

ملال نصيرة

أستاذة محاضرة ب- بجامعة عبد الحميد بن باديس -مستغانم -

الأمن السيبري في العالم، لان العالم بأسره صار مستهدفا من طرف شخص واحد أو من طرف جماعة أو هيئة إجرامية تدرك جيدا قيمة المعلوماتية، وحساسية نظام المعلومات، ولعل ما يؤكد هذا الاختيار بشكل أفضل، هو دعوة الأمم المتحدة إلى إرساء مثل هذه الثقافة بين أُمم العالم كله.

الحديث عن الأمن السيبري اليوم، يدعمه كذلك، الترابط المستمر بين الشبكات المختلفة ودخولها في إطار شبكة موحدة دولية، من شأنها تقليص كل المسافات وبشكل غير مسبوق، فبالإضافة مع ما يعنيه هذا الترابط الكبير من تطور كبير ودعم أكبر للتنمية على المستوى العالمي، وربط شعوب العالم فيما بينها، إلا انه يدل أيضا ويؤدي إلى مخاوف أكبر من أي وقت سابق، فالكل سيكون داخل شبكة موحدة، هذه الشبكة لا تضم فقط أجهزة كمبيوتر لمستخدمين عاديين، أو لأشخاص يرغبون في التسلية واللعب على الخط، أو لمجموعة أصدقاء يحبون الحوار والدردشة المباشرة والحية مع بعضهم. وإنما تضم هذه

الشبكة أنظمة جد معقدة تخص الحكومات والهيئات والمؤسسات المختلفة، وبالتالي فالمجتمع الذي نتكلم عنه في هذا الصدد، هو مجتمع معلوماتي بشكل متكامل. ونظرا لذلك كله فان الإجماع سائد اليوم على تجاوز ما سمي بأمن نظم المعلومات، لان الأمر لم يبق محصورا بالشكل الذي كان عليه من قبل، وإنما دائرة الخطر في توسع مستمر ومتزايد، مما يستدعي تفكيرنا من نوع آخر ، أي التفكير حول الأمن السيبري.

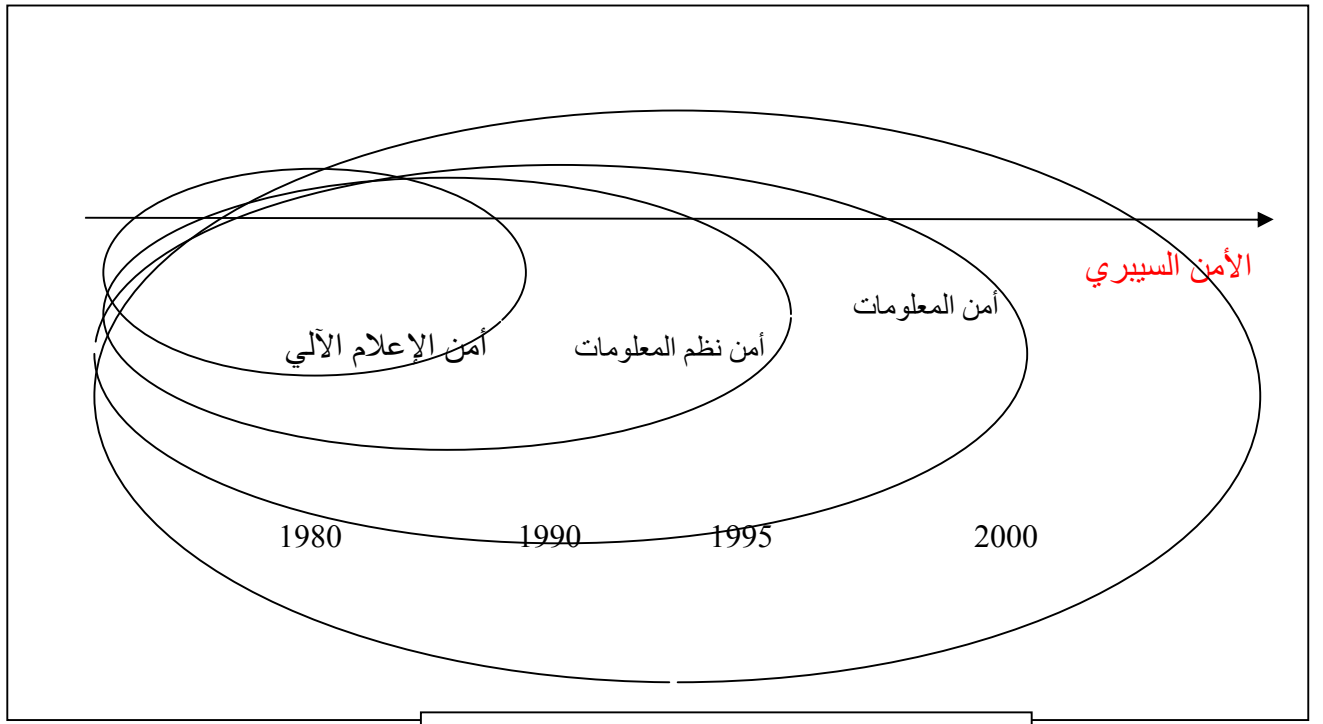
1- مراحل ظهور الأمن السيبري :

