

المحاضرة الثالثة محل الجريمة السيبرانية وأضرارها وحجمها

تمهيد وتقسيم :

أصبح وجود الجريمة السيبرانية وما يترتب عليها من خسائر ضخمة أمرا مسلما به، ف لأهمية المعلومات يسعى المنتمون لجميع فئات المجتمع بكل ما أوتوا من قوة من الحصول عليها سواء بالطرق المشروعة أو غير المشروعة، الأمر الذي حدا بالبعض إلى تقرير سوقين لشراء المعلومات إحداها شرعي والثاني يطلق عليه "السوق السوداء للمعلومات"، والذي يرتبط بالجانب الأكبر من الجرائم التي تستهدف الأنشطة الاقتصادية والاجتماعية للمجتمع، ومن الممكن بالتالي أن تكون هذه المعلومات تهدد أو تنتهك حرمة الحياة الخاصة وغيرها من الحقوق التي وضع المشرع لها الحماية القانونية.

ولذلك سوف نقسم المحاضرة بإذن الله تعالى إلى المحاور التالية:

المحور الأول: محل الجريمة السيبرانية:

المحور الثاني: أضرار الجريمة السيبرانية:

المحور الثالث: حجم الجريمة السيبرانية:

المحور الأول: محل الجريمة السيبرانية:

وتعتبر الجرائم السيبرانية من طائفة الجرائم المنصبة على المعلومات والبيانات، والتي من الممكن أن تتمثل في شكل برامج تطبيقية أو برامج تشغيل، وبمعنى آخر فإن محل الجريمة السيبرانية يتمثل في النظام المعلوماتي ومكوناته، وذلك على النحو التالي :

(١) إن محل الجريمة السيبرانية هو المعلومات الإلكترونية: أما المقصود بالمعطيات الكمبيوتر ، أي البيانات فالمعطيات في اللغة الفرنسية تقابل "البيانات" في اللغة الإنجليزية والمعطيات في اللغة الفرنسية هي الكلمة التي آثر على استعمالها المشرع الجزائري في مقابل كلمة البيانات .

مع العلم أن كلا من القانونين الفرنسي والجزائري يخلوان من ذكر كلمة المعلومات رغم أن البعض فضلوا استخدام مصطلح معلومات وأنا أنضم إلى هذا الرأي لأنه من الضروري التفرقة بين المعطيات والمعلومات، فالمعطيات عندما تعالج آليا تأخذ تسمية المعلومات.

وعلى سبيل المثال تعرض مشروع تعديل قانون العقوبات السويسري للجنة الخاصة بالذمة المالية وتناول تجريم استخدام - دون حق - المعلومات أو البرامج المسجلة إلكترونيا.

وفي المقابل تعرض قانون العقوبات السويسري للاستخدام غير المشروع للحاسوب، وكذلك للتغيير غير المشروع للمعلومات أو لتحرير معلومات غير سليمة، حيث تقع هذه الجرائم في إطار نصوص قانون العقوبات الخاصة بتزوير المحررات أو الشهادات.

(٢) البرامج بكل أنواعها، سواء المدخلة أو المعالجة أو المخزنة داخل الجهاز، ويتمتع كل برنامج بحماية أيا كانت صورته، ويمثل ذلك برامج الكمبيوتر التي تدخل في المادة ذاتها (توجيه المجموعة الأوروبية الصادر في ١٤ مايو ١٩٩١م رقم ٧)، ونلاحظ أن البرامج أو أنظمة الكمبيوتر تتمتع بالحماية تماما كبرامج التطبيق.

ويستبعد من نطاق الحماية ولا يكون محلا للجريمة السيبرانية الأفكار والمبادئ التي تكون أساس كل عرض أيا كان البرنامج فلا تكون محلا للحماية بهذه الصفة التوجيه الأوروبي الصادر في ١٤ مايو ١٩٩١م المادة الأولى. كذلك يستبعد من نطاق الحماية الأفكار والمبادئ التي تكون أساس النطق ولغة البرمجة.

وبصفة عامة يستبعد من الحماية الأسس والمبادئ التي تعبر عن القواعد المجردة للبرنامج المعلوماتي، وذلك كالمبادئ الحسابية وأنماط البرنامج وقواعد الإدارة وقواعد الحساب المستخدمة عند إعداد البرنامج، وكذلك القواعد الحسابية، وقد قضى بأن القواعد الحسابية التي تقوم على تعاقب العمليات الحسابية والتي تصف العبارات المنطقية لمشكلة، والمعطيات لا تتمتع بحماية القانون الخاص للبرامج المعلوماتية وإنما يمكن أن تستفيد المعطيات أحيانا من حماية القواعد العامة للملكية الأدبية والفنية وأسس المعطيات تشكل اليوم محلا للنظام خاص.

إذن فموضوع الجريمة السيبرانية أي محلها، يتمثل في الحق الذي يتم التعدي عليه هو الحق في المعلومات بذاتها، وبما تمثله من أموال أو أصول أو أسرار أو بيانات شخصية أو لها قيمة بذاتها كالبرامج فالمعلومات الالكترونية جديرة بالحماية حتى عن المعلومات الورقية، فتظهر جدارة المعلومات المبرمجة آليا بالحماية الجنائية عن المعلومات التي تحتويها الملفات الورقية من ضعف النوع الأول من المعلومات ومن أهميته في آن واحد، فالمعلومات المعالجة آليا ضعيفة داخل النظام عنها داخل الملفات الورقية. هذه الأخيرة يمكن إخفاؤها بسهولة عن المعلومات داخل النظام، كما أن المعلومات المعالجة آليا تتميز بالضخامة والتنوع، ومنها ما يتعلق بالحياة الخاصة للأفراد.

كل هذه الاعتبارات دعت مشرعي كثير من البلاد إلى استحداث صور من التجريم لحماية المعلومات داخل الكمبيوتر من الاطلاع عليها، بينما لا يوجد مثيل لتلك النصوص بالنسبة للمعلومات المسجلة داخل الملفات الورقية.

ويرجع السبب أيضا في أهمية حماية المعلومات الإلكترونية إلى أن من يدخل نظام الكمبيوتر غالبا ما يكون قد اخل بحرمة المكان دون أن يقوم بدخول هذا المكان في حالات كثيرة. يضاف إلى ذلك أن نظام الكمبيوتر يتيح التعرف على كمية هائلة من المعلومات بسهولة ويسر وفي وقت قصير، الأمر الذي لا يتوافر

في حالة الملفات الورقية التقليدية ورغم أن الدخول إلى النظام يعتبر أمراً بسيطاً إلا أن الأضرار الناتجة عنه تعتبر أمراً خطيراً، وتختلف طبعا الدوافع في ارتكاب هذا النوع من الإجرام .

المحور الثاني : أضرار الجريمة السيبرانية:

نلاحظ أن المعلوماتية بوصفها عنصراً استراتيجياً دائماً ما تكون هدفاً كامناً للأفعال الجنائية. فالأنظمة المعلوماتية تتيح الفرصة لارتكاب الجرائم التقليدية بطريقة غير تقليدية، ومن أمثلتها سرقة المعلومات والأسرار المودعة في قواعد المعلومات، والغش والإتلاف وإفساد المعلومات المخزنة في تلك القواعد، وأن سرعة انتشار شبكات المعلومات عبر الحدود والتغيير التقني المطرد والمتعاضد في هذا المجال أدّى إلى اختراق كثير من نظم المعلومات عن طريق خطوط التليفون، أو عن طريق إجبار وإغراء العاملين عليها والحصول منهم على كلمة السر (Code) - أي أن من له مفتاح البيانات للكمبيوتر يستطيع تجميع كل المعلومات المسجلة التي تكون غالباً شخصية - وبالتالي التدخل فيها مما زاد من فرص إساءة استخدام النظام كوسيلة تقنية أو ارتكاب تغيير في البرامج والمعلومات المخزنة فيه.

وتهدف الأجهزة الأمنية وأجهزة العدالة الجنائية في مختلف الدول إلى منع الجريمة والعمل على الوقاية منها بشتى السبل والوسائل، ولقد عرفت المجتمعات الإنسانية ومنها العربية جرائم مختلفة وواجهتها بأساليب متعددة ومتنوعة، لكن التطور التقني الذي نعيشه اليوم في كافة مناطق العالم وبلدانه والمتمثل باستخدام الكمبيوتر والإنترنت أدى إلى استحداث جرائم لم تكن معروفة من قبل، ولذا فهي جرائم مستحدثة، وهي بدون شك من نوع فريد.

وتتمثل الأضرار المعلوماتية في نوعين من المخاطر، أحدهما مخاطر عمدية والأخرى غير عمدية: وتتمثل المخاطر العارضة أو غير العمدية في الأضرار الناشئة عن العوامل الطبيعية مثل المياة أو خلل كهربى، وتؤدي إلى الإتلاف الجزئي أو الكلي للمعدات المعلوماتية و الدعائم التي تحتزن المعلومات، أو تعطيل المعدات والكيانات المنطقية حتى ولو كانت لفترة زمنية قصيرة، وكذلك الأخطاء الخاصة بنقل واستعمال المعلومات وهو أمر وارد طالما أن الإنسان يتدخل في عملية معالجة المعلومات، وأخطاء التشغيل ، وأخطاء التصميم والتنفيذ.

أما المخاطر المعلوماتية العمدية فهي تتعدد وتتنوع من سرقة إلى إتلاف المعدات المادية، وغش واختلاس أموال وكيانات منطقية، ومعلومات وغيرها، ولا شك أن تلك المخاطر سوف تؤدي إلى حدوث كثير من الأضرار والتي ستؤثر بشكل سلبي على الحكومة ومؤسسات الأعمال ومعاملات الأفراد وتؤدي إلى خلق جرائم جديدة وبصفة خاصة في مجالات التوقيع الإلكتروني، والتجارة الإلكترونية، والبريد الإلكتروني .

نجد انتشار الجرائم السيبرانية وذلك نتيجة ازدياد استخدام نظم المعلومات في شتى الميادين العلمية والاقتصادية إلى جانب استخدام الإنترنت على نحو متسارع، فمن أبرز أضرار الجرائم السيبرانية هي:

1. تهدد الجرائم السيبرانية عموما الحق في المعلومات انسيابها، وتدفعها واستخدامها، وأن الأهمية الإستراتيجية والثقافية، والاقتصادية للمعلومات، تجعل من أنماط الاعتداء عليها خطورة جد بالغة بكونها تهدد في الحقيقة البناء الثقافي، والاقتصادي للدولة.

2. إن بعض جرائم السيبرانية تمس الحياة الخاصة أو ما يسمى بحق الإنسان في الخصوصية، وهذه الجرائم تخلف وراءها - إلى جانب الضرر الكبير بالشخص المستهدف في الاعتداء - شعورا عريضا لدى الأفراد بمخاطر التقنية ، من شأنه أن يؤثر سلبا في تفاعل الإنسان مع التقنية ، علي الرغم من أهمية هذا التفاعل اللازم لمواجهة تحديات العصر الرقمي.

3. تطال بعض جرائم السيبرانية الأمن القومي والسيادة الوطنية في إطار ما يعرف بحروب المعلومات أو الأخلاقية الإلكترونية وتحديدًا جرائم التجسس وجرائم الاستيلاء على المعلومات المنقولة خارج الحدود.

4. تشيع جرائم السيبرانية فقدان الثقة بالتقنية - لا لدى الأفراد فحسب - وإنما لدى أصحاب القرار في الدولة، وهو ما سيؤثر في الحقيقة على استخدام التقنية في قطاعات المجتمع، وبدوره يؤثر على امتلاك الدولة للتقنية التي أصبحت تمثل حجر الزاوية في جهود التنمية وتطور المجتمع.

5. إن الجرائم السيبرانية هي وليدة التقنية، وهي في نفس الوقت تهدد التقنية ذاتها، وبالتالي تهدد الفجر المشرق للمستقبل، والمؤسس على التفاعل الإيجابي ما بين الإنسان والتقنية العالمية.

وبناء علي ما سبق نجد أنه علي الرغم من تحقيق النظام المعلوماتي لمزايا لا يمكن إنكارها فإنه يعد في ذات الوقت مجالا لمخاطر لا يستهان بها؛ حيث أصبح مصدرا جديدا بل وخطيرا في ارتكاب العديد من الجرائم وهي ما يطلق عليها الجرائم السيبرانية. ولذلك سوف نتحدث عن الأضرار المعلوماتية من خلال بيان الدور الذي يلعبه كل من الحاسوب والإنترنت في نطاق المعلوماتية، وذلك علي النحو التالي :

أولا : الحاسوب في نطاق الجريمة السيبرانية.

ثانيا : الإنترنت في نطاق الجريمة السيبرانية .

أولاً: الحاسوب في نطاق الجريمة السيبرانية:

الحاسوب - كأداة تخزين لديه قدرة هائلة علي تخزين وتنظيم واستغلال عدد غير محدود من المعلومات ولديه القدرة أيضا علي استرجاعها في فترة زمنية وجيزة، فإذا كان الحاسوب هو رمز القوة وأداة السلطة، إلا أنه يسهل التعدي عليه دائما سواء عن طريق أحداث طبيعية أو أحداث من صنع الإنسان . وتلك الأحداث يمكن أن تدمره كلية أو بصفة جزئية.

ومن أهم دواعي استخدام الحاسوب هي قدرته التخزينية، وهي أكثر الموضوعات اتصالا بالجريمة فلولا تخزين المعلومات لما كان هناك جريمة اعتداء على هذه المعلومات بالسرقة، أو الإتلاف، أو الاعتداء على المعلومات، وأيضا فإن تخزين المستندات أدى إلى إثارة المشكلة القانونية المتمثلة في إمكانية تزوير المستندات إلكترونيا، ومحاولة إيجاد حل لها، ومدي انطباق نص التزوير عليها.

والجدير بالذكر أنه ظهرت في السنوات الأخيرة لغات برمجة حديثة سهلة الاستخدام، وبعضها موجه إلى المستخدم العادي ولا يحتاج استخدامها إلي خبرة كبيرة . وقد أدى ظهور هذه اللغات إلى وضع قوة المعالجة في أيدي أعداد كبيرة من المستفيدين، مما جعل عملية الحصول علي المعلومة عملية سهلة خاصة مع ظهور لغات للاستفسار يمكن بواسطتها استخراج المعلومات والإحصاءات المطلوبة بسهولة من قواعد البيانات من علي أجهزة الكمبيوتر. أي أن الشخص العادي يستطيع الآن البرمجة، و يستطيع البحث في قواعد البيانات مما أتاح له ذلك الاطلاع علي معلومات محظورة، فضلا عن احتمالات تعديل هذه المعلومات أو تدميرها.

ويلعب الكمبيوتر ثلاثة ادوار في ميدان ارتكاب الجرائم ، ففي حقل ارتكاب الجرائم يكون للكمبيوتر الأدوار التالية:

الأول : قد يكون الكمبيوتر هدفا للجريمة :

وهي نوعية من الجرائم يكون هدف المجرم فيها التوصل إلى سرقة بيانات من الحاسوب، أو إحداث إضرار به، أو بنظام تشغيله.

ومن أوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة عندما توجه الهجمات إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المساس بالسلامة، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها، وهدف هذا النمط الإجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام، وغالبية هذه الأفعال الإجرامية تتضمن الدخول غير المصرح به إلى النظام الهدف، والتي توصف بشكل شائع في هذه الأيام بأنشطة الهاكرز كناية عن فعل الاختراق.

والأفعال التي تتضمن سرقة للمعلومات تتخذ أشكالاً عديدة معتمدة على الطبيعة التقنية للنظام محل الاعتداء، وكذلك على الوسيلة التقنية المتبعة لتحقيق الاعتداء، فالكامبيوترات مخازن للمعلومات الحساسة كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية وخطط التسويق وغيرها وهذه تمثل هدفاً للعديد من الجهات بما فيها أيضاً جهات التحقيق الجنائي، والمنظمات الإرهابية، وجهات المخابرات والأجهزة الأمنية وغيرها، ولا يتوقف نشاط الاختراق على الملفات والأنظمة الحكومية بل يمتد إلى الأنظمة الخاصة التي تتضمن بيانات قيمة سواء كانت هذه البيانات تمس الحياة الخاصة أو الحياة العامة.

فعلى سبيل المثال قد يتوصل أحد المخترقين للدخول إلى نظام الحجز في أحد الفنادق لسرقة أرقام بطاقات الائتمان، وكذلك الاعتداء على الملكية الفكرية كسرقة الأسرار التجارية وإعادة إنتاج ونسخ المصنفات المحمية وتحديد برامج الحاسوب. وفي حالات أخرى فإن أفعال الاختراق التي تستهدف أنظمة المعلومات الخاصة تستهدف منافع تجارية، أو إرضاء أطماع شخصية كما أن الهدف في هذه الطائفة يتضمن أنظمة سجلات طبية، وأنظمة الهاتف، وسجلاته، ونماذج تعبئة البيانات للمستهلكين وغيرها.

الثاني : الجرائم التي يكون الحاسوب وسيلة لارتكابها :

وهذه النوعية من الجرائم تحدث عندما يستخدم المجرم الحاسوب لتسهيل ارتكاب بعض الجرائم التقليدية. كما في حالة استغلال الكمبيوتر للاستيلاء على الأموال بإجراء تحويلات غير مشروعة، أو استخدام التقنية في عمليات التزييف والتزوير، أو استخدام التقنية في الاستيلاء على أرقام بطاقات ائتمان وإعادة استخدامها والاستيلاء على الأموال بواسطة ذلك، حتى إن الكمبيوتر كوسيلة قد يستخدم في جرائم القتل، كما في الدخول إلى قواعد البيانات الصحية والعلاجية وتحويلها أو تحويل عمل الأجهزة الطبية والمخبرية عبر التلاعب ببرمجياتها، أو كما في اتباع الوسائل الإلكترونية للتأثير على عمل برمجيات التحكم في الطائرة أو السفينة بشكل يؤدي إلى تدميرها وقتل ركبها.

الثالث: وقد يكون الكمبيوتر بيئة الجريمة:

وهي الجرائم التي يكون فيها الحاسوب أداة لحفظ الأدلة يكون وسيطاً في الحصول عليها. وذلك كما في تخزين البرامج المقرصنة فيه، أو في حالة استخدامه لنشر المواد غير القانونية، أو استخدامه كأداة تخزين أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية ونحوها.

نلاحظ على هذا التقسيم أن الكمبيوتر يمكن أن يلعب الأدوار الثلاثة معاً، كما أن مثل هذا التقسيم السالف ليس جامعاً مانعاً للتعبير عن جرائم الحاسوب؛ إذ إن هناك من الجرائم التي ترتكب بواسطة

الحاسوب ومع ذلك لا يمكن إدراجها في أي من الأقسام الثلاثة السابقة مثل جريمة سرقة وقت الحاسوب بمعنى استخدام وقت الحاسوب في أغراض لا تتعلق بالعمل الرسمي وهي جريمة من الجرائم السيبرانية في التقنين الأمريكي.

إما من حيث دور الكمبيوتر في اكتشاف الجريمة، فإن الكمبيوتر يستخدم الآن على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم ، عوضا عن أن جهات تنفيذ القانون تعتمد على النظم التقنية في إدارة المهام من خلال بناء قواعد البيانات ضمن جهاز إدارة العدالة والتطبيق القانوني، ومع تزايد نطاق جرائم السيبرانية، واعتماد مرتكبيها على وسائل التقنية المتجددة والمتطورة، فإنه أصبح لزاما استخدام نفس وسائل الجريمة المتطورة للكشف عنها، من هنا يلعب الكمبيوتر ذاته دورا رئيسا في كشف جرائم السيبرانية وتتبع فاعليها بل وإبطال أثر الهجمات التدميرية لمخترقي النظم وتحديد هجمات الفيروسات وقرصنة البرمجيات.

ثانيا : الإنترنت في نطاق الجريمة السيبرانية:

وطالما أن الإنترنت هو فضاء معلوماتي حر و مفتوح، لا يعرف للحدود معنى، فلا مجال للانتقائية فيه فهو يخفي في جعبته محتويات ذات طابع إجرامي فيستخدم الإنترنت في ارتكاب العديد من أنواع الجرائم السيبرانية المختلفة.

فلقد شهدت التسعينيات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات، فظهرت أنماط جديدة كأشطة إنكار الخدمة التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد، وأكثر ما مورست ضد مواقع الإنترنت التسويقية الناشطة والهامة التي يعني انقطاعها عن الخدمة لساعات خسائر مالية بالملايين.

ونشطت جرائم نشر الفيروسات عبر مواقع الإنترنت لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت، وكذلك سرقة بطاقات الائتمان لاستخدامها في شراء المنتجات عبر الإنترنت، وسرقة كلمة المرور الخاصة بالدخول إلى المواقع والاستيلاء علي البيانات الأمنية، والعسكرية والسياسية والاقتصادية، والتجارية، والاسمية، وزرع الفيروسات المدمرة للأجهزة ونشر المواد الإباحية التي تمس قيم المجتمع الأخلاقية بشتى وسائل عرضها المصورة أو المسجلة، وتجسدت أيضا في تزوير البطاقات البنكية وفي استعمال عبارات العنف والعنصرية، ومرورا بالمحادثات المشبوهة التي قد تتمخض عنها دعارة الأطفال، إلى قضايا الإرهاب.

وتعد قرصنة البرامج من الجرائم التي ارتبطت بنشأة الحاسوب بصفة عامة، إلا أن ظهور شبكات المعلومات قد ساعد على نحو كبير في زيادة حجم هذه الجريمة؛ لما وفرته هذه الشبكات من مجال خصب لارتكابها وتسويقها.

وبازدياد كم المعلومات و بازدياد حركتها (انتقالها من مكان إلى آخر خلال الشبكات المحلية و عبر الشبكات الكبيرة و في العالم كله من شرقه إلى غربه عبر شبكة الإنترنت) ، أصبح أمن المعلومات في خطر، فهي دائما معرضة لأخطار عديدة ، ليس أقلها ضياع المعلومة أو تغيير مضمونها، وليس أخطرها اطلاع الغير عليها فالأشياء الثمينة والنادرة والهامة تكون دائما عرضة لمحاولات الآخرين الوصول إليها لاقتنائها أو إتلافها، ومع ذلك يجب أن يوضع في الاعتبار صعوبة مراقبة تداول المعلومات التي تكون مستهدفة.

وأصبح من المألوف الآن أن تتعامل البرامج مع بيانات موجودة في أماكن بعيدة ، و أصبح الدخول إلى قواعد البيانات العالمية في أي مكان من العالم والحصول منها على معلومات أمرا سهلا ومتاحا، وقد انتشر هذا الأسلوب بكثرة في الآونة الأخيرة، مع ما يصاحب هذه التسهيلات من زيادة احتمالات انتهاك المعلومات، ففي بعض الأحيان قد لا يكون من السهل أن تسيطر علي من يدخلون إلي قاعدة البيانات الخاصة بك أو أن تتحكم فيما يصلون إليه من معلومات.

وإن محركات البحث تمثل الوسيلة الأهم من بين وسائل الوصول المباشر للمعلومات المطلوبة من قبل المستخدم ، وتقوم محركات البحث والأدلة الإرشادية - في تطور أوسع على شبكة الإنترنت - بعمليات جمع وتبويب وتحليل بيانات الاستخدام على نحو واسع ، مستخدمة إما وسيلة الكوكيز أو غيرها من حزم النبضات / البتات اللاصقة (sticky bits) التي تخزن في كميبيوترات الزائرين؛ من أجل مساعدة الموقع على التعرف على الاتجاهات الخصوصية للزائر ومساعدته في تحديد اتجاهات الإعلان وتقديم المحتويات والمشكلة المثارة أن غالبية هذه المواقع لا تطلع المستخدم بذلك، وإن كان ثمة توجه في إطار التنظيم الذاتي لقطاعات التجارة الإلكترونية والإعلان على الإنترنت أن يتم إعلام المستخدم قبل القيام بذلك وإتاحة الخيار له للقبول والرفض.

والوسيلة الأخطر فهي ما تعرف بـ **(برمجيات التتبع والالتقاط الشم)** وهي وسيلة تتبع لجمع أكبر قدر من المعلومات السرية والخاصة عن طريق ما يعرف بأنظمة جمع المعلومات (تشممها) . ولقد ارتكبت العديد من جهات الرقابة أنشطة إساءة استخدام البيانات الخاصة حتى في أكثر الدول المتقدمة، وكان الهدف من وراء هذه الاعتداءات في الغالب سياسيا أو اقتصاديا، لهذا كانت البيانات المستهدفة هي بيانات المعارضة السياسية والصحفيين وناشطي حقوق الإنسان، وهو ما اقتضى تزايد النشاط الدولي في حقل حماية الخصوصية من أنشطة الرقابة الإلكترونية.

بل وصل حد التجسس على الخصوصية إلى إنشاء الدول المتقدمة ذاتها أكبر شبكات تجسس مثلت من الخطورة ما دفع ناشطي حماية الخصوصية في بيئة الإنترنت إلى تنظيم حملات مهاجمة إلكترونية لهذه الشبكات بهدف تعطيل عملها .

وهكذا يقفز الهاجس الأمني إلى صدارة اهتمامات المؤسسات التي تفكر في خوض غمار التجارة عبر الإنترنت. ولذلك يتطلب أمن البيانات المنقولة عبر الإنترنت إخفاءها عن أنظار المتربصين بها، وذلك بتسييرها عبر أنفاق خاصة تمر داخل الإنترنت.

ومما تجدر الإشارة إليه أنه من الصعوبة بمكان فصل جرائم الحاسوب عن جرائم الإنترنت، نتيجة لارتباط الإنترنت بالحاسوب ارتباطا تقنيا، إلا أن هذه الصعوبة سوف تتقلص كثيرا إذا أدركنا أن تقنية الحاسوب أعم كثيرا من تقنية الإنترنت، فالمؤشرات السائدة تشير إلى أن تقنيات جديدة للحاسوب تبرز في الأفق قريبا .

ومن الأمثلة التي تدل على أن تقنية الحاسوب أعم كثيرا من تقنية الإنترنت أنه أصبح الآن إمكانية اختراق الحواسيب المعزولة دون الإتصال بالإنترنت عن طريق خطوط الطاقة وعبر الموجات فوق الصوتية وغيرها من التقنيات المستحدثة.

والجرائم المتعلقة بالإنترنت التقليدية منها والمستحدثة تتميز بخصائص معينة تنفرد بها عن غيرها من الجرائم هي:

الخاصية الأولى : الحاسوب هو أداة ارتكابها :

هذه الخاصية ليست قصرا على الجرائم المتعلقة بشبكة الإنترنت، فكما قد يكون الحاسوب أداة لارتكاب هذا النوع من الجرائم فهو - أيضا - أداة لارتكاب العديد من الجرائم السيبرانية كالتزوير المعلوماتي وسرقة المعلومات المخزنة بالحاسوب ، وغيرها أضف إلى ذلك أن ارتكاب جرائم الإنترنت لا تتم في جميع الأحوال بواسطة الحاسوب فقط وإنما قد تتم بواسطة أجهزة الهاتف النقال خاصة وأن الولوج إلى شبكة الإنترنت من الممكن أن يتم بواسطة هذه الهواتف .

الخاصية الثانية : ترتكب بواسطة الإنترنت :

الجرائم السيبرانية من الجرائم الحديثة التي يستخدم فيها الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها. ويعد الإنترنت حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات بكافة أنواعها والأشخاص وغيرها التي غالبا ما تكون الضحية.

الخاصية الثالثة : المجرم المعلوماتي عبر الإنترنت يختلف عن المعلوماتي عبر الحاسوب :

وهذا الاختلاف مرجعه إلي أن المجرم عبر الإنترنت لا يتمتع بمدارك علمية أو تخصصية ذات طابع أكاديمي، وإنما هو أبسط بكثير. و بمعنى أكثر تحديدا يمكن القول إن البدايات الأولى للمجرم السيبراني كانت علي درجة كبيرة عالية من التخصص و التقنية، ثم إن هذا المفهوم للمجرم المعلوماتي أصبح أكثر اتساعا من مجرد المتخصص الدارس لعلوم الحاسوب إلي الشخص الذي يملك تقنية الإنترنت دون حاجة لأن يكون دارسا لها . لذلك لا نتعجب أن يكون هناك محام، أو طبيب، أو مهندس، أو أديب، أو عامل، أو طالب أو تلميذ من مرتكبي الجريمة السيبرانية.

ولذلك فإنني أخالف الرأي القائل بأن الخبرة الكبيرة والدراية الفائقة بكل ما يتعلق بالحاسوب والإنترنت هي ما تميز مرتكب الجريمة السيبرانية بشكل عام.

الخاصية الرابعة: تتسم بالخطورة البالغة:

الجرائم المتعلقة بالإنترنت تتسم بالخطورة البالغة من عدة نواح : فمن ناحية أولى نجد أن الخسائر الناجمة عنها كبيرة جدا قياسا بالجرائم التقليدية خاصة جرائم الأموال ومن ناحية ثانية : نجدها ترتكب من فئات متعددة تجعل من التنبؤ بالمشتبه فيه أمرا صعبا. ومن ناحية ثالثة: تنطوي علي سلوكيات غير مألوفا . وهذا ما حدا بمكتب التحقيقات الفيدرالية الأمريكي "FBI" أن يطلق عليها وصف الوباء.

والجرائم الناشئة عن الاستخدام غير المشروع للإنترنت يمكن تقسيمها إلي فئتين من الجرائم علي النحو التالي:

الفئة الأولى: تسمى الجرائم غير السيبرانية في شبكة الإنترنت، وفيها تكون الشبكة قد استخدمت كوسيلة في ارتكاب الجرائم العادية، وتنطبق عليها النصوص التقليدية القائمة في القوانين العقابية .

وإذا كان عصر المعلومات أو عصر ثورة المعلومات هو نتاج طفرة الاتصالات وطفرة تقنية المعلومات، فإن ما جاء به من أنشطة غير مشروعة، تنطوي بلا شك علي أنشطة إجرامية تقليدية تأخذ شكلا مستحدثا .

الفئة الثانية وتسمى الجرائم السيبرانية في شبكة الإنترنت، وهنا تكون المعلومات والمواقع في شبكة الإنترنت الهدف والغاية من ارتكاب الجريمة، وبالتالي نكون بصدد أفعال إجرامية جديدة يثار التساؤل تجاهها حول مدى انطباق النصوص التقليدية القائمة عليها .

ويوجد تقسيم آخر لجرائم الإنترنت إلي قسمين :

أولهما: عندما تكون شبكة الإنترنت هي هدف الجريمة :

كمهاجمة الشبكة بالفيروسات أو إحداث أضرار بالشبكة أو بنظام التشغيل وجعل الأجهزة غير صالحة للعمل أو الاكتساح أو التشويش.

ثانيهما: عندما تكون شبكة الإنترنت هي الوسيلة المستخدمة في ارتكاب الجريمة:

وتشمل الجرائم الآتية:

١. جرائم تقع علي الأشخاص وتضم جرائم الأخلاق كالقذف، والسب، والتشهير عبر الإنترنت، والاستغلال الجنسي للأطفال، والاعتداء علي حرمة الحياة الخاصة.

٢. جرائم تقع علي الأموال وتشمل السرقة، والنصب، وغسيل الأموال، وترويج المخدرات، والاحتيال عبر الإنترنت.

٣. جرائم الإعتداء علي الملكية الفكرية، كالإعتