماذج قادرة على التدخل المباشر عند وقوع حوادث صناعية، مما يمهد الطريق لحلول مصممة لتلبية احتياجات مختلف المواقع الصناعية.
- تحقيق توازن دقيق بين الابتكار والمسؤولية يمثل حجر الأساس لمستقبل الأمن الصناعي؛ حيث يتقاطع تطور التقنيات الناشئة مع التحديات العملية والخبرة البشرية، وهو ما يعزز من مستويات الحماية والاستجابة الفعالة.
- في مواجهة التهديدات الأمنية، تؤدي التقنيات الناشئة دورًا محوريًّا في تقليص زمن الاستجابة، من خلال رصد مصدر الاختراق بسرعة، مما يتيح التدخل الفوري والحد من الأضرار المحتملة.

المستخلص

تتناول هذه الورقة الإسهامات الإيجابية للتقنيات الناشئة في مجال السلامة والأمن الصناعي، وتأثيرها في بيئات التشغيل، مع تسليط الضوء على أمثلة لأجهزة الاستشعار والمحاكاة، إضافةً إلى تطبيقاتها الأمنية وتأثيرها، مع استعراض مميزاتها وأهميتها في الكشف الاستباقي عن المهددات التي تواجه المنشآت الصناعية.

كما تطرقت الورقة إلى المخاطر المرتبطة بالطائرات المُسيَّرة، والروبوتات، والتزييف العميق، والشبكة المظلمة، والتحديات المترتبة عليها، مع استعراض سُبل مواجهتها.

Abstract

This paper explores the positive contributions of emerging technologies in the field of industrial safety and security, and their impact on operational environments. It highlights examples of sensors and simulations, along with their security applications and effects. The paper also reviews their features and importance in proactively detecting threats faced by industrial facilities.

Furthermore, the paper addresses the risks associated with drones, robots, deepfakes, and the dark web and the challenges they pose. It presents an overview of strategies to tackle these issues.

وقدمت الورقة بعض التوصيات، مؤكدةً ضرورة تبني سياسات فعالة لتعزيز الوعي في استخدام التقنيات الناشئة في مجال الأمن الصناعي. كما شددت على أهمية أن تكون هذه التقنيات مصنوعة أو مطورة محليًّا، لضمان فعاليتها في حال وقوع هجوم إلكتروني، مع اعتماد سياسات استباقية لاحتواء المخاطر والتهديدات المحتملة.

كذلك، أكدت الورقة ضرورة تعزيز قدرات رجال الأمن الصناعي؛ لتمكينهم من التصدي لهذه التهديدات، إلى جانب الارتقاء بمستوى البيانات والمعلومات التقنية، وتطوير الكفاءات العربية من خلال الدورات التدريبية الداخلية والخارجية، وإجراء المزيد من الدراسات والبحوث، مع العمل على وضع دليل موحد لتنظيم هذا المجال.

The paper offers some recommendations, emphasizing the need for effective policies to raise awareness about the use of emerging technologies in industrial security. It stresses the importance of having these technologies manufactured or developed locally to ensure their effectiveness in the event of a cyberattack. Proactive policies to contain potential risks and threats are also advocated.

Additionally, the paper highlights the need to enhance the capabilities of industrial security personnel to enable them to counter these threats. It suggests improving the level of technical data and information, developing Arab competencies through internal and external training courses, conducting further studies and research, and working towards a unified guide to regulate this field.

المقدمة

تُعَدُّ التقنيات الناشئة، كما يسميها الخبراء، من أبرز التطورات الحديثة التي شهدها العالم في مجال التكنولوجيا الإلكترونية؛ حيث أحدثت تغييرات جوهرية في أساليب العمل والتعامل في مختلف مجالات الحياة. وقد امتد تأثير هذه التقنيات ليشمل قطاع الأمن الصناعي، الذي يُعَدُّ أحد الأعمدة الأساسية لضمان سلامة الإنسان في بيئات العمل المختلفة. وعلى الرغم من التقدم العلمي في مجال الصناعة، فإن المخاطر الصناعية تبقى هاجسًا يهدد أمن الأفراد وسلامتهم.

إن التقنيات الناشئة لها آثار عميقة في مسار الأمن الصناعي، ووجود هذه التقنيات، على الرغم من فوائدها في تقدم الصناعة، إلا أن مخاطرها قد تزايدت مع نشوئها. وهو أمر متوقع مع حاجة الإنسان المتنامية إلى التقنيات الحديثة في شتى مناحي الحياة، وبالذات في مجال الصناعة. لذلك، فإن الكثير من المخاطر قد تولَّدت واستُحدثت، على الرغم من كونها لم تكن معروفة قبل اكتشاف هذه التقنيات.

لذلك، وإزاء هذه المخاطر الصناعية المتزايدة نتيجة لهذه التقنيات الناشئة، كان لا بد من التعرف على هذه المخاطر المتجددة، وكيفية التصدي لها، والتقليل من آثارها، والوقاية منها.

إنَّ العالمَ العربيَّ يعيش، مثل بقية العالم، المحنةَ ذاتها فيما يتعلق بالمخاطر الصناعية المتعددة بعد الهيمنة الصناعية. وعلى الرغم من الدور البارز الذي تؤديه التقنية في تقدم الصناعة وتسريع العملية الإنتاجية بطريقة غير مسبوقة، إلا أنها في الوقت نفسه تمثل مخاطر جديدة وغير معروفة من قبل، الأمر الذي يتطلب العمل على مواجهة هذه المخاطر التقنية، التي ربما يكون التصدي لها أيضًا عبر تقنيات مقابلة، لتجنبها قدر الإمكان.

وتقع السلامة والأمن الصناعي على مفترق طرق تكنولوجي؛ حيث يعيد الابتكار تعريف نماذج الحماية والمراقبة التقليدية. ويوفر التقدم في التقنيات الناشئة، مثل: الذكاء الاصطناعي، ودمج البيانات، والروبوتات المستقلة، فرصًا غير مسبوقة لسلامة المواقع الصناعية. وتحاول هذه الورقة عرض بعض هذه التطورات، وتسليط الضوء على تأثيراتها وتطبيقاتها العملية والتحديات التي تطرحها.

لذلك، أصبح من الأهمية إجراء دراسة علمية لآثار تلك التقنيات الناشئة في الأمن الصناعي، وإيجاد وسائل تأمين حديثة ضد المخاطر الصناعية؛ إذ لم يعد الإنسان في مأمن من المخاطر الصناعية، سواء تلك المرتبطة بالبيئة الملوثة أو الناتجة عن المنتجات الصناعية.

وتسعى هذه الورقة إلى استعراض تأثير التقنيات الناشئة في الأمن الصناعي، بمفهومه الحديث والشامل، سواءً أكان ذلك إيجابًا أم سلبًا، وذلك من خلال تحديد نوعية المخاطر وطبيعتها، ثم التعرف على مخاطرها الحقيقية، والتطرق إلى طرق الوقاية منها، وإيجاد الحلول المناسبة للتصدي لهذه المخاطر الناشئة عن هذه التقنيات في مجال الأمن الصناعي.

كما أنها ستحاول إيجاد الأسس والقواعد الرئيسة لإصدار دليل الأنظمة والتعليمات الخاصة بالأمن الصناعي، في إطار مفهومه الحديث.

التقنيات الناشئة ومجالات الأمن الصناعي والسلامة

إن الأمن الصناعي يرمي إلى إيجاد البرامج المناسبة؛ لتلافي ما يمكن أن يؤثر، بطريقة أو بأخرى، في سلامة العاملين والممتلكات وسير العملية الإنتاجية، وذلك عن طريق متخصصين في هذا المجال تتوافر فيهم الخبرة والكفاءة؛ لتصميم هذه البرامج وتحقيق الهدف المنشود، ألا وهو توفير جميع أساليب الحماية الوقائية (أبو الليف، 1996).

ومن مهام الأمن الصناعي تحديد وتحليل المخاطر الأمنية ومخاطر السلامة، بالإضافة إلى وضع جميع الترتيبات والإجراءات والاستعدادات والحلول المناسبة والضرورية، مع مراعاة تكامل هذه الإجراءات بعضها مع بعضٍ.

وبما أن هذا العصر يمكن أن نُسَمِّيه عصر التقنيات الناشئة بمختلف تسمياتها، كالذكاء الاصطناعي وغيره، فإن هذه التقنيات الحديثة تؤدي أدوارًا مهمة ومميزة في الحماية التقنية للمنشآت الصناعية، والتي لم تكن متوافرة من قبل. كما أنها تُستخدم لتوسيع نطاق الكادر الأمني وتعزيز رؤيته، حيث ترفع من قدرته وتُهَيِّئه آليًّا لأي مخاطر تتطلب المزيد من الانتباه لتفعيل الإجراءات المناسبة لمنع وإيقاف هذه المخاطر. ويمكن تصنيف المتطلبات الأمنية التقنية إلى عدة تصنيفات (أبو شامة، ودماس، 2019).

ولتحديد مدى إسهام التقنيات في التنبؤ بالمخاطر والمحاذير، وتسريع الإجراءات، والقدرة على اكتشاف التهديدات بسرعة أكبر من السابق، يمكن الإشارة إلى بعض الإسهامات التالية.

ومع تطبيق معايير السلامة في المصانع، ظهرت الحاجة إلى إيجاد حلول بديلة تُطبق هذه المعايير بشكل أسرع وأكثر دقة، وذلك للمحافظة على سلامة العمال وسلامة بيئة العمل.

وعلى عكس الأشخاص الذين قد يتعرضون للأخطاء المهنية والمخاطر المختلفة، مثل: الأخطار الكيميائية، والحرائق، والانفجارات، وغيرها، تتمتع

الآلة بقدرة هائلة على تحمل هذه المخاطر من خلال التقنيات الحديثة. حيث يمكن اكتشاف الأوقات التي لا يلتزم فيها العاملون بمعايير السلامة، والإبلاغ عن الحوادث بسرعة، والتعرف على الصوت والصورة والمواقف المختلفة. كما يمكن للآلة تتبع سير العمل والتنبؤ بالحوادث والمواقف الخطرة من خلال تحليل البيانات، والكشف عن الأخطاء باستخدام الكاميرات الذكية، والإبلاغ عنها في الوقت المناسب.

كذلك، يمكن للذكاء الاصطناعي المشاركة في مراقبة أوقات الراحة للعمال وضمان سلامتهم، بالإضافة إلى إدراك المخاطر بشكل استباقي، وتحسين استجابة الموظفين أثناء وقوع الخطر.

ويمكن حصر مزايا هذه التقنيات في مجال الأمن الصناعي في: التغلب على المشكلات المعقدة، واكتشاف الاحتيال، والتشخيص الطبي لإصابات العمل، وزيادة كفاءة العمل عبر التشغيل المستمر على مدار الساعة طوال الأسبوع، وتنفيذ المهام اليدوية دون أخطاء، وتوظيف الموارد البشرية في مجالات أخرى، والقدرة على اتخاذ قرارات أكثر ذكاءً، وتحليل البيانات بسرعة تفوق قدرة البشر، حيث يمكن التنبؤ بالبيانات واقتراح أفضل مسار مستقبلي للعمل الصناعي. وعادةً ما تُستخدم هذه التقنيات (منذ فترة) لتوسيع نطاق الكادر الأمني؛ حيث تعمل على تعزيز القدرة الأمنية، والتنبيه آليًّا إلى أي حالة مشبوهة تتطلب مزيدًا من الانتباه.

الإسهامات الإيجابية للتقنيات الناشئة:

المراقبة على المنشآت الصناعية

تساعد التقنيات الناشئة في مراقبة المنشآت الصناعية؛ حيث تُستخدم الطائرات دون طيار (الدرونز) والكاميرات المزودة بتقنيات الذكاء الاصطناعي للمراقبة، مما يوفر تغطية واسعة النطاق للمناطق الحيوية. وفي مجال الأمن الصناعي، يمكن برمجتها لتحديد التهديدات، بما في ذلك التهديدات الداخلية. كما تتيح البيانات التي تجمعها هذه التقنيات اتخاذ القرارات المناسبة، وتحديد المخاطر، وتحسين بروتوكولات السلامة، وتعزيز مراقبة المواقع الخطرة، وضمان الامتثال للمعايير التنظيمية. إن تنفيذ هذه الأدوات يوفر الأمان للمراقبة، إلى جانب الاستجابة السريعة لحالات الطوارئ، مما يقلل من الحاجة إلى القوى العاملة، ويحسن ربحية الأعمال. ومع التقدم المستمر، من المتوقع أن تسهم الطائرات المُسَيَّرة بشكل أكبر في تعزيز عمليات التفتيش الصناعي.

ويشير هنا المفهوم الشمولي إلى تحليل وإدارة مجموعات البيانات الضخمة التي يتم إنشاؤها من مصادر مختلفة في البيئات الصناعية؛ إذ توفر هذه البيانات القادمة من أجهزة الاستشعار، والسجلات، وأنظمة المراقبة، والمصادر الخارجية، رؤيةً تفصيليةً لظروف العمل في المؤسسات الصناعية والمخاطر المحتملة التي قد تتعرض لها.

تحليل وتسريع المعلومات الأمنية

تؤدي التقنيات الناشئة دورًا مهمًّا في تحليل المعلومات الأمنية الخاصة بالمصانع، وتسريع عمليات اتخاذ القرار، واقتراح الحلول باستخدام تقنيات الذكاء الاصطناعي.

إدارة البيانات الأمنية بكفاءة

نظرًا لحجم البيانات الكبير الذي يتم نقله يوميًّا بين العملاء والمصنع، وبين الأجهزة والشبكات، فإنه من الصعب على محللي الأمن السيبراني فحص كل جزء من البيانات يدويًّا للبحث عن المخاطر المحتملة. لذا، يُعدُّ الذكاء الاصطناعي الأداة الأكثر كفاءة لاكتشاف التهديدات التي قد تمر كنشاط يومي غير ملحوظ؛ إذ يمكنه فرز وتحليل كميات ضخمة من البيانات، وتتبع حركة المرور داخل المصانع بشكل آلي، وتقديم تحليلات دقيقة عن أنشطة الخوادم. كما يتمتع الذكاء الاصطناعي بالقدرة على التعرف على أي مخاطر قد تكون مختبئة ضمن البيانات الخاصة بالمنشأة الصناعية.

تقليل وقت الاستجابة

تمتلك التقنيات الناشئة القدرة على اكتشاف التهديدات بسرعة، مما يُعَدُّ أمرًا بالغ الأهمية. فالاعتماد على العنصر البشري وحده قد يستغرق وقتًا أطول، وقد لا يحقق أفضل النتائج. بينما تستطيع التقنيات الناشئة مسح كميات هائلة من البيانات في وقت واحد، وتحديد التهديدات الإلكترونية لحظيًّا، مما يسهم في تسريع عمليات الاستجابة، وتحقيق أعلى مستويات الأمان داخل المصانع.

التنبؤ بالتهديدات المستقبلية

نظرًا للكم الهائل من البيانات التي تتم معالجتها يوميًّا في المصانع، يصبح التنبؤ بالتهديدات المستقبلية أمرًا صعبًا على المحللين. ولكن، بفضل قدرة التقنيات الناشئة على تحليل كميات ضخمة من البيانات في وقت واحد، يمكنها اكتشاف أي نشاط ضار أو تهديد محتمل في وقت مبكر، مما يسمح باتخاذ إجراءات وقائية لمنع وقوع المخاطر. ويُعدّ هذا الأمر مفيدًا في تقليل الهدر في الوقت والموارد، وتحسين كفاءة الأيدي العاملة، وضمان جاهزية المنشآت لمواجهة التهديدات الأمنية بشكل استباقي.

تعزيز الجهد اليدوي في اكتشاف التهديدات

يمكن للتقنيات الناشئة تحسين الجهود المبذولة لاكتشاف التهديدات؛ حيث تعتمد على البيانات السابقة للهجمات الأمنية، وتستخدمها لتحسين استجابة الأجهزة الأمنية، مما يرفع من كفاءة التصدي للهجمات المستقبلية.

تأثير التقنيات الناشئة في سلامة بيئات التشغيل الصناعية:

أطلقت الثورة التكنولوجية العنان لتغيرات كبرى وغير مسبوقة في المشهد الصناعي؛ حيث أعادت تعريف النهج المتبع في التعامل مع أمن بيئات التشغيل الصناعية. وفي هذا السياق، برزت التقنيات الناشئة كعناصر أساسية، ليس فقط لتحسين كفاءة الأنظمة التقليدية، بل أيضًا لفتح الباب أمام تقنيات متطورة لمعالجة نقاط الضعف في حماية الشركات الصناعية.

وتهدف السلامة الصناعية إلى تقليل وإدارة المخاطر في البيئات الصناعية، مثل: المصانع والمنشآت، ويمتد ذلك إلى جميع المستويات داخل المنشأة لضمان الحماية الشاملة للأشخاص. ويتمثل الهدف الرئيس في منع

الإصابات والحوادث في العمل، من خلال اتخاذ تدابير وقائية لحماية العمال والمرافق، بالإضافة إلى إدارة المخاطر الاستباقية، التي تشمل السلامة الصناعية مع الحفاظ على البيئة، وضمان معايير السلامة والصحة المهنية.

ومع ظهور تحديات جديدة تتعلق بسلامة بيئة العمل الصناعي، وفي ظل تعزيز الكفاءات التشغيلية، أصبحت المنشآت تستهدف رفع معايير السلامة في أماكن العمل وحمايتها من أي اعتداء، مما يُمهد للتكامل الناجح للتكنولوجيا الناشئة في بيئات التشغيل الصناعية المتطلبة.

التقنيات الناشئة التي تؤثر في عمليات التصنيع الصناعي:

هناك العديد من التقنيات الناشئة التي تؤدي دورًا رئيسًا في تحسين عمليات التصنيع الصناعي، ومن أبرزها:

1. أجهزة الاستشعار المتصلة بإنترنت الأشياء

تُعد أجهزة استشعار السلامة الصناعية أدوات أساسية في مجال السلامة الصناعية، بفضل نظام الكشف غير التلامسي، الذي يتفاعل حصريًّا مع المتغيرات والتناقضات الموجودة في المناطق الحرجة. وتكمن أهمية هذه الأجهزة في سرعة تركيبها وسريتها، مما يجعلها أداة فعالة في منع المخاطر، خاصة في الحالات التي يصعب فيها رصد الظروف غير الآمنة بالعين المجردة.

وتبرز فائدة هذه الأجهزة في سيناريوهات خطرة، مثل: تسرب الغازات السامة؛ حيث يُعد الاكتشاف المبكر أمرًا بالغ الأهمية لتجنب العواقب الوخيمة. كما يمكنها مراقبة مجموعة متنوعة من العوامل، بما في ذلك: الأجواء الخطرة، ودرجات الحرارة القصوى، والجهد والتيار والتردد الكهربائي، وظروف الطقس والضغوط ومستويات السوائل. وبفضل اتصال الإنترنت، يمكن نقل البيانات واستلامها فورًا من مختلف المواقع الصناعية، مما يضمن تحليل البيانات لحظيًّا، ويُسهم في تخطي القيود البشرية من خلال اكتشاف المخاطر التي قد لا تستطيع الحواس البشرية ملاحظتها، مما يضمن بيئة عمل آمنة وفعالة (Jesus, 2023).

2. أجهزة المحاكاة

يعتمد الأمن الصناعي على إدارة المخاطر، وهنا تؤدي تقنيات الواقع الافتراضي دورًا مهمًّا؛ إذ تتيح للموظفين الانغماس في محاكاة واقعية للمواقف الخطرة، مما يحسن عملية اتخاذ القرار والاستجابة للطوارئ. وتُقدم هذه التكنولوجيا تجربة تدريبية تفاعلية؛ حيث توفر محاكاة دقيقة لظروف العمل المختلفة. كما يمكنها محاكاة سيناريوهات مخصصة تتكيف مع أنظمة الذكاء الصناعي، مما يتيح لها تحليل الأنماط، وتحديد الاتجاهات، واكتشاف الأعطال بشكل فوري، وهو ما يُوفر للتقنيين معلومات مفصلة ومحدثة عن المخاطر المحتملة داخل بيئات العمل الصناعية.

أثر التقنيات الناشئة في السلامة الصناعية:

يرتبط تطوير عمليات الإنتاج ارتباطًا وثيقًا بإدارة المخاطر التي تتعرض لها المنشأة. وبالتالي، فإن السلامة

الصناعية تُعد جزءًا أساسيًّا من سلسلة القيمة لأي كيان صناعي. ولقد أعادت التقنيات الناشئة تعريف نماذج الحماية، مما ساعد على منع المخاطر وتقليلها داخل المنشآت.

وتتيح التكنولوجيا الحالية إمكانية تحديد موقع المشغل في المناطق التي لا تصلها إشارات الاتصال أو تغطية الشبكات، كما توفر بعض آليات المراقبة الحديثة وسائل لحماية الأشخاص الذين يتعين عليهم تشغيل الآلات المتنقلة في المصانع أو مواقع العمل، مما يسهم في تقليل الحوادث والحد من آثارها السلبية. وقد أدى تطبيق تدابير الوقاية من المخاطر والحد منها إلى توفير أدوات تعزز من كفاءة الأنظمة التقليدية، إضافة إلى تطوير تقنيات جديدة لمعالجة الثغرات القائمة.

خطوط التطبيق:

هناك أمثلة على التنفيذ الناجح لأنظمة السلامة؛ حيث تُستخدم نفس التقنيات التي تُعزز الإنتاجية في الصناعات لتطبيقها في مجالي الوقاية والتدريب، ومن أبرزها:

1) **الواقع الافتراضي:** يمكن للمشغلين استخدامه لتلقي التدريب في أدوارهم الوظيفية دون التعرض للمخاطر الناتجة عن قلة الخبرة، كما يمكنهم اختيار أفعالهم وردود أفعالهم أثناء سيناريوهات الطوارئ.
2) **أنظمة الاستشعار:** تساعد المراقبة المستمرة للآلات على منع الحوادث الناجمة عن التآكل والتلف لمكوناتها، كما تتيح مراقبة الممتلكات لضمان بيئة آمنة، إضافةً إلى اكتشاف العوامل الضارة ومراقبة المشغلين لحمايتهم جسديًّا.
3) **البيانات الضخمة والذكاء الاصطناعي:** يُسهم جمع ومعالجة الكم الهائل من البيانات الناتجة عن العمليات الصناعية في تطوير خوارزميات قادرة على التنبؤ بالحوادث واكتشاف المخاطر قبل حدوثها.
4) **المركبات غير المأهولة:** تُستخدم الطائرات دون طيار في مواقع البناء الكبيرة؛ لتحل محل المشغلين في تنفيذ الأعمال عالية المخاطر، كما تُستخدم لتفتيش المناطق التي يصعب الوصول إليها وأداء المهام على ارتفاعات كبيرة.
5) **الهياكل الخارجية:** تُعد نوعًا من الدروع أو الدعم الآلي المخصص للعمال؛ حيث تُستخدم هذه الهياكل لتقليل المخاطر المهنية وضمان سلامة المستخدمين عند أداء الأعمال المتكررة أو المطولة، إضافةً إلى تحسين جودة الأداء الوظيفي.

التقدم في التنفيذ:

تضمن أنظمة السلامة التشغيل السليم للشركة، وعلى الرغم من أنها قد لا تكون ذات تأثير مباشر على صورة الشركة، إلا أنها تُعتبر من العوامل المؤثرة في سلسلة القيمة. بالإضافة إلى ذلك، فإن منع المخاطر التي قد تُعَرِّض الإنتاجية للخطر يقلل من الخسائر الاقتصادية. وقد أشار "جارسيا تريجو" إلى التأثير السلبي الذي قد تُحدثه الحوادث في بيئات العمل، موضحًا أن بعض القطاعات الصناعية قد نجحت في تطبيق التقنيات الناشئة بفاعلية. وأضاف قائلًا:

"تُظهر المجالات اللوجستية، مثل: المستودعات الآلية ومستودعات التخزين البارد، وهي أجزاء من الصناعة الكبرى، اهتمامًا متزايدًا بحماية نفسها من حوادث العمل المحتملة. كما أن هناك اهتمامًا متزايدًا بإدارة المعلومات التي تجمعها هذه المعدات؛ حيث يتم نقلها إلى بيئات سحابية جديدة" (Trejo, 2024).

ويُعد التحكم في خدمات التخزين الخارجية ومراقبتها عنصرًا مهمًّا لتوسيع نطاق المراقبة واعتماد أساليب عمل جديدة؛ إذ يتم تسجيل البيانات التي تجمعها أجهزة استشعار السلامة، مثل: حركة المشغلين في المناطق الخطرة، والحوادث بين المستخدمين النهائيين للآلات المتحركة، إلى جانب متغيرات أخرى؛ ليتم تخزينها على المنصات الرقمية المتخصصة، وتحليلها لاحقًا، وتُسْتَخْدَم لإنشاء خطط وبرتوكولات تدريبية تتكيف مع الاحتياجات المحددة للمناطق المتأثرة، ولتحقيق هذه الغاية سيكون دور مقدمي التكنولوجيا أساسيًّا في هذا المجال، حيث يتمثل التحدي الحقيقي في التعرف على أحدث التقنيات المتاحة ومواكبة تطوراتها المستمرة.

وفي هذا الصدد، يُعد وجود قسم بحث وتطوير مؤهل، ومدرب، وذو خبرة، ومُنسق جيدًا، أمرًا حيويًّا (Trejo, 2024).

التطبيقات الأمنية للتقنيات الناشئة:

يُمكن للتقنيات الناشئة تحليل كميات هائلة من البيانات المتعلقة بالأمن الصناعي، مما يسهم في كشف الهجمات والتهديدات، كما تُتيح تطوير أنظمة أمان قوية في القطاعات الصناعية المختلفة؛ حيث يمكنها التعرف على الأنماط غير الطبيعية والتصدي للهجمات السيبرانية بشكل آلي وفوري. علاوة على ذلك، يمكن استخدام هذه التقنيات في تطوير أنظمة إدارة الهويات والوصول لضمان أمن المنشآت الصناعية وحمايتها من التهديدات الداخلية والخارجية.

دمج البيانات

تعمل التقنيات الناشئة على إحداث تحول جذري في مراقبة المخاطر وإدارتها في الصناعة، وذلك بفضل قدرات التعلم العميق والتعرف على الأنماط. حيث تتيح هذه التقنيات تحليل كميات ضخمة من البيانات من مصادر متنوعة بشكل فوري، مما يُمكنها من الكشف عن الاتجاهات الخفية، والتنبؤ بالحوادث قبل وقوعها، وتحسين الاستجابة لحالات الطوارئ.

وتلعب أنظمة دمج البيانات دورًا مهمًّا في تجميع المعلومات غير المتجانسة، مثل: المراقبة بالفيديو، والبيانات الحسية، وسجلات الصيانة، والتنبيهات الأمنية؛ حيث توفر نظرة عامة متكاملة وقابلة للتنفيذ، مما يسهم في تعزيز المراقبة الاستباقية، ويقلل من مخاطر الحوادث والاختراقات الأمنية.

المميزات الأمنية للتقنيات الناشئة في مجال الأمن الصناعي:

لقد أحدثت التقنيات الناشئة ثورة في قطاع الأمن الصناعي؛ حيث وفرت مزايا متقدمة عند تطبيقها. فهي تُستخدم في تحليل البيانات الضخمة للتنبؤ بأي جريمة أو حادث داخل القطاع الصناعي، كما تُمكن من استخدام الروبوتات والطائرات المسيرة للمراقبة،

بالإضافة إلى أنظمة التعرف على الوجه لتحديد هوية المشتبه بهم، مما يمثل تغييرًا جذريًّا في أساليب الأمن الصناعي التقليدية.

وأبرز مميزات هذه التقنيات:

أ) التنبؤ بالمخاطر: حيث يمكن تحليل المعلومات والبيانات لتحديد أماكن وتوقيت المخاطر، مما يُمكن الجهاز الأمني للصناعة من توجيه الموارد بشكل أكثر فعالية، وذلك على نحو أفضل من الطرق التقليدية (Interpol ICRI, 2019).

ب) تمكين رجال الأمن الصناعي من تحديد أفضل الإستراتيجيات للتعامل مع المشتبه بهم داخل المنشآت، عبر تحليل شخصياتهم وسلوكياتهم (البكر، 2020).

ت) الكشف عن أي جريمة (اعتداء، تخريب، حادث) باستخدام الخوارزميات المتقدمة، التي تحلل المعطيات المرتبطة بالجريمة (Kerkara, 2019).

ث) تصنيف المشتبه بهم بسهولة وموضوعية مقارنة بالبشر، كما يمكنه تحديد المناطق الأكثر خطورة في المواقع الصناعية (Dorota, 2019).

ج) تسريع تحليل المعلومات الأمنية واقتراح الحلول المناسبة.

ح) التعرف على الهوية باستخدام أنظمة متقدمة، مما يسهم في تحديد المشتبه فيهم والمفقودين بسرعة وكفاءة، ودعم تحقيقات البحث الجنائي.

خ) تحليل الأدلة الرقمية بدقة أعلى، مما يُمكن الجهات الأمنية من استخراج البيانات ومعالجتها بسرعة من الأجهزة الإلكترونية.

د) المراقبة الذكية باستخدام الطائرات دون طيار والكاميرات المعتمدة على الذكاء الاصطناعي، مما يُتيح تغطية شاملة للمناطق الصناعية الحساسة.

ذ) إن كمية البيانات التي يتعامل معها محلل الأمن السيبراني هائلة، مما يجعل التنبؤ بالتهديدات المستقبلية أمرًا معقدًا وصعبًا. ولكن مع قدرة الذكاء الاصطناعي على معالجة كميات كبيرة من البيانات في وقت واحد، فإنه يُمكن أن يساعد على اكتشاف أي نشاط مشبوه أو تهديدات محتملة للمنشآت الصناعية في وقت مبكر، مما يتيح فرصة لمنع هذه التهديدات قبل وقوعها. ويُعد هذا الأمر مهمًّا في تقليل الهدر في الوقت، وتحسين كفاءة استخدام الموارد البشرية، وتعزيز قدرة المنشأة على حماية أصولها بشكل أكثر فاعلية.

ر) تساعد التقنيات الحديثة على تعزيز الجهد البشري في اكتشاف التهديدات الأمنية من خلال الاستفادة من البيانات المتاحة حول الهجمات السابقة؛ حيث أظهرت التقارير أن 60% من المديرين التنفيذيين في المنشآت لاحظوا تحسنًا في أداء فرق الأمن السيبراني لديهم بعد دمج خدمات الذكاء الاصطناعي ضمن إستراتيجيات الحماية الخاصة بهم (تقرير Cap-gemini عن تطوير الأمن السيبراني، منشآت 2023 - Monshaat).

ز) يسهم الذكاء الاصطناعي في تقليل تكاليف الأجهزة الأمنية؛ حيث تتأثر العديد من المنشآت بشكل عام بالتكاليف المترتبة على انتهاكات البيانات، والتي قد تستمر آثارها المالية لفترات طويلة، مما يجعل من الصعب تجاهل هذا الجانب.

وبما أن المجرمين لا يُظهرون أي نية للتوقف عن محاولاتهم، فقد كشفت الدراسات أن المنشآت

التي تعتمد على الذكاء الاصطناعي في مجال الأمن السيبراني تشهد انخفاضًا في التكاليف بنسبة تصل إلى 80% مقارنة بالمنشآت التي لا تستفيد من هذه التقنيات (IBM Cost of Data Breach, 2021)

تأثير التقنيات الناشئة في أمن البيانات التشغيلية الصناعية:

لقد أسهم تطور برامج الحاسوب والتقنيات الناشئة في تحسين إدارة وصيانة المنشآت الصناعية، مما أدى إلى تعزيز سلامة الموظفين. كما أن الأتمتة الصناعية أدت إلى تقليل تعرض العمال للمخاطر عبر تقليل التدخل البشري في المواقف الخطرة، مما جعل تأثير التقنيات الناشئة على السلامة الصناعية ملحوظًا، خاصة في قطاع النفط والغاز.

وتؤدي هذه التقنيات المبتكرة دورًا محوريًّا في الحماية من المتغيرات الحساسة، مثل: المواد الكيميائية، ودرجات الحرارة المرتفعة، والضغوط الشديدة. وبفضل ذلك، أصبحت إدارة المخاطر في بيئات التشغيل الصناعية عنصرًا أساسيًّا في التحول نحو مستقبل أكثر أمانًا، حيث يُعد الأمن الصناعي من الركائز الأساسية في تطوير العمليات التجارية.

ومع أن البيانات الصناعية تتطور باستمرار، فإن تطبيق التقنيات المتقدمة في مجال السلامة الصناعية يوفِّر خيارًا مثاليًّا للتكيف مع التغيرات التنظيمية والمتطلبات المتقلبة. ونتيجة لذلك، تُسهم هذه التقنيات في تحسين الكفاءة التشغيلية في مجالات، مثل: الاستكشاف، والاستخراج، والنقل، والتوزيع، كما تؤدي إلى رفع معايير السلامة الصناعية إلى مستويات غير مسبوقة.

استخدام التقنيات الناشئة لمكافحة الإرهاب في المنشآت الصناعية:

إن مكافحة الإرهاب باستخدام هذه التقنيات في المنشآت الصناعية يعد خيارًا واعدًا وممكنًا من خلال الآتي:

أولًا) عملية التحليل الآلي للبيانات تُعد مفيدة للغاية، خاصة مع وجود نماذج تنبؤية دقيقة.

ثانيًا) إن تقنية الذكاء الاصطناعي يمكنها تطوير مصادر منفصلة لجميع المعلومات العدائية المتوقعة للمنشأة الصناعية، مما يُتيح التحقق من صحة المعلومات دون الاعتماد على نظام مركزي واحد قد يكون عرضة للاستهداف، وهو ما يحدّ من إمكانية استغلاله سواء من قِبل الإرهابيين أو الضحايا.

ثالثًا) تهيئة الظروف لتبادل المعلومات بشكل أفضل بين الجهات الفاعلة والوكالات الدولية، مما يسهم في تحسين القدرة على التحليل التنبؤي (جيركي، 2014).

لذلك، فإن هذه التقنيات، ومنها الذكاء الاصطناعي، تُعد أداة فعالة في دعم المحللين الأمنيين لتحديد نقاط القوة والضعف في مواجهة الإرهاب. ومع ذلك، لا تزال التكنولوجيا بعيدة عن أن تحل محل القوى البشرية المتخصصة في الأمن الصناعي بالكامل.

الكشف الاستباقي عن التهديدات للمنشآت الصناعية:

غالبًا ما تعمل تدابير الأمن السيبراني التقليدية بطريقة تفاعلية، حيث تستجيب للتهديدات بعد حدوثها. ومع ذلك، يمكن للذكاء الاصطناعي تحديد

أنماط الشذوذ في البيانات التي قد تشير إلى هجوم إلكتروني محتمل على المنشآت الصناعية، مما يُتيح الكشف الاستباقي عن التهديدات.

ويمكن للتعلم الآلي، أحد فروع الذكاء الاصطناعي، تحليل كميات هائلة من البيانات والتعلم من الأنماط السابقة للتنبؤ بالتهديدات واكتشافها قبل أن تلحق الضرر بالمنشأة.

التحديات والمخاطر الأمنية الصناعية:

على الرغم من الفوائد الكبيرة التي تحققها التقنيات الحديثة والناشئة في مجال الأمن الصناعي، فإنها تطرح العديد من التحديات والمخاطر الأمنية التي يجب معالجتها. وتشمل بعض هذه المخاطر استغلال الأنظمة الذكية من قبل المهاجمين، والتلاعب بالبيانات والمعلومات الصناعية، والعديد من التهديدات الأخرى.

كما أن هذه التقنيات الناشئة، التي تُستخدم لحماية المنشآت الصناعية، يمكن أن يتم استغلالها من قبل المجرمين لشن هجمات إلكترونية ضارة عن بُعد. وعلى الرغم من أن هذه التقنيات يمكنها التعامل مع كمية ضخمة من البيانات، ونقلها يوميًّا بين العملاء والمنشأة الصناعية، وبين الأجهزة والشبكات، فإنه لا يمكن لمحللي الأمن السيبراني فحص جميع البيانات يدويًّا بحثًا عن المخاطر المحتملة.

وقد ذكرت دراسة حديثة أن 56% من المنشآت وجدت أن محللي الأمن السيبراني غارقون في حجم التهديدات التي يواجهونها. كما أن 23% من المحللين غير قادرين على التحقق بفعالية من التهديدات المكتشفة (Capgemini report, 2023).

وقد تم تصنيف الأمن الإلكتروني كمجال خصب بشكل خاص لمواطن الضعف الناجمة عن الذكاء الاصطناعي، حيث إن من أبرز وظائف الأدوات الاصطناعية - سواء المعلوماتية أو الإلكترونية المادية منها - هو التلاعب الفعال بالمعلومات. ويمكن للمجرمين تغذية أنظمة المراقبة الذكية بمعلومات مزيفة أو مضللة، مما قد يؤدي إلى تعطيل أنظمة الأمن في المنشآت الصناعية.

وبالرغم من أن التقنيات الناشئة توفر إمكانات هائلة للأمن الصناعي، فإنها لا تخلو من التحديات الأخلاقية والخصوصية فيما يتعلق بمعالجة البيانات. ونظرًا لأن أنظمة الذكاء الاصطناعي تعتمد على التعلم من البيانات، فإنه يجب إدارة هذه المعلومات واستخدامها بشكل مسؤول. ويُعد تحقيق التوازن بين التقدم التكنولوجي والمبادئ الأخلاقية أمرًا أساسيًّا لتسخير الإمكانات الكاملة لهذه التقنيات دون المساس بالخصوصية الفردية أو المعايير المجتمعية.

بالإضافة إلى ذلك، هناك قلق متزايد من أنه كما يمكن للمؤسسات الأمنية، مثل الأمن الصناعي، استخدام هذه التقنيات لتعزيز أمنها السيبراني، فإنه يمكن للمجرمين الإلكترونيين استغلالها لشن هجمات أكثر تطورًا وشراسة. وتؤكد هذه الازدواجية على أهمية التعلم المستمر والتكيف في مجال الأمن السيبراني.

إن العالم الرقمي الذي أحدثته التقنيات الناشئة أصبح ساحة دائمة التغيير؛ حيث أصبحت التهديدات الإلكترونية التي تستهدف الأجهزة الأمنية، ومنها أجهزة الأمن الصناعي، أكثر انتشارًا من أي وقت مضى؛ إذ يطور قراصنة الإنترنت مهاراتهم الإجرامية باستمرار، ويستغلون نقاط الضعف في الأنظمة الأمنية لهذه المنشآت، مما يمكنهم من شن هجمات متطورة تتجاوز

الإجراءات الأمنية التقليدية، وهو ما يُعرض بيانات هذه المنشآت إلى خطر القرصنة والسرقة (Amal, M. 2023).

التحديات السيبرانية للأمن الصناعي في عصر التقنيات الناشئة:

إن أحد أبرز التحديات، التي تواجه الأمن الصناعي في هذا العصر الرقمي، هو التطور المتصاعد للتهديدات السيبرانية، التي تتفاقم الآن. ومع استمرار هذا التقدم التقني، أصبح من الضروري استكشاف كيف يمكن للتكنولوجيا أن تتفاعل بشكل فعال مع هذه التهديدات المتقدمة والتصدي لها. لقد أصبح عالم الإنترنت ساحة معركة للمتسللين والمنظمات الإجرامية؛ إذ يسعى كل منهم إلى استغلال نقاط الضعف لأغراض مختلفة، بدءًا من المكاسب المالية إلى النفوذ السياسي (بانافع، 2024).

وفي ظل نقص عدد المهنيين ذوي الخبرة، لا سيما في بعض الدول العربية، أصبح من الضروري على المنشآت الصناعية والمسؤولين الأمنيين فيها إدراك تعقيدات الأمن السيبراني وتقنيات الذكاء الاصطناعي، بالإضافة إلى الحاجة الملحة إلى التدريب والتعلم متعدد التخصصات لمواجهة هذه الاختراقات الإلكترونية المحتملة على المنشآت الصناعية، والعمل على استخدام الذكاء الاصطناعي لتعزيز أمنها السيبراني، وخاصة في بعض المؤسسات الصناعية، مثل: مؤسسات النفط والكهرباء، والمياه والصناعات الحربية، ومثيلاتها.

الافتقار إلى المهارات التكنولوجية للتقنيات الجديدة:

لتحقيق سلامة بيئات التشغيل الصناعية، من الضروري استخدام هذه التقنيات بشكل مثالي. لذلك، من الضروري أن تمتلك فرق العمل المهارات اللازمة لاستخدام المعدات والأدوات التي تسمح بضمان الإجراءات التي يتم تنفيذها في المرافق الصناعية، كما أن الافتقار إلى المعرفة لن يعوق عملية التحول الرقمي فحسب، بل يمكن أن يؤدي أيضًا إلى حدوث أعطال وتوقف الإنتاج وحوادث في مكان العمل.

عدم النضج الرقمي:

التحول الرقمي هو عملية تعتمد بشكل أساسي على مدى قدرة المنظمة الصناعية على تبني مخطط تكنولوجي في بنيتها التحتية، وربما يكون هناك بعض الصناعات التي ليس لديها تعريف ناضج لأهمية التكنولوجيا وتأثيرها في سلامة المنشأة الصناعية وعملياتها. ونتيجة لذلك، تنشأ مقاومة للتغيرات المقترحة على ممارسات العمل المحددة، وكذلك لتنفيذ معدات وتقنيات وبرامج إدارة المخاطر في بيئات التشغيل الصناعية (Jesus, 2023).

دور الطائرات دون طيار في الهجمات على المنشآت الصناعية

إن التقنيات الناشئة الأكثر تقدمًا، التي ستمكن أي إرهابيين أو معتدين من شن هجمات مستقبلية، هي الطائرات دون طيار (الدرونز)، وهي أسلحة ذكية صغيرة الحجم ورخيصة، يمكن أن تستغلها الجماعات الإرهابية للقيام بعمليات إرهابية على المنشآت الصناعية، وذلك من خلال تحميلها بالمتفجرات، مع صعوبة رصدها بسبب حجمها الصغير؛ أي إن الجماعات الإرهابية يمكنها شراء طائرات الدرونز، التي

تمتلك القدرة على اختراق معظم أنظمة الدفاع البرية، مما يشكل تحديًا أمنيًّا خطيرًا، خاصة على المنشآت الصناعية."

وتتمتع هذه الطائرات بالقدرة على توفير التباعد، مما يمكن الإرهابيين والمعتدين من شن هجمات متعددة في وقت واحد تقريبًا، مما يؤدي إلى تضخيم تأثيرها الإجمالي بسرعة. وإحدى أهداف هذا النوع من الهجوم هو خلق جو من الخوف للتأثير في الجمهور المستهدف - السكان المدنيين أو المسؤولين الأمنيين - لإجبارهم على ما يريدون أو فرضه.

إنَّ التطور السريع في تصميم الطائرات دون طيار، وزيادة قدراتها، وسهولة الحصول عليها وتشغيلها بتكلفة منخفضة، يجعلها خيارًا مثاليًّا للإرهابيين في المستقبل. وسابقًا، كانت العديد من الجماعات الإرهابية تشن هجماتها على أمل أن يضحي أعضاؤها بأنفسهم أثناء الهجوم أو القبض عليهم أو قتلهم، ولكن مع استخدام هذه الطائرات قد يُسْمَحُ لفرد أو مجموعة صغيرة بتنفيذ هجمات متعددة دون التضحية بالنفس. وبالفعل بدأت الجماعات الإرهابية باستخدام هذا النوع من الطائرات لتنفيذ الهجمات وتنسيقها.

إن التحسينات السريعة في تكنولوجيا الطائرات دون طيار وقدرتها المتزايدة من شأنها أن توفر للجماعات الإرهابية سبلًا جديدةً لبث الخوف والاعتداء. وفي هذا السياق، ينظر إلى هذا النوع من الطائرات باعتباره من أخطر وسائل الهجوم على المنشآت الصناعية، وبالذات الجيل الجديد منها، وهي الطائرات الصامتة دون صوت، وربما تكون قاتلة بشكل واسع، خصوصًا مع ازديادها وانخفاض تكلفتها مؤخرًا. وتشير التقديرات إلى أن بعض التنظيمات المسلحة ستتبنى هذا النوع من الطائرات؛ لتصبح أكثر فتكًا وقوةً.

ومما يزيد التحديات الأمنية هو صعوبة التشويش على الدرونز وآلية التحكم بها؛ نظرًا لأنها تعمل بصورة مستقلة عن أي تواصل بشري.

وعلى الرغم من أن هذه الطائرات قادرة على حمل شحنات تدميرية صغيرة لكنها شديدة الخطورة، مما قد يؤدي إلى أضرار كارثية، مثل: استهداف مستودعات النفط والوقود، ومخازن الأسلحة، وأعمدة شبكات الكهرباء، ومصانع الكيماويات، إلا أنه يمكن أيضًا تزويدها بأجهزة تفجير عالية القوة. وبهذا، لن يكون الإرهابيون بحاجة إلى اختراق الإجراءات الأمنية في المنشآت الصناعية؛ إذ يكفيهم زرع قنبلة داخل الطائرة وإرسالها لاقتحام المنشأة أو الهدف. كما يمكن استغلال كاميرا الطائرة لتحديد الأهداف بدقة والتصويب عليها.

وليس من الصعب الاستنتاج بأن الجمع بين العبوات الناسفة وطائرات الدرونز سيكون أمرًا واردًا. وعلى الرغم من أن الدرونز التجارية لا تستطيع حمل سوى شحنات تدميرية صغيرة، إلا أن التطور الكبير في تقنية النانو المستخدمة في تصنيع المتفجرات أدى إلى زيادة قوتها التفجيرية بمقدار الضعف مقارنة بالمتفجرات التقليدية، مما يتيح للدرونز إمكانية حمل متفجرات ذات قوة تفجيرية أكبر واستهداف المنشآت الصناعية بكفاءة أعلى.

كما أن هذه التكنولوجيا تمتلك القدرة على تدمير نفسها ذاتيًّا، مما يضمن إخفاء هوية منفذي الهجوم. إن استخدام الإرهابيين للدرونز في تنفيذ عملياتهم تمكنهم من التغلب على كثير من العوائق المادية الراهنة، فقد اهتمت المصانع وبالذات الصناعات الكبرى

ببناء الحواجز والأسلاك الشائكة وغيرها من الحواجز لتأمين المنشآت الصناعية وضمان عدم تمكن الإرهاب من الوصول إليها بسهولة - ولكن الدرونز تتغلب على أغلب هذه العوائق بسهولة.

ونشر مجلس "دفينس ون" (Defense One) لأستاذ العلوم الأمنية بجامعة جورج تاون، ديفيد روس، 2023، مقالًا بعنوان (الإرهابيون سيستخدمون الذكاء الاصطناعي)، أشار فيه إلى أن الإرهابيين سيستغلون الذكاء الاصطناعي واستخدام آليات التشفير الحديثة. كما أوضح أن المحللين الأمنيين لم يكونوا على صواب في تقدير قدرة عناصر الميليشيات على استخدام تكنولوجيا الطائرات المسيرة. فقد اعتقدوا أن سلاح الطيران سيكون قادرًا على إسقاطها من السماء، ولكن المنظمات الإرهابية كانت ذكية بما يكفي، فعملت على تكييف طائرات مسيرة صغيرة تتناسب مع أغراضها الإرهابية دون إمكانية الكشف عنها من قبل الرادار. لذلك، فإن المنشآت تحتاج إلى وضع احتياطات تقنية لمواجهة ما يمثله ذلك من خطورة على تلك المنشآت؛ حيث سيكون لها أثر بالغ كتقنية مستجدة على الأمن الصناعي.

الروبوتات:

يُعتبر مجال الروبوتات أكثر تطبيقات الذكاء الاصطناعي تقدمًا؛ حيث يعتمد على بناء هيكل مادي يعمل وفق منظومة برمجية تتيح له تنفيذ المهام المطلوبة منه (Stanford, 2016).

فيما يخص الأمن الصناعي، يمكن الاستفادة من الروبوتات في المجالات التالية:

1) **تفتيش المواقع الخطرة داخل المنظومة الصناعية.**
2) **إزالة الألغام.**
3) **الحراسات الأمنية للمنشآت الصناعية.**

ومع ذلك، قد تخلق الروبوتات مشكلات أمنية بسبب أنظمة التشغيل والبرمجيات المستخدمة فيها؛ حيث إن برمجيات الذكاء الاصطناعي قد لا تتوافق مع بعض القوانين. والدليل على ذلك أن العديد من التشريعات المقارنة اعتبرت البرمجيات عملًا فكريًّا يخضع لقانون الملكية الفكرية (المندور، 2022).

روبوت الأمن الصناعي:

يُعد الروبوت رباعي الأرجل متعدد المهام نموذجًا متقدمًا في مجال الصناعة؛ حيث يُستخدم في الدوريات الأمنية داخل المنشآت الصناعية. كما يوجد روبوت ذكي لمكافحة الحرائق، مما يُعزز منظومة الأمن والسلامة؛ حيث يُقال إنه يقدم أداءً يعادل ثلاثة أضعاف الأداء البشري، ويعمل على مدار 24 ساعة، مقارنة بالأيدي العاملة البشرية التي تعمل من 8 إلى 12 ساعة يوميًّا.

كذلك، هناك روبوت دورية الأمن الذي يتميز بإمكانية التشغيل في جميع الظروف المناخية، ويستخدم أجهزة استشعار متقدمة لتحديد المواقع والكشف والاتصال. وعلى الرغم من الفوائد الكبيرة التي تقدمها الروبوتات في مجال الأمن الصناعي، فإنه يمكن استغلالها من قبل المعتدين بنفس القدر الذي تُستخدم فيه لحماية المنشآت، مما يُشكل تحديًا أمنيًّا خطيرًا.

روبوتات المراقبة الذاتية:

يمثل نشر الروبوتات لمراقبة المواقع الصناعية خطوة متقدمة؛ حيث تُجهز هذه الروبوتات بأجهزة

استشعار متطورة، ومدعومة بالذكاء الاصطناعي، مما يُمكنها من القيام بدوريات أمنية مستقلة، ورصد الحالات الشاذة والإبلاغ عنها دون تدخل بشري مباشر. كما أن هذه الروبوتات قادرة على التنقل في بيئات معقدة، وتجنب العقبات، وتعديل مسارها وفقًا لمتطلبات المراقبة.

يسهم استخدام هذه الروبوتات في تقليل العبء على رجال الأمن الصناعي، كما يزيد من كفاءة المراقبة، خاصة في المناطق التي يصعب الوصول إليها أو التي تشكل خطورة على العاملين في الأمن الصناعي. ومع ذلك، لا يمكن تجاهل التحديات والمخاطر الأمنية التي قد تنجم عن هذه التقنيات؛ حيث إنها غير مهيأة لمقاومة التهديدات بنفس طريقة البشر.

السيارات ذاتية القيادة:

تُشكل السيارات ذاتية القيادة تحديًا أمنيًّا جديدًا للمنشآت الصناعية؛ إذ يمكن استغلالها في تنفيذ عمليات تخريبية أو إرهابية دون الحاجة إلى وجود سائق. فهذه المركبات مزودة بأنظمة استشعار متقدمة، وتعمل دون تدخل بشري، ولا تتطلب أي تحكم مباشر أثناء تشغيلها.

إلا أن السيارات ذاتية القيادة تُثير تساؤلات قانونية عديدة، لا سيما عند تسببها في أضرار للآخرين؛ حيث يصعب التنبؤ بنتائج تشغيلها، كما أنها قد لا تستجيب بشكل مناسب للمواقف غير المتوقعة. علاوة على ذلك، فإن تعقيد أنظمتها التقنية قد يؤدي إلى أعطال، مما يزيد من احتمالية وقوع حوادث تُسفر عن أضرار مادية أو خسائر في الأرواح. ومن المخاطر الكبرى التي تترتب على السيارات ذاتية القيادة إمكانية تحميلها بمتفجرات واستخدامها كقنابل متحركة (المدبولي، 2023).

وهذا يعني أن الإرهابيين يمكنهم برمجتها لتنفيذ هجمات على المنشآت دون الحاجة إلى تدخل بشري مباشر، مما يزيد من تعقيد التحديات الأمنية في هذا المجال.

التزييف العميق:

يُعَدُّ التزييف العميق (Deep Fake) من التقنيات الناشئة التي أصبحت تُستخدم بشكل متزايد في الجرائم الإلكترونية والإرهاب؛ حيث يُمكّن المجرمين من إنشاء مقاطع فيديو مزيفة لأشخاص حقيقيين يظهرون وكأنهم يقولون أو يفعلون أشياء لم يقوموا بها (Sallya, 2020).

هذه التقنية تُستخدم لخداع العيون البشرية، كما أن أنظمة الكشف الآلي لم تثبت فعاليتها الكاملة في التصدي لها حتى الآن. ويمكن استغلالها لاختراق المنشآت الصناعية؛ حيث يُمكن استخدامها لانتحال صفة مسؤولين رسميين بهدف التسلل إلى المواقع الحساسة، أو لاختراق الأنظمة الأمنية بهدف سرقة بيانات حساسة أو تنفيذ عمليات تخريبية.

كذلك، يمكن استخدام هذه التقنية في التصيد الاحتيالي، من خلال جمع بيانات عبر الإنترنت لأغراض الابتزاز (ماثيو، 2020). وتشير الدراسات إلى أنه بين عامي 2016 و2017، تم نشر حوالي 14 مليون رسالة تتضمن محتوى مضللًا عبر الحسابات الآلية على تويتر، من أصل 400 ألف تغريدة منشورة (عبدالعزيز، 2017).

ويُعد التزييف العميق من أخطر أدوات التضليل المعلوماتي، ليس فقط بسبب تأثيره في تشكيل رأي عام مضلل، ولكن أيضًا بسبب تأثيره السلبي على دقة

المعلومات التي يعتمد عليها صناع القرار، مما يُضعف من قدرتهم على اتخاذ قرارات سليمة (فيلاسينولا، 2023).

الشبكة المظلمة (The Dark Web):

الويب المظلم هو نظام إلكتروني أنشأته معامل البحث التابعة للبحرية الأمريكية لتوفير وسائل اتصال سرية للوحدات العسكرية بطريقة غير مباشرة (عبر الإنترنت) دون إمكانية اكتشاف تلك الوحدات أو تعقبها أو متابعتها. وتستخدم الشبكة المظلمة أجهزة الحاسوب التي تعمل عبر بروتوكول معين يُعرف باسم التشفير التراكمي (Cryptographic)، والذي يسمح للمستخدمين بإجراء تواصلات خفية دون الكشف عن موقعهم أو بياناتهم.

وللوصول إلى هذه الشبكة، يحتاج المستخدم إلى برمجيات مخصصة، وأكثرها استخدامًا حاليًّا هو (The Onion Router Project)، الذي يُخفي هوية المستخدمين بالكامل، مما يجعل تعقبهم أمرًا صعبًا للغاية. وهناك اعتقاد سائد بأن رجال الأمن يجدون صعوبة في تتبع هذا النشاط الخفي، بل ذهب البعض إلى الاعتقاد بأن تعقب هذه الشبكة يُعد شبه مستحيل، خصوصًا في بريطانيا وبعض الدول الأوروبية والولايات المتحدة الأمريكية (German, 2020).

وفيما يخص الأمن الصناعي والشبكة المظلمة، فإن هناك تحديات تواجه سلطات المنشآت الصناعية وأخطرها العمليات الإرهابية ضد هذه المنشآت. وتشير الأدلة إلى أن الإرهابيين أصبحوا أكثر استخدامًا لهذه الشبكة لتنفيذ أنشطتهم؛ حيث توفر لهم سرية تامة وإخفاءً كاملًا لهوياتهم. كما أن العديد من المنظمات الإرهابية تعتمد على الشبكة المظلمة في عدة أنشطة، منها: تجنيد الأفراد عبر الإنترنت دون الكشف عن هويتهم، وشراء بطاقات هوية وجوازات سفر مزورة لاستخدامها في عمليات تخريبية، وتنظيم الهجمات الإرهابية على المنشآت الصناعية دون إمكانية تعقب المتورطين. وتمكن هذه التقنية الإرهابيين والمجرمين من الوصول إلى خبراء في تصنيع المواد الكيميائية والمشعة، كما تتيح لهم شراء الأسلحة والمواد المتفجرة من الأسواق السوداء التي توفرها الشبكة المظلمة. لذلك، يجب على رجال الأمن الصناعي إدراك خطورة الإرهاب الإلكتروني عبر الشبكة المظلمة، واتخاذ تدابير علمية وتقنية للحد منه؛ إذ يمكن أن تنتقل هذه الأنشطة عبر الحدود دون إمكانية كشفها بسهولة. وقد تكون المنشآت الصناعية الكبرى من بين أكثر الجهات تعرضًا للاستغلال السيئ للشبكة المظلمة؛ حيث تُستخدم هذه الشبكة في ارتكاب جرائم خطيرة بطرق سرية وبسريعة فائقة، ومنها:

1) الاتجار في المواد الخطرة والمحظورة عالميًّا، والتي يتم بيعها باستخدام العملات المشفرة؛ لتجنب تعقب عمليات البيع والشراء.
2) المتاجرة غير المشروعة في الأدوية والمواد الطبية، حيث تُستغل المواد التي تُنتجها المنشآت الصناعية لأغراض غير قانونية.

آفاق مستقبلية: حلول وبدائل

يُعَدُّ مستقبل الأمن الصناعي مع التقنيات الناشئة واعدًا بتحقيق المزيد من التقدم المذهل؛ إذ يمكن لهذه التقنيات، بفضل إمكاناتها في التعلم والتكيف، أن توفر أنظمة مراقبة ديناميكية تتأقلم مع التغيرات في

البيئة والتهديدات الجديدة التي تواجه الأمن الصناعي. كما يمكن تطويرها إلى نماذج أكثر تطورًا، قادرة على التدخل المباشر في حالة وقوع حادث صناعي. ومع إتقان هذه التقنيات، فإنها ستمهد الطريق لحلول متقدمة في مجال السلامة والأمن الصناعي، مصممة لتلبية الاحتياجات المحددة لكل موقع صناعي. وبالتالي، يمكننا التطلع إلى مستقبل يصبح فيه الأمن الصناعي أكثر كفاءة ومرونة.

إن التوازن الدقيق بين الابتكار والمسؤولية في الأمن الصناعي يشكل حجر الأساس لمستقبل يعتمد على التقنيات الناشئة، والتحديات العملية، والخبرة البشرية. كما يذكر أليكس أودين، رئيس قسم التسويق والاتصالات في شركة Running Braino Robotics بفرنسا، في مقاله المنشور بتاريخ 10 يونيو 2024، أنه يجب أن نكون أكثر وعيًا بكيفية تشكيل واستخدام هذه التكنولوجيا الناشئة؛ إذ إن هناك تقاربًا نحو مستقبل رقمي أكثر أمانًا بفضل هذه التقنيات الناشئة، حيث يمثل الذكاء الاصطناعي أداةً فعالةً لجعل هذا المستقبل أكثر أمنًا وقوة (أليكس أودين، 2024).

وفي حال وقوع هجوم إلكتروني، فإن الاستجابة السريعة أمر بالغ الأهمية بالنسبة للمنشأة الصناعية؛ إذ يمكن للذكاء الاصطناعي المساهمة في تقليص أوقات الاستجابة من خلال تحديد مصدر الاختراق ومداه بسرعة، مما يسمح لفرق الدفاع المدني المسؤولة بحماية المنشأة أو المنطقة المستهدفة بالتصرف الفوري والحد من الضرر المحتمل.

ومن الإسهامات العامة المقترحة، أن تعمل المنظمة العربية للحماية المدنية، التابعة لمجلس وزراء الداخلية العرب، على إصدار دليل موحد للأنظمة والتعليمات الخاصة بالتقنيات الناشئة في مجال الأمن الصناعي. ويشمل هذا الدليل:

- تحديد المخاطر المحتملة التي تواجه المنشآت الصناعية العربية.
- وضع إستراتيجيات للوقاية من المخاطر والتصدي لها، إضافة إلى آليات التعامل معها حال وقوعها.
- تقديم نموذج افتراضي لمحاكاة هجوم بطائرة مسيَّرة على منشأة صناعية عربية إستراتيجية، مثل: منشآت النفط أو الكهرباء أو المياه أو التصنيع الحربي، بهدف وضع خطط استجابة فعالة.

وبذلك، يمكن الاستفادة من هذه التقنيات الناشئة في العديد من المجالات، لا سيما الأمن الصناعي.

الخاتمة والتوصيات:

في الختام، ومع تعاظم المخاطر الصناعية، يجب أن يُنظر إلى الأمن الصناعي من منظور شامل ومعاصر؛ بحيث يستوعب التقنيات الناشئة التي توفر له أسلوبًا تقنيًّا حديثًا للمحافظة على أمن المنشآت الصناعية، وأن يشمل جميع الأنظمة والتعليمات الخاصة بالمجالات الأربع التي يتضمنها الأمن الصناعي، وهي: السلامة، والأمن، ومكافحة الحرائق، وسلامة البيئة.

وهناك مجموعة من التحديات التي أفرزتها تطبيقات التقنيات المستجدة؛ فالذكاء الاصطناعي والروبوتات، على سبيل المثال، قد تتفوق على الذكاء البشري، مما يثير بعض التحديات لرجال الأمن الصناعي، ويتمثل ذلك في عدم قدرتهم على السيطرة والتحكم الكامل في هذه الأنظمة وتأثيرها في النظام الأمني الصناعي. بالإضافة إلى ذلك، قد تتجاوز هذه

التقنيات الناشئة قدرة رجل الأمن الصناعي على المراقبة والرصد؛ نظرًا لصعوبة إدراك كل تهديد أمني وتقييم مدى خطورته.

إن هذه الورقة تقدم حلولًا وبدائل للإجراءات المتبعة لمواجهة تلك التحديات المستجدة، مما يمكن صُنَّاع القرار من النظر فيها، كما تقدم آفاقًا مستقبليةً لإحراز المزيد من التقدم؛ ليكون الأمن الصناعي أكثر فاعلية، خصوصًا في الصناعات الإستراتيجية والحيوية، مثل: صناعة النفط، والوقود، والكهرباء، والمياه، وغيرها.

وفي هذا السياق، اقترحت الورقة مجموعة من التوصيات، هي:

أ) الاستعداد للتطورات المتسارعة في التقنيات الناشئة، من خلال تمكين رجال الأمن الصناعي من الإلمام بأحدث الابتكارات وفهم آلياتها، بما يتيح لهم الاستفادة منها بفعالية في التصدي لمختلف التحديات الأمنية.

ب) تبني سياسة استباقية لاحتواء المخاطر والتهديدات التي تواجه الأمن الصناعي، بما يضمن جاهزية رجال الأمن الصناعي للتصدي لها.

ت) العمل على تطوير البنية التحتية التكنولوجية، وتعزيز البيانات والمعلومات التقنية في مجال الأمن الصناعي.

ث) تطوير الكفاءات الأمنية العربية في مجال الأمن الصناعي ومواكبة المستجدات التقنية، من خلال:

- عقد دورات تدريبية داخلية وخارجية في مجال التقنيات الناشئة؛ بحيث تصبح كيفية التفاعل مع الأنظمة الحديثة مهارة أساسية.
- تزويد الدورات التدريبية بالأبعاد التفصيلية للتقنيات الناشئة، وارتباطها بالأمن الصناعي وتأثيراتها المختلفة.
- التركيز في التدريب على إدارة حالات الطوارئ التي تنطوي على استخدام التقنيات الحديثة، وغيرها من الحالات التي تستدعي الاستعانة بهذه التقنيات لتعزيز التأمين ودرء المخاطر التي تهدد الأمن الصناعي. وينبغي أن يكون التدريب احترافيًّا؛ بحيث يصبح المتدربون قادرين على التعامل مع الأزمات بفعالية وسرعة واستجابة منسقة.

ج) تشجيع المعاهد الصناعية على تكثيف الدراسات والبحوث العملية حول أثر التقنيات الناشئة في الأمن الصناعي، وتحليل تأثيراتها الإيجابية والسلبية، في ظل التطور الصناعي الذي تشهده الدول العربية، وبخاصة في القطاعات الحيوية والإستراتيجية.

ح) إنشاء معامل ومختبرات حديثة لإجراء التجارب العلمية والبحوث التطبيقية التي تخدم مجالي السلامة والحماية المدنية.

خ) صياغة تشريعات عربية متكاملة تتعلق بقضايا التقنيات الناشئة، والأمن الصناعي، والسلامة الصناعية، على أن تتضمن هذه التشريعات تصنيف المخاطر وأسبابها، وسبل الوقاية منها، وآليات مكافحتها، انطلاقًا من مفهوم شامل وحديث للأمن الصناعي.

د) العمل على إصدار دليل موحد للأنظمة والتعليمات الخاصة بالتقنيات الناشئة في مجال الأمن

الصناعي، يشمل تحديد المخاطر المحتملة للمنشآت الصناعية العربية، وآليات الوقاية منها، وخطط التصدي والتعامل مع التهديدات المحتملة، مع تقديم أمثلة افتراضية مثل الهجمات بالطائرات المسَيَّرة على المنشآت الصناعية العربية الإستراتيجية والحيوية، مثل: منشآت النفط، والكهرباء، والمياه، والتصنيع الحربي، وذلك لتعظيم الاستفادة من هذه التقنيات في تعزيز الأمن الصناعي، وخاصة في الصناعات العربية الحيوية.

المراجع

المراجع العربية:

- أبو الليف، عبد المحسن (1996). الأمن الصناعي. الرياض: جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية.
- أبو شامة، ودماس (2019). الأمن الصناعي المعاصر. الرياض: جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية.
- أليكس أودين (2024، 10 يونيو). رئيس قسم التسويق بمؤسسة Running Braino Robot-ics، فرنسا.
- تقرير Capgemini عن تطوير الأمن السيبراني في موقع منشآت 2023.
- بانافع، أحمد (2024): ما هي أبرز تحديات الأمن السيبراني مع تقدم الذكاء الاصطناعي؟، موقع اقتصاد سكاي نيوز العربية.
- البكر، عبد العزيز (2020). الذكاء الاصطناعي في عالم الجرائم المعلوماتية، منشور على موقع الجزيرة الإلكتروني، 25 أكتوبر 2020. https:// www.al-jazirah.com/2020/20201025/ar5.htm#google_vignette
- حمداني، علي (1995). السلامة والأمن الصناعي. جامعة القاضي عياض، مراكش، المملكة المغربية.
- سويف، محمد محمد (2023). جرائم الذكاء الاصطناعي: المجرمون الجدد. كلية الحقوق، جامعة طنطا، دار الجامعة الجديدة للنشر، مصر.
- المدبولي 2023 - (https/web-org/web)
- ماركو جيركي، فهم الجريمة السيبرانية: الظاهر والتحديات والاستجابة القانونية (جنيف، منشورات الاتحاد الدولي للاتصالات، نوفمبر 2014) ص 114 – 116.
- عبد العزيز، سارة (2017). باحثة في العلوم السياسية: Rush of Artificial Intelligence to Security and Future of Work. مؤسسة Round Corporation w.w.Raud-org.
- فيلاسينولا، جون (2023). السباق العالمي للتفوق التكنولوجي: استكشاف الآثار الأمنية. معهد بروكنجز، مجلد ISPI، الصفحات (131 – 141).
- ماثيو، كولدول (2020). البوابة العربية لاختبار التقنية. دبي، الإمارات العربية المتحدة: نشر في 5 أغسطس 2020.
- المندور، مصطفى (2022). مدى كفاية القواعد العامة للمسؤولية المدنية في تعويض أضرار الذكاء الاصطناعي. مجلة حقوق جامعة دمياط للدراسات القانونية والاقتصادية، العدد 2، يناير 2022، دمياط، مصر.
- منشآت (2023، 24 يناير). مستقبل الحماية الرقمية باستخدام الذكاء الاصطناعي (.AI-ds Thakaa, sa).
- نوري، طلال محمد (1409). الأمن الصناعي –

أمن - سلامة - إطفاء. بحث تخرج، المعهد العالي للدراسات الأمنية، المديرية العامة لكلية الملك فهد الأمنية، الرياض، المملكة العربية السعودية.

المراجع الأجنبية:

- Dorota, Jelonek (2019) The Artificial Intelligence Application, con.and Reo, Springer, Cham (p.24).
- Edai, Somme, Kegiburn, Seckin, Codal (April 2020) Journal at computer and Information Science: Vol,5 No1 Sakarya University.
- German, Davis (2020) Journal at Low, Volume 8 Northum.
- Interpol: ICRI (2019) (Artificial intelligence for Low Enforcement Turin - Italy.
- Jesus, Vogler (Inspent) (13 Dec,2023).
- Kerkara, A.R. (2019) Artificial Intelligence for Bussinero. Springer, Briefio in Bussinero, Springer: Cham. (p.11).
- Mekki, Amal (2023) Team Leader, Arabic Department of Swissifer Ch. (15 May 023).
- Reference: Gemini A.I. Platform from Goole (26 Dec,2024).
- Sally, Adde (2020) "What are Deep-Fake: and how are they created". Article IEE Spectrum - 29 Aprile 2020.
- Stanford (2016) "Artificial Intelligence and Life in 2030" Available at http:ai100 stanford.ed.35-t-2016.
- IBM Cost of Data Breach 2021, https://www.ibm.com/reports/data-breach
- (April 2020) Journal of Computer and information science: Vol.5 No1 Sakarya University.
- Pedro García-Trejo (2024) The impact of emerging technologies on industrial safety. MAPFRE Global Risks: https://www.mapfreglobalrisks.com/en/risks-insurance-management/article/the-impact-of-emerging-technologies-on-industrial-safety/

Received 30 Jan. 2025; Accepted 10 Feb. 2025; Available online 19 Mar. 2025

مركز البحوث الأمنية
جامعة نايف العربية للعلوم الأمنية
الرياض، المملكة العربية السعودية

Security Research Center
Naif Arab University for Security Sciences
Riyadh, Saudi Arabia

الكلمات المفتاحية: الأمن الصناعي، السلامة الصناعية، التقنيات الناشئة، المخاطر الأمنية، المنشآت الصناعية.

Keywords: Industrial security, industrial safety, emerging technologies, security risks, industrial facilities.

Production and hosting by NAUSS

* Corresponding Author: Security Research Center
Email: srcenter@nauss.edu.sa
doi: 10.26735/XRLP3906