يوضح الشكل (1) ⁽²⁾ مراحل التطور أمن النظام المعلوماتي وصولا إلى ما يسمى بالأمن السيبري، ويبدأ بأمن الإعلام الآلي ،أمن نظم المعلومات ثم أمن المعلومات، وأخيرا الأمن السيبري :

يعتبر الأمن السيبري أو السبرنطقي من المفاهيم الجديدة التي ظهرت مع مطلع القرن الواحد والعشرين ، مثله في ذلك مثل مفاهيم أخرى كالجرمة السيبرية ولعل هذا المفهوم الأخير، باعتباره علما يهتم بدراسة الجرائم التي ترتكب داخل الفضاء السيبري وتنعكس على عالمنا هذا ، فهذه الجرائم أدت إلى رسم خطوط حمراء جديدة بالنسبة للدول والمؤسسات والأفراد، بحيث تعتبر هذه الخطوط عبارة عن حدود التي لا يجب تجاوزها من قبل المجرمين والقرصنة، لأنه إن حدث وتجاوز هؤلاء هذه الحدود ،فان نظاما كبيرا كعالمنا سيكون هدفا مباشرا لعمليات تخريب وإجرام وبالتالي تكون النتيجة خسائر فادحة بالنسبة لمجوع الدول والمؤسسات والأفراد .

إن الغالبية من الناس ، بما فيهم المختصين في ميدان الإعلام الآلي، يرون بأن مثل هذه الجرائم لا يمكنها أن تطال إلا شبكة فقط مثل الانترنت ، لكن الواقع الذي تنقله يوميا وسائل الإعلام المختلفة، بما في ذلك شبكة الانترنت، يدل على إن تلك الجرائم أو الهجمات السيبرية، لها تأثير سلبي واضح في كل الأحوال على العالم "الخارجي"، أي على عالم حياتنا اليومية، وبالتالي بات من الضروري، بل من الملح، تحديد نمط التفكير المتعلق بتلك الجرائم، وتغيير الاعتبارات وتحديد المفاهيم المتعلقة بالحماية والأمن، هذه الضرورة الأمنية هي التي كانت تشكل مواضيع اجتماعات دولية مثل احتفال الاتحاد الدولي للاتصالات السلكية واللاسلكية بذكرى تأسيسه، والذي يقام كل سنة، بحيث تختار مواضيع جادة للنقاش في الميدان.

وتأكيدا للطرح الذي قدمناه حول جدية مسألة امن وحماية نظم المعلومات أو حماية وامن ما هو أكبر بكثير من نظم المعلومات فقد كان موضوع اجتماع سنة 2006 لهذا الاتحاد⁽¹⁾، الأمن السيبري مباشرة، وذلك تحت شعار " من اجل ترقية ثقافة الأمن السيبري في العالم". اختيار كهذا يدعو فعلا إلى القلق بشأن المستقبل الأمني على جميع الأصعدة، مدام الكل مرتبط ارتباطا مباشرا اليوم بنظام معلوماته فلا عجب أن يقرع جرس الإنذار ولو بشكل متأخر مسألة



شكل 1- المراحل الاربعة لتطور الامن المعلوماتي

على العديد من المقالات والأخبار لحوادث أمنية ترجع في أصلها إلى هجمات إرادية أو حوادث غير إرادية، تمس نظام المعلومات عن طريق الشبكات .

وكذا من خلال الاطلاع على العديد من التقارير الرسمية وغير الرسمية التي تتعرض بشكل مباشر أو غير مباشر لمسألة امن وحماية نظم المعلومات، أو حتى مسألة الأمن السيبراني، مثل التقارير التي تصدر عن الهيئة⁽³⁾ المختصة في امن نظم المعلومات بحكومة الولايات المتحدة الأمريكية، والتي تقدم من حين لآخر اقتراحات ومشاريع أمنية لحماية الفضاء السيبراني الأمريكي، الذي يعتبرونه الأكثر تهديدا في العالم ، حتى مثل هذه الهيئة التي تعنون تقاريرها مباشرة بعنوان "الأمن السيبراني" Cyber Security، رغم أنها حددت مجالات النشاط الحيوية، والحساسية للنظام الأمريكي، والتي تقدمها من ناحية الأولويات، ووجوب تقديم واحد منها على الأخرى دون إقصاء أيا من تلك المجالات أو النشاطات، إلا أن أغلب هذه التقارير، لم تحمل في طياتها تعريفا محددا للأمن السيبراني، وبالتالي حاولنا على ضوء التعريف السابق وعلى ضوء ما ذكرناه من حقائق معاشة اليوم، تقديم تعريف للأمن السيبراني، وكان على الشكل التالي:

" نسمي عملية امن سيبري، كل عملية تفكير، بحث، وضع ، تنفيذ، تتبع ومراقبة سياسة أو إستراتيجية مدججة لأمن النظام الكلي لدولة أو مؤسسة أو مجموعة معينة أو حتى أفراد، وهذا من خلال تأمين بالمقام الأول نظام معلوماتها وتأمين الشبكات التي تربط بين تلك الأنظمة"،

وبالتالي فإن هذا الشكل يلخص بشكل جيد مقارنة التطور التاريخي لظهور الأمن السيبراني ، والذي يعود في الأصل أو في بدايته إلى أمن الإعلام الآلي . إلا أنه وبحكم مصدر هذه الوثيقة ، فإن صائع هذه المقاربة التاريخية لأمن المعلومات قد قدمها من ناحية تقنية أكثر، لأن امن المعلومات يسبق امن نظم هذه المعلومات، وهذا الأخير يسبق امن الإعلام الآلي .

كما ان مسألة امن المعلومات قديمة جدا قدم الإنسان، وقد تبدأ منذ اللحظة الأولى التي بدا الإنسان يقدر فيها قيمة المعلومة وخطورة تسربها ووقوعها في يد العدو .

وبالتالي فان الأمن السيبراني لا ينحصر على الإعلام الآلي فقط، كما أن نظام المعلومات لا يعتمد فقط على عتاد وبرامج الإعلام الآلي .

2- تعريف الأمن السيبراني:

من الصعب بكثير تحديد ماهية الأمن السيبراني، وخاصة في مجال تحديد ما إذا كان علما أم فنا أم مجرد إجراء فقط، إلا أن أهمية اليوم الذي نظمه الاتحاد الدولي للاتصالات السلكية واللاسلكية، تكمن في وضع تصور قد يكون الأول من نوعه حول ماهية امن السيبراني، و بالتالي فقد قدم هذا الاتحاد الأمن السيبراني على انه " سيرورة، وليس حلا ، والذي يضم مجموع الوسائل الموضوعة لصد هجمات وجرائم إرادية (كالاختراق و التطفل) أو غير إرادية (الهفوات)، والتي من شأنها ان تهدد أنظمة المعلومات أو الشبكات الاتصالية"، قد يكون هذا التعريف ناقصا بحكم انه صادر عن جهة مختصة في الاتصالات السلكية واللاسلكية فقط، إلا أننا ومن خلال اطلعنا

العسكرية و التقنية، هذا الإلحاح يخص وضع استراتيجيات من شأنها تأمين نظم المعلومات قبل وبعد وضعها وربطها عبر الشبكات بأنظمة أخرى.

3- مجال الأمن السيبري :

استوحينا فكرة هذا العنصر من الوثيقة الالكترونية السابقة Pierre-Luc)

<< Cybersécurité : La fin de RSSI >> (Refalo) ، و التي تهتم بشكل مباشر بالأمن السيبري . و إضافة إلى الشكل السابق الذي عرض أهم مراحل ظهور الأمن السيبري ، فقد قدم الكاتب في نفس الوثيقة مخططات أخرى ، من بينها تلك التي تبين أو يقترح من خلالها الإطار القانوني للأمن السيبري . ويقترّب هذا المخطط كثيرا بما تصورنا انه مجال نشاط الأمن السيبري مسبقا .

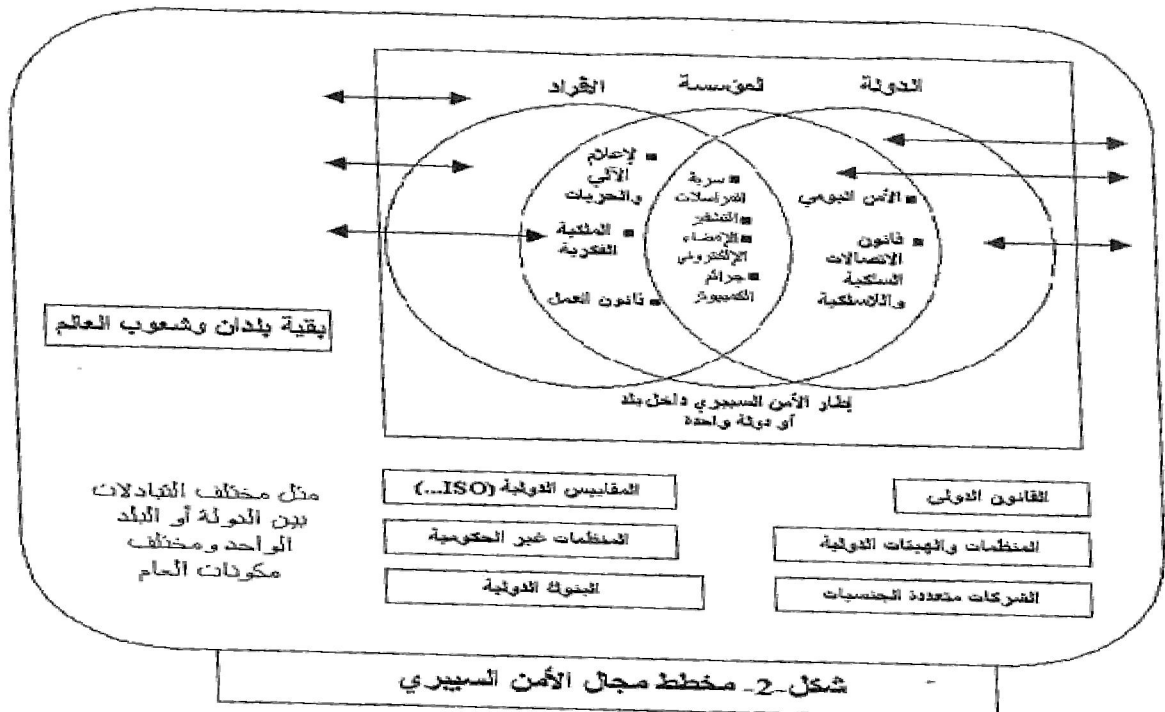
وخلافا لأمن أنظمة المعلومات أو امن الإعلام الآلي. يتوسع مجال نشاط الأمن السيبري ليشمل كل ما يمكن أن يستهدف عن طريق عمليات إجرامية (واعية أو غير واعية) . و هنا نقصد مباشرة العالم بأسره .

وبناء على نفس المخطط ، قمنا بتطويره وإضفاء نظرة شمولية عليه . والشكل (2) يوضح بشكل أفضل :

ومنه فان الأمن السيبري، ليس حالة معينة فقط، كما انه لا يتعلق بسياق واحد، وإنما هو سيورة غير خطية لعمليات قبلية وبعدية لحماية مجتمع مفتوح⁽⁴⁾ على كل الأخطار .

ونظرا إلى الأهمية البالغة للأمن السيبري، يمكننا اعتباره العلم الذي يدرس العمليات الإرادية والمنظمة لتأمين وحماية الشبكات ونظم المعلومات، وهذا على عكس Cybercriminalité، العلم الذي يدرس العمليات الإرادية وغير الإرادية التي من شأنها تهديد تلك النظم والشبكات، وقد استخدمنا كثيرا تعبير الإرادة للدلالة على دور الإنسان داخل هذه المعطيات الجديدة.

يتبرر تبني مثل هذا العلم الجديد -الأمن السيبري- بشكل أكبر في الدول المتقدمة، أين تعتمد نظم معلومات جد معقدة باستخدام أحدث التكنولوجيات لتسيير شؤونها اليومية، وتقدم خدمات أكثر من حيث النوع و الكم، إلا انه يتبرر أيضا في الدول المتأخرة نوعا ما، وهذا حسب التقارير الدولية الرسمية، نظرا لتصاعد معدل الجريمة السيبرية التي تتخذ من هذه البلدان مراكز أساسية، وذلك باستغلال شبكة الانترنت في قيادة العمليات الإجرامية باعتبارها شبكة عالمية تضم اغلب الشبكات الأخرى والأصغر حجما. وبالتالي يظهر إلحاح كبير (معلن أو غير معلن) من طرف حكومات تلك الدول والمؤسسات التي تشكل مجالاتها الاجتماعية والاقتصادية وحتى



حاولنا من خلال هذا المخطط أن نبين مدى توسع دائرة نشاط الأمن السيبري فإذا كانت نظرة المختصين في امن نظم المعلومات تأخذ بعين الاعتبار فقط، التبادلات على مستوى حكومة واحدة أو مؤسسة واحدة او مجموعة معينة من الأفراد ينشطون في مجال واحد، فالأمن السيبري هو ما دعت إليه مباشرة الأمم المتحدة، أي هو ما يجب تعميم مبادئه وترسيخ ثقافته والشكل (2) يوضح ذلك بشكل أفضل، بحيث وضعنا الكل في إطار واحد . وبالتالي يكون فعل واحد من تلك المكونات يؤدي إلى ردود فعل بقية المكونات.

وهذه نظرة سبرنطيقية محضة . ومن جهة أخرى، وبنظرة سبرنطيقية أخرى . فان الشكل (2) ، يبين أن التعاون في ميدان الأمن السيبري يجب أن يكون بين مختلف مكونات العالم (دول وحكومات، مؤسسات وشركات، هيئات ومنظمات، شعوب) دون استثناء واحدة منها. لان الترابط المستمر بينها عن طريق شبكات الاتصال، كفيل بان يؤثر على الجميع في حال إصابة واحدة من تلك المكونات. كما أن النشاط الجماعي يكون أقوى من النشاط الفردي. لأنه يتكون من مجموعة تجارب و أفكار مختلفة ومتكاملة . وبالتالي فان الكل أقوى من مجموع الأجزاء منفصلة عن بعضها .

4- أهمية الأمن السيبري :

قد لا تظهر الحاجة إلى تخصيص عنصر مستقل للتعريف بأهمية الأمن السيبري، ولكن ارتفاع عدد الجرائم والاستعمالات اليومية غير المتوازنة وغير العقلانية لنظم المعلومات والشبكات، هذا الارتفاع في عدد الجرائم والمشاكل يدل على أن ثقافة الأمن لم تستقر بعد في أذهان العامة من الناس، كما أنها لم تستقر جيدا بعد في أذهان المختصين.

وبالتالي يكون تحسيس القادة و أصحاب القرار في مختلف المجالات بقضية الأمن السيبري، تعلق بشكل واضح بكون شبكة الانترنت باعتبارها الشبكة التي تربط بين اكبر عدد ممكن من الشبكات الأخرى، أصبحت أكثر عرضة لهجمات (من الأيسر إلى الأعقد). والتي لا يمكن حصر نتائجها السلبية على المرتبطين بها. والأمثلة كثيرة لإثبات الخطر أو الأخطار الحالية وكذا المستقبلية، وخاصة تلك المتعلقة منها بالانترنت. فمواقع حساسة جدا تم اختراقها وسرقة المعلومات منها، أو إتلافها بشكل تام، نذكر من بين تلك المواقع الحساسة : Yahoo أين تم سرقة قاعدة بيانات مهمة تخص مستخدمي البريد الالكتروني، وموقع Amazon المتخصص في بيع الكتب على الخط، والذي تعرض بدوره إلى حادثة خطيرة من نوعها، بحيث تم سرقة عدد معتبر من الكتب المعروضة للبيع، ومن جهة أخرى، سرقة معلومات حول أرقام سرية للزبائن والمتعلقة بأرقام حساباتهم البنكية، الشيء نفسه حصل مع موقع Ebay الذي يعتبر بمثابة سوق على الخط. وتبقى هذه الأمثلة بسيطة جدا مقارنة بأمثلة أخرى تدعو للقلق بشأن استخدام شبكة الانترنت. ولكن الخدمات التي تقدمها هذه الأخيرة، لا يمكن تجاوزها من طرف المستخدمين، أفراد كانوا أم مؤسسات.

ويكمن الحل الوحيد في بحث سبل تأمين فعلي ومستدام لهذه الشبكة وللشبكات المرتبطة بها. وهنا يتمحور دور إستراتيجية وسياسة مستدامة للأمن السيبري، والتي يجب أن تأخذ حيزا كبيرا من اهتمام الجميع (حكومات، مؤسسات وأفراد) .

وإذا القينا نظرة شاملة لما يمكن أن ينتج كخسائر بسبب انعدام شبكة مثل الانترنت وباقي الشبكات، والنظم، وحوامل المعلومات والقنوات . فإننا نتوجه خصوصا إلى دول العالم الثالث، الذي تعتبر الجزائر واحدة منها. ففي مثل هذه البلدان، تستخدم الانترنت مباشرة وبشكل كبير، إلى عمليات تحميل (Téléchargement) (Download) ملفات بشكل مجاني. وكلمة مجاني لا تعني في كل الأحوال بان هذه الملفات موضوعة مجانا، وإنما هناك جهات أخرى تبث نسخ (تكون في أحيان كثيرة نسخا أصلية) لكتب أو برامج مرتفعة الثمن، أو صور ممنوعة من النشر، أو مقاطع فيديو، أو أفلام كاملة أو أغاني، والقائمة طويلة مما يمكن أن يحمل عن طريق الانترنت . ففي المغرب العربي عموما ، و في الجزائر خصوصا، تعاني شركات مثل TPS و BEIN SPORT، Canal Satellite بالنسبة لباقات القنوات لفضائية، تعاني هذه الأخيرة، من نشر شبه منتظم يكاد يوازي عمل هذه الشركات فيما يخص شيفرات باقاتها التلفزيونية، من جهة أخرى، تعاني شركات مثل شركات تصنيع الهواتف النقالة (مثل APPEL ، Samsung ،.....)، من النشر غير المرخص به ، لأهم البرامج الخاصة بالموبايل . هذا بالإضافة إلى اختراق حقوق المؤلف بالنسبة للعديد من الكتاب و المفكرين. تعتبر هذه المعطيات الأولية، عبارة عن تحديات صريحة لاستراتيجيات التامين، والمختصين في هذا الميدان .

فأهمية الأمن السيبري، تمكن في أن مشاكل ذات طابع عالمي، يمكنها أن تؤثر بشكل كبير على قطاعات محلية خاصة على مستوى بلدان العالم الثالث. التي تعاني أصلاً من مشكلة تسريع دخولها الشبكات الدولية، مما يحد منها بان رفع حواجز الاتصال بين الأمم والدول، من شأنه رفع الضائقات المالية، وتقليص الهوية التكنولوجية بين دول الشمال ودول الجنوب.

إلا أن هذا التسريع في تعميم تكنولوجيات الاعلام والاتصال وخصوصاً عتاد الاعلام الالي من شأنه ان يقلب السحر على الساحر، حيث، بدلاً من أن تتطور هذه البلدان، فإنها بهذه الاستعمالات غير عقلانية، قد تؤدي باقتصادتها وبأمنها القومي إلى هوية يصعب عليها إلى خروج منها.

لا داعي بعد ذكر هذا كله إلى قول بان الأمن السيبري مهم جداً، لأنها عبارة قد تؤدي إلى التفكير بسيطة يجب التفكير فيها . في وقت الذي تنفذ فيه وبشكل أوسع و أذكى ، عمليات إجرامية تمس نظم المعلومات لقطاعات الحيوية حتى انه يصعب على المختصين أنفسهم أحياناً تفسير أسباب ومصادر وكذا يصعب تقدير خسائر تلك الجرائم.

الهوامش

1. UIT (Union internationale des télécommunications) dans son réunion de commémoration di 17 mai 2006.
2. Pierre – Luc Refalo « Cyber sécurité : La Fin de RSSI ». L'informatique Professionnelle* 215 juin - juillet 2003 .page 42.(document électronique PDF).-Traduction personnelle du Français en arabe
3. National Coordination Office Information Technology Research And Development
4. مصطلح المجتمع المفتوح عثرنا عليه في وثيقة رسمية للحكومة الكندية، والتي تستخدمه للتعبير عن مجتمعها الذي أصبح مفتوحاً على كل الأخطار المحدقة، خاصة بسبب وضع أنظمتها المعلوماتية الحيوية على شبكات داخلية و خارجية.