

سبل استغلال الذكاء الاقتصادي في مواجهة المخاطر الرقمية

Ways to Exploit Economic Intelligence in the Face of Digital Risks

أ.د. طاف زهير

أ. محمدي أسماء

جامعة طاهري محمد، بشار، الجزائر

جامعة طاهري محمد، بشار، الجزائر

zedtaf@gmail.com

sanaamakhiloui@gmail.com

تاريخ القبول: 2019/02/08

تاريخ الاستلام: 2018/07/28

الملخص:

تكمن أهمية الدراسة في طبيعة الموضوع التي تعالجه وتهدف إلى إبراز الطرق التي يمكن من خلالها استغلال ممارسات الذكاء الاقتصادي للكشف من جهة، والحد من جهة أخرى من مخاطر وتهديدات المحيط الرقمي، ومن الاستعمال غير المؤمن لتكنولوجيات الإعلام والاتصال الحديثة. وللإجابة على الإشكالية التالية: "كيف يمكن الاستفادة من عمليات الذكاء الاقتصادي في التصدي لتهديدات البيئة الرقمية؟"، تم الاعتماد على الأسلوب الوصفي التحليلي كمنهجية أساسية للدراسة، وذلك من خلال ما هو متاح من أدبيات وبحوث تتعلق بالموضوع في بناء جوانب الدراسة النظرية والتحليلية المتعلقة بالمخاطر الرقمية التي تتعرض لها المؤسسات وكذا الجوانب المتعلقة بالذكاء الاقتصادي وممارساته في مواجهة تلك المخاطر، وقد تم كذلك الاعتماد على المنهج التحليلي لتقييم نشاط الذكاء الاقتصادي في مواجهة المخاطر الرقمية.

الكلمات المفتاحية: تكنولوجيات الحديثة للإعلام والاتصال، جرائم الكترونية، ذكاء اقتصادي، محيط رقمي، مخاطر رقمية.

Abstract:

The importance of the study lies in the nature of the topic that it addresses and aims to highlight the ways in which economic intelligence practices can be exploited to detect, on the one hand, and reduce the risks and threats of the digital environment, and from the unsecured use of modern information and communication technologies. To answer the following problem: "How can economic intelligence operations be used to address the threats of the digital environment?", the descriptive analytical method analytical related to the digital risks to enterprises as well as aspects of economic intelligence and practices in the face of these risks, and also relied on the analytical approach to assess the activity of economic intelligence in the face of digital risks.

KeyWords: Digital Environment, Digital Risks, Economic Intelligence, Electronic Crimes, Modern Information And Communication Technologies.

JEL Classification: M1, O3.

* مرسل المقال: محمدي سميحة (sanaamakhiloui@gmail.com).

المقدمة

على مدى العقدين الماضيين، أصبحت تكنولوجيا المعلومات والاتصالات (ICT)، بما في ذلك الإنترنت، جزءاً أساسياً من عمل الاقتصاد ورافعة حقيقية للتنمية في جميع القطاعات. وحتى يمكن مخاطبة تحديات المستقبل في القرن الواحد والعشرين الذي أصبح أكثر تعقيداً مما كان عليه العالم في السنوات الماضية، والذي صار يشكل عالماً متواصلاً معتمداً على بعضه البعض، وعلى التحولات السريعة في الإنتاج وجودته المتناهية في سوق عالمية تنافسية، والواقع أن الأنشطة الرئيسية للمؤسسات تعتمد الآن على البيئة الرقمية.

فالبيئة الرقمية، أمر بالغ الأهمية لأداء اقتصادياتنا ومجتمعاتنا، فهي تحفز النمو والابتكار والشمولية، والفوائد التي تجلبها تمتد إلى جميع قطاعات الاقتصاد وجميع جوانب التقدم الاجتماعي، تتعلق بالطابع العالمي والمفتوح والمترابط والدinاميكي لتكنولوجيات المعلومات والاتصالات والهياكل الأساسية ومع ذلك، فإن أوجه عدم اليقين المرتبطة باستخدام هذه البيئة أخذه في الازدياد، وأصبحت التهديدات الرقمية أكثر عدداً في السنوات الأخيرة، مع ما يترتب على ذلك من عواقب اقتصادية واجتماعية كبيرة على المؤسسات. وفي زمن العولمة، تكون تكنولوجيات المعلومات والاتصالات الجديدة للجهات الفاعلة الاقتصادية مصدراً للتبادل وتطوير الأعمال تستخدم لأغراض التدخل والتجسس الصناعي، فإنها تصبح سلاحاً ضد أعمالنا والعمالة. ويتزايد إدراك أصحاب المصلحة بأنه من الضروري البحث عن الأداة الفعالة للسيطرة على هذه المخاطر الرقمية وتعظيم الفرص، والمساعدة في عملية صنع القرار للاستفادة الكاملة من الفوائد الاقتصادية والاجتماعية للبيئة الرقمية، فالبحث عن أداة تحد من المخاطر الرقمية الآن مسألة تتعلق بأمن المجتمع، لذا فالذكاء الاقتصادي يعتبر من السبل الفعالة لذلك ويعتبر ضرورة لمستقبل المؤسسات وأمنها. على ضوء ما سبق تتجسد مشكلة الدراسة في التساؤل التالي:

كيف يمكن الاستفادة من عمليات الذكاء الاقتصادي في التصدي لتهديدات البيئة الرقمية؟
وتندرج تحت هذه الإشكالية أسئلة فرعية:

- ما المقصود بالبيئة الرقمية؟
- أين تكمن مخاطرها وما هي عواقبها؟
- وكيف يمكن توظيف الذكاء الاقتصادي لمواجهة تلك المخاطر؟
- بناءً على الإشكالية الرئيسية والإشكاليات الفرعية يمكن وضع الفرضيات الرئيسية التالية:
- تنتج المخاطر الرقمية من عدم التحكم في التكنولوجيا ونقص التكوين.
- مخاطر البيئة الرقمية تتعدى خطر تعرض الأجهزة للفيروسات بل تهدد التراث المعلوماتي للمنظمة وتجعلها عرضة للتجسس الاقتصادي.
- عمليات الذكاء الاقتصادي تساعد بالتنبؤ بالمخاطر الرقمية والتصدي لها بفعالية.

- تكمن أهمية وأهداف دراستنا في التعرف على نظام الذكاء الاقتصادي وكيف يمكن أن يساعد المؤسسة في مواجهة المخاطر الرقمية.

تم الاعتماد على الأسلوب الوصفي التحليلي كمنهجية أساسية للدراسة، وذلك من خلال ما هو متاح من أدبيات وبحوث تتعلق بالموضوع في بناء جوانب الدراسة النظرية والتحليلية المتعلقة بالمخاطر الرقمية التي تتعرض لها المؤسسات وكذا الجوانب المتعلقة بالذكاء الاقتصادي وممارساته في مواجهة تلك المخاطر، وقد تم كذلك الاعتماد على المنهج التحليلي لتقييم نشاط الذكاء الاقتصادي في مواجهة المخاطر الرقمية.

أما فيما يخص المحاور الرئيسية التي تشكلت منها الدراسة يمكن تحديدها فيما يلي:

- الذكاء الاقتصادي وماهيته.
- البيئة الرقمية والمخاطر الرقمية.
- التدابير الأمنية ودور الذكاء الاقتصادي في مواجهة المخاطر الرقمية.
- واقع ممارسات الذكاء الاقتصادي في مواجهة المخاطر الرقمية في الجزائر.

1. نبذة مختصرة عن دراسات سابقة في الموضوع:

أما الدراسات السابقة التي تمت في هذا الموضوع يمكن ذكر منها:

- دراسة (Samer ALHawari, Adel Hamdan, and Maher Abu Hamdeh) لموضوع Framework For Managing Electronic Risk(Development of a Conceptual) ، التي تطرق فيها الى المخاطر الالكترونية وبحث في عمليات ادارتها. (ALHawari, Hamdan, Abu Hamdeh, 2009)
- دراسة بعنوان "Insurance - Risk and opportunity in an increasingly digital world -Governance Leadership Network"، حين تطرقت الى مخاطر في العالم الرقمي وما تفرزه تجاه مؤسسات التأمين، حيث أشارت الدراسة إلى أن الجريمة الالكترونية هي الجانب المظلم من العالم الرقمي. وكلما أصبحت شركات التأمين وزبائنهم أكثر اعتمادا على المستوى الرقمي، ازدادت مخاطر الضرر المالي والسمعة وحتى المادي. يدرك المديرون أن الأمن جزء أساسي من الرقابة حيث إذا كانوا لا يستطيعون حماية المؤسسة بشكل معقول، أو زبائنهم، وما شابه ذلك، ينبغي ألا نتوقع ان ينجحوا في المساعي الرقمية. (Tapestry networks, 2015)

- دراسة عمامرة نبيلة، مغتات صابرينة لموضوع ' أهمية الأمن المعلوماتي كمدخل لتفادي الجرائم المعلوماتية في ظل الاقتصاد الرقمي، حيث خلص بأنه أصبح استخدام البيئة المعلوماتية والرقمية في كافة المجالات والمعاملات الخاصة بالاقتصاد أمرا لا يستهان به، بل أصبح ضرورة ملحة ما يستدعي المراقبة البحثية، العلمية والعملية للتعامل مع هذه البيئة وإيجاد الحلول اللازمة لتهدداتها بإتباع طرق وذلك من خلال سياسة الأمن المعلوماتي، والتي يجب أن تكون محكمة وأن تتوزع على كل مستويات الهيكل التنظيمي للمؤسسات والمنظمات (من مستخدمين، موظفين، إدارة، زبائن، واستشاريين)، وأن تكون قابلة للتطبيق والمراجعة المستمرة بعكس كل تغيرات الاقتصاد الرقمي في بيئة عمل

المنظمة أول بأول وجعلها مرنة وفعالة لأطول فترة ممكنة. وهذا لضمان نجاحها في سبيل مواجهة الجرائم المعلوماتية التي أصبحت بالفعل تهدد الأمن المعلوماتي. (عمارة ومغتات، 2014)

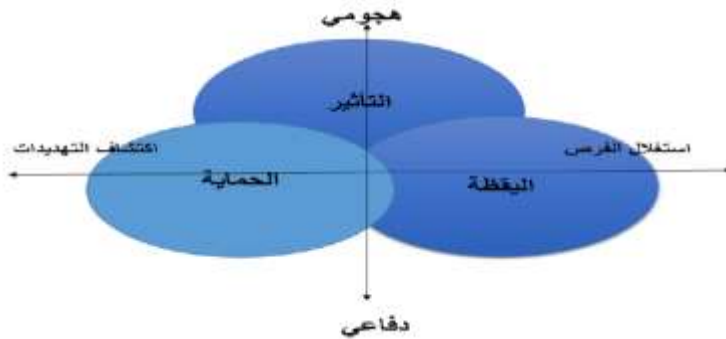
- دراسة يحياوي مفيدة، وشارب خالد 'الجريمة الإلكترونية والجهود الجزائرية للحد منها' تبين من هذه الدراسة البعد الإجرائي لجرائم الكمبيوتر والانترنت والذي ينطوي على تحديات ومشكلات جمة، لذلك فانه من الضروري سد الفراغ التشريعي وسرعة المواجهة التشريعية ووضع قواعد قانونية خاصة بالقانون الجزائري لملائمة هذه الجرائم الإلكترونية، وقانونية وحجية أدلة جرائم الكمبيوتر والانترنت، ومشكلات الاختصاص القضائي والقانون الواجب التطبيق لمواكبة التشريعات المختلفة لتحديات العصر الرقمي أو المجتمع الإلكتروني. (يحياوي وشارب، 2014)

من خلال دراسة حراق مصباح، هبول محمد، 'القرصنة الإلكترونية في ظل الاقتصاد الرقمي، مخاطرها وسبل مواجهتها' تبين أنه يمكن حصر القرصنة الإلكترونية والتقليل من تداعياتها من خلال إتباع سبل حمانية معينة مجتمعة لا متفرقة، وفي مقدمتها السبل التقنية من خلال توفير بنية تحتية أمنية للتجارة الإلكترونية وهو الأمر الذي يتوقف على استخدام تقنيات مثل: التوقيع الإلكتروني، البصمة الإلكترونية، الشهادات الرقمية، استخدام مضادات الفيروسات والجدران النارية والتي تنطوي هي الأخرى على أهمية بالغة في حماية الحواسيب وأنظمتها والمواقع الإلكترونية من هجمات الاختراق والتجسس. ولأن الحماية التقنية وحدها لا تكفي دوما فلا بد من حماية قانونية وعقوبات تشريعية اتجاه الأضرار التي يخلفها القراصنة على مصالح مختلفة الأطراف، ولكن رغم تطور التشريعات الغربية في هذا المجال تبقى التشريعات العربية بدون موقف وهو أمر سلبي يهدد اقتصادياتها، فلا بد من الإسراع لتدارك هذا التأخر. إلى جانب الإجراءات الحمانية السابقة تبقى ضرورة التوعية بمخاطر هذه الظاهرة ضرورة التوعية الدينية والأخلاقية، كون أغلب الجرائم الإلكترونية التي تحدث سببها نقص الوازع الديني والأخلاقي لدى كثير من الشباب. (حراق، 2014)

2. الذكاء الاقتصادي

الذكاء الاقتصادي مفهوم جديد نسبيا ولا يوجد تعريف واحد له فهو يستند بوصفه حكما رشيدا إلى ثلاث ركائز، الركيزة الأولى اليقظة: تتمثل في حشد وسائل وأدوات الرصد لكشف وتحليل المعلومات والأحداث ذات الصلة لنشاط الأسواق وأصحاب المصالح الذين يديرونها: الفرص، التهديدات، المخاطر، العملاء، المنافسين....، الركيزة الثانية التأثير: تقوم المؤسسة بتنفيذ الاستراتيجيات التأثير لتوجيه عمل الجهات الفاعلة في الأسواق والأقاليم، والمنافسات التنافسية، والتعاون لصالح مصالحها وأخيرا: الأمن الاقتصادي تواجه المؤسسة في أسواقها الذكاء الاقتصادي لمنافسيها. ويجب أن تدمج في إستراتيجيتها عملية للأمن الاقتصادي تشمل رصد وحماية المعارف والتقنيات الرئيسية للشركة، فضلا عن أمن نظم معلوماتها والبيانات الرئيسية (الملفات، والخطط، وإستراتيجية التسويق، والتجارة. et Gonzalez, 2017) والشكل التالي يوضح أهم وظائف الذكاء الاقتصادي:

الشكل رقم 01: وظائف الذكاء الاقتصادي



المصدر: ترجمة لما جاء في: (Delbecque, 2006, p64) بتصرف.

الذكاء الاقتصادي يعتبر سلسلة من المهام مستوحاة من مفاهيم الأنجلوسكسونية (ذكاء الأعمال، الذكاء تنافسي، ذكاء تنظيمي) للاستفادة من التحولات في الاقتصاد المعاصر:

1.2. ذكاء الأعمال (L'intelligence d'affaires، Business Intelligence):

هو تركيب من البيانات والمعلومات والمعرفة حول بيئة الأعمال في إحدى المؤسسات التي تجري أعمالها (عند الحاجة)، بحيث تمنح لها ميزة تنافسية كبيرة مما يتيح لهم اتخاذ قرارات واضحة. (Abiodun, 2007, p : 39)

2.2. الذكاء التنافسي (L'intelligence compétitive ou concurrentielle):

انشأ هذا المفهوم في و.م.أ وهو مستوحاة من سيمون SIMON في كتابه الشهير العلم الجديد للإدارة (1960)، حيث عرف الذكاء التنافسي بأنه "المرحلة الأولى من عملية صنع القرار لاستكشاف البيئة لتحديد الحالات التي تستدعي اتخاذ قرار، (Loic, Harriet, 2014, p49)، فهو العملية التي تسمح برفع القدرة التنافسية في السوق من خلال فهم أفضل من المنافسين والظروف التنافسية. (Robert Charles Abiodun, 2007, p 39)

3.2. الذكاء التنظيمي Organizational Intelligence: هو الذكاء التنظيمي يأتي من خلال جمع وتحليل وتفسير ونشر المعلومات المفيدة لعملية اتخاذ القرار في المنظمة.

أول تعريف للذكاء الاقتصادي في عام 1967 في كتاب Harold Wilensky ويعرف "الذكاء الاقتصادي نشاط إنتاج المعرفة لتحقيق الأهداف الاقتصادية والإستراتيجية للمنظمة، التي تم جمعها وإنتاجها في سياق قانوني ومن مصادر مفتوحة". (Dufau, 2010) ومن الضروري الجمع بين تقنيات الذكاء الاقتصادي والإدارة الإستراتيجية وعمليات صنع القرار. فالذكاء الاقتصادي لا تتعلق بتراكم المعلومات: فهي مسألة إنتاج المعرفة ذات الغرض التنفيذي الذي تعتمد نوعيته على مهارات تفسير العامل البشري وتحليله.

كان أول تعريف عملي للذكاء الاقتصادي كان سنة 1994 من طرف Martre: "مجموعة العمل في المحافظة العامة للتخطيط بفرنسا، حيث تم تعريفه على أنه "مجموعة الأعمال المرتبطة بالبحث، معالجة وبث المعلومة المفيدة للأعوان والمتدخلين الاقتصاديين لصياغة إستراتيجياتهم"، (Martre, 1994, p 11) وتتم هذه الأعمال بشكل قانوني مع

كل ضمانات الحماية اللازمة للحفاظ على أصول الشركة في أفضل الظروف من الجودة والوقت والتكلفة. (Larivet, 2001, p6)

فعمليات الذكاء الاقتصادي متسقة، مستمرة، متكررة، تؤدي إلى تغييرات كبيرة في السلوك الفردي والجماعي، وإحداث تغييرات في آليات صنع القرار. فتطوير الذكاء الاقتصادي يغطي أيضا جميع مجالات العمل: الإدارة، والتسويق، والتمويل، وتنظيم الإنتاج، والبحوث، والموارد البشرية... (CETISME, 2017)

في تعريف ل (Besson et Possin, 1998) الذكاء الاقتصادي هو التحكم المكثف للمعلومات وإعادة إنتاج المعارف الجديدة. هو فن الكشف عن التهديدات والفرص من خلال تنسيق عملية الجمع، الفرز والتخزين والتحقق من صحتها، التحليل وتوزيع المعلومات المفيدة أو الإستراتيجية لأولئك الذين هم في حاجة إليها (Joachim Queyras, 2005, p92)

يرى Harbulot christian (1999) أن الذكاء لاقتصادي هو: "البحث وترجمة المعلومة المتاحة للجميع بغرض فك شفرات نوايا المتعاملين ومعرفة قدراتهم ويشمل الذكاء جميع عمليات الرقابة في البيئة التنافسية ويتميز عن الاستعلامات التقليدية بطبيعة حقل تطبيقه لأنه يعنى بمجال المعلومات المفتوحة ويقتضى بالضرورة احترام الأخلاقيات المهنية" (حمدي، 2017)

- نادي المعلوماتية للشركات الفرنسية (CIGREF) في تقرير بعنوان "تدويل الشركات" في عام 2001، عرف الذكاء الاقتصادي بوصفه تنويجا لعملية طويلة في الأصل يقظة وثائقية.. (Leonenetti, 2008, p108)

حسب Allain-dupré et Duhard: هي في المقام الأول أداة لدعم القرارات؛ وهو يستند إلى معلومات القرار، أي المعلومات التي تشكل موردا استراتيجيا للشركة، والغرض منه هو الحد من عدم اليقين من أجل جعل القرار غير عشوائي. (Guy, 2001, p262.)

وكخلاصة لما سبق، يمكن تعريف الذكاء الاقتصادي بأنه: "مجموعه من المفاهيم والأساليب والأدوات التي توحد جميع الإجراءات المنسقة للبحث، الاقتناء، المعالجة، التخزين ونشر المعلومات المفيدة للشركات التي تعتبر منفردة أو في شبكات، كجزء من وتؤدي هذه العمليات المنسقة والدائمة والمتكررة إلى تغييرات كبيرة في السلوكيات الفردية والجماعية، وإحداث تغييرات في آليات صنع القرار. ويتعلق تطور الاستخبارات الاقتصادية أيضا بمجموع قطاعات المؤسسة: الإدارة، والتسويق، والمالية، وتنظيم الإنتاج، والبحوث، والموارد البشرية. (Delecroix, 2005, p59)

3. البيئة الرقمية:

من أبرز معالم التحول من البيئة التقليدية إلى البيئة الرقمية إحلال مستودعات المعلومات الالكترونية محل المطبوعات والأرصدة الورقية، وتغيير طبيعة الإجراءات والعمليات التي يتم فيها التعامل مع هذه الأرصدة ووسائط حفظها ونقلها. (الكميشي، 2016، ص302)

1.3. تعريف البيئة الرقمية: يطلق عليها البعض البيئة التكنولوجية، فهي مجموعة من العناصر متفاوتة المهام والاختصاصات والدرجات الوظيفية والقناعات والكفاءات العلمية المتفاعلة فيما بينها وفق منظومة لإنجاز مهام محددة، وبعبارة فان البيئة الرقمية هي نتيجة لتطبيقات التكنولوجيا المختلفة في المؤسسات، وتفاعل الإنسان ومدى تقبله للتغيرات التكنولوجية الجديدة، (لخاطي، 2014، ص 49) وباختصار البيئة الرقمية هي: هي البيئة التي تعتمد بصورة أساسية على تكنولوجيا المعلومات والاتصال. (رحابلي، 2015)

أما الخطب الجديدة في المؤسسات فهي يمكن أن تتضمن ما يلي: (Djema, 2014)

- حوكمة المعلومات.

- رصد السمعة الكترونية.

- الاستماع إلى شبكة الإنترنت، ووسائل الإعلام الاجتماعية وبناء إستراتيجية وسائل الإعلام الاجتماعية.

- الصفقات الرقمية. Les métiers numériques.

- ظهور التقنيات العلائقية (ذات العلاقة) والثقافة الرقمية.

2.3. ماهية المخاطر الرقمية وخصائصها: إن الخطر بمفهومه الشائع هو ما يمكن أن يتسبب في ضرر أو أذى لحياة الإنسان المادية أو المعنوية كملكاته، والبيئة المحيطة به، وماله، ووقته، وسمعته، وحتى علاقاته الاجتماعية، فالمخاطرة مصطلح مرتبط بالخطر، فهو يعبر عن ذلك المقياس لدرجة الخطورة، والذي تحكمه مجموعة من البديهيات، يمكن حصرها فيما يلي: (بن ديب، 2008)

- لا توجد أنشطة بدون مخاطرة، فالخطر مصاحب لحياة الإنسان.

- المخاطرة جزء لا يتجزأ من عملية صنع القرار.

- بعض المخاطر قد تختبئ، ولكن ما تلبث أن تظهر مخاطر أخرى.

إذن وفقا لهذه البديهيات، فالمخاطرة مسئولية الجميع في المؤسسة لأن الخطر لا يفرق بين أي جهة فيها، وبما أن الخطر مصادره عديدة، فإن له عدة حلول من بينها حل أمثل قد يكون خفيا، المطلوب من إدارة المؤسسة البحث عنه وتفعيله.

والخطر هو أثر عدم اليقين على تحقيق الأهداف، ويعني مصطلح "المخاطر الرقمية" فئة المخاطر المتصلة باستخدام البيئة الرقمية وتطويرها وأدائها في سياق أي نشاط. ويمكن أن ينجم هذا الخطر عن مزيج من التهديدات وأوجه الضعف اللازمة للبيئة الرقمية. (OCDE, 2015, p32)

ينشأ الخطر الرقمي عن زيادة الاعتماد على نظم تكنولوجيا المعلومات والعمليات الرقمية، (Shaun, 2011, p161)

ويتكون من عناصر ذات صلة بالبيئة الرقمية، والبيئة المادية، والأشخاص المشاركين في النشاط، والعمليات التنظيمية التي بنيتها. (OCDE, 2015, p32)

- David (2001) تحديد المخاطر الكترونية هو أي خطر الناجمة عن استخدام التكنولوجيا الالكترونية الجديدة، ولا سيما من استخدام الحاسوب والاتصالات السلكية لاسلكية والإنترنت.

- جورج George (2000) احتمال أن تواجه المنظمة تأثيرا سلبيا كبيرا أثناء الحصول على تكنولوجيا المعلومات ونشرها واستخدامها أما داخليا أو خارجيا. (ALHawari, Hamdan, and Abu Hamdeh, 2017)

ويتميز الخطر الرقمي بالخصائص التالية: (OCDE, 2015, p33-34)

- يرتبط ذلك بـ "عدم اليقين الرقمي"، ويصاحب أي اعتماد على تكنولوجيا الاتصالات الكترونية درجه معينة من عدم اليقين فيما يتعلق باستخدام البيئة الرقمية "عدم اليقين الرقمي".
- تؤثر على التوافر والنزاهة والسرية (أي "الأمن"). والأحداث التي يحتمل أن تؤدي إلى آثار هي الإخلال بالسرية والسلامة وتعطيل توافر الأنشطة أو البيئة الرقمية التي تحدث فيها أو التي تستند إليها بصورة مباشرة أو غير مباشرة.
- له تأثير سلبي. وفي اللغة المشتركة، يكون لمصطلح "المخاطر" عموما دلالة سلبية بحتة، ولذلك فإن التوصية تركز على أوجه عدم اليقين التي يمكن أن تعرض للخطر تحقيق الأهداف الاقتصادية والاجتماعية.

● هي ذات طبيعة اقتصادية واجتماعية، وأثار أو عواقب عدم اليقين الرقمي اقتصادية واجتماعية، وقد تؤثر على الموجودات الملموسة أو غير الملموسة. ولذلك يجب أن يصاغ الخطر من الناحيتين الاقتصادية والاجتماعية: خسارة مالية، وفقدان القدرة التنافسية، والفرص الضائعة، الإضرار بسمعة أو صورة، وفقدان الثقة، وما إلى ذلك. (حيث أوضحت دراسة نشرتها شركة التأمين البريطانية Lloyd's في لندن ان الإنترنت العالمي يمكن ان يولد خسارة اقتصادية متوسطة 53 ملياراً، وكانت الدراسة مهمة بالخسائر الاقتصادية المحتملة التي ستنتج عن القرصنة التي يقوم بها مقدم خدمات السحب (الحوسبة غير المادية) والشبكة الكترونية لنظم تشغيل الحواسيب التجارية). (Engelaar, 2017)

3.3. مراحل ظهور وتطور المخاطر الرقمية: يمكن التمييز بين ثلاث فترات رئيسي لظهور وتطور المخاطر الرقمية: (Gruselle, 2013, p10)

- 1990-2000: في التسعينات، فان هجمات الكمبيوتر هي في الأساس فعل المتخصصين في الحاسوب، يسعون إلى إظهار كفاءتهم عن طريق القرصنة على المواقع أو الخوادم المحمية بشدة، والتي عادة ما تكون تابعة لوكالات الأمن أو الدفاع.
- 2000-2008: إن استغلال المهارات التقنية للقرصنة "من أجل الشهرة" قد أدى إلى جريمة رقمية حقيقية، احترافية ومتخصصة تهدف إلى تحقيق الأرباح المادية للمنظمات الإجرامية. ففي المقام الأول، تجلت جرائم الانترنت، من خلال ظهور وزيادة حالات هجوم على مواقع تجارية على الإنترنت وبيع المنتجات المقلدة إلى حين توافر وسائل الهجمات بالإنترنت. وأعاد القرصنة تجميعهم في زلزلة وقسموا العمل الإجرامي.

● منذ 2008: بالإضافة إلى استمرار ظاهره الجرائم الالكترونية، أصبح الفضاء الرقمي مجال تدخل للدول، والجماعات السياسية المحنجة وبعض الجهات الفاعلة الاقتصادية للقيام بعمليات تهدف إلى تخريب وسائل الإنتاج أو الشبكات، والحصول على معلومات أو بيانات.

4.3. أنواع المخاطر الرقمية: هناك أنواع عديدة من المخاطر الرقمية منها: (ALHawari, Hamdan, and Abu (2017, Hamdeh)

أ. **مخاطر الفيروسات:** فيروس الكمبيوتر معدي. فإنه يكرر نفسه ويصيب جهاز كمبيوتر، الذي لديه اتصال إلى أجهزة الكمبيوتر الأخرى عن طريق الشبكات أو أنواع مختلفة من الأقراص.

ب. **مخاطر الإنترنت:** الإنترنت هو نظام اتصال الكمبيوتر العالمي الذي يسمح الاتصال السريع والواسع. مع أي طريقه جديدة للاتصال، وهناك مخاطر فضلا عن الفوائد. وينبغي للأشخاص الذين يتواصلون عبر الإنترنت أن ينظروا بعناية في هذه المخاطر: فقدان التحكم في المعلومات، وخصوصية البيانات، وسلامه البيانات، وفقدان التحكم في المعلومات الذي يزيد من المخاطر المرتبطة بالمعلومات.

ت. **مخاطر الأعمال الإلكترونية:** الأعمال التجارية الإلكترونية هي إدارة الأعمال التجارية بمساعدة أدوات الاتصالات السلكية واللاسلكية والاتصالات القائمة على الاتصالات السلكية واللاسلكية. المخاطر مثل فشل البرمجيات قد يكون راجعا إلى الفيروسات وفشل شبكة وأجهزة الكمبيوتر.

ث. **مخاطر البريد الإلكتروني:** العديد من المخاطر على البريد الإلكتروني ليست جديدة ومماثلة لتلك المرتبطة بريد المكتب البريدي، الفاكسات أو البريد الصوتي. حجم مخاطر البريد الإلكتروني أكبر من أي وسيلة اتصال أخرى موجودة، لأن التكنولوجيا تجعل تغيير وإعادة توجيه البريد الإلكتروني جهد.

وتنشا عن أداره هذه المخاطر عدة تحديات جديدة لكبار موظفي المخاطر: (The Economist Intelligence Unit, 2005, p2)

● معظم مديري المخاطر ليس لديهم خلفيه التكنولوجيا، وذلك لأداره المخاطر الرقمية يتطلب تعاونا وثيقا بين المخاطر ووظائف تكنولوجيا المعلومات.

● إن نفس التكنولوجيا التي تمكن الشركات من تحويل عملياتها التجارية إلى الرقم الرقمي تسمح أيضا للمجرمين والمطلعين بارتكاب أشكال جديدة من الاحتيال والسرقة

● تخلق التكنولوجيات الجديدة تهديدات جديدة، تتطلب من الشركات باستمرار أعاده تقييم وتكييف إستراتيجيتها لأداره المخاطر الرقمية.

5.3. الجريمة الالكترونية: لمصطلح "الجريمة الالكترونية" الوارد في البلاغ رقم 267 المؤرخ 22 أيار/مايو 2007 الصادر عن المفوضية الأوروبية "، يقصد بتعبير "الجريمة الالكترونية" الأفعال الإجرامية المرتكبة باستخدام شبكات الاتصال الكترونية ونظم المعلومات أو ضد هذه الشبكات والنظم". (ALLIOT, 2009, p5)

فالجريمة السيبرانية تشكل في عالم معولم واحدا من الأشكال الجديدة للجريمة عبر العالم، التي يمكن أن تكون عواقبها خطيرة بشكل خاص بالنسبة للمواطنين والضعفاء والقطاع الاقتصادي لجميع الأمم على هذا الكوكب. وهناك أربعة أنواع رئيسية لها وخاصة التي تتعرض للمؤسسات: (ALLIOT, 2009, P11)

- الإعلام وسرقة البيانات
 - اقتحام الشبكات
 - اعتراض الاتصالات أو تدفق البيانات
 - التلاعب في الموظفين والشركاء، والأخيرة التي تعرف باسم "الهندسة الاجتماعية".
- والشكل الموالي يوضح بعض المخاطر الرقمية.

الشكل رقم 02: أنواع المخاطر الرقمية



Source: (Managing digital risks in the retail world)

4. التدابير الأمنية

ينبغي للقادة وصانعي القرار ضمان أن تكون التدابير الأمنية ملائمة ومتناسبة مع المخاطر، وأن يسترشدون في تقييم الخطر الرقمي باختيار وتنفيذ وتحسين التدابير الأمنية المتخذة للحد من المخاطر على المستوى المقبول وعلى النحو المحدد في تقييم هذا الخطر ومعالجته. وينبغي أن تكون هذه التدابير ملائمة ومتناسبة مع المخاطر، وأن تختار مع مراعاة الآثار السلبية واليجابية التي قد تترتب عليها بالنسبة للأنشطة الاقتصادية والاجتماعية التي تهدف إلى حمايتها، وكذلك على حقوق الإنسان والقيم الأساسية، إضافة إلى النظر في جميع أنواع التدابير، سواء أكانت هذه التدابير مادية أو عددية أو أنها تنطبق على الأشخاص أو العمليات أو التكنولوجيات التي تنطوي عليها الأنشطة. وينبغي للمنظمات أن تبحث عن مواطن ضعف وان تقدم ردا مناسباً في أقرب وقت ممكن.

ولابد أن يكون الإبداع جزءاً لا يتجزأ من الحد من الخطر الرقمي على مستوى مقبول من التقييم والمعالجة لهذا الخطر. وأن تضطلع بدور في تصميم وتنفيذ الأنشطة الاقتصادية والاجتماعية التي تعتمد على البيئة الرقمية، وفي وضع وتطبيق التدابير الأمنية.

واستنادا إلى تقييم المخاطر الرقمية، ينبغي اعتماد خطة للتأهب والاستمرارية للتخفيف من الآثار الضارة للحوادث الأمنية وتعزيز استمرارية الأنشطة الاقتصادية والاجتماعية وقدرتها على الصمود. وأن تحدد التدابير الكفيلة بمنع أنشطة الحوادث الأمنية الرقمية وكشفها والاستجابة لها وضمان استئنافها. وأن ينص أيضا على آليات لتوزيع مستويات واضحة من التصعيد من حيث حجم وشدة آثار هذه الحوادث، فضلا عن إمكانية نشرها على الأطراف الفاعلة الأخرى في البيئة الرقمية. وينبغي النظر في إجراءات الإخطار المناسبة كجزء من تنفيذ الخطة. (OCDE, 2015,p13)

أهم خطوة أولى في معالجة المخاطر الرقمية هي إدراك أنها ليست مسألة يمكن تركها لأداره تكنولوجيا الإعلام أو لأداره المخاطر وحدها. ويفرض الترابط بين النظم الكترونية عالمية وتكون البقطة ضرورية في عدد من المستويات المختلفة داخل منظمة. وينبغي وضع سياسة لموظفي الإنترنت واستخدام البريد الكتروني، إلى جانب مبادئ توجيهية لفحص الموظفين الجدد. ويجب أن تنطبق هذه المبادئ التوجيهية أيضا على المتعاقدين الخارجيين عندما تتاح لهم إمكانية الوصول إلى نظم تكنولوجيا الاتصالات الخاصة بالمؤسسة.

وأفضل الدفاعات ضد التهديدات التي تشكلها المخاطر الرقمية هي تلك التي تبدأ على قمة المنظمة ذات الإدارة الفعالة وإجراءات أداره الشركات التي تعتبر أمن المعلومات من الأولويات. ويمكن من هذه النقطة إنشاء إجراءات الموظفين المناسبة وبرامج التدريب؛ ويجب رصد هذه التدابير واختبارها وتكييفها بصورة منتظمة حسب الاقتضاء. وعندئذ، لا يمكن رفع أي حواجز تكنولوجية بصورة فعالة إلا بعد تركيب هذه الدفاعات الإدارية ومستويات الموظفين. وقد تشمل نظم الأمن الحاسوبية، على سبيل المثال، البرامج المضادة للفيروسات، والجدران النارية، وبرامج التشفير، وكشف التسلل، ونظم ترشيح المحتوى. وللجميع القدرة على توفير مستوى كبير من الحماية، ولكن يجب تحديثها وتوسيع نطاقها حسب الاقتضاء لمواكبة أي تكنولوجيا جديدة قد يختار عملك استخدامها.

غير ان التكنولوجيا لا يمكن أن تكون أمنة تماما بمجرد أضافه المزيد من التكنولوجيا. ولا يمكن تجاهل البعد الإنساني وينبغي أن يكون الموظفون الأفراد التابعون للمنظمة اقوي خط دفاع لهم. والنظم الأمنية لتكنولوجيا الأمن هي أجهزة رد الفعل ولا ينبغي استخدامها بمعزل عن بعضها البعض، ولكنها تتوافق مع مجموعه من السياسات والإجراءات والبرامج التدريبية الرسمية في جميع أنحاء الشركة. (Skinner, 2018)

5. الذكاء الاقتصادي لمواجهة المخاطر الرقمية

يتفق الخبراء على الحاجة إلى تقاسم المهارات والمعلومات. ومن وجهه نظر الاستخبارات، فإن تبادل المعلومات عن التهديدات الكترونية يمكن من إنتاج استخبارات التهديد السيبراني (Cyber Threat Intelligence) CTI. وتشكل الاستخبارات الرقمية للتهديدات عملية متقدمة تمكن المنظمة من جمع رؤى قيمة تستند إلى تحليل المخاطر السياقية والظرية ويمكن تكييفها مع المشهد الخاص بالتهديدات المحددة للمنظمة وصناعتها وأسواقها.

ويمكن لهذه المعلومات الاستخباراتية أن تحدث فرقا كبيرا في قدرة المنظمة على استباق الانتهاكات قبل وقوعها، وقدرتها على الاستجابة السريعة والحاسمة والفعالة للانتهاكات المؤكدة، والشروع بشكل استباقي في إنشاء آليات دفاعية، قبل

وهذا النظام هو الانضباط القائم على الدورة الاستخباراتية (تحليل الاحتياجات، وجمع المعلومات وتحليلها ونشرها). والغرض منه هو إنتاج المعلومات الاستخباراتية المتصلة بالإنترنت، وذلك على سبيل المثال من أجل تغذية نظم الكشف المبكر أو الأجهزة الخاصة بها.

هذه الاستخبارات على ومن الفضاء الرقمي هو خط الدفاع الأول ضد المخاطر الرقمية. فهي تسمح باستباق الهجمات والتكيف والمساهمة في إسناد الإنترنت عن طريق تحديد مصدرها أو مؤلفها، أو عن طريق الكشف عن الاتجاهات المتعلقة بالأساليب المستخدمة والمجالات المتأثرة.

لذلك هناك صلة وثيقة بين الاستخبارات وأمن الفضاء الإلكتروني. (Keupp, Mermoud, Dimitri, 2017) فقد اقترح العديد من الاقتصاديين وخبراء التأمين النماذج الكمية للتغلب على النقص المزمن في الاستثمار في مجال الأمن السيبراني. وقد برهنت نماذج الاستثمار هذه نظريا على إمكانية تبادل المعلومات بين الهياكل الأساسية الحيوية. بالنسبة للمنظمة، يساعد تبادل المعلومات على الحد من المستوى الأمثل للاستثمار في مجال أمن الفضاء الإلكتروني. ومن وجهة النظر الاقتصادية، يتيح تبادل المعلومات، في جملة أمور، الحد من عدم تماثل المعلومات، والعوامل الخارجية السلبية، وقبل كل شيء، توقع التهديدات من أجل زيادة مرونة نظم المعلومات. ومع ذلك، فإن مشاكل الاحتفاظ بالمعلومات مستمرة، وهو ما لا يسمح باستغلال الإمكانيات الكاملة لتبادل المعلومات لمنع التهديدات السيبرانية. ونتيجة لذلك، يقترح بعض المنظمين إجبار الهياكل الأساسية الحيوية لمشاركة المعلومات. ومن المهم تحديد الحوافز الاقتصادية والاجتماعية التي يمكن أن تمكن الهياكل الأساسية الحيوية من تبادل المعلومات بصورة عفوية وطوعية.

وقد أظهرت عدة دراسات أن التبادل المتعمد للمعلومات بشأن المخاطر الرقمية، في إطار شراكة بين القطاعين العام والخاص، أكثر كفاءة من الإكراه. ولذلك فمن المهم تحديد الحوافز الاقتصادية والاجتماعية التي يمكن أن تمكن الهياكل الأساسية الحيوية من تبادل المعلومات بصورة عفوية وطوعية. ولذلك يلزم وضع نموذج جديد لفهم آلية الحوافز لتوجيه السلوك نحو التبادل الطوعي للمعلومات. وتظل الثقة شرطا أساسيا ولكنه غير كاف لتبادل المعلومات. ولذلك، حددت 'الثقة' كمتغير معتدل في النموذج النظري المعروض أدناه. وقد صدقت لجنة علمية دولية على هذا النموذج وقدم في مؤتمر علمي.

الشكل رقم 04: الميكانيزم النظري الذي يمكن الفاعلين من تبادل المعلومات، وهو نموذج ناتج عن الاقتصاد

السلوكي ونظرية Tversky و Kahneman



Source : (Keupp, Mermoud & David, 2017,p44).

- بالنسبة على مستوى الدولة يجب أن تكون المؤسسة مزودة بأداة تجريبية إستراتيجية قادرة على الكشف الاستباقي عن المخاطر والفرص. مستوحاة من الاستخبارات، فالذكاء الاقتصادي يوفر شبكة من التحليل الذي يسمح لفك السفلي من الخرائط وتسليح الدولة فكريا لفهم القوي في العمل، لفك التحالفات واستراتيجيات الإجراءات.

- يتيح الذكاء الاقتصادي أيضا التحسين الأمثل لنقل المعارف والمنهجيات بين المجال العسكري والمجال الاقتصادي. الذكاء الاقتصادي هو أيضا وسيلة لخلق الأمن الاقتصادي للمؤسسات. (Keupp, Mermoud, Dimitri, 2017)

مع تطوير الرقمية في مجتمعنا والنتيجة المترتبة على الإنترنت، وخطر سرقة البيانات من خلال اختراق نظم المعلومات قد زادت بشكل كبير. فالتكنولوجيا الرقمية، إذا كانت فرصة للتنمية الاقتصادية للشركات وأداه لخدمه سيادة الدول، يمكن أن تخدم أيضا مصالح المتنافسين عن طريق، على سبيل المثال، قرصنة البيانات السرية والإستراتيجية. ولذلك يجب أن توفر الشركات والدولة استجابة متسقة وفعالة لهذا الخطر من أجل الحفاظ على ثروة التراث غير المادي للجهات الفاعلة الاقتصادية، والسيادة الوطنية والتأثير على مستوى الاقتصاد العالمي.

ففي فرنسا وفي مواجهة هذا التحدي الكبير، يشير باحثون إلى التزام فرنسا بمكافحة سرقة البيانات. وشدد على أن إنشاء الوفد المشترك بين الوزارات للذكاء الاقتصادي (D2IE) يشهد على الوعي الفرنسي في هذا المجال، وعلى استعداده للعمل في اتجاه مصالحه، ويشير في الوقت نفسه إلى ضرورة مواصلة الجهود على الصعيدين الوطني والأوروبي.

6. واقع ممارسات الذكاء الاقتصادي في مواجهة المخاطر الرقمية في الجزائر

تعاني المنظومة الوطنية والإقليمية للرصد والاستشراف على حد سواء في الجزائر خلل أو قصورا في تجميعنا لمعلومة الإستراتيجية على المستوى الإقليمي والمحلي تحديدا، والتي تضمن مرافقة الدولة لمؤشرات التنمية الاقتصادية والاجتماعية القاعدية. (داي، 2016)

حيث جاء في لتقرير حول النظام الوطني للمعلومات الاقتصادية والاجتماعية وتحولاته شهر جوان 2004 الذي تمت مناقشته في الجلسة العلنية رقم 24 للمجلس الوطني الاقتصادي والاجتماعي. أن من بين العوامل المعيقة لإقامة نظام للذكاء الاقتصادي واليقظة تعود إلى: العوامل المتعلقة بالوسائل التقنية والفنية، العوامل المتعلقة بالسياسات العامة، العوامل المرتبطة بنظام الحاكمية في أجهزة الدولة والمؤسسات، العوامل الثقافية وأخيرا العوامل المرتبطة بالموارد البشرية في البلاد. (خلفاوي، 2012، ص16) وبالتالي لا يوجد أي ممارسات للذكاء الاقتصادي في مواجهة المخاطر الرقمية.

الخاتمة

العالم الرقمي عالم من التواصل والنفوذ والقيادة. ويجب أن يرسخ الذكاء الاقتصادي ممارساته في مجال الثقافة الرقمية. ولذلك يصبح الاتصال عنصراً أساسياً وقاطعاً في وظيفة نظام المعلومات، بنفس الطريقة التي يتم بها الإدارة المالية، وأداره المشاريع، وأداره الموارد البشرية، وأداره التغيير.

قد تكلف المخاطر الرقمية خسائر جسيمة للمؤسسات باختلاف أنواعها وأصبحت الوسائل التقليدية لا تستطيع وحدها التصدي لهذا النوع من المخاطر، وقد فرضت ممارسات الذكاء الاقتصادي الآن مكانه خاصة في توفير الحماية للمؤسسات، لاسيما بما يكتنفه من عمليات تساعد في توقع المخاطر من خلال عمليات البقطة ومشاركة المعلومة المناسبة.

بعض النتائج والاقتراحات:

- يجب أن يدرك مديري المخاطر طبيعة المخاطر التي يمكن تتعرض لها المؤسسة وأنواعها.
- لا بد أن يتفهم أخصائيو المخاطر في الشركة دور كل منهم في أداره المخاطر الرقمية.
- ويجب على المعنويون في المؤسسة أن يحددوا بوضوح أدوارها في التعامل مع المخاطر بأقصى قدر من الفعالية.
- هناك مجال رمادي بين مسؤوليات اللجنة المعنية بالتكنولوجيا والمسؤولية التقنية في التعامل مع المخاطر ويرجع ذلك جزئياً إلى الطبيعة المعقدة للتكنولوجيا والتحديات المتمثلة في الإبلاغ عن المسائل الفنية. فترك المخاطر الرقمية تماماً لإدارة تكنولوجيا الإعلام ليس من المستحسن.
- تعتبر ممارسات الذكاء الاقتصادي حالياً أنجع سبل الإدارة الحديثة، لذا من الضرورة إدماج ممارساته في المؤسسات ولاسيما في مواجهة المخاطر.
- من أهم مبادئ الذكاء الاقتصادي مشاركة المعلومة لذا وجب على الميسرين توعية أفراد المؤسسة بذلك وحتى على المستوى الكلي مشاركة المعلومة المفيدة بين المؤسسات الوطنية يعتبر سلاح ضد الخطر الخارجي.
- تعتبر الثقة أهم ما يساعد على نشر ثقافة مشاركة المعلومة لذا لا بد من تدعيم المؤسسات بنظام التحفيز الذي يساهم في تسهيل ذلك.

المراجع المستعملة:

- باشا. رابع حمدي، ولقوي. عبد الحفيظ، جوان 2017، إستراتيجية التشبيك رافعة ذكاء اقتصادي تطبيق حول حملات صناعة الرأي، مجلة الباحث لاقتصادي، العدد السابع.
- بن ديب. عبد الرشيد، 25 و 26 نوفمبر 2008، "مدخل استراتيجي لإدارة المخاطر"، الملتقى الدولي الثالث حول: إستراتيجية إدارة المخاطر في المؤسسات: الآفاق والتحديات، كلية العلوم الاقتصادية وعلوم التسيير، بجامعة حسيبة بن بوعلي بولاية الشلف.

- رحابلي. محمد، وبلهوشات. الزبير، 2015، حقوق المؤلف والحقوق المجاورة في البيئة الرقمية: الحالة الجزائرية، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، المجلد 29 (34).
- الكميشي. لطيفة علي، 12-14/03/2016، الكتاب في البيئة الرقمية، المؤتمر الدولي الثالث لتقنيات المعلومات والاتصالات في التعليم والتدريب، الخرطوم-السودان.
- لحواطي. عتيقة"، 2014، استرجاع المعلومات العلمية والتقنية في ظل البيئة الرقمية ودوره في دعم الاتصال العلمي بين الباحثين"، أطروحة مقدمة لنيل درجة دكتوراه ل م د في علم المكتبات والتوثيق تخصص: تقنيات المعلومات في الأنظمة الوثائقية، جامعة قسنطينة 2.
- Abiodun R. C, 16 février 2007, L'annotation pour la recherche d'information dans le contexte d'intelligence économique, these Présentée pour l'obtention du Doctorat de l'Université Nancy 2, Spécialité Sciences de l'information et de la communication, Présentée et soutenue.
- ALHawari. S., Hamdan. A, & Abu Hamdeh. M., Development of a Conceptual Framework For Managing, Electronic Risk, Retrived on:16/06/2017 in : <http://www.iefpedia.com/english/?p=255>.
- Alliot-Marie. M., 24 mars 2009, Le guide pratique du chef d'entreprise face au risque numérique, Lille, grand palais.
- Alliot-Marie. M., référence Managing digital risks in the retail world, http://www.willis.co.uk/documents/Industries/Willis_Retail_Risk_Insight_Digital_Risks_in_the_Retail_World.pdf, vu ; 25/07/2017
- Billon. J.L., Gonzalez. A., guide de l'intelligence économique pour les TPE/PME en Cote d'ivoire, centre du commerce international, p11. Publié dans: <http://fr.calameo.com/>, Vue ; 31/05/2017.
- CETISME, 2002, Intelligence économique Un guide pour débutants et praticiens , le Conseil Régional de Lorraine, rapport publié: <http://www.abhatoo.net.ma/>, Vue ;19/02/2017.
- Delecroix. B., 2005, La mesure de la valeur de l'information en intelligence économique , Thèse pour l'obtention du grade de Docteur en Sciences de l'Information, *Spécialité* : Information scientifique et technique, Université de Marne-La-Vallée.
- Djemaa. H., 22-23/4/2014, L'intelligence économique d'entreprise face au défi du numérique, Première Conférence scientifique internationale annuelle de l'Intelligence économique: Systèmes numériques et Intelligence économique, Université Khemis Miliana.
- Dufau M. J. P., 6-7 juillet 2010, L'intelligence économique, établi en application de l'article 12.7 du règlement et présenté à la Commission, Document N°19, Assemblée parlementaire de la Francophonie, XXVIème session, Dakar.
- Engelaar. R., Une cyberattaque mondiale pourrait coûter jusqu'à 50 milliards de francs, <https://www.rts.ch/info/>, vu ; 25/07/2017.

- Gestion du risque de sécurité numérique pour la prospérité économique et sociale, 2015, Recommandation de l'OCDE et Document d'accompagnement, éditions OCDE, Paris.
- Gruselle. B., Février 2013, Enquête sur la sécurité numérique des entreprises, recherches & documents, N° 01.
- Harriet. L., L'intelligence économique a la lumière des concepts managériaux : l'étude de cas d'une entreprise du secteur énergétique, thèse présentée pour Obtenir le grade de docteur de l'université de Bordeaux, Spécialité Sciences de gestion, Présentée et soutenue publiquement le :1/12/2014.
- Insights on governance, risk and compliance, November 2014, Cyber threat intelligence – how to get ahead of cybercrime, EY, Building a better working world.
- Keupp.M.M., Mermoud.A. & David D.P.,2017, Pour une approche économique de la cybersécurité, Military Power Revue der Schweizer Armee-Nr.1.
- Larivet. S, 13-14-15 juin 2001, Intelligence économique: acception française et multi dimensionnalité, Xième Conférence de l'Association Internationale de Management Stratégique, Faculté des Sciences de l'administration Université Laval Québec.
- Leonenetti. X, 7 novembre 2008, Etat, entreprises, « intelligence économique, quel rôle pour la puissance publique ?, these Pour le doctorat en droit, université Paul Cezanne-Aix-Marseille III.
- Martre. H, 1994, (travaux du groupe présidé): Intelligence Economique et Stratégie des Entreprises, rapport du commissariat général au plan,, la Documentation française, Paris.
- Massé. G. & Thibault. F., 2001, Intelligence économique, un guide pour une économie de l'intelligence, 1^{ère} édition, De Boeck Université.
- Pather. S., Remenyi. B. & Remenyi. D, 2001, Managing Risks of ICT projects, Academic Publishing Ltd, 1edition, UK.
- Queyras. J., 22 novembre 2005, L'intelligence économique territoriale dans un centre d'information du service public ; Application à la coopération scientifique et universitaire franco-Bresilienne, Thèse pour l'obtention du Doctorat en sciences de l'information et de la communication à l'Université du Sud Toulon-Var.
- Risk and opportunity in an increasingly digital world -Insurance Governance Leadership Network, Tapestry networks, May 2015, TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM
- Skinner. P., Assessing and managing digital risks, A guide for businesses published by The International Underwriting Association and The Department of Trade and Industry. Vu le : 7/11/2018, pws-uk.com.
- The Economist Intelligence Unit, September 2005, Digital risk the challenge for the CRO, An Economist Intelligence Unit white paper, sponsored by Ace, Cisco, Deutsche Bank, IBM and KPMG.