

# الآفاق المستقبلية لسوسيولوجيا المخاطر الصناعية في ظل تفاقم التهديدات السيبرانية

## *The Future Prospects of the Sociology of Industrial Risks in the Context of Escalating Cyber Threats*

صفية خلاف \*

المركز الجامعي بركة /الجزائر

أ.د سعيد زيوش \*\*

المركز الجامعي بركة /الجزائر

تاريخ الإرسال: 2023-12-17 تاريخ القبول: 2024-02-16 تاريخ النشر: 2026-07-11

**ملخص:** تزايدت في السنوات الأخيرة التهديدات السيبرانية التي تمس مختلف القطاعات خاصة القطاع الصناعي، حيث شكلت هذه التهديدات خطرا حقيقيا على الأنظمة الصناعية ، فالتعرض للجرائم السيبرانية من شأنه أن يوقف الإنتاج في المنشآت الصناعية الكبرى و زيادة خطر الحوادث المهنية و فقدان الوظائف، و تعطيل عمل الأنظمة الحيوية، و بالتالي تراجع النمو الإقتصادي لهذه الدول.

لذا تهدف هذه الورقة البحثية لتسليط الضوء على أثر التهديدات السيبرانية على القطاع الصناعي، و كذا استراتيجيات الدول لفرض السيادة الرقمية على أنظمتها الصناعية.

\* المؤلف المرسل: خلاف صفية

\*\* البريد الإلكتروني للمؤلف الثاني: said.ziouchesaid@cu-barika.dz

**Abstract:** In recent years, cyber threats have increasingly been targeting various sectors, especially the industrial sector. These threats pose a real danger to industrial systems. Falling victim to cybercrimes can halt production in major industrial facilities, increase the risk of occupational accidents, leads to job losses, and disrupt vital systems, ultimately causing a decline in economic growth for these countries. Therefore, this research paper aims to shed light on the impact of cyber threats on the industrial sector and the strategies employed by nations to establish digital sovereignty over their industrial systems.

**Key words:** Digital Sovereignty, Cybersecurity, Cyber Threats, Occupational Accidents

## مقدمة:

شهدت المجتمعات الحديثة تغيرات واسعة مست مختلف القطاعات، فمع توسع استخدام الانترنت و انتشار التكنولوجيا الرقمية، ظهرت تحديات جديدة و متزايدة في مجال سوسيولوجيا المخاطر الصناعية، وتعتبر التهديدات السيبرانية أحد أهم التحديات التي تواجه الأنظمة الصناعية في القرن الواحد و العشرين، إذ تفرض هذه التهديدات أنماطا جديدة من المخاطر الصناعية تستدعي تفكيراً معمقاً و دراسات سوسيولوجية متقدمة لمواجهتها و التصدي لها، و التي قد تتسبب في تعطيل الأنظمة الحيوية أو القضاء على اقتصاد هذه الدول، وقد تمحورت إشكالية ورقتنا البحثية حول التساؤل التالي: كيف تؤثر التهديدات السيبرانية على مؤسسات القطاع الصناعي؟

و بناءاً على ذلك تم تقسيم هذه الورقة البحثية إلى أربعة أجزاء رئيسية، يتناول الجزء الأول: سوسيولوجيا المخاطر الصناعية، و يتحدث الجزء الثاني عن الأمن السيبراني و التهديدات السيبرانية، و يطرح الجزء الثالث بعض نماذج لمؤسسات

صناعية اخترقت أنظمتها، أما الجزء الأخير فيعرض استراتيجيات الدول لفرض السيادة الرقمية على القطاعات الصناعية.

## 1. أولاً : سوسيولوجيا المخاطر الصناعية:

### 1.1 نشأة علم اجتماع المخاطر:

شهدت المجتمعات البشرية في العصر الحديث تحولات كبيرة، حيث تحول نهج هذه المجتمعات من التركيز على الأمان إلى التركيز على المخاطر، و لم ترتكز تلك التحولات على جوانب معينة في الحياة الاجتماعية، بل امتدت إلى جميع جوانبها، و أثرت على الجوانب الصحية و الاقتصادية و الثقافية و البيئية للمجتمعات، و يمكن تلخيص هذه التغيرات في خمس نقاط رئيسية هي:

-التغير الأول: الانتقال من المجتمع الصناعي التقليدي إلى المجتمع المعلوماتي الذي يعتمد على البيانات و المعلومات، مما أدى إلى نشأة فضاء افتراضي جديد تحدث فيه التفاعلات السياسية و الاقتصادية و الثقافية بين اطراف من جميع أنحاء العالم، حيث يمكن أن يشترك الأفراد و المؤسسات و الحكومات من خلاله في الحوار و تبادل المعلومات و الأفكار بشكل آني، و بفضل هذا النموذج المعرفي لمجتمع المعلومات يمكن لهم الاستفادة من موارد المعرفة المتاحة عبر الانترنت، و تبادل الخبرات و التكنولوجيا، مما يسهم في تطوير الثقافة و الاقتصاد و العلاقات الدولية.

