لجان التدقيق ودورها في المؤسسة في ظل التطور المتسارع لفضاء الجريمة الإلكترونية

The Audit committees and their role in the organization in the light of rapid development of cybercrimes

د. جيلالي عياد غلام الله[1]

جامعة الشلف– الجزائر

ghoulemayad@yahoo.fr

تاريخ الاستلام: 2019/12/05 تاريخ النشر: 2020/06/03

Abstract:
with the rapid development of (ICT) Information & Communication Technology, A new type of crimes have emerged called the Cybercrimes, which has become the first and the most dangerous threat to the organizations, institutions and states data and information causing an increasing rate in their annual costs. Accordingly, the audit committees have played the main role as consultative and supervisory institution to realize the organizations electronic security policy in order to struggle this new kind of crimes. although, the attention to this kind of risks and the role of auditing committees in the Algerian organizations still far from the standards and procedures in which this phenomenon is managed compared with other organizations on the international level. So, there is no controversy in the Algerian organizations between the various stakeholders that the policies related to the cybercrimes are absent due to the absence of audit committees, and the Algerian state still until now with no longer procedures that require commit organizations either private or public to take the necessary measures for the electronic security and the cyber crime fighting.
Key words: computer audit, audit committee, cyber-security, cybercrime

مقدمة:

من المعلوم أن وظيفة التدقيق ظهرت في المنظمة نتيجة التغير الذي حصل ما بين قيمة السوق والقيمة الحقيقية للمنظمات التي نمت في إطار غير منظم خلال تلك الفترة، في هذه الوضعية أجمع المستثمرون على إعطاء الثقة للسوق، مما تحتم أن يفرض علم الرقابة المحاسبية نفسه، فظهرت وظيفة التدقيق، وكان الهدف منها في الأول هو الكشف عن الأخطاء والغش، ومع تطور محيط المنظمات وتأثيراته السلبية عليها تطورت وظيفة التدقيق إلى مهمة تعطي رأيا معللا على صحة وتنظيمية والصورة الصادقة للقوائم المالية، ثم بالإضافة إلى ذلك كمهمة استشارية وقائية عن طريق التوصيات التي تقدمها، حتى تعطي للمنظمة قيمة مضافة، ومن مهمة التدقيق الداخلي والخارجي ونتيجة للفضائح الكبرى التي لحققت المنظمات خلال ثمانينات القرن الماضي إلى لجان التدقيق هدفها التنسيق بين الإدارة والمدقق الداخلي والخارجي في تنظيم أعمال كل منهما، من أجل تفادي الأخطار التي تصيب المنظمات والتي غالبا ما يكون مرتكبها أفرادا من داخل المنظمة مما يسهل كشفه والحد منه عن طريق استحداث لإجراءات جديدة مناسبة له، ولكن مع التطور المتسارع الذي عرفته تكنولوجيات الإعلام والاتصال وأصبحت كل ممتلكات ومعلومات ومعطيات المنظمات على المستوى العالمي تدار بها، فعملية الغش، الاحتيال، السرقة، التخريب والتحريف على أصول المنظمات تحولت، فظهر بما يسمى حاليا بفضاء الجريمة الإلكترونية كخطر جديد موجود في كل مكان وفي أي زمان وممكن أن يصيب أي نشاط في المنظمة على المستوى العالمي، وأصبحت تمثل الخطر الجسيم والأول على المنظمة وهي تتضاعف يوميا وبتكنولوجيات جديدة تتحدى التي تمتلكها المنظمات كآليات لفضاء الأمن الإلكتروني، مما غير من مهمة التدقيق التقليدية إلى مهمة

[1] المؤلف المرسل: جيلالي عياد غلام الله: ghoulemayad@yahoo.fr

التدقيق على المعلوماتية من أجل تفادي الأخطار التي تلحق بالمنظمات من طرف أفراد مجهولين ومن أي جهة في العالم، والتعرف عليهم صعب، وحتى إن تمكنت المنظمة من ذلك فإنه يصعب التحقيق مع القراصنة نظرا للقوانين والعلاقات التي تحكم الدول.

الإشكالية

في ظل التطور السريع والمتنامي في كل لحظة لفضاء الجريمة الإلكترونية على أصول المنظمات، فما هو الدور الذي تلعبه لجنة التدقيق باعتبارها هيأة مكلفة بمتابعة فعالية أنظمة الرقابة الداخلية وإدارة المخاطر والأمن الإلكتروني لمكافحة فضاء الجريمة الإلكترونية؟

الفرضيات:

- **الفرضية الأولى:** لا توجد فروق ذات دلالة معنوية بين تكوين وسير(إدارة) لجان التدقيق في المؤسسات الجزائرية وبين تكوين وسير لجان التدقيق التي تتفق والأنظمة المعمول بها دوليا.
- **الفرضية الثانية:** لا توجد فروق ذات دلالة معنوية بين لجان التدقيق وإدارة المخاطر في المؤسسات الجزائرية وبين لجان التدقيق وإدارة المخاطر التي تتفق والأنظمة المعمول بها دوليا.
- **الفرضية الثالثة:** لا توجد فروق ذات دلالة معنوية بين لجان التدقيق وفضاء الجريمة الإلكترونية في المؤسسات الجزائرية وبين لجان التدقيق وفضاء الجريمة الإلكترونية التي تتفق والأنظمة المعمول بها دوليا.

هدف الدراسة

الهدف الرئيسي هو التحقق من الدور الذي تلعبه لجنة التدقيق فيما يتعلق بالأمن الإلكتروني للحد من مخاطر الجريمة الإلكترونية في المؤسسات الجزائرية، وهذا عن طريق:

1- المهام التي تسند لها من طرف مجلس الإدارة بواسطة ميثاق لجنة التدقيق المحدد لواجباتها وإشرافها على نظام الرقابة الداخلية وإدارة المخاطر والأمن الإلكتروني؛

2- كذلك باعتمادها على هياكل الرقابة الأخرى بتقديم توصياتهم على مجالات النقص في الوسائل والآليات المخصصة لمواجهة الجريمة ا لإلكترونية؛

3- التعرف على الجريمة الإلكترونية والتحسيس بها داخل المؤسسات الجزائرية؛

4- محاولة الوصول إلى الأساليب والطرق التي تتعامل بهم المؤسسات الجزائرية مع الجريمة اللإلكترونية للوقاية منها ومحاربتها.

أهمية الدراسة

1- المساهمة في مساعدة المؤسسات الجزائرية بشكل عام في اتخاذ القرارات المناسبة التي من شأنها أن تجسد هياكل لجان التدقيق على مستوى مجالس الإدارة حتى تساهم في مساعدتهم على الحماية من الجريمة الإلكترونية بالطريقة المثلى؛

2- تسليط الضوء على لجان التدقيق والجريمة الإلكترونية في المؤسسات الجزائرية، وتوضيح الإجراءات اللازمة التي تقوم بها لجان التدقيق بصفة عامة في هذا المجال، حتى تكون دعامة للمؤسسة الجزائرية تستند عليها في عملها.

منهج الدراسة: اعتمد الباحث على المنهج الإستنباطي كأساس للبحث، مستعينا بأدوات التحليل الإحصائي والبيانات والأرقام والإحصائيات والمقارنات في الموضوع، ولا يغنينا الإستعانة بأية أداة أخرى نراها ضرورية عند الحاجة.

الدراسات السابقة: من بين الدراسات التي فحصها الباحث ولها علاقة بالحث المعالج هي:

1- دراسة قام بها معهد لجان التدقيق الفرنسي سنة 2012 تحت عنوان " المؤشر حول أخطار الإحتيال" " Benchmark sur les risques de fraude " هذه الدراسة أنجزت على مجوعات منتمية إلى البورصات لوضح سبب الإرتفاع المفاجئ لعمليات الإحتيال التي أصبحت تتعرض لها هذه المجموعات نتيجة للمكانة التي أصبحت تحتلها تكنولوجيات الإعلام والاتصال في هذه المجموعات وهذا مما عرضها إلى أخطار الجرائم الإلكترونية والتي تضاعفت خلال السنين الأخيرة، فوجدت أنها كانت نتيجة للخلل في أنظمة رقابتها الداخلية أو عدم اليقظة للهجومات الإلكترونية والتي لم تكن هذه المؤسسات منشغلة بهذه الأعمال الخبيثة والتي أصبح لها تأثيرا كبيرا على أصولها، سواء ما تعلق بضياع الأموال أو على صورتها وسمعتها، والتي منها الفساد، تحويلات الأموال، التلاعب بالقوائم المالية، ...الخ وما هو الدور الذي تلعبه لجان الدقيق في هذه المجموعات؟

وتوصلت الدراسة إلى مهام لجنة التدقيق التي لها علاقة مع أخطار الإحتيال بأن هناك قليل من مهام لجان التدقيق التي لها علاقة مع أخطار الإحتيال ماعدا مجموعة واحدة أحصت بأن هناك مهمتين مختلفتين للجنة التدقيق وهما:تعرف لجنة التدقيق على الأخطار المحصاة، فحص لجنة التدقيق لحصيلة الرقابة لأخطار الإحتيال الداخلية والخارجية، والمجموعات الأخرى أحصت أن هناك نمط واحد من المهمة التي لها علاقة مع أخطار الإحتيال.

2- دراسة قامت بها KMPG SA شركة ذات مسئولية محدودة للخبرة المحاسبية ومحافظي الحسابات الفرنسية تحت عنوان "مواضع اهتمام لجان التدقيق لسنة 2017" " Points d'attention 2017 pour les comités d'audit "، من بين النقاط التي أشارت إليها الدراسة هي إدارة المخاطر أصبحت على المحك نظرا للتطورات التكنولوجية وفضاء الجريمة الإلكترونية، فما هو الدور الذي تلعبه لجنة الدقيق فيما يتعلق بجعل المدقق الداخلي يركز على عوامل الأخطار الجوهرية ويضمن ملائمة إدارة المخاطر للمؤسسة.

خلصت الدراسة إلى النتائج التالية: لجنة التدقيق تساعد المدقق الداخلي وتحدد دوره في حصر منطقة الأخطار الجوهرية للنشاط، والتي شمل الأخطار التشغيلية (مثل: فضاء الجريمة الإلكترونية وأخطار تكنولوجيات الإعلام والاتصال)، وكذلك أنظمة الرقابة الموضوعة لإدارة هذه الأخطار، وكذلك تساعده على وضع مخطط التدقيق المتكيف والمؤسس على الأخطار وكيفية تعديله وفقا لأخطار التي تتعرض لها النشاطات، ودمج الأخطار التي تهدد المنظمة بمجملها عند تطور البيئة التشغيلية لها، وتعمل على امتلاكه للموارد والمهارات والخبرات الضرورية لأداء هذه المهمات، وتشجع المدقق الداخلي على لعب دور المحرك في التنسيق مع الآخرين لإدارة المخاطر.

3- دراسة قام بها معهد لجنة التدقيق الفرنسي سنة 2016 تحت عنوان " معيار:جدول أعمال لجان التدقيق" " Benchmark: Ordre du jour des comités d'audit "، خلصت الدراسة إلى أن متوسط دراسة موضوع الأخطار وإدارتها في جدول أعمال لجنة التدقيق بالنسبة للمجموعات التي كانت محل الدراسة يشغل حوالي ساعة ونصف من وقتها أي بنسبة 40% من الوقت المخصص للموضوع، تخصص للتعبير وطرح الآليات وهوية وطريقة الأخطار ونشاطات التحكم في الأخطار وأنظمة الأمن التي تم وضعها، ولوحظ كذلك أن الوقت المخصص لهذه المواضع يختلف كثيرا من مجموعة إلى أخرى ويتراوح مابين ست ساعات وعشر دقائق.

والموضوع الثاني هو "نظام الرقابة الداخلية وإدارة المخاطر" المضمون من طرف هيكل التدقيق الداخلي، خلصت الدراسة أنه يمثل ثلث الوقت المخصص للموضوع ويتم فيه فحص التخطيط وتقدم مهام التدقيق الداخلي، محصلة برنامج العمل، محصلة أعماله، وجد أن 80% من لجان التدقيق على مستوى هذه المجموعات تخصص على الأقل اجتماع واحد في السنة للتدقيق الداخلي وعلاقته بإدارة المخاطر، وأن إشكالية فضاء الأمن الإلكتروني تأخذ مكانة هامة من الانشغالات الأولى للمجموعات وهياكل قيادتها.

4- دراسة أنجزت على الشركات المنتمية إلى كاك 40 CAC ومجموعها 40 شركة، تحت عنوان "معيار ممارسة مجموعات كاك 40 آلية نظام الرقابة الداخلية" " Benchmark pratiques CAC40, dispositif de contrôle interne"، ففي موضوع مهام لجان

التدقيق المتعلقة بإدارة المخاطر وأنظمة الرقابة الداخلية، أحصت لها 17 نمط من المهمات، 7 متعلقة بإدارة المخاطة و 10 متعلقة بنظام الرقابة الدخلية.

بالنسبة لإدارة المخاطر: صنفت إلى صنفين كبيرين هما: تقييم سيرورة إدارة المخاطر، و تقييم المخاطر.

فالمهمة المتعلقة بفحص سيرورة إدارة المخاطر (خاصة جوانب الرقابة ومتابعة الأخطار)، عادة مايتم الإبلاغ عنها (وتمثل 80% من شركات المجموعة)، وقليل من المجموعات التي لم تبلغ عنها، والمهمة المتعلقة بفحص خريطة الأخطار هذه لها دورية منظمة وتمثل مابين 30 إلى 40%، والمهام الأخرى المتعلقة بإدارة المخاطر يتم التبليغ بها من طرف المجموعات، لكن في الأمور التي تمثل أفضلية لهم وتمثل 20%، والمهام المتعلقة بفحص سيرورات تقييم الأخطار وتقييم فعالية إجراءات إدارة المخاطر تظهر أنها تمت لأول مرة في المجموعات.

خلاصة الدراسات: أن كل واحدة من هذه الدراسات تناولت جانبا من الجوانب التي لها علاقة بالأمن والجريمة الإلكترونية وتأثيراتها على المنظات وتمت في الدول الغربية، لكن من خلال هذا البحث يريد الباحث الوصول إلى الأساليب والطرق التي تتعامل بهم المؤسسات الجزائرية مع الجريمة اللإلكترونية للوقاية منها ومحاربتها استنادا إلى المعايير والسيرورات المعمول بها في المنظمات والهيئات على المستوى الدولي.

خطة البحث: للإجابة على الإشكالية المطروحة، والمعالجة لعنوان البحث، ارتأى الباحث تقسيم البحث إلى ثلاثة أقسام، الأول متعلق بالمفاهيم والجريمة والأمن الإلكتروني، والثاني متعلق بلجان التدقيق ودورها في الوقاية من الجريمة الإلكترونية، والثالث خاص بالدراسة الميدانية للجان التدقيق والجريمة الإلكترونية بالمؤسسات الجزائرية.

المحور الأول: مفاهيم، أنواع، تكاليف، أثار والإجراءات القانونية للجريمة والأمن الإلكتروني

تصيب الجرائم الالكترونية الهيئات والمنظمات الخاصة والحكومية في عدة نشاطات وأثرها يختلف من هيئة إلى هيئة ومن دولة إلى دولة، وعليه فإن مفاهيمها والتكاليف المخصصة لمحاربتها يختلف حسب نظرة كل دولة للخطر الذي يلحق بها، ومن خلال هذا المحور نتعرض إلى هذه المفاهيم والإجراءات المتبعة بالنسبة لكل الدول والمنظمات لمحاربتها.

أولا: مفهوم فضاء الجريمة الإلكترونية Sybercriminalité

لا يوجد مفهوم موحد على المستوى العالمي خاص بفضاء الجريمة الإلكترونية، فكل دولة أو منظمة أو هيأة تعطي له مفهوما وفقا لنظرتها وأثر الجريمة الإلكترونية عليها، فمنها من تعطي له تعريفا من منظور اقتصادي واجتماعي مثل الدول المهتمة بأوضاعها الداخلية، ومنها من تعطي له تعريفا من منظور سياسي مثل الدول غير ديمقراطية، ومنها من تعطي له تعريفا من منظور سياسي واقتصادي مثل الدول الشبة متطورة، ومنها من تعطي له تعريف من منظور اقتصادي وجيو سياسي مثل الدول التي اقتصادها وسياستها مسيطرة دوليا، ولكن هناك تعريف شبه موحد لأنه يخص الأدوات المؤثرة والمتأثرة بفضاء الجريمة الإلكترونية، والذي قدمه في دراسة أجراها مكتب الأمم المتحدة لمحاربة المخدرات والجريمة ولخصه الباحث فيما يلي: بأنها "أي عمل غير قانوني يمس تكاملية موقع إفتراضي (كومبيوتر أو غيره كالهاتف أو سمارت فون Smartphone...الخ) معين باستخدام أداة كومبيوتر أو تكنولوجية معلومات أخرى كالهاتف أو سمارت فون Smartphone من قبل المجرم كأداة للجريمة أو جريمة تقليدية (احتيال أم تهديد...الخ) أما الموقع الإفتراضي هو المستهدف من طرف المجرم (السرقة أو الإحتيال، تحريف أو تدمير البيانات...الخ)".

والجريمة الإلكترونية هي جريمة جنائية يمكن ارتكابها على أو غير نظام حاسوب آلي يتصل عادة بشبكة الأنترنات، وبالتالي هي شكل من أشكال الجريمة أو الجنح الإلكترونية، حيث تقع في مكان افتراضي (فضاء الجريمة الإلكترونية)، وعولمة الشبكات هي أحد العوامل التي ساعدت على تطورها[1].

ثانيا: أنواع الجريمة الإلكترونية:

هناك عدة أنواع للجريمة الإلكترونية، وسوف نتعرض لأهم أنواع الجرائم الإلكترونية الشائعة ومنها[2]:

2-1- الهجوم من النمط التقليدي: هذا النوع من الجرائم يستعمل التكنولوجيات المستعملة في شبكات الإعلام الآلي والاتصال، عامة الهدف منها هو الاستفادة من جدارة المستخدمين لإزالة المعلومات السرية منهم واستخدامها بشكل غير قانوني، ويوجد عدة أشكال للجرائم من النوع التقليدي، وهي ليست ثابتة، عددها يرتفع باستمرار حسب تطور وسائل تكنولوجية المعلومات، ومن هذه الجرائم ما يلي:

ابتزاز الأموال؛ مختلف التهديدات بغرض الإنتقام؛ التعرف على الهويات؛ الإحتيالات المتعلقة ببطاقة الدين؛ الإحتيالات التجارية؛ خيانة الثقة والإحتيالات المختلفة؛ اختطاف القاصرين.

2-2- الهجوم من النمط التكنولوجي: تطور هذا النوع بقوة وبصفة متسارعة منذ ظهوره، ويستعمل أساسا عددا من نقاط الضعف في أجهزة تكنولجيات الإعلام والإتصال، وأكثر هذه الهجومات شيوعا ما يلي:تنصيب (تثبيت) برامج تجسس؛ تركيب برامج القرصنة؛ التعدي على ممتلكات الغير؛ الإتلافات المختلفة للمعلومات والبرامج...الخ؛ إتلاف المواقع الإلكترونية؛ سرقة المعلومات؛ رفض الخدمة على الموقع؛ العمل من مواقع الإعلام الآلي الضحية.

ممكن أن يستند الهجوم من النمط التكنولوجي على واحد أو مجموعة من الدوافع التالية:

استراتيجية (سرقة معلومات حساسة مرتبة)؛ إيديولوجية (تحويل الأفكار السائدة أو تيار الأفكار إلى أفعال غير مشروعة)؛ إرهابية (كزعزعة النظام القائم)؛ الجشع أو الطمع Cupide (السعي للحصول على مكاسب مالية أو مادية)؛ المتعة والتلاعب Ludique (للمتعة والترفيه)؛ الإنتقام (رد فعل على أي إحباط).

هذه الهجومات تهدف إلى التمكن من سرية أو تكاملية أو ما هو موجود في أجهزة تكنولوجيات الإعلام والاتصال أو الجميع.

فلنشر برامج ضارة، يركز المخترق عامة على أحد البدائل التالية:

2-3- الهجوم الإنتهازي Attaque opportunisme: الهجمات الإنتهازية هي هجمات غير موجهة مباشرة إلى أشخاص أو منظمات معينة، ولكنها تهدف إلى الحصول على أكبر عدد ممكن من الضحايا، ومعظم الأفراد والمنظمات هي عرضة لهذا النوع من الهجومات، ومنها[3]:

إنجاز أو شراء برامج خبيثة: البرامج الخبيثة (الضارة) تعطي المهاجم أداة تحكم مطلقة على أجهزة تكنولوجيات الإعلام والاتصال لضحيته، ونتيجة لذلك فهي تعتبر بمثابة حجر الزاوية للعديد من الهجمات الانتهازية؛

إرسال أو تأجير خدمة الرسائل الإقتحامية SPAM: فالوصول إلى عدد كبير من الضحايا، لا يتم إلا بتوزيع جيد لهذه الرسائل، أي يجب أن تكون قادرة على الوصول إلى جمهور واسع سواء بغرض الإحتيال أو لإصابة أجهزة تكنولوجيات الإعلام والإتصال، قد يكون إرسال رسائل البريد الإلكتروني أو الرسائل الإقتحامية على الشبكات الطريقة المفضلة للوصول إلى الغرض؛

إنشاء مواقع غامضة ونشر المواقع الموجودة: الحضور على شبكة الأنترنات غير مهم بالنسبة للمؤسسات الشرعية فقط، ولكن حتى فضاء الجريمة الإلكترونية ينشئ مواقع للتصيد والإعلانات والحيل، والصفحات التي تحتوي على الإستغلال من شأنها أن تصيب أجهزة تكنولوجيات الإعلام والإتصال الخاصة بمستخدمي الأنترنات؛

2-4 – هجوم مستهدف Attaque ciblée:[4] الهجومات المستهدفة قد يكون من الصعب للغاية مواجهتها، كل هذا يتوقف على الطاقة والوقت الذي تستعمله المجموعة الإجرامية، وهو أخطر أنواع الهجومات، وبشكل عام ينجح الهجوم المنظم جدا والمستهدف عندما

يركز المهاجم بشكل حصري على ضحيته، ويمكن أن تحدث هذه الهجومات في مراحل مختلفة، وسوف نوضح أدناه بعض الخطوات الهامة لهذا النوع من الهجومات، ومنها:

جني المعلومات Récolte d'information: قبل الهجوم على هدف معين، عادة ما يأخذ الهاكر مسحا لأي معلومات، ممكن أن تكون على شكل خريطة (صورة فوطوقرافية مفصلة) للمؤسسة أو الفرد الذي يستهدفه، يمكن أن يكون أرقاما هاتفية له أو الرسائل الإلكترونية المنشورة على الأنترنات تكون كآلية للهجوم على الضحية؛

مسح الشبكة Le balayage du réseau: أحيانا يختبر المتسللون الأنظمة المستهدفة لمعرفة ما إذا كانت نشطة لتحديد ماإذا كانت هناك ثغرات أمنية، هذه العملية ممكن أن تؤدي إلى إطلاق إنذارات عن الهجومات وغالبا لاتعطي نتائج مرضية، لهذا هذه العملية تخص بعض الحقول المحددة جدا للتطبيق فقط؛

الهندسة الإجتماعية L'ingéniérie sociale: غالبا ما يكون الهجوم على أنظمة الكمبيوتر مستحيلا نظرا للحماية القوية له، في حالة الهندسة الإجتماعية فبدلا من استخدام عيب فني في النظام المعلوماتي سيستخدم الجاني بدلا من ذلك مصداقية الإنسان، فيحاول على سبيل المثال بأنه شخص آخر له علاقة مع المستخدم من أجل الوصول إلى المعلومات، مثل كلمة المرور على سبيل المثال، هذا السيناريو أصبح ممارسة شائعة وغالبا ما يستخدم المتسللون الضعف النفسي على فرد ما أو يستدعي الإستعجال للحصول على المعلومات المرغوب فيها بسرعة؛

الملف الخدعة (المفخخ) Le fichier piégé: في هذه الحالة يستخدم الهجوم بواسطة البريد الإلكتروني المفخخ (الخدعة)، على سبيل المثال يحتوي على "حصان طروادة" في أي برنامج مما يسمح له بمجرد تنشيطه من قبل المستخدم بالتحكم عن بعد في جهاز كمبيوتر الضحية، وحصان طروادة تشير إلى رموز الكمبيوتر المخادعة وهي تطبيق أي شفيرة خاصة يستخدمها الحسوب لأغراض تلف أو تعطيل برمجة كمبيوتر أو ربما سرقة المعلومات الشخصية.

ثالثا– الجريمة الإلكترونية وتكاليف الأمن الإلكتروني

يعتبر فضاء الجريمة الإلكترونية التهديد الثالث للدول العظمى بعد السلاح الكيماوي، والسلاح البكتيريوبيولوجي والنووي[5]، فلمواجهة الأخطار الحالية لفضاء الهجومات الإلكترونية Syberattaque أغلب المنظمات على المستوى العالمي أصبحت تركز مواردها الخاصة بالأمن الإلكتروني Sybersécurété على الوقاية منه، فحسب Gartner الرائد في الدراسات والإستشارة في أنظمة المعلوماتية وصلت تكاليف الأمن لأنظمة المعلوماتية على المستوى العالمي إلى 67 مليار أورو سنة 2015، أي بزيادة قدرها 08% مقارنة مع السنة التي سبقتها[6]، في حين أنفق 3,1 مليار أورو سنة 2004، وسوف تصل إلى 152 مليار أورو سنة 2020، أين أصبحت الميادين الأساسية لمصدر الخطر والتي يجب حمايتها هي الهاتف النقال ونظام Could (ونعني به إرسال الموارد والخدمات تبعا للطلب عبر الشبكة الإجتماعية ويعني كذلك التخزين والدخول إلى المعلومات عبر الشبكات الإجتماعية، لكن الأقراص الصلبة لجهاز الحاسوب وشبكات الربط الداخلية لاتدخل في هذا النظام) والشبكات الإجتماعية وتجارة الذكاء في السوق الإفتراضي، ونظرا للعمليات المفجعة والكارثية التي ما انفكت تصيب المنظمات يوميا اكتفت بوضع حاجز أمام فضاء الهجومات الإلكترونية وليس محاربتها والقضاء عليها[7].

ونظرا للواقع الجديد الذي فرض نفسه والمتعلق بالإنتشار الواسع والغير مسبوق لتكنولوجيات الإعلام والإتصال، والذي شجع كثيرا محترفي مهنة الهجومات لإلكترونية مما أصبحت تمثل التهديد الأول للأصول الأساسية للدول والمنظمات على المستوى العالمي، وللحد من الأثار الجسيمة لهذه الظاهرة، خصصت موارد وميزانيات لعملية الأمن الإلكتروني، فوفقا للدراسات الحديثة لتكلفة هذه العملية تبن أن الدول الكبرى تأتي في المركز الأول، فالولايات المتحدة الأمريكية تمثل لوحدها 40% أي 26 مليار أورو من السوق العالمي للأمن

الإلكتروني، وبنمو قدره 4% سنويا وأوروبا بدون روسيا تمثل 25% أي 17 مليار، ومعدل النمو الأكبر هو الهند والصين، حيث الصين تكلفها 5,5 مليار أورو أي بنسبة 8 % وبنمو قدره 12 %، الهند 2 مليار أورو بنسبة 3 % وبنمو سنوي قدره 18%، والمانيا تمثل منه 6% ب 4,3 مليار أورو وبنمو قدره 5%، تليها بريطانيا 3,7 مليار أورو بنسبة 5,5%، وبنمو 5%، روسيا 3,1 مليار أورو أي بنسبة 5% وبنمو سنوي قدره 6% وفرنسا 4,6% بـ 3 مليار أورو ونمو قدره 5%، كوريا الجنوبية 2,6 مليار أورو بنسبة 3,8% وبنمو 5 %، إيطاليا 1,9 مليار أورو بنسبة 2,8 % وبنمو قدره 8%، كندا 1,2 مليار أورو بنسبة 1,8% وبمعدل نمو 8%، اسرائيل 1,2 مليار أورو بنسبة 1,8% وبمعدل نمو 7%، أستراليا 0,9 مليار أورو بنسبة 1,3% وبمعدل نمو 8%، باقي دول العالم 6,3 مليار أورو بنسبة 9,3% وبمعدل نمو 9%.[8]

فأثار الجرائم الإلكترونية ستتضاعف على المستوى العالمي من سنة 2015 إلى سنة 2021 أي من 3 تريليون أورو إلى 6 تريليون أورو، بما فيها الفساد، إتلاف المعلومات، الأموال المسروقة، الإنتاجية الضائعة، سرقة الملكية الفكرية، سرقة المعلومات الشخصية والمالية، تحويل الأموال، الغش، التشويش على بورصات الأعمال عن طريق الهجومات، تحليلات مواقع الهجوم، استرجاع المعلومات والأنظمة المهاجمة والإضرار بصور المنظمات[9].

كما هو معلوم حاليا على المستوى العالمي فإن أغلب الأجسام (الأغراض أو الأشياء) هي مربوطة Les objets connectées، حيث سنة 2016 وصلت إلى 3.5 مليار جسم مربوط (موصول) وحسب التوقعات سوف يصل إلى 50 مليار جسم مربوط سنة 2020، والتي سوف تكوّن في المستقبل مجتمعاتنا الحديثة سواء في الميدان الصناعي أو العسكري أو في المدينة، وصارت هي الأخرى أكثر عرضة من غيرها إلى الجرائم الإلكترونية، والذي فرض علينا تأمينها من هذه الجرائم، فتكلفة سوق فضاء الأمن الإلكتروني للأجسام الموصولة سوف يصل إلى 36,95 مليار أورو سنة 2023، وعلى سبيل المثال فسوق فضاء الأمن الإلكتروني للسيارات سوف يعرف قفزة كبيرة وسيصل إلى ما قيمته 759 مليون أورو سنة 2023 بنمو متغير وفقا لكل نشاط، فمصنعي ومجهزي السيارات أخذوا رهانات فضاء الأمن الإلكتروني بجدية لمواجهة الظاهرة، فالإتفاقية الدولية المتعددة السنوات بين رونو– نيسان وميكروسوفت المتعلقة بالأمن الإلكتروني للسيارات الموصولة التي تمت سنة 2016 تبرهن على الوضعية[10].

فالفجوة الحالية في المؤسسات الكبرى وفي الإدارات، تظهر عدم قدرة هذه المنظمات الوقوف أمام هذه الهجومات على الرغم من الوسائل المادية وغير المادية المعتبرة التي استثمرت من طرفها في فضاء الدفاع الإلكتروني، فالمسألة ليست معرفة أن هجوما سوف يصيب المنظمة، وإنما المشكل هو متى وكيف يحدث ذلك، أي لابد من تحديد فضاء الحماية الإلكترونية من الزاوية الكلية، حيث تكون دفاعات المنظمة جاهزة دائما قبل وأثناء وبعد الهجوم، فوظيفة لجان التدقيق لابد أن تكون لها قاعدة صلبة من ناحية الفعالية والتكوين وتمتلك وسائل كافة للتدخل وامتلاكها لرؤية ذات 360 درجة هي ضرورية لتقديم استشارات موضوعية لمساعدة المنظمة على توقعات فضاء الجرائم الإلكترونية ومقاومتها ومن أجل إعداد وتحسين الإستراتيجيات، السياسات وإعداد بروتوكول مخصص لحماية كل المنظمة اتجاه فضاء التهديدات الإلكترونية[11].

رابعا– فضاء الجريمة الإلكترونية هو تهديد متنامي للمنظمة

فتعدد حالات الإحتيالات والغش، الإختلاسات، الهجومات الإلكترونية خلال السنوات الأخيرة جعل الأهمية المتزايدة لفضاء الأمن الإلكتروني في المنظمات على المستوى العالمي، فالأضرار المالية لنشاطات فضاء الجرائم الإلكترونية التي أصابت المنظمات على المستوى العالمي، هي جد معتبرة، وقدرت سنة 2014 مابين 400 إلى 600 مليار دولار سنويا.[12]

ففي فرنسا طبقا لتقرير الوكالة الوطنية لأمن أنظمة المعلوماتية ANSSI وضحت في تقرير نشاطها لسنة 2018 التطور السريع لفضاء الجرائم الإلكترونية والتي بلغت 4000 إشارة هجوم تم استلامها سنة 2004، أي بزيادة قدرها 50% عن سنة 2015، وفي سنة 2018 بلغت 1869 إشارة مقابل 2435 سنة 2017، الأعداد تناقصت من ناحية العدد نظرا لإجراءات الحماية التي اعتمدت، لكن زادت من ناحية الأخطار ذات الهدف المهم والتكلفة[13].

وفي ألمانيا، قالت جمعية بيتكوم الألمانية العاملة في قطاع تكنولوجية المعلومات أن أكثر من نصف الشركات العاملة في البلاد تعرضت لتجسس أو أعمال تخريب أو سرقة بيانات في السنتين الأخيرتين (2015 و2016)، ووقع عدد من الهجومات الإلكترونية في الآونة الأخيرة، مثل فيروس الفدية الذي وقع في ماي 2017، وخلصت الدراسة إلى أن نحو 53% من الشركات في ألمانيا وقعت ضحية لعملية تجسس صناعي أو تخريب أو سرقة بيانات خلال نفس السنتين، أي بارتفاع قدره 51% عن دراسة أجريت سنة 2015، في الوقت نفسه زاد حجم الخسائر الناتجة عن هذه الهجمات بنسبة 8%، أي نحو 55 مليار أورو سنويا بحسب نتائج المسح الذي شمل 1066 من المديرين والأشخاص المسئولين عن الأمن الإلكتروني في قطاعات مختلفة، وتوصلت الدراسة، إلى أن من يقف وراء هذه الهجمات القسط الأكبر وراءه موظفون سابقون أو حاليين في تلك الشركات، تم يليه المنافسون أو الزبائن أو الموردون أو مقدمو الخدمات، ثم الهواة، وبعدها الجريمة المنظمة وفي الأخير وكالات الإستخبارات الأجنبية[14].

وصرح SIR LAIN LOBBON مدير مصالح الإستعلامات المكلف بالأمن الوطني في بريطانيا، بأنه "هناك 70 عملية فضاء جريمة إلكترونية تقع كل شهر ضد شبكات الحكومة والصناعة، والسر التجاري تتم سرقتها في الكيانات الصناعية"[15].

فالأشكال المتعددة لفضاءات الجرائم الإلكترونية (جرائم منظمة، جوسسة صناعية، الغش على الرؤساء، سياسة، قرصنة منفردة، استعمالات سيئة القصد...الخ)، أبعادها أصبحت عالمية وزادت من خطر وضبابية كشف هذه التهديدات، وأضعفت من طاقة الإستجابة الفعالة لها، فمهارة وغش وحذاقة الهجومات الخارجية والداخلية بلغت أقصى مداها وساهمت في الصعوبة بمكان من التحكم في خطر فضاء الجريمة الإلكترونية.

فالفضاء الإلكتروني الواسع، سمح للقراصنة في أي مكان وفي العالم من القيام بهجوماتهم في عدة دول، وأن هذه الدول تسيرها قوانينها الخاصة، مما صعب التحقيقات في الموضوع وتطبيق القوانين بالنسبة للدول المتضررة، أي محيط قانوني غير مناسب، فالدول المنظمة للقوانين المتعلقة بالموضوع وعلى المستوى العالمي أصبحت تدرك الأخطار المتنامية لفضاء الجرائم الإلكترونية ليس فقط على المؤسسات العمومية والعسكرية ولكن حتى بالنسبة لمؤسسات الخاصة[16].

الأضرار التي أصبحت تصيب المنظمات من الهجومات المتعلقة بفضاء الجرائم الإلكترونية فهي أشد ضراوة على أجهزة المعلوماتية وسيطرة نظام Big data المتعلق بتنظيم معلومات المنظمات، حيث تصاعدت بصفة رهيبة في السنوات الأخيرة، وزيادة على المعطيات الرقمية للمنظمات، فضاء الهجومات الإلكترونية ممكن أن يهدد كل الممتلكات المقيمة للمنظمات، فماهو الأثر الحقيق للجهومات الإلكترونية على المنظمات؟ فالهجوم الإلكتروني ممكن أن يصيب:

قاعدة المعطيات والأصول المالية للمنظمة بواسطة الغش، السرقة، الإبتزاز، النهب، السلب...الخ؛ الملكية الفكرية والسر التجاري (المهني) بواسطة القرصنة؛ العلامات وجودتها على الشبكات الإجتماعية بواسطة المقاطعة، الكذب وتشويه الصورة؛ استمرارية الإستغلال بواسطة التخريب أو التشويش على العمليات؛

خامسا– الإجراءات القانونية المتخذة في بعض الدول فيما يتعلق بالحماية من الجرائم الإلكترونية

نظرا لفداحة الأضرار التي أصابت المنظمات والدول على المستوى العالمي وخاصة الدول الكبرى ذات الإقتصاد القوي، بادرت إلى استحداث قوانين وإجراءات تلزم المنضمات والهيئات بها من أجل حماية أصولها من التهديدات الإلكترونية، ومنها:

ففي انجلترا في جويلية سنة 2013 استدعت الحكومة المؤسسات المنتمية إلى Indice FTSE 350 للمشاركة في (حصيلة صحة المؤسسات والإحتياطات المتبعة بفضاء الأمن الإلكتروني لقيادة المؤسسات) في إطار هذه الرقابة رئيس المؤسسة ورئيس لجنة التدقيق يقومان بملء استفسار الذي بموجبه يتم تقييم تسيير المسائل المتعلقة بحماية الملكية الفكرية ومعلومات الزبائن في المؤسسة، هذه المقاربة هدفها ضمان تحسيس المؤسسات بأهمية الأمن الإلكتروني وخطر الجرائم الإلكترونية الذي كان هو جدول أعمال المجلس المشترك بين الحكومة والمؤسسات[17]. وفي الولايات المتحدة الأمريكية لجنة الأمن والتبادل (Securities and exchange commission(SEC، نشرت توجيهات إلى المنظمات تجبرها بإظهار مسائل فضاء الأمن الإلكتروني في تقارير التسيير السنوية التي تقدمها الإدارة إلى الجمعية العامة للمصادقة عليها، فيطلب من المنظمات تقييم أخطار أثار الجرائم الإلكترونية إذا كانت من أحد العناصر التي تؤثر على الإستثمار في المنظمة وعليها أن تعتبر أن أي أثر لفضاء الجرائم الإلكترونية هو مصدر للخطر، وإعداد آلية مناسبة لمواجهته ومراقبته، والتصريحات بالأخطار أو أثر إلكتروني مادي، ممكن أن تكون محل عملية عالمية لمواجهته، أو من الممكن عدم القدرة على اكتشافه قبل وقت معين، وكذلك كيفيات تغطيته أو مواجهته بفضاء الأمن الإلكتروني[18]. وفي فرنسا مع قانون البرمجة العسكرية لديسمبر سنة 2013 ومرسومه المؤرخ في 27 مارس 2015 المتعلق بتكثيف واجبات الأمن للمتعاملين ذوي الأهمية(الشأن) الحيوية، فأعطت الدولة إلى الوكالة الوطنية لأمن أنظمة المعلوماتية سلطات جديدة، حيث أسندت لها مهمة القيام بعملية المراقبة على مستوى منظمات المتعاملين ذوي الأهمية الحيوية أين تفرض عليهم مستوى معين من التجهيزات المعدة للأمن الإلكتروني وفي نفس الوقت التبليغ عن كل الهجومات الإلكترونية التي تتعرض لها، حتى تستطيع أن تراقب شبكاتها في حالة حدوث أزمة[19]. وفي أوروبا، تبنى البرلمان الأوروبي في 13 مارس 2014 موقفه من القراءة الأولى المتعلقة بالتوجيهات الخاصة بأمن شبكة المعلوماتية، وفي 18 ديسمبر 2015 اللجنة الدائمة لممثلي الإتحاد الأوروبي صادقت على اتفاقية مع البرلمان الأوروبي من أجل إعداد نص متعلق بأمن شبكة المعلوماتية للمصادقة عليه من طرف المجلس ثم البرلمان[20].

وفي الجزائر، على غرار جميع دول العالم، فالجزائر لم تكن استثناء من باقي الدول بالنسبة للجرائم الإلكترونية، فقامت السلطات العمومية بإصدار عدة تشريعات في الموضوع ومنها القانون رقم 04/09 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والذي من خلاله وضح ما هي الأعمال التي تعتبر من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وكيفيات مراقبتها والقواعد الإجرائية لها وإلتزامات مقدمي هذه الخدمات والتعاون والمساعدة القضائية الدولية والهيأة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[21]، إلا أن هذه القوانين تعرضت فقط للآليات القانونية لمكافحتها (القضاء والشرطة)، ولم تتعرض مثل قوانين باقي الدول إلى الإجراءات والآليات التي تفرض على المؤسسات العمومية والخاصة القيام بها لحماية معلوماتها وممتلكاتها من الجرائم الإلكترونية، كما تم إنشاء الهيأة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها عن طريق المرسوم الرئاسي رقم 215/15 المؤرخ في 2015/10/8، حيث هذه الهيأة تتكون من موظفي

الأمن وتابعة كلية للهيئات الأمنية والقضائية وهدفها هو مراقبة الأعمال التي تتعلق أكثر بأمن الدولة، وعدل بالمرسوم المؤرخ في 06 يونيو 2019 بالجانب المتعلق بأعضاء الهيأة.

المحور الثاني: رهانات المنظمات ودور لجنة التدقيق والوسائل المتخذة لمحاربة الجريمة الإلكترونية

المنظمات يجب أن تقوم بأعمال كثيرة لحماية معطياتها لتقي نفسها من السرقة والإحتيال والتخريب، فالأمن المطلق الذي تقوم به المنظمات لحماية نفسها من فضاء الهجومات الإلكترونية غير موجود ومستحيل، "فالخصم (المهاجم) الذي يمتلك موارد وحسابات مدروسة ومؤسسة وكافية، تكون النهاية بلا شك هو الوصول إلى وسيلة لإحباط أفضل دفاع، والوصول إلى نقاط الضعف سواء المتعلقة بأمن المعلومات أو أمن الشبكات، وحتى أمن الأفراد"[22]، فالآن أصبحت الحرب على المستوى العالمي حرب إلكترونية بامتياز، سواء بين الدول أو المنظمات حيث المهاجمون أصبحوا يملكون وسائل تتحدى وسائل دفاع المنظمات، بالإضافة إلى ذلك لهم من المهارة والكفاءة في هذا المجال تفوق مهارة وكفاءة أفراد المنظمات، فكل منظمة لابد أن تجد توازن مابين الدفاع عن أهم أصولها ضد هجومات فضاء الجرائم الإلكترونية وتكلفة إجراءات الأمن الإلكتروني، فدفاع أنظمة المعلوماتية ضد كل أشكال الإختراقات الإلكترونية هو رهان أساسي لإستراتيجية الإعلام الآلي للمنظمات، وفضاء التهديدات الإلكترونية Sybermenaces، لابد أن يكون جزءا من سياسة إدارة المخاطر والإدارة للمنظمات، وخريطة المخاطر لابد أن تعكس الخطر المحتمل للهجوم الإلكتروني ضد الأصول أو السيرورات الجوهرية.

عدد من المنظمات أعدت عدة سناريوهات لهجومات فضاء الجرائم الإلكترونية من أجل اختبار قدرتها على المقاومة والرد في حالة الهجوم الإلكتروني، هذا السيناريو يتضمن وصف لحالة هجوم إلكتروني، المسببات، الغايات وتقنية احتمال وقوع قرصنة.

أولا: دور لجنة التدقيق اتجاه الجريمة الإلكترونية

فوظيفة لجنة التدقيق بالنسبة للمنظمة اتجاه الجرائم الإلكترونية تظهر كوظيفة وقائية مستقلة مثلها مثل وظائف الرقابة الأخرى (التدقيق الداخلي والخارجي، نظام الرقابة الداخلية، إدارة المخاطر)، لأنها أصلا تعتمد في عملها على هذه الأنظمة، فالخبرة والمهارات والمعرفة المكتسبة هذه تؤهلها لتحديد نقاط القوى والضعف في المنظمة المتعلقة بفضاء الأمن الإلكتروني وتقييم وتدعيم طاقتها في هذا المجال.

فليس من المفاجئ أن لجان التدقيق بالإستعانة بالمدقق الداخلي والخارجي تكتشف بوضوح العواقب الوخيمة التي تراها تمس المنظمة جراء احتمال حدوث هجوم الكتروني، كما قال James Reichard، مسؤول التدقيق بشركة Simon Property Group وأستاذ تدقيق الإعلام الآلي "بأنه وحسب تجربتي أن المنظمات متبنية مقاربة كلية فيما يتعلق بحماية معلوماتها" ويعتبر أن مسئولي التدقيق الداخلي خصوصا لهم القدرة على تكوين أعضاء مجلس الإدارة ولجان التدقيق حول مختلف المجهودات الواجب بذلها للمقاومة ضد فضاء التهديدات الإلكترونية والتعرف على الخلل الموجود في أنظمة الأمن الإلكتروني بالمنظمة. "فالمشكل المتعلق بفضاء الأمن الإلكتروني هو طبيعة الأخطار والوسائل الجديدة التي يستعملها المهاجم التي تبقى غير معروفة من طرف المنظمة، فلهذا مجالس الإدارة ولجان التدقيق ليس لهم نفس التوقع عن درجة الأخطار التي يمكن أن تحدث خللا في النشاط" ويضيف نفس الكاتب "كما يناط بمسئول التدقيق الداخلي ولجان التدقيق إشراك مدراء أنظمة المعلوماتية أو أعضاء منها بالبدء بتحسيس الفرق حول ما أنجز في المنظمة من عمليات تخص فضاء الأمن الإلكتروني".

فلجان التدقيق ومجالس الإدارة لابد أن تعلم من طرف مسئولي التدقيق الداخلي بالتكنولوجيا التي ليس بواسطتها نحقق الأهداف العملية، وإنما كذلك لابد أن نجعل المنطقة أكثر يقضة اتجاه الهجومات الإلكترونية، فعندما تحصل لجان التدقيق والتدقيق الداخلي على الوسائل والدعائم الضرورية تطور مهارتها وتعتمد المقاربات الضرورية للقيام بالفحص وتزود مصالح الأمن الإلكتروني بنقاط القوى والضعف في سيرورات الأمن الإلكتروني[23].

الرهانات المتعلقة بالأمن الإلكتروني في ضل التوسع المتزايد والمتسارع يوميا لتكنولوجيات الإعلام والإتصال في الوقت الراهن، أصبحت أولوية من أولويات لجنة التدقيق على مستوى المنظمات، والتي أصبح مفروضا عليها الإجابة على أسئلة دقيقة تتمثل أغلبها فيما يلي[24]:

ما هي الأصول الأساسية (مادية، غير مادية، فضاء افتراضي...الخ) التي يمكن أي تصيبها هجومات فضاء الجريمة الإلكتروني؟ والتي يجب حمايتها؛ كيف تتم حماية الأصول الأساسية؟ ما هو مستوى الخطر المقبول عند تعرضها إلى خطر الجريمة الإلكترونية؟ ما هي أنظمة الرقابة الموضوعة لمراقبة فضاء الشبكات (بما فيه Cloud) وموردها وكذلك تركيبات الأجهزة للمنظمات، مثل أجهزة المحمول؟؛ من هو المسئول عن حمايتها؟؛ المنظمة يوجد ضمن مستخدمها مستخدمين مكونين ولهم تجربة فيما يتعلق بالحماية من أخطار الفضاءات الإلكترونية ؟؛ الموارد المخصصة للأمن الإلكتروني (ميزانية، موارد بشرية...الخ)، هي كافية؟؛ كيف تتصرف المنظمة اتجاه حادث جسيم؟.

1– تفاعل لجنة التدقيق مع قيادة المنظمة في مجال الأمن الإلكتروني لمكافحة الجريمة الإلكترونية

التفاعلات بين لجنة التدقيق وقيادة المنظمة ممكن أن تكون حول ثلاثة ميادين[25]:

الميدان الأول: القيادة والعنصر البشري

في هذا الميدان مطلوب من لجنة التدقيق أن تقيم درجة اهتمام القيادة بإدارة فضاء الأمن الإلكتروني وتجسيد ثقافة أمن متعلقة بترقية المستخدمين الأساسين والمهارات.

فما هي التفاعلات التي تكون بين الإدارة ولجنة التدقيق فيما يتعلق بهذا الميدان؟، النمط المعروض أدناه يأخذ بعين الإعتبار نشاطات الإدارة وأعمال لجنة التدقيق.

فالنشاطات التي ممكن أن تقوم بها الإدارة و**تُعلم** بها لجنة التدقيق هي:

تحديد الأصول الأساسية / المعطيات الحساسة الواجب تأمينها إلكترونيا؛ إحصاء العلاقات بين الشركاء والمتعاملين الثانويين الأساسين (المهمين)؛ تحديد سياسة متعلقة بفضاء الدفاع الإلكتروني؛ إعداد برنامج لتحسيس المستخدمين؛ تطوير مسار تكوين خاص بالمستخدمين الأساسين.

أما لجنة التدقيق بواسطة **الإشراف** تتصرف كالتالي:

تفحص الأصول الأساسية المحصاة؛ تفحص هياكل إدارة الدفاع الإلكتروني الموضوعة من طرف قيادة المنظمة؛ تفحص سيرورات التكوين وتحسيس المستخدمين مقارنة مع فضاء الأمن الإلكتروني؛ تطلب متابعة برنامج التكوين ومحاربة فضاء الهجومات الإلكترونية.

الميدان الثاني: العمليات، أنظمة المعلوماتية والمطابقة

مطلوب من لجنة التدقيق في هذا الميدان تقييم درجة الأخذ في الحسبان فضاء الأمن الإلكتروني في أنظمة المعلوماتية والعمليات يوميا.

فما هي التفاعلات التي تكون بين الإدارة ولجنة التدقيق فيما يتعلق بهذا الميدان؟، فالنمط المعروض أدناه يأخذ بعين الإعتبار نشاطات الإدارة وأعمال لجنة التدقيق.

فالنشاطات التي ممكن أن تقوم بها الإدارة و**تُعلم** بها لجنة التدقيق هي:

ضمان القيام بالإلتزامات القانونية فيما يتعلق بالمطابقة؛ تحديد المسئوليات فيما يتعلق بالأمن الإلكتروني؛ تحديد الوسائل والموارد المخصصة للأمن الإلكتروني؛ ضمان إدخال إشكالية الأمن الإلكتروني ضمن أنظمة المعلوماتية؛ تحديد مؤشرات متابعة نشاطات الرقابة والآثار الناجمة عن فضاء الجرائم الإلكترونية.

وفي هذا الميدان فلجنة التدقيق بواسطة **الإشراف** تتصرف كالتالي:

فحص الوسائل والموارد المتاحة المخصصة للأمن الإكتروني؛ مقابلة لجنة الإعلام الآلي للمنظمة من أجل فهم إدماج إشكالية الأمن الإلكتروني ضمن نظام المعلوماتية؛ معرفة الرقابات الجوهرية (الأساسية) الموضوعة في أنظمة المعلوماتية وجمع عناصر التقييم لإدارتها؛ مراجعة وفحص مؤشرات المتابعة المعدة من طرف الإدارة؛ فحص تقرير مآثر الهجومات الإلكترونية على أنشطة المنظمة.

الميدان الثالث: إدارة المخاطر واستمرارية الإستغلال

مطلوب من لجنة التدقيق تقييم درجة التكفل بفضاء أمن المخاطر ضمن آلية إدارة المخاطر.

فما هي التفاعلات التي تكون بين الإدارة ولجنة التدقيق فيما يتعلق بهذا الميدان؟، فالنمط المعروض أدناه يأخذ بعين الإعتبار نشاطات الإدارة وأعمال لجنة التدقيق.

فالنشاطات التي ممكن أن تقوم بها الإدارة و**تُعلم** بها لجنة التدقيق هي:

تقوم بالربط بين أخطار هجومات الفضاءات الإلكترونية والمعطيات الحساسة؛ تطور سياسة إدارة المخاطر؛ تقييم كفاءة آلية فضاء الأمن الإكتروني؛ تقييم طاقة الإستجابة والرقابة اتجاه هجومات الفضاءات الإلكترونية؛ إعداد مخطط إدارة الأزمات.

أما لجنة التدقيق بواسطة **الإشراف** تتصرف كالتالي:

تراجع وتصادق على مستوى رد الإدارة على الأخطار المتعلقة بالأمن الإلكتروني؛ فحص سيرورات إدارة المخاطر لفضاء الجريمة الإلكترونية؛بالتعرف على طاقة الإستجابة ضد هجومات الفضاءات الإلكترونية؛ تقييم مدى نضج مخطط إدارة الأزمات.

2- التصرفات والممارسات بالنسبة لأعضاء القيادة ولجنة التدقيق اتجاه الجريمة الإلكترونية

من الأعمال المهمة التي تقوم بها الإدارة وتوكل الإشراف والمتابعة عليها للجنة التدقيق هي[26]:

- مجلس الإدارة يحدد مقاربته المتعلقة بالإشراف على آلية إدارة مخاطر فضاء الهجومات الإلكترونية ويوكل مهمة المتابعة إلى لجنة التدقيق تبعا لمهامها المحددة بالقانون الداخلي لمجلس الإدارة، فعندما توكل هذه المهمة إلى لجنة التدقيق، هذه الأخيرة تقوم بإبلاغ نتائج أعمالها أثناء اجتماع مجلس الإدارة، حيث يجب أن يكون فضاء الأمن الإلكتروني موضوع جدول أعماله على الأقل مرة في السنة؛
- مجلس الإدارة و/أو لجنة التدقيق المعينة تضمن بأن المؤسسة قامت بإحصاء المعلومات الخطيرة للأصول الإستراتيجية التي تريد أولوية الحماية لها سواء ماتعلق الأمر بالمعطيات المالية، معطيات تجارية، معطيات عملية، معطيات حول الأفراد أو الملكية الفكرية...الخ
- مجلس الإدارة و/أو لجنة التدقيق المعينة تضمن بأن برامج التكوين في المؤسسة تضمنت عناصر (منابع) الخطر لفضاء الجريمة الإلكترونية؛
- مجلس الإدارة و/أو لجنة التدقيق المعينة تكون على علم بالتنظيم والموارد المخصصة لآلية الأمن الإلكتروني، بما فيها وجود مسئول على أمن أنظمة الإعلام الآلي (المعلوماتية)؛
- مجلس الإدارة و/أو لجنة التدقيق المعينة تحصل على شرح من الإدارة لآلية الرقابة والكشف، بما فيها إدارة عواقب هجوم فضاء جريمة إلكترونية؛
- مجلس الإدارة و/أو لجنة التدقيق المعينة تفحص عملية آلية الرد ضد فضاء الهجوم الإلكتروني داخل المنظمة (خلية إدارة الأزمات، ...الخ)؛
- مجلس الإدارة و/أو لجنة التدقيق المعينة تضمن إعداد سيرورة لفحص عمل آلية أمن الفضاء الإلكتروني، بما فيها عند الضرورة القيام بتدقيق مستقل عليها؛
- مجلس الإدارة و/أو لجنة التدقيق المعينة تفحص ارتدادات حالات هجومات فضاء الجرائم الإلكترونية داخل المنظمة؛
- مجلس الإدارة و/أو لجنة التدقيق المعينة يفحص نتائج الإختبار المنجزة من طرف الإدارة؛

● مجلس الإدارة و/أو لجنة التدقيق المعينة يضمن تجسيد برنامج للتحسينات مستمر من أجل التكيف مع تطور نوعيات (كيفيات) هجومات الفضاءات الإلكترونية.

3- الأطراف الفاعلة التي تعتمد عليها لجنة التدقيق لأداء مهمتها في إدارة الجريمة الإلكترونية:

حتى يسمح للجنة التدقيق متابعة ميكانيزم إدارة المخاطر بالمنظمة والمتعلقة بأمن الفضاء الإلكتروني، يظهر من الضروري أن تنسق وتوثق بين الإدارة العامة ووظائف إدارة المخاطر، التي تمد لجنة التدقيق بالمعلومات والضمانات التي تحتاجها لإنجاز مهمتها، وهذه الوظائف هي[27]:

3-1- وظيفة إدارة المخاطر: التي هي مسئولة عن إحصاء ومتابعة أخطار المنظمة ووضع خريطة للأخطار التي ممكن أن تصيب كل فرع في المنظمة جراء الهجومات الإلكترونية؛

3-2- وظيفة نظام الرقابة الداخلية: التي هي مسئولة عن ضمان تطبيق تعليمات الإدارة فيما يتعلق بالأمن الإلكتروني وتعمل على تحسين فعاليتها وتجسيد التنظيم، الطرق، المناهج، الإجراءات، السيرورات الخاصة بكل نشاط في المنظمة من أجل ضمان استمراريتها؛

3-3- وظيفة التدقيق الداخلي: الذي هو الأخر مكلف دوريا بمراجعة الوسائل التي يمتلكها التشغيليون لإدارة ومراقبة المنظمة، أهدافه هو فحص أن الهياكل شفافة ومتطابقة مع أنظمة الرقابية وأن الإجراءات المتخذة تضمن السلامة الكافية للنشاطات وأن العمليات المنجزة لا تحتوي على أخطاء وأن المعلومات الموزعة هي صادقة؛

بالإضافة إلى ذلك لجنة التدقيق تستشر الفاعلين الخارجيين مثل:

3-4- محافظ الحسابات: الذي يعلم الإدارة وهياكل القيادة عن الضعف في أنظمة الرقابة الداخلية المعتمدة من طرف الإدارة والخاصة بتهديدات الجرائم الإلكترونية التي ممكن أن تصيب حسابات الشركة؛

3-5- الخبراء المستقلين: وعند الضرورة تلجأ لجنة التدقيق إلى الخبراء المستقلين من أجل الحصول على تقييم أخر حول فعالية أنظمة الرقابة الداخلية وإدارة المخاطر المعتمدة لمواجهة فضاء الهجومات الإلكترونية.

الخلاصة: حاليا الهجومات الإلكترونية لايمكن بأي حال من الأحوال فصلها عن الحقيقة الإقتصادية للمنظمات، فالأخطار المتعلقة بالتكنولوجيات الجديدة مستمرة في الإنتشار بنظام متسارع ومتنامي أكثر فأكثر، فلجان التدقيق تستطيع أن تلعب دورا مهما في مساعدة المنظمة لتعيش في عالم هو فريسة لفضاء الهجومات الإلكترونية نتيجة التطورات الغير مسبوقة في تكنولوجيات الإعلام والإتصال، وخاصة مساعدة مجالس الإدارة على طرح الأسئلة المهمة فيما يتعلق بمسألة فضاء الهجومات الإلكترونية وكيفيات الوقاية منها، فالمنظمات التي تستطيع تطوير المهارات المتحصل عليها لمواجهة هذه التهديدات سواء على المستوى الإستراتيجي و التكتيكي هي التي تستطيع أن تعيش وتتنامى وتنجح، وفي حالة تمكن لجان التدقيق من الدعم والموارد الضرورية تستطيع أن تكون شريكا أساسيا للمنظمة.

المحور الثالث: الجرائم الإلكترونية وواقع لجان التدقيق في المؤسسات الجزائرية

يحاول الباحث من خلال هذا العنصر التعرض إلى واقع الجرائم الالكترونية في الجزائر والإجراءات المتخذة من قبل السلطات العمومية، وكذلك المؤسسات ودور لجان التدقيق لمحاربة الجرائم الالكترونية بالإضافة إلى دراسة ميدانية أجريت على عدة مؤسسات اقتصادية عمومية.

أولا: واقع الجريمة الإلكترونية والإجراءات المتخذة في المؤسسات الجزائرية

مما لاشك فيه أن الجرائم الإلكترونية أصبحت لا تمس دولا دون الأخرى، فالواقع الذي يفرضه التقدم التكنولوجي والمعلوماتي بات المحدد الأساسي والإستراتيجي للبناء الإقتصادي للدول، وأصبحت الجريمة الإلكترونية تهدد الهياكل ومعطيات هذه المنظمات، فالوسائل التقنية لم

تخترع الجريمة الإلكترونية، بل كانت ضحية لها في معظم الأحوال، حيث أن هذه الوسائل تعرضت لسوء الإستغلال، لهذا وجب حمايتها من مثل هذه الطرق المسيئة لاستغلالها.

والمؤسسات الجزائرية مثلها مثل مؤسسات باقي الدول ليست بمنأى منها، فالتقرير السنوي لـ 2017 لوزارة العدل سجل بأن هناك ثلاثة ملايين محاولة لإختراق ملفاتها، كما كشفت في نفس السنة مصالح الدرك والشرطة الجزائرية في الملتقى الدولي المنعقد بمدينة قسنطينة حول " مخاطر الإستعمال السيئ للأنترنات " في إحصائية مشتركة عن أن الجزائر سجلت 2500 جريمة إلكترونية تتعلق بالقرصنة والإبتزاز والتشهير والتحرش الإلكتروني والإحتيال، وأنها ارتفعت خلال 3 سنوات من 200 جريمة إلى 2000 جريمة، وأن الجرائم الإلكترونية ترتفع كلما ارتفع عدد مستخدمي الأنترنات، حيث تم تسجيل 29 مليون جزائري تستخدم الأنترنات مع نهاية سنة 2017، من بينهم 19 مليون يستخدمون مواقع التواصل الإجتماعي فيسبوك، ولم يسلم من الجرائم الإلكترونية وزراء ونواب في البرلمان وإطارات عليا في الدولة، خاصة ما تعلق بالإبتزاز والتشهير والتهديد، وكانت غالبيتها عبر مواقع التواصل الإجتماعي، وأن 80% من الجرائم الإلكترونية المرتكبة تمت عن طريق موقع التواصل الإجتماعي فيسبوك[28] ، والمثال على ذلك والذي أثر حتى على المستوى العالمي الهاكر الجزائري حمزة بن دلاج حيث وصف من أخطر عشر هاكر في العالم، حيث استطاع أن يفك أعقد شفرات البنوك في العالم وقام باختراع برمجية خبيثة تدعى "العين المتجسسة"، تقوم بسرقة البيانات الحساسة من أجهزة الحاسوب، ويعتقد أنها أصابت 50 مليون حاسوب عبر العالم، وقام بالسطو على 217 بنكا عبر العالم، وتسبب في خسارات مالية فادحة للعديد من المؤسسات المالية، حيث كان يقوم بتحويل هذه المبالغ إلى فلسطين وعدد من الدول الفقيرة، بالإضافة إلى قرصنة عدد من مواقع قنصليات أوروبية، كما قام بهجوم على 8000 موقع فرنسي وتسبب في غلقها وتوزيع عدد من التأشيرات مجانيا على عدد من الشباب الجزائري، ومهاجمة العديد من المواقع الإسرائيلية، كما تمكن من تسريب العديد من المعلومات السرية عن الجيش الإسرائيلي إلى الفلسطينيين، وحول حوالي 3,4 مليار دولار واضعف سطو قام به هو 10 مليون دولار[29].

ولمواجهة هذه الظاهرة العالمية، قامت السلطات العمومية في الجزائر بإحداث تشريعات وإجراءات تنبه الإدارات والمؤسسات بأخطار الجريمة الإلكترونية، مثل القانون رقم 04/09 الذي صنف الجرائم الإلكترونية كما يلي[30]:

1- الجرائم المتصلة بتكنولوجيات الإعلام والإتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية؛

2 - منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين ؛

3- معطيات معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها؛

4- مقدمو الخدمات: – أي كيان خاص أو عام يقدم لمستعملين خدماته، القدرة على الإتصال بواسطة منظومة معلوماتية و/ أو نظام للإتصالات – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأجهزة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الإتصال، والوجهة المرسل إليها، والطريق الذي تسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة؛

5- الإتصالات الإلكترونية: أي تواصل أو اتصال أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

وتعليمة الوزير الأول التي تطالب فيها الإدارات والمؤسسات العمومية بعدم استخدام نظام التشغيل ويندوز Windows10، بسبب عدم ضمان النسخة الجديدة لسلامة الملفات، وإمكانية وصول شركة ميكروسوفت إلى المعلومات الشخصية لمستخدميها، حيث التحديث الذي تقوم به ميكروسوفت على نظام ويندوز يهدد حماية وتخزين المعطيات الرقمية في الإدارات والمؤسسات العمومية الجزائرية، ولفتت التعليمة انتباه المؤسسات بان تسويق ويندوز10 يقدم عرضا تفضيليا بتحديث مجاني للإصدارات ويندوز 7 و8 والتي هي مستعملة في الحواسب الموجودة بالهيئات والمؤسسات الجزائرية، وهذا ما يتيح لميكروسوفت الحصول على معلومات ووثائق المستخدم بما فيها تلك البالغة الحساسية[31].

ثانيا– عينة الدراسة وأدوات المعالجة الإحصائية

في ظل هذه التحديات التي أصبحت تفرضها الجرائم الإلكترونية على الهيئات والمؤسسات الجزائرية، وباعتبار أن لجنة التدقيق كما هو معروف على المستوى العالمي أصبحت الهيكل الأول في المنظمات الذي يعتمد عليه من أجل حمايتها من المخاطر التي سوف تلحق بها باعتبارها الهيكل المنسق بين الإدارة والتدقيق الداخلي والتدقيق الخارجي في هذا المجال والمكلفة بمتابعة مهام كل منهم، فهل لجنة التدقيق في الجزائر تلعب نفس الدور الذي تقوم به مثيلاتها في المنظمات على المستوى العالمي؟

لكن في واقع المنظمات الجزائرية أراد الباحث التحق من تجسيد والدور الذي تقوم به لجان التدقيق على مستوى المنظمات فيما يتعلق بالجرائم الإلكترونية، فقام بدراسة ميدانية للموضوع على عدة مؤسسات وطنية كنموذج والتي تنشط بولاية الشلف وعين الدفلى وهي: (مؤسسة باتيميتال، مؤسسة ميناء تنس، مؤسسة تسيير ومراقبة ملاجئ الصيد البحري، مؤسسة الخزف الصحي، مؤسسة الأسمنت، مؤسسة البناء والتجديد)، وتم توزيع 136 استبيان على الأفراد المعنيين مباشرة بلجنة التدقيق وهم:

- 114 مسئول إداري (مدراء، نواب مدير، مسئولين آخرين حسب طبيعة كل مؤسسة)؛
- 16 مدقق داخلي؛
- 6 محافظ حسابات لهذه المنظمات.

أما أدوات الدراسة، استعمل الإستبيان كأداة للدراسة الميدانية وأعد بالطريقة المقيدة ليسهل على المستجوبين استخدامها، وحتى تكون نتائجها أكثر موضوعية، مع تحديد مجموعة من العبارات لكل عنصر سؤال من عناصر الإستبيان.

أما المعالجة الإحصائية تمت باستخدام الحاسب الآلي لبرامج الرزم الإحصائية للعلوم الإجتماعية الجاهزة Statistical Package for Social Sciences SPSS، في حساب التكرارات المقابلة لكل عبارة موزعة على الإجابات الثلاث (موافق، لا أدري، غير موافق)، وهذا من خلال استخدام التوزيع الطبيعي الذي هو المناسب لهذا النوع من العيينات، وللوصول إلى نتائج معبرة وواقعية عن الدراسة استخدم الباحث أدوات المعالجة الإحصائية التالية:

المتوسط الحسابي: وهو القيمة التي تتجمع حولها مجموعة قيم ومن خلالها نستطيع الحكم على قيم كل المجموعة.

التباين La variance: حتى نستطيع أن نتعرف على كون الفروقات بين أفراد العينة حول مستوى رضاهم عند مؤشر ها دالة او غير دالة وهذا لاختبار كل فرض من فروض الدراسة.

القيمة الحرجة للإحتمال P .Value: وهي القيمة الإحتمالية المقابلة لدالة كثافة الإحتمال والتي تعتبر الحد الفاصل للفروض (العدم والبديل، فإذا كانت قيمتها أصغر من 0,05 (مستوى المعنوية لمعامل ثقة 95%) يتم رفض فرض العدم وقبول الفرض البديل، أما لإذا كانت قيمتها أكبر من 0,05 يتم قبول فرض العدم ، أي القيمة موجودة في مجال الثقة للتوزيع المعتمد حيث:

Ho المتوسط الحسابي للعينة = درجة القبول

H1 المتوسط الحسابي للعينة > درجة القبول

حساب صدق الإستبيان والثبات: تم حساب معامل الثبات بتطبيق الإستبيان على عينة أفراد تم اختيارهم على الأساس الذي أشرنا إليه أعلاه، وكان معامل ثبات الإستبيان = 0,96 وهي درجة مناسبة جدا حسب المختصين، أم صدق الإستبيان يساوي الجذر التربيعي للثبات أي = 0,98.

درجات حد القبول: هي عبارة عن عدد عبارات كل محور مضروب في القيمة الحرجة للإستبيان (5)، حيث الجدول التالي يبين المحاور (الفرضيات) وعدد عبارات كل محور موجودة في المعالجة للفرضيات أدناه:

جدول رقم 01: جدول درجات حد القبول

(الفرضيات)المحاور	عدد عناصر كل محور	درجة حد القبول
– تكوين وسير(إدارة) لجان التدقيق بالمؤسسات الجزائرية	7	35
– لجنة التدقيق وإدارة المخاطر في المؤسسات الجزائرية	7	35
– لجنة التدقيق وفضاء الجريمة الإلكترونية بالمؤسسات الجزائرية	11	55
– الإجمالي	**25**	**125**

المصدر: من إعداد الباحث

ثالثا– اختبار الفرضيات: من بين 136 استمارة موزعة تم استرجاع 116 استمارة منها 110 للإداريين، 11 مدقق داخلي و4 محافظي حسابات، وهذا نظرا لخروج بعض الإداريين في عطل والبعد لمحافظي الحسابات والآخرين لظروف أخرى.

1– اختبار الفرضية الأولى: لا توجد فروق ذات دلالة معنوية بين تكوين وسير(إدارة) لجان التدقيق في المؤسسات الجزائرية وبين تكوين وسير لجان التدقيق التي تتفق والأنظمة المعمول عليها دوليا.

الجدول التالي يبين الملخص العام لنتائج الإستبيان بعد المعالجة الإحصائية باستخدام برنامج الرزم الإحصائية الجاهزة للعلوم الإجتماعية SPSS باستخدام الحاسب الآلي:

الجدول رقم 02: محور الإستبيان: تشكيل (تكوين) وسير(إدارة) لجان التدقيق بالمؤسسات الجزائرية

العناصر	النسبة المئوية للإجابات			المتوسط الحسابي	التباين	p.value	مستوى الدلالة
	موافق	لا أدري	غير موافق				
– ميثاق لجنة التدقيق يوافق عليه من طرف الإدارة؛	8,2	82,4	9,4	8,333	89,956	0,000	معنوية
– لجنة التدقيق تراجع سنويا ميثاقها وتطلب من مجلس الإدارة القيام بالتعديلات التي تراها ضرورية؛	3	88,5	8,5	2,857	86,693	0,000	معنوية
– ميثاق لجنة التدقيق يحتوي على المهام التي تخولها لها الإجراءات المعمول بها عالميا؛	6,3	72,9	20,8	8,333	23,068	0,000	معنوية
– يمنع رئيس مجلس الإدارة بأن يكون عضوا في لجنة التدقيق؛	14,3	71,4	14,3	14,286	51,298	0,001	معنوية
– تجتمع لجنة التدقيق دوريا لفحص المواضع التي تتعلق بنشاطات المنظمة والتي تدخل في إطار صلاحياتها؛	0	85,7	14,3	14,286	49,331	0,001	معنوية
– تستدعي لجنة التدقيق أفراد آخرين لحضوري اجتماعاتها عند الضرورة؛	10	80	10	10	68,613	0,001	معنوية
– تلتقي لجنة التدقيق مع المدقق الدخلي والخارجي بدون							

حضور الإدارة.	08	79,5	12,5	7,935	64,662	0,000	معنوية
المتوسطات العامة لمحور: تكوين وسير(إدارة) لجان التدقيق بالمؤسسات الجزائرية	7,4	80,6	12	9,447	61,946	0,000	معنوية

المصدر: من إعداد الباحث بناء على نتائج الاستبيان

التحليل الإحصائي لنتائج الإستبيان:

– **المتوسط الحسابي**: من خلال الجدول نلاحظ انخفاض المتوسطات الحسابية المتحصل عليها والخاصة بكل عنصر والمتوسط العام للعناصر من عناصر "تكوين وسير(إدارة) لجنة التدقيق بالمؤسسات الجزائرية عن درجة حد القبول والتي هي 35 كما أشرنا إليها أعلاه، أي: H1 المتوسط الحسابي للعينة < درجة القبول، على مستوى كل مؤسسة من المؤسسات محل الدراسة (مؤسسة باتيميتال، مؤسسة ميناء تنس، مؤسسة تسيير ومراقبة ملاجئ الصيد البحري، مؤسسة الخزف الصحي، مؤسسة الأسمنت، مؤسسة البناء والتجديد)، وهذا الانخفاض شمل كل العناصر بدون استثناء (ميثاق لجنة التدقيق يوافق عليه من طرف الإدارة بـ 8,333؛ لجنة التدقيق تراجع سنويا ميثاقها وتطلب من مجلس الإدارة القيام بالتعديلات التي تراها ضرورية بـ2,857؛ ميثاق لجنة التدقيق يحتوي على المهام التي تخولها لها الإجراءات المعمول بها عالميا بـ 8,333؛ يمنع رئيس مجلس الإدارة بأن يكون عضوا في لجنة التدقيق بـ 14,286 ؛ تجتمع لجنة التدقيق دوريا لفحص المواضع التي تتعلق بنشاطات المنظمة والتي تدخل في إطار صلاحياتها بـ 14,286؛ تستدعي لجنة التدقيق أفراد آخرين لحضوري اجتماعاتها عند الضرورة بـ 10؛ تلتقي لجنة التدقيق مع المدقق الداخلي والخارجي بدون حضور الإدارة بـ 7,925)، وهذه القيم تعتبر معنوية، أي رفض الفرضية وقبول الفرضية البديلة.

– **التباين**: نلاحظ كذلك من خلال النتائج المتحصل عليها في الجدول من البرنامج الإحصائي على المستوى التفصيلي بالنسبة لكل عنصر، هناك فروقات كبيرة بالنسبة لقيم كل عنصر عن مؤشرها، وهذا ما يعني أن إجابات أفراد العينة بالنسبة لكل المؤسسات حول مستوى رضاهم عن تكوين وسير(إدارة) لجان التدقيق بالمؤسسات الجزائرية وما بين تكوين وسير(إدارة) لجان التدقيق والأنظمة المعمول بها دوليا غير دالة، أي رفض الفرضية وقبول الفرضية البديلة، و كذلك بالنسبة للمتوسط العام للتباين.

– **القيمة الحرجة للإحتمال P.Value**: القيمة الحرجة للإحتمال، هي أقل من 0,05 كما هو موضح من نتائج التحليل الإحصائي بالجدول أعلاه، بالنسبة لكل عنصر من عناصر محور: تكوين وسير لجنة التدقيق بالمؤسسات الجزائرية، وهذا بالنسبة لكل المؤسسات محل الدراسة والمذكورة أعلاه، وهذا يرجع إلى أسباب جوهرية تتمثل في عدم مطابقة تكوين وسير لجان التدقيق في المؤسسات الجزائرية وما بين تكوين وسير لجان التدقيق التي تتفق والأنظمة المعمول عليها دوليا، وعلى هذا الأساس يتم رفض فرض العدم على المستوى التفصيلي بالنسبة لكل عنصر من عناصر محور " تكوين وسير لجنة التدقيق في المؤسسات الجزائرية " وقبول الفرض البديل عل المستوى التفصيلي بالنسبة لهذه العناصر.

والخلاصة نقول أن الفرضية الأولى غير محققة وقبول الفرضية البديلة.

2– اختبار الفرضية الثانية: لا توجد فروق ذات دلالة معنوية بين لجان التدقيق وإدارة المخاطر في المؤسسات الجزائرية وبين لجان التدقيق وإدارة المخاطر التي تتفق والأنظمة المعمول بها دوليا

الجدول التالي يبين الملخص العام لنتائج الإستبيان بعد المعالجة الإحصائية باستخدام الحاسب الآلي لبرنامج الرزم الإحصائية الجاهزة للعلوم الإجتماعية SPSS:

الجدول رقم 03: محور الإستبيان: لجان التدقيق وإدارة المخاطر بالمؤسسات الجزائرية

العناصر	النسبة المئوية للإجابات			المتوسط الحسابي	التباين	p.value	مستوى الدلالة
	موافق	لا أدري	غير موافق				
– تقوم لجنة التدقيق بتقييم الأخطار المرتبطة بالإستراتيجيات وأهداف النشاطات؛	8,3	82,3	9,4	8.333	89,956	0,000	معنوية
– سياسة إدارة المخاطر هي معلومة بصفة واضحة لدى لجنة التدقيق؛	13,8	75,3	10,9	13,768	61,114	0,000	معنوية
– هناك مفهوم أو لغة مشتركة لإدارة المخاطر بالمنظمة وتعلم بها لجنة التدقيق؛	5	81,5	13,5	4,969	62,139	0,000	معنوية
– يوجد خريطة للأخطار التي ممكن أن تصيب المنظمة وتشارك لجنة التدقيق في إعدادها؛	12,5	71,5	16	12,5	48,205	0,001	معنوية
– المنظمة تكلف لجنة التدقيق بمسئولية الإشراف على أنظمة الرقابة الداخلية وإدارة المخاطر؛	00	78,5	21,5	21,429	21,279	0,000	معنوية
– الإرتباطات بين المخاطر هي معروفة ومفهومة لدى لجنة التدقيق؛	7,1	90,5	2,4	7,143	99,588	0,000	معنوية
– تتحقق لجنة التدقيق من أن المخاطر تم إحصاؤها وأبلغت في الوقت المناسب داخل المؤسسة لتسمح للمعنيين بالقيام بمسئولياتهم.	03	88,5	8,5	2,857	86,693	0,000	معنوية
المتوسطات العامة لمحور: لجان التدقيق وإدارة المخاطر بالمؤسسات الجزائرية	7,1	81,17	11,72	10,143	66,996	0,000	معنوية

المصدر: من إعداد الباحث بناء على نتائج الاستبيان

التحليل الإحصائي لنتائج استبيان الفرض الثاني: لجنة التدقيق وإدارة المخاطر في المؤسسات الجزائرية،

التحليل الإحصائي لبيانات هذه الدراسة باستخدام الحاسب الآلي لبرنامج SPSS، أظهر النتائج التالية:

– المتوسط الحسابي: انخفاض المتوسطات المتحصل عليها بالنسبة لكل عنصر (نشاط) من عناصر لجنة التدقيق وإدارة المخاطر في المؤسسات الجزائرية عن درجة القبول، حيث العناصر (تقوم لجنة التدقيق بتقييم الأخطار المرتبطة بالإستراتيجيات وأهداف النشاطات بمتوسط حسابي 8,333، سياسة إدارة المخاطر هي معلومة بصفة واضحة لدى لجنة التدقيق بمتوسط حسابي قدره 13,768، هناك مفهوم أو لغة مشتركة لإدارة المخاطر بالمنظمة وتعلم بها لجنة التدقيق بمتوسط حسابي 4,969، يوجد خريطة للأخطار التي ممكن أن تصيب المنظمة وتشارك لجنة التدقيق في إعدادها، بمتوسط حسابي 12,5، المنظمة تكلف لجنة التدقيق بمسئولية الإشراف على أنظمة الرقابة الداخلية وإدارة المخاطر بمتوسط حسابي قدره 21,429، الإرتباطات بين المخاطر هي معروفة ومفهومة لدى لجنة التدقيق بمتوسط حسابي 7,143، تتحقق لجنة التدقيق من أن المخاطر تم إحصاؤها وأبلغت في الوقت المناسب داخل المؤسسة لتسمح للمعنيين بالقيام بمسئولياتهم بمتوسط حسابي 2,857، المتوسطات العامة لمحور: لجان التدقيق وإدارة المخاطر بالمؤسسات الجزائرية هو: 10,143، وقيم هذه المتوسطات الحسابية للعناصر، كلها أقل من درجة حد القبول الخاصة بهذا المحور والتي هي 35 كما يوضحه الجدول أعلاه، وكذلك النسب المئوية للإستجواب (موافق، لاأدري، غير موافق)، تبين ذلك كما يظهر في جدول المحور أعلاه، وهذه القيم تعتبر معنوية، أي رفض الفرضية وقبول الفرضية البديلة.

– التباين: بالنسبة للتباين نلاحظ من خلال النتائج المتحصل عليها من البرنامج وكما هي موضحة بالجدول أعلاه على المستوى التفصيلي (المؤسسات) وكذلك بالنسبة لكل عنصر من عناصر هذا المحور، هناك فروقات كبيرة بالنسبة لقيم كل العبارات عن مؤشرها، وهذا ما يعني

أن إجابات أفراد العينة (المسئولين الإداريين، المدققين الداخليين، محافظي الحسابات) حول مستوى رضاهم عن: لجنة التدقيق وإدارة المخاطر في المؤسسات الجزائرية غير دالة، أي رفض الفرضية وقبول الفرضية البديلة، وحتى بالنسبة لقيمة المتوسط العام لهذا المحور والتي هي 66,996، وهي بعيدة جدا عن مؤشرها، و تعتبر معنوية.

– القيمة الحرجة للإحتمال:

كما نلاحظ في الجدول السابق أن كل قيم عبارات: لجنة التدقيق وإدارة المخاطر في المؤسسات الجزائية وحتى المتوسط العام لها هي أقل من 0,05، وهذا بالنسبة لكل المؤسسات محل الدراسة، وهذا يرجع إلى أسباب جوهرية تتمثل في عدم ملائمة لجنة التدقيق وإدارة المخاطر في المؤسسات الجزائرية مع لجنة التدقيق وفضاء وإدارة المخاطر التي تتفق والأنظمة المعمول بها دوليا، وعلى هذا الأساس يتم رفض فرض العدم على المستوى التفصيلي بالنسبة لكل عبارة من عبارات لجنة التدقيق وإدارة الماطر في المؤسسات الجزائرية، وبالنسبة لكل المؤسسات محل الدراسة، وقبول الفرض البديل على المستوى التفصيلي بالنسبة لهذه العبارات والمؤسسات.

وبهذا نقول أن الفرضية الثانية غير محققة وقبول الفرضية البديلة.

3– اختبار الفرضية الثالثة:

لاتوجد فروق ذات دلالة معنوية بين لجان التدقيق وفضاء الجريمة الإلكترونية في المؤسسات الجزائرية وبين لجان التدقيق وفضاء الجريمة الإلكترونية التي تتفق والأنظمة المعمول بها دوليا.

الجدول التالي يبين الملخص العام لنتائج الإستبيان بعد المعالجة الإحصائية باستخدام برنامج الرزم الإحصائية الجاهزة للعلوم الإجتماعية SPSS باستخدام الحاسب الآلي:

الجدول رقم 04: محور الإستبيان: لجان التدقيق وفضاء الجريمة الإلكترونية في المؤسسات الجزائرية

العناصر	النسبة المئوية للإجابات			المتوسط الحسابي	التباين	p.value	مستوى الدلالة
	موافق	لا أدري	غير موافق				
– أنظمة الرقابة مواكبة للتطورات التكنولوجية، خاصة استراتيجية المؤسسة في تحديث عتاد المعلوماتية؛	10,3	85,7	04	14,286	49،331	0,001	معنوية
– تتحقق لجنة التدقيق من إجراءات كشف أخطار الجريمة الإلكترونية؛	4,8	87,3	7,9	04,870	97,949	0,000	معنوية
– هناك أصول أساسية (جارية، غير جارية، معنوية، معطيات ...الخ، تتحقق لجنة التدقيق من وضع حماية لها من الجريمة الإلكترونية؛	18	73	09	17,777	35,446	0,001	معنوية
– هناك مستوى خطر مقبول ممكن تحمله فيما يتعلق بالتعرض للجريمة الإلكترونية، تتحقق منه لجنة التدقيق؛	14,8	76,5	08,7	14,815	53,146	0,001	معنوية
– هناك نظام رقابة معمول به ميدانيا لمراقبة الشبكات، الموردين، والتركيبات على الأجهزة، تتحقق منه لجنة التدقيق؛	16,7	72,2	11,1	13,888	39,448	0,001	معنوية
– هناك مسئول عن الحماية من الجريمة الإلكترونية، تتحقق لجنة التدقيق من وجوده؛	10	80	10	10	68,613	0,001	معنوية
– تفحص لجنة التدقيق كافة الموارد المخصصة للحماية من الجريمة الإلكترونية (ميزنية، م. بشرية، عتاد...الخ)؛	08	79,5	12,5	7,935	64,662	0,000	معنوية
– تتأكد لجنة التدقيق من كيفية تصرف الإدارة اتجاه حادث إلكتروني طارئ؛	2,4	90,5	07,1	7,143	99,588	0,000	معنوية
– تتلقى لجنة التدقيق معلومات ذات جودة عالية عن فضاء الجريمة							

الإلكترونية من المصالح المعنية؛ – في حالة هجوم إلكتروني، هناك درجة معينة تكون فيها مؤسستكم قادرة على التصرف؛ – يوجد بمؤسستكم فرقة مؤهلة للتحكم بسرعة في الأضرار المحتملة في حالة وقوع هجوم إلكتروني.	03 24,4 32,5	88,5 43,7 60	08,5 31,9 7,5	2,857 24,370 7,692	86,693 0,311 0,1	0,000 0,013 0,01	معنوية معنوية معنوية
المتوسطات العامة لمحور: لجان التدقيق وفضاء الجريمة الإلكترونية بالمؤسسات الجزائرية	**12,2**	**76**	**11,8**	**11,431**	**54,117**	**0,002**	**معنوية**

المصدر: من إعداد الباحث بناء على نتائج الاستبيان

التحليل الإحصائي لنتائج إستبيان محور : لجان التدقيق وفضاء الجريمة الإلكترونية في المؤسسات الجزائرية

من الملاحظات التي استنتجها الباحث، أن كل هذه المؤسسات تعالج بياناتها بواسطة أجهزة الإعلام الآلي (أي إلكترونيا)، وأنها في نفس الوقت تعتمد على وسائل الحماية المتوفرة في السوق مثل البرامج والتطبيقات ...الخ، من أجل حماية أصولها من التلف ومن السرقة والهجومات الإلكترونية المحتملة، وهذا بواسطة مصالح وهياكل الإعلام الآلي التي تتوفر عليها هذه المؤسسات كل حسب إمكانياتها المادية والبشرية والمالية، لكن هذه العملية تنجز كمهمة وفقا لمتغيرات محيط تكنولوجيات الإعلام المستعملة، بعيدة عن وجود سياسة استراتيجية حماية إلكترونية للمؤسسة ولاوجود لفرقة حماية إلكترونية أنشئت من طرف المؤسسة لهذا الغرض، وفي غياب كلي للتنسيق بين هياكل الرقابة الأخرى (لجان التدقيق، المدقق الداخلي، المدقق الخارجي...الخ)، وحتى أغلب أفراد المؤسسة ليست لهم فكرة عن لجنة التدقيق أصلا، لهذا نجد في هذا المحور أن بعض العناصر متوفرة في المؤسسة، ولكن ليست بالكيفية التي تستجيب إلى توجيهات أجهزة الرقابة، وخاصة لجان التدقيق، التي هي غير موجودة تقريبا في كل المؤسسات محل الدراسة، ولكن حسب اطلاع الباحث على كيفيات عمل لجان التدقيق بالمؤسسات التي بها هيكل لجنة التدقيق، فإنها ما تزال بعيدة عن الشكل الذي تؤسس عليه لجان التدقيق، سواء من ناحية التشكيلة أو من ناحية ميثاقها أو من ناحية المهام والدور التي تقوم به ...الخ، لكن من خلال النتائج المتوصل إليها، وكما هو في الجدول أعلاه، تظهر ما يلي:

– **المتوسط الحسابي**: بالنسبة للمتوسطات الحسابية المتحصل عليها قيمها كله منخفضة عن درجة حد القبول وهي 55 كما هي موضحة في الجدول أعلاه (أي عند حساب H0 و H1)، والخاصة بكل عنصر من عناصر لجنة التدقيق وفضاء الجريمة الإلكترونية في المؤسسات الجزائرية على مستوى كل مؤسسة من المؤسسات محل الدراسة، وهذا الإنخفاض شمل كل العبارات بدون استثناء، وهي تعتبر معنوية، أي رفض الفرضية وقبول الفرضية البديلة.

– **التباين**: بالنسبة للتباين نلاحظ من خلال النتائج المتحصل عليها من البرنامج وكما هي موضحة بالجدول أعلاه على المستوى التفصيلي (المؤسسات)، هناك فروقات كبيرة بالنسبة لقيم كل العبارات عن مؤشرها، وهذا ما يعني أن إجابات أفراد العينة (المسئولين الإداريين، المدققين الداخليين، محافظي الحسابات) حول مستوى رضاهم عن: لجنة التدقيق وفضاء الجريمة الإلكترونية في المؤسسات الجزائرية غير دالة، أي رفض الفرضية وقبول الفرضية البديلة، إلا في حالة عبارتي (في حالة هجوم إلكتروني هناك درجة تكون فيها مؤسستكم قادرة على التصرف، وعبارة: يوجد بالمؤسسة فرقة مؤهلة للتحكم بسرعة في الأضرار المحتملة في حالة هجوم إلكتروني، حيث قيمهما على التوالي هي: 0,311 و 0,1)، حيث نجد في أغلب المؤسسات فيها فروقات هذين العنصرين قريبة عن مؤشرها، لكن قيمة المتوسط العام لهذا المحور هو 54,111، وهو بعيدا جدا عن مؤشره، وهي تعتبر معنوية.

– **القيمة الحرجة للإحتمال**: هي أقل من 0,05 بالنسبة لكل عبارة من عبارات: لجنة التدقيق وفضاء الجريمة الإلكترونية في المؤسسات الجزائرية، وهذا بالنسبة لكل المؤسسات محل الدراسة، وهذا يرجع إلى أسباب جوهرية تتمثل في عدم ملائمة لجنة التدقيق وفضاء الجريمة الإلكترونية في المؤسسات الجزائرية مع لجنة التدقيق وفضاء الجريمة الإلكترونية التي تتفق والأنظمة المعمول بها دوليا، وعلى هذا الأساس يتم رفض فرض العدم على المستوى التفصيلي بالنسبة لكل عبارة من عبارات لجنة التدقيق وفضاء الجريمة الإلكترونية في المؤسسات الجزائرية، وبالنسبة لكل المؤسسات محل الدراسة، وقبول الفرض البديل على المستوى التفصيلي بالنسبة لهذه العبارات والمؤسسات.

وفي الأخير نقول أن الفرضية الثالثية غير محققة وقبول الفرضية البديلة.

خاتمة:

من خلال المعالجة للموضوع المتعلق بلجنة التدقيق ودورها في ظل التطور المتسارع لفضاء الجريمة الإلكترونية في المؤسسات الجزائرية، تبين أن وظيفة التدقيق بصفة عامة تأثرت في نشأتها وتطورها بتطور الحياة الإجتماعية والاقتصادية والسياسية للمجتمعات وفي كل مرحلة تحرز على مكانتها من المنفعة والقدرة التي تلبي بها حاجيات الأفراد وأصحاب المصالح، فمنذ تاريخ ظهورها إلى يومنا هذا عرفت مهنة التدقيق عدة تغيرات، لكن مع الظهور والتطور السريع والمتنامي في كل لحظة بوتيرة غير مسبوقة في التاريخ لتكنولوجيات الإعلام والإتصال، والذي أرغم المنظمات والهيئات على المستوى العالمي التعامل بها، ولدت هذه التكنولوجيات أعمالا أصبحت تكوّن تهديدات وأخطار على أصول ومعلومات هذه المنظمات التي تتعامل بها، مثل أخطار السرقة، إتلاف المعطيات، الفساد، سرقة الأموال، سرقة الملكية الفكرية، سرقة المعلومات الشخصية والمالية، تحويل الأموال، الغش، ...الخ، وأصبح مصدر الخطر ليس من داخل المنظمة الذي يسهل اكتشافه من طرف هياكل التدقيق وتصحيحه، بل صار مجهولا ومصدره ممكن أن يكون في أي جهة في العالم، يصعب الوصول إليه، وأصبحت هذه الأخطار أكثر جسامة على المنظمات من الأخطار التي كانت ترتكب في الماضي، فمهنة التدقيق في العالم الإفتراضي تغيرت وأصبحت تركز على آليات تستعملها المنظمات لحماية ممتلكاتها من الجرائم الإلكترونية التي ترتكب من طرف أفراد يمتلكون تقنيات ومهارات تفوق تلك التي يمتلكها أفراد المنظمات، في ظل هذه الوضعية برز دور لجان التدقيق والتي تعتبر حاليا هيكل الرقابة الوحيد على المستوى الدولي الذي يقوم بمهمة التنسيق بين الإدارة والمدقق الداخلي والخارجي في تنظيم أعمال كل منها، والذي له مسئولية الرقابة والإشراف على أنظمة الرقابة الداخلية وإدارة المخاطر والعمل على تجسيد آليات وإجراءات والوسائل المادية، المالية، البشرية لسياسات الأمن الإلكتروني التي وضعت من طرف المنظمة لمواجهة تهديدات الجرائم الإلكترونية لتفادي الأضرار التي ممكن أن تلحقها بالمنظمة، وأصبح هذا النوع من الجرائم حسب المنظمة العالمية للتجارة من ضمن خمس أخطار الكبرى ذات التهديدات المتنامية التي تصيب نشاطات الأعمال لعدد كبير من الدول وصارت قلب الرهان الجيوسياسي لها، وفعالية هذا الدور بالنسبة للجان التدقيق يتفاوت من منظمة إلى منظمة ومن دولة إلى دولة حسب الأوضاع الاقتصادية والاجتماعية والسياسية لكل مجتمع، لكن في الجزائر وكما تبن من خلال البحث أن جل المؤسسات إن لم نقل كلها، لجان التدقيق لم تولد بها بعد، والمؤسسات التي بها لجان تدقيق فإنها مازالت في مرحلتها الأولى وبعيدة كل البعد عن المعايير الدولية التي تدار بها لجان التدقيق، وهذا نظرا لظروف تاريخية مرت بها المؤسسات الجزائرية، حيث إلى حد الآن مازالت متأخرة كثيرا عن تبنى أنظمة ومعايير الإدارة الحديثة التي تدار بها المنظمات على المستوى الدولي، أما في يتعلق بالإهتمام بموضوع سياسات الحماية الإلكترونية من الجرائم الإلكتروني لم تعد إلى حد الآن في نظر قيادات المؤسسة الجزائرية خطرا من الأخطار الكبرى بل انشغالا مثل الانشغالات الأخرى المتعلقة بباقي النشاطات.

النتائج:

- الجرائم الإلكترونية أصبحت التهديد الأول والأخطر على ممتلكات ومعطيات المنضمات والهيئات والدول على المستوى العالمي؛
- تكاليف الأمن الإلكتروني مافتئت تتزايد سنة بعد سنة بوتيرة متفاوتة بين الدول كل حسب جسامة التهديدات وأثرها عليها؛
- موضوع الأمن والجرائم الإلكترونية لابد أن يكون موضوع جدول أعمال مجلس الإدارة على الأقل مرة في السنة؛
- مجلس الإدارة لابد أن يحدد مقاربة الإشراف لآلية إدارة مخاطر الهجومات الإلكترونية ويكلف مهمة المتابعة لها للجنة التدقيق طبقا لمهامها المحددة في القانون الداخلي للمنظمة ولجنة التدقيق تبلغ نتائج أعمالها أثناء انعقاد مجلس الإدارة؛
- لابد من تطوير الخبرة الخاصة بالأمن الإلكتروني على مستوى مجلس الإدارة ليصبح أمرا ضروريا بالنسبة لكل المؤسسات؛
- لا يوجد هناك جدال في المؤسسات الجزائرية بين مختلف المعنيين بقضية الأمن الإلكتروني لمواجهة الجرائم الإلكترونية؛
- الدولة الجزائرية إلى حد الآن مازالت لم تعد إجراءات تلزم المؤسسات والمنظمات والهيئات سواء كانت خاصة أو عامة باتخاذ الإجراءات اللازمة للأمن الإلكتروني ومحاربة الجرائم الإلكترونية؛
- السياسات المتعلقة بالأمن الإلكتروني ومحاربة الجريمة غائبة، نظرا لغياب أو عدم وجود لجان تدقيق بالمؤسسات الجزائرية؛
- لا يوجد إهتمام في المؤسسات الجزائرية من طرف هيئات الرقابة (التدقيق الداخلي، التدقيق الخارجي، أنظمة الرقابة الداخلية وإدارة المخاطر) بموضوع الجرائم الإلكترونية وسياسات الأمن الإلكتروني؛
- الدول ذات الاقتصاد القوي والمنضمات والهيئات الكبرى التي لها سمعة عالمية، لها اهتمام كبير بلجان التدقيق وسياسات الأمن الإلكتروني والجريمة الإلكترونية، بينما الدول ذات الاقتصاد الضعيف والمؤسسات الهشة، ومن بينها الجزائر، مازال بعيدا كل البعد عن المعايير الدولية المعتمدة؛

التوصيات

1- على السلطات العمومية للدولة الجزائرية إعداد نصوص تشريعية تفرض على المؤسسات والهيئات العمومية والخاصة الإلتزام بمستوى معين من تجهيزات الأمن الإلكتروني لمواجهة التهديدات الإلكترونية، لأنها أصبحت تمثل الخطر الجسيم والأول على المستوى العالمي بالنسبة للمنظمات؛

2- على مجالس الإدارة في المؤسسات والهيئات العمومية والخاصة الجزائرية الإسراع في إنشاء لجان التدقيق وإعطائها صلاحيات وفقا للمرجعيات والمعايير الدولية التي تسير بها، لأنها هي الهيأة التي أصبح لها على المستوى العالمي مهمة التنسيق بين الإدارة والمدقق الداخلي والخارجي في تنظيم أعمال كل منهما، وتقديم التوجيهات والإرشادات للمنظمات والهيئات فيما يتعلق بسياسة الأمن الإلكتروني وإدارة المخاطر لوقايتها من الأخطار؛

3- وضع آليات وبرامج على مستوى المؤسسات والهيئات الهدف منها القيام بتحسيس الفاعلين في المؤسسات والهياكل التي علاقة بالرقابة والتدقيق (الملاك، الإدارة العامة، التدقيق الداخلي، التدقيق الخارجي، لجان التدقيق، المستخدمين) بأخطار الجرائم الإلكترونية وأثارها على المنظمات وأهمية لجان التدقيق لمحاربتها.

قائمة المراجع الهوامش:

[1] - Steven MALLBY et autres : L'équipe chargé de l'étude « étude détaillée su la cybercriminalité », Office des nations unies contre la drogue et le crime, UNITED NATIONS, Ebauche, NEW York, Février, 2013, PP 11-14.
[2] - Gérard PELIKS "la cybercriminalité", un livre blanc de Forum ATENA, 2013, PP : 5-18.
[3] - https://cybercriminalité-penal.fr/les-differents –formes-de-cybercriminalité/ اطلع عليه بتاريخ 2019/06/12
[4] - Jonathan Lemonnier,What is trojan horse malware ?, من موقع www.avg.com اطلع عليه بتاريخ 2019/03/25
[5] - ROSE (C) Chercheur dans le domaine de la piratage sur l'internet, Discours prononcé lors de l'ouverture du G8 sur la cybercrimanilité, Paris 2000.
[6] - WWW.theIIA.org/resarch, Consulté le15/01/2019.
[7] - « Le rôle de l'audit interne face aux cyber risque », Enquête mondiale CROK, édition IIA, 2015.
[8] - www.marketsandmarkets.com/market-reports/iot-securetymarket-67064836.html.
[9] - www.marketsandmarkets.com/market-reports/iot-securetymarket-67064836.html.
[10] - Livre blanc, op-cit, p :15.
[11] - « Le rôle de l'audit interne face aux syberrisques », - www.theIIA.org/resarch, Consulter le15/05/2019
[12] - www.ifa-asso.com, Consulté le12/04/2019.
[13] - DOMINIQUE Filppone « Le syber-espionnage plus actif que jamais », Rapport d'activité ANSSI 2018, publie, le 15 Avril 2019, pp33-35.
[14] – وكالة أنباء "رويترز" بتاريخ 2017/07/17.
[15] - www.audit-commitee-institute.fr,consulté le 25/04/2019.
[16] - Jean-Jacques Tourre Pilote du groupe de travail « Le cyber risque dans la gouvernance de l'entreprise », CIGREF réussir le numérique, Paris, Octobre 2016,p2 .
[17] - Groupe de travail présidé par ALDO Cardoso « Rôle de comité d'audit en matière de cyber sécurité », institut français des administrateurs, 2016, p3.
[18] - Groupe de travail présidé par ALDO Cardoso « Rôle de comité d'audit en matière de cyber sécurité », op-cit,p3.
[19] - Decret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale
[20] - Groupe de travail présidé par ALDO Cardoso « Rôle de comité d'audit en matière de cyber sécurité », op-cit,p4.
[21] – قانون رقم 04/09 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر رقم 47.
[22] - www.ifa-asso.com, consulté le 20/05/2019.
[23] - WWW.theIIA.org/resarch, op-cit , Consulté le15/05/2019.
[24] - www.audit-commitee-institute.fr,consulté le 30/04/2019.
[25] - Groupe de travail présidé par ALDO Cardoso « Rôle de comité d'audit en matière de cyber sécurité », op-cit, p:6-8.
[26] - www.ifa-asso.com, consulté le 20/05/2019.
[27] - Enquête internationale réalisée par audit commitée institute « la pratique des comités d'audit en France et dans le monde », France, mars 2015, pp:12-22.

[28]– مقال ليونس بوزيان بجريدة العين الإخبارية الإماراتية بعنوان " الجزائر.. 2500 جريمة إلكترونية سنة 2017" بتاريخ 2018/01/21.

[29] – حمزة-بن-دلاج ar.wikipedia.org/wiki

[30] – قانون رقم 04/09 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر رقم 47.

[31]- Circulaire du premier ministre n° 297/PM, Octobre 2015.