-التغير الثاني: هو الانتقال من الحداثة إلى العولمة، و يقصد بذلك العولمة السياسية و شعاراتها الديمقراطية و احترام حقوق الإنسان، العولمة الاقتصادية التي تسعى خلق سوق عالمية واحدة، العولمة الثقافية التي تعني بروز ثقافة كونية و تعميم ثقافة السوق و الاستهلاك.

-التغير الثالث: أدت التغيرات في الاقتصاد و السياسة و الثقافة و التكنولوجيا إلى إثارة تحديات و مسائل جديدة مثل: الخصوصية و الأمن السيبراني نتيجة لزيادة المخاطر الأمنية و الاقتصادية، و هو ما أدى إلى ظهور ظاهرة تعرف ب"مجتمع المخاطر" الذي نعيشه اليوم.

-اندثار النموذج القديم للأمن القومي، فحماية أمن الدول لا تقتصر اليوم على الحماية من التهديدات العسكرية حماية المعلومات من التجسس و الهجمات السيبرانية، و التصدي للهجمات الإلكترونية التي قد تؤثر على استقرار الدولة، و هذا ما يفسر التحول نحو التركيز على الأمان الإلكتروني و حماية البنية التحتية للمعلومات.

بروز قيم حضارية جديدة أهمها "المسح العالمي للقيم"، الذي يعني إجراء أبحاث لفحص كيفية تغير و تطور القيم في العالم، و كيفية تأثير العوامل الثقافية و الاجتماعية و الاقتصادية و الدينية على تلك القيم. (بحاياوي، 2020، ص10، ص11).

## 2.1 تعريف مجتمع المخاطر:

هو المجتمع الذي يعاني من عدة مشكلات من حوادث الطرقات إلى الجريمة بكل أنواعها، إلى الجرائم الجنسية و الإدمان على المخدرات و فساد الأغذية و و انتشار الأمراض و الأوبئة و تلوث البيئة، و مشكلات البطالة و الفقر و و الإرهاب، و غيرها من المشكلات الصحية النفسية منها و الفيزيولوجية الخطيرة، و التي تهدد أمن المجتمع بكل فئاته، و سنعرض تعريفات لبعض الباحثين الاجتماعيين في هذا السياق:

يعرفه "أولريش بيك": " هو طريقة منهجية للتعامل مع المخاطر و انعدام الأمن الناجم، و يتم عرضه من قبل الحادثة نفسها"

و يعرفه "أنتوني غيدنز": " هو المجتمع الذي تتزايد فيه الفجوة الطبقية بين الأغنياء و الفقراء، فهذا المجتمع يعد من مجتمعات المخاطر"

أما "نيكلاس لوكمان" فيعرفه في كتابه " المخاطرة، نظرية سوسيولوجية": " المخاطر أذى محتمل يخيف الفرد و يركز على قرار اتخذه بنفسه، إنها عملية حسابية تأخذ بعين الاعتبار الخسارة و الفائدة المحتملة بالاستناد إلى الزمن". (يحيوي، 2020، ص6، ص7).

يشير تعريف "أولريش بيك" إلى أن علم اجتماع المخاطر يؤسس لسياسات جديدة لمعالجة المخاطر المرتبطة بالتقدم التكنولوجي، حيث تعتمد على طرق منهجية تستعمل أساليب متطورة لفحص و تحليل المخاطر، و تطوير استراتيجيات لتعزيز الأمان من أجل مواجهة التحديات المستقبلية.

و يرى "أنتوني غيدنز" أن مجتمع المخاطر هو المجتمع الذي يعاني من فجوة اجتماعية و اقتصادية بين طبقاته، مما يؤدي إلى تحديات و مشكلات اجتماعية تزيد من احتمالية حدوث اضطرابات و توترات في المجتمع.

أما " نيكلاس لوكمان" فيشير إلى معنى المخاطر، حيث يقوم الأفراد بتقدير الأذى المحتمل الذي يمكن أن يحدث نتيجة لاتخاذ قرار مقابل الفوائد المحتملة، في هذه العملية الحسابية يأخذ الشخص بعين الاعتبار حجم الخسائر و المنفعة المحتملة و يقيّمها بالنسبة للوقت.

### 1. 3 مفهوم علم اجتماع المخاطر:

علم اجتماع المخاطر هو فرع من فروع علم الاجتماع العام، يركز على دراسة الظواهر المرتبطة بالأخطار في سياقها الاجتماعي و التاريخي، و يهتم بفهم أسباب و نتائج المخاطرة و كيفية تأثيرها على الأفراد و المجتمعات و محاولة تفسيرها من وجهة نظر اجتماعية، كما يعنى بدراسة الأخطار التي نشأت نتيجة التحولات

الاجتماعية و الثقافية التي ظهرت في عصر الحداثة و ما بعدها، و هي الفترة التي شهدت تطورات تكنولوجية و معرفية هائلة، و يرجع الفضل في تعزيز و تطوير مفهوم "مجتمع المخاطرة" إلى جهود عالم الاجتماع الألماني "أولريش بيك"، حيث يشير هذا المفهوم إلى المجتمعات التي تعيش المخاطر و التحديات الاجتماعية الحديثة، و التي من شأنها أن تؤثر على الحياة اليومية و الاستقرار الاجتماعي. ( بن عودة، 2017/2018، ص 4).

#### 1. 4 خصائص علم اجتماع المخاطر: يتميز علم اجتماع المخاطر بمجموعة من الخصائص، نذكرها فيما يلي:

- تنشأ المخاطر الاجتماعية نتيجة للتفاعلات الاجتماعية و الثقافية و ليس عن قوى طبيعية، لذا فهي تعكس التحديات التي يواجهها المجتمع بناء على تصرفات الأفراد.
- المخاطر الاجتماعية هي نتيجة حتمية للتقدم العلمي و التكنولوجي.
- أدى تطور الصناعة و زيادة إنتاج السلع و الخدمات إلى زيادة التفاعلات الاجتماعية و الاقتصادية، مما أدى إلى زيادة المخاطر الاجتماعية، مثل: التلوث البيئي، ظروف العمل الغير آمنة، عدم المساواة الاقتصادية.
- ساهمت العولمة و ثورة الاتصالات في تكوين العديد من المخاطر الاجتماعية، مما جعل تبادل المعلومات أسهل و أسرع، هذا الاتصال المتسارع ساعد الجماعات الإرهابية و القراصنة على الاستفادة من هذه التكنولوجيا لتنظيم أنشطتها بشكل أكثر فاعلية، الأمر الذي يتطلب تعاوناً دولياً لمجابهة هذه المخاطر الاجتماعية.
- تتجاوز المخاطر الاجتماعية الحدود الجغرافية للدول، فهي مشتركة بين مجتمعات مختلفة.

-تؤثر هذه الأخطار على جميع الأفراد و المجتمعات، بغض النظر عن مستوى الدخل أو الثروة أو الحالة الاجتماعية أو الاقتصادية، و لا تتوقف عند حدود الطبقات الاجتماعية.

-تنتشر هذه المخاطر بسرعة فائقة بسبب شبكات الانترنت و وسائل الاتصالات السريعة.

-لا يمكن التعويض عن أضرار المخاطر الاجتماعية: ففي حالة الكوارث الطبيعية أو النزاعات المسلحة مثلا، قد تستمر الآثار النفسية و الاجتماعية و الاقتصادية لفترات طويلة، و قد يستعصي الأمر عن تعويض الخسائر البشرية بصفة خاصة.

-يتطلب الحد من انتشار هذه المخاطر تعاوناً بين الحكومات و المجتمعات الدولية، و يستلزم ذلك التبادل المعرفي، دعم الحكومات المحلية، تعزيز النظام الصحي و التعليمي، و العمل المشترك في مجال الأمن الاجتماعي. ( بن عودة، 2018/2017، ص5).

**1.5 نظرية "أولريش بيك" حول مجتمع المخاطر:** تم اختيار عرض نظرية "أولريش بيك" حول " مجتمع المخاطر" في هذه المداخلة ، كونها تشير إلى المخاطر التي تمس المجتمعات الصناعية من جراء استعمال تكنولوجيا المعلومات، و نتيجة لذلك تنشأ الهجمات السيبرانية التي تهدد مستقبل القطاع الصناعي، و تتسبب في التراجع الإقتصادي.

تمثل نظرية "أولريش بيك" حول "مجتمع المخاطر" منهجا جديدا في دراسة علم الاجتماع، و التي قدمها في كتابه الشهير " مجتمع المخاطر: نحو مفهوم حديث للتقدم الاجتماعي" عام 1986، و تركز هذه النظرية على تحول المجتمعات الحديثة من مجتمعات صناعية إلى مجتمعات معرفية، و تسلط الضوء على أهم المخاطر و التحديات التي تواجه المجتمعات في العصر الحديث.

و وفقا لنظرية "بيك" يعيش المجتمع اليوم في بيئة " مجتمع المخاطر"، حيث أصبحت التكنولوجيا و الصناعات المتقدمة تنتج مخاطر جديدة و متزايدة تهدد الإنسان و البيئة على حد سواء، و تنشأ هذه المخاطر نتيجة لاستخدام التكنولوجيا الحديثة: النووية و البيئية و تشمل التلوث و الكوارث البيئية، و تحذر هذه النظرية من فكرة أن هذه المخاطر قد تكون غير محسوسة و يكون لها تأثير مستمر بشكل دائم، كما أنها تتجاوز الحدود الوطنية و تؤثر في كل المجتمعات .( يحيوي ، 2020، ص 22، ص26).

و في سياق استخدام تكنولوجيا المعلومات، تشير نظرية "بيك" إلى أن تكنولوجيا المعلومات تحمل معها تحديات و مخاطر، تشمل تهديدات الأمن السيبراني، انتهاك الخصوصية، و التي قد تقطع بسببها الروابط الاجتماعية، فالتهديدات السيبرانية تزيد من مستوى القلق و عدم الأمان بين الأفراد، مما يؤثر على استعمال الأنظمة الرقمية و التقليل من استخدام التكنولوجيا، و بالتالي يسبب خسائر اقتصادية.

## 2. ثانيا: التهديدات السيبرانية:

**2.1 مفهوم الأمن السيبراني:** يحتل الأمن السيبراني مكانة بالغة الأهمية في مجال النظم المعلوماتية عند الدول، في ظل تراكم كم هائل من المعلومات و البيانات و القيام بتخزينها و معالجتها، على أجهزة الكمبيوتر و أجهزة أخرى، إذ تحتوي العديد من هذه البيانات على معلومات حساسة، قد تتعلق بالملكية الفكرية أو معلومات شخصية أو بيانات مالية، و تنتقل هذه المعلومات بين الشركات و المؤسسات عبر الشبكات إلى أجهزة أخرى، لذا فإن الوصول غير المصرح به لها يمكن أن يتسبب في عواقب خطيرة، مما يستوجب على هذه الشركات و المؤسسات أن تحمي بياناتها و معلوماتها من هذه الهجمات الخطيرة، و التي يمكن أن تمس الأمن القومي للدول. ( كلاع، 2022، ص 299).

يشير مصطلح الأمن السيبراني إلى القوانين السياسية، و الأدوات، و النصوص، و المفاهيم، و الآليات الأمنية، و طرق إدارة المخاطر، و الممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات و الاتصالات، و يستخدم هذا المصطلح لحماية الدول و الأفراد من التهديدات السيبرانية و الهجمات الإلكترونية، كما يعرف بأنه الحالة المطلوبة لحماية نظم المعلومات و الاتصالات، حيث يكون لها القدرة على مقاومة و التصدي للتهديدات الناتجة عن الفضاء السيبراني، و التي قد تعرض المعلومات للضرر أو التغيير أو التجسس. ( محمد، 2022، ص458، 457 ).

و بحسب التقرير الصادر عن " الاتحاد الدولي للاتصالات" يعرف الأمن السيبراني على أنه: " عبارة عن مجموعة الوسائل التقنية و التنظيمية و الإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، و سوء الاستغلال، و استعادة المعلومات الإلكترونية، و نظم الاتصالات و المعلومات التي تحتويها، و ذلك بهدف ضمان توافر و استمرارية عمل نظم المعلومات، و تعزيز حماية و سرية و خصوصية البيانات الشخصية، و اتخاذ جميع التدابير اللازمة لحماية المواطنين و المستهلكين من المخاطر في الفضاء السيبراني." ( محمد، 2022، ص 458).

يشمل مصطلح الأمن السيبراني العديد من الجوانب المرتبطة بالحماية الرقمية و الأمان الإلكتروني، و يتضمن هذا المفهوم القوانين السياسية التي تضعها الدول لتنظيم استخدام وسائل التكنولوجيا من برمجيات و أجهزة، و حماية الدول و الأفراد من التهديدات السيبرانية و الهجمات التي قد تتضمن الاختراقات الإلكترونية، و الفيروسات الضارة، و الاحتيال الإلكتروني على الأنظمة الحيوية للدول، و يشكل الأمن السيبراني الدرع الحصين لحماية نظم المعلومات و التصدي للتهديدات، سواء عن طريق تقنيات التشفير القوية أو إجراءات الحماية كالتحديث المستمر للبرمجيات و الأجهزة.

إذن فالأمن السيبراني ليس مجموعة الأدوات التقنية فحسب، بل يشمل نظاما متكاملا من الوسائل التقنية و التنظيمية و الإدارية لضمان سلامة و أمان الأنظمة و البيانات في العالم الرقمي المتطور و المتغير باستمرار.

**2.2 مفهوم التهديدات السيبرانية:** تشكل التهديدات السيبرانية تحديا كبيرا أمام المجتمعات التي تحدث فيها، حيث يمكن للمهاجمين عبر الانترنت تخطي الحدود الدولية و تنفيذها من أي منطقة في العالم، و استهداف أعداد لا حصر لها من الأفراد و الشركات، و تزداد التحديات التي تشكلها هذه التهديدات باتساع نطاق الجرائم و تعقيد التكنولوجيا المستخدمة في تنفيذها، مما يصعب عملية كشف هوية الجناة، لذا يجب على الحكومات و المجتمع الدولي توحيد الجهود من أجل مواجهة هذه التهديدات و تقديم المجرمين إلى العدالة. (بارة، 2017، ص 259).

يعرفها "فيورتنس" بأنها: " هجوم عبر الانترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها، تهدف إلى تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، و هي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى". (سعودي، حسناوي، 2022، ص 106).

أي أن التهديدات أو الهجمات السيبرانية تتمثل في غزو و اختراق مواقع إلكترونية أو أنظمة معلوماتية، حيث يقوم المهاجمون غير مرخص لهم بالدخول إلى هذه المواقع بهدف تعطيل الخدمات أو تدمير البيانات المخزنة فيها أو سرقتها، و غالبا ما تكون هذه الهجمات جزءا من الصراعات السياسية أو العسكرية بين الدول، و يمكن أن تؤثر هذه الهجمات على البنية التحتية للدولة و أمنها الوطني، لذا فهي تتطلب مواجهة فعالة و فورية من السلطات المختصة لمنع وقوع أضرار جسيمة.

كما يشير مفهوم التهديدات السيبرانية إلى الهجمات و الأنشطة الخبيثة التي تستهدف الأنظمة الإلكترونية عبر استخدام التكنولوجيا و الحواسيب لأغراض مثل:

تدمير بنية المعلومات للأعداء و إعاقة أنظمة الدفاع الجوي، و اختراق أنظمة المعلومات الحساسة مثل: البريد الإلكتروني لمكاتب رؤساء الدول، و عمليات التجسس وفق خطط مدروسة. (عطية، 2019، ص 108).

### 2.3 أنماط التهديدات السيبرانية: تأخذ التهديدات السيبرانية عدة أنماط، منها:

- هجمات التجسس التقليدي: التي تستخدمها دول ضد دول أخرى، حيث تنفذ هجمات سرية للحصول على المعلومات و البيانات المتعلقة بمؤسسات الدولة سواء المدنية أو العسكرية، و تتنوع أغراض هذه الهجمات السياسية و المالية و الدينية و المذهبية، الهدف منها استخراج المعلومات الحساسة لتحقيق مكانة متقدمة في الصراعات و التنافسات الدولية.

- الهجمات الإلكترونية التكتيكية: و يعتمد فيها المهاجمون على تخريب نظم معلومات الخصم، و ذلك معلومات كاذبة داخل أنظمة الذكاء الخاصة بالعدو و تشويه الرؤية و الاستراتيجيات الخاصة بالخصم، و يستخدم هذا النوع من الهجمات الخبث الإلكتروني لإلحاق الأضرار بالخصم دون الحاجة إلى الهجوم المباشر، مما يمكن المهاجمين من تعطيل و تقويض القدرة على الاستجابة و اتخاذ القرارات الهامة للخصم.

- تعطيل نظم معلومات الخصم: و التي تستهدف الحكومات و الشركات و تعطيل نظم المواصلات و النقل و الانترنت، حيث يستهدف هذا النوع من التهديدات السيبرانية البنية التحتية الرقمية التي لها تأثير كبير على الاقتصاد الوطني، إذ يمكن أن يتسبب الهجوم عليها في خسائر مالية كبيرة و أضرار اقتصادية قد تمتد لفترة طويلة يصعب التعافي منها بسرعة. (شرقي، 2023، ص 275).

### 2.4 مصادر التهديدات السيبرانية: هناك العديد من مصادر التهديدات

السيبرانية، نذكر منها:

-شبكة الانترنت: تعتبر الانترنت و الحواسيب من المصادر الرئيسية للتهديدات في العالم الافتراضي، نظرا لقدرتهما الغير محدودة على اختراق الحدود الدولية خاصة في الدول التي تعاني من ضعف التكنولوجيا، و يمكن للدول الرائدة في مجال تكنولوجيا المعلومات اختراق شبكات هذه الدول بكل سهولة و الوصول إلى أسرار المؤسسات الحكومية و مناطقها السيادية، بالإضافة إلى تعطيل شبكاتها، مما يجعلها تواجه تحديات تقنية و فجوات أمنية، ففي الوقت الحالي أصبح من السهل جدا إرسال فيروسات للدول الضعيفة تكنولوجيا و ابتزازها من أجل احتلالها أو الحصول على معلومات سرية و سيادية منها، و ذلك باستخدام برامج خبيثة، مثل: الفيروسات، الديدان، أحصنة طروادة، برامج التجسس، و غيرها..، و قد عزز من نجاح هذه الهجمات وجود مؤسسات دولية و قرصنة ذوي كفاءة عالية يقومون بأداء هذه المهام.

الوسائل التكنولوجية كمصدر للتهديد: أصبحت وسائط الاتصال الحديثة أدوات قوية لنقل المعلومات إلى الخارج، بفضل التقنية الرقمية و الذكاء الإلكتروني، و التجسس على الأفراد و المؤسسات و إعطاء تفاصيل دقيقة عن خصوصياتهم ، مثل: الهواتف الذكية و شاشات التلفزيون و ساعات اليد، إذ تحمل هذه الأجهزة تطبيقات يمكن أن تستخدم لتحديد الموقع، و كاميرات يمكنها الوصول إلى الأماكن بشكل غير مرئي داخل المنازل، بالإضافة إلى مشاركة معلومات حساسة مع الجهات المعادية، مما يشكل تهديدا للأمن القومي للدول.( باسمايل، 2022، ص 147، ص148).

### ثالثاً: نماذج مؤسسات صناعية اخترقت أنظمتها:

مع الاستعمال المتزايد للأنظمة المعلوماتية، و مع انتشار الأجهزة المتصلة بالشبكة الدولية للمعلومات و تنوعها، مثل: الهواتف الخلوية و أجهزة الحاسوب الشخصية و كذا اللوحات الرقمية، يتزايد عدد الأفراد الذين يستعملون الفضاء السيبراني، و بالتالي يزداد عدد الاعتداءات و الجرائم السيبرانية، و التي تشمل التجسس الإلكتروني، الهجمات الضارة مثل الفيروسات و برامج الاختراق، و منع الخدمة التي تعطل خدمات الانترنت، و سرقة بيانات الشخصية و الرسائل الاقترامية، كل هذه التهديدات تضر بمصادقية تكنولوجيا المعلومات و الاتصالات، و تمثل تهديداً لسلامة أمن و المعلومات الحساسة للحكومات و المؤسسات، و من أمثلة الهجمات السيبرانية على المؤسسات الصناعية ما أصاب محطات الطاقة الأوكرانية عام 2017 ، و الذي تسبب في بقاء أوكرانيا لساعات طويلة في الظلام، و الهجوم السيبراني على شركة أرامكو السعودية الذي كلفها تغيير خمسين ألف قرص صلب لأجهزتها الحاسوبية و لم تستطع استخدام الانترنت لمدة خمس أشهر. (فوزي، ص109، ص110).

كما تعرضت أنظمة الكمبيوتر لشركة كوريا الجنوبية للطاقة المائية و النووية التي تديرها الدولة لهجمات إلكترونية عام 2014، و تعرضت البرازيل عام 2008 لهجمات سيبرانية من طرف قرصنة أدت إلى قطع الكهرباء لمدة تزيد عن أسبوع، حيث توقفت قطارات الأنفاق و إشارات المرور و ثاني أكبر محطة إنتاج قوة كهربائية و تأثر بسبب ذلك أكثر من ستين مليون شخص، و تعرض خط أنابيب النفط التركي عام 2008 لهجمات سيبرانية أدى إلى اشتعاله، و استهدف قرصنة إيرانيون سيبرانيون قطاع الطيران و البيتروكيماويات بواسطة فيروس "الصخرة الدوارة" عام 2019، و قد شهدت إيران عدة انفجارات لمصانع في مدن مختلفة، مثل: تسرب غاز الكلور في مركز "كارون" للبيتروكيماويات في مدينة "ماشهر"، و

انفجار مصنع الأكسجين في بلدة "باقر" و انفجار منشأة صواريخ تابعة للحرس الثوري الإيراني غرب مدينة طهران، و حريق في مصنع الألمنيوم في بلدة "لامرد"، كما أعلنت مجموعة تسمى "المنقمون" الإيرانية مسؤوليتها عن هجوم سيبراني على شبكة المياه و الكهرباء الإسرائيلية عام 2020. (كلاع، 2022، ص 300، 301، 302).

من خلال ما تم عرضه في هذه الفقرة، يتبين أن الهجمات السيبرانية تؤثر بشكل كبير على مجموعة متنوعة من القطاعات الصناعية، حيث يمكن أن تتسبب في:

-توقف الإنتاج: فتعطيل الأنظمة الصناعية الأوتوماتيكية، يؤدي إلى توقف الإنتاج في المنشآت الصناعية، مما يسبب خسائر مالية ضخمة للشركات.

-خطر سلامة العمال: يمكن أن تسبب الهجمات السيبرانية المتعلقة بالصناعات الكيميائية مثل النفط و الغاز، بتعطيل نظم السلامة و زيادة خطر الحوادث الصناعية، مما يهدد حياة العمال.

-توقف الخدمات: تهدد الهجمات السيبرانية تعطيل الخدمات المرتبطة بصناعات مثل: الكهرباء و الماء، و التي تعتبر أساسية في الحياة اليومية للأفراد، مما يخلق حالة من عدة الاستقرار في المجتمع.

-التراجع الاقتصادي: تسبب الهجمات السيبرانية تعطيل الصناعات الكبرى و فقدان الوظائف مما يتسبب في تخفيض الإنتاج و تراجع النمو الاقتصادي.

#### رابعاً: الاستراتيجيات المتبعة لفرض السيادة الرقمية على القطاعات الصناعية:

في ظل التطورات التكنولوجية الهائلة، ظهر مفهوم السيادة الرقمية و الذي أصبح كجزء لا يتجزأ من السيطرة على قطاع الصناعة، و تجاوز مفهوم السيادة الحدود الإقليمية للدول بفعل تكنولوجيا المعلومات، ففي بداية ظهور هذا المفهوم ارتبط ارتباطاً وثيقاً بأمن الدولة، و مع نهاية الحرب الباردة أتيحت الفرصة أمام

المهندسين و الشركات لابتكار حلول للعديد من المشكلات الاجتماعية و الاقتصادية، و تجسدت الهيمنة الأمريكية على الانترنت عن طريق مناداتها بمبادئ مثل: حرية التعبير و رأسمالية السوق الحر و الديمقراطية الليبرالية مما أسهم في تقويض سيادة الدول رقميا، الأمر الذي دفع العديد من الدول مثل: الصين، روسيا، ألمانيا، و فرنسا السعي لتحقيق مفهوم السيادة الرقمية على فضاءاتها السيبرانية، حماية لمجتمعاتها.

ف نجد مثلا أن الصين قد اقترحت في مؤتمر بودابست حول القضايا السيبرانية خمسة مبادئ للتعاون الدولي في الفضاء السيبراني، أولها السيادة مشيرة إلى أنها: " حق كل دولة في صياغة سياساتها و قوانينها في ضوء تاريخها و ثقليدها و ثقافتها و لغتها و عاداتها"، و قد تحدث الرئيس الصيني في المؤتمر العالمي الأول للانترنت عام 2014 في ذات السياق قائلا: " ينبغي علينا احترام حقوق كل بلد في تطوير و استخدام و إدارة الانترنت، و الامتناع عن استغلال الموارد و القوى التكنولوجية لانتهاك السيادة الرقمية للدول الأخرى"، لذلك أصدرت عام 2017 "قانون الأمن السيبراني" بغرض ضبط و تنظيم الفضاء السيبراني لحماية الدولة و المجتمع.

و نجد أن فرنسا قد قامت بالاستغناء عن محركات البحث التابعة للشركات الأمريكية، و استبدلتها بمحركات ألمانية-فرنسية تسمى كوانت، بالإضافة إلى إصلاحات في الجانب الرقمي للتصدي للهيمنة الأمريكية.

أما بالنسبة للولايات المتحدة الأمريكية فتفرض تطبيق فكرة السيادة الرقمية في الفضاء السيبراني بحجة أن هذا الأخير مفهوم عالمي، و لا يصح بناء حواجز سيادية حول دخول و خروج المعلومات من و إلى الدولة، و في ذلك تكريس للهيمنة الرقمية الأمريكية على النظام الدولي. ( شرقي، 2023، ص278-ص280).

## خامسا: خصائص التداخل بين الأمن السيبراني وسوسيولوجيا المخاطر

تداخل الأمن السيبراني وسوسيولوجيا المخاطر الصناعية يمثل مجالا هاما يشمل دراسة التأثيرات الاجتماعية والبيئية للتهديدات والهجمات السيبرانية على المؤسسات والمنظمات الصناعية. إليك بعض النقاط المهمة التي تتناول هذا التداخل:

1- تأثير التكنولوجيا على الصناعة: يعكس هذا التداخل كيفية تأثير التكنولوجيا والأتمتة في الصناعة على الأمان السيبراني. تزايد استخدام التكنولوجيا في الصناعة يزيد من تعرضها للهجمات السيبرانية ويتطلب تطوير استراتيجيات أمن سيبراني أقوى.

2- الآثار الاقتصادية والاجتماعية: هجمات الأمان السيبراني يمكن أن تؤثر بشكل كبير على الاقتصاد والمجتمع. تعطل الإنتاج وتسبب فقدان وظائف في الصناعة وقد تؤدي إلى تأثيرات اجتماعية سلبية.

3- التشريعات واللوائح: تأثير هجمات السيبرانية على الصناعة يعزز من أهمية وجود تشريعات ولوائح فعالة لحماية المعلومات والبنية التحتية الحيوية للصناعة. هذه التشريعات تلعب دورا كبيرا في تحديد مسؤوليات المؤسسات الصناعية وتعزيز الأمان السيبراني.

4- تقييم المخاطر: يجب على المؤسسات الصناعية أن تقوم بتقييم المخاطر السيبرانية بناءً على طبيعة أنشطتها وأثرها على المجتمع. هذا يشمل تحليل العوامل الاجتماعية والاقتصادية التي يمكن أن تؤثر على أمان الصناعة.

5- التعليم والتوعية: يجب تعزيز التعليم والتوعية بأمان السيبراني في الصناعة والمجتمع بشكل عام. هذا يمكن أن يساهم في تحسين الوعي بمخاطر الأمان السيبراني وتعزيز الاستجابة السريعة للتهديدات.

فهم هذا التداخل بين الأمن السيبراني وسوسيولوجيا المخاطر الصناعية يساعد في تطوير استراتيجيات أمنية أفضل وفهم التأثيرات الاجتماعية والاقتصادية للهجمات السيبرانية على الصناعة والمجتمع بشكل أفضل. (ستيف، 2023)

### خاتمة:

من خلال ما تم عرضه في هذه المداخلة، نستنتج أن التحولات السريعة في عالم التكنولوجيا الرقمية قد أفرزت مشكلات جديدة تؤثر على قطاع الصناعة، تتمثل في التهديدات السيبرانية، و التي تتطلب فهما عميقا لكيفية تأثيرها على الهياكل الاجتماعية و الاقتصادية للمجتمعات ،و يستدعي التصدي لها و مواجهتها تعاونا و تنسيقا دوليا فعالا.

### قائمة المراجع:

بارة،سمير.(2017) . "الأمن السيبراني في الجزائر: السياسات و المؤسسات".المجلة الجزائرية للأمن الانساني، (4)، ص 259 .  
تم استرجاعه يوم: 2023/10/19، <https://www.asjp.cerist.dz/en/PresentationRevue/474>

باسماعيل، عبد الكريم.( 2022 ). "تأثير الفضاء الافتراضي على الأمن القومي". مجلة البحوث و الدراسات: 19 (1): ص 147، ص148.

استرجاعه تم ، <https://www.asjp.cerist.dz/en/Articles/202> يوم: 2023/10/19.

بن عودة، محمد. ( 2017 / 2018 )، "سلسلة دروس في علم اجتماع المخاطر"، موجهة لطلبة السنة الثالثة علم الاجتماع، كلية العلوم الاجتماعية و الإنسانية، خميس مليانة، جامعة الجليلي بونعامة ، ص 5.

سعودي، آمال. حسناوي، مهدية. (2022). "الأمن السيبراني: دراسة في الآليات الأمنية للوقاية من الهجمات السيبرانية". مسطرة إجرائية لأعمال الملتقى الدولي - الأمن السيبراني و التحديات المعاصرة- ، ص 106.

شرقي، عبد الغاني. (2023). "التحديات السيبرانية و إشكالية السيادة: إعادة قراءة لسيادة و استقلالها". مجلة السياسة العالمية : 7 (2)، ص 275، ص 278-280. <https://www.asjp.cerist.dz/en/article/223394> تم استرجاعه يوم: 2023/10/22.

عطية، إدريس. (2019). "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري". مجلة مصداقية (1) ، ص 108 . <https://www.asjp.cerist.dz/en/article/125955> تم استرجاعه يوم: 2023/09/15.

فوزي، إسلام. (2019). "الأمن السيبراني: الأبعاد الاجتماعية و القانونية تحليل سوسيولوجي". المجلة الاجتماعية القومية: 56 (2)، ص 109، ص 110. [https://jns.journals.ekb.eg/article\\_205220.html](https://jns.journals.ekb.eg/article_205220.html) تم استرجاعه يوم: 2023/10/26.

كلاع، شريفة . (2022). "الأمن السيبراني و تحديات الجوسسة و الاختراقات الإلكترونية للدول عبر الفضاء السيبراني".مجلة الحقوق و العلوم الانسانية: 15 (1)، ص 299، ص300-ص302.

، تم استرجاعه <https://www.asjp.cerist.dz/en/article/186191>

يوم: 2023/10/20.

محمد، مسيكة. ( 2022 ). "الفضاء السيبراني و تحديات الأمن القومي".مجلة العلوم القانونية و الاجتماعية: 7 (4)، ص45، ص 458 .  
<https://www.asjp.cerist.dz/en/article/205884>، تم استرجاعه يوم: 2023/10/15.

يحياوي، نجاه. ( 2020 )، "محاضرات في مقياس: علم اجتماع المخاطر"، مطبوعة موجهة لطلبة السنة الثالثة علم الاجتماع، كلية العلوم الإنسانية و الاجتماعية، بسكرة، جامعة محمد خيضر، ص 6، ص7، ص10، ص11، ص22-ص26.

Steve Ursillo, Jr. Christopher Arnold, Cybersecurity Is Critical for all Organizations – Large and Small, <https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small> , تاريخ الاطلاع 2023-10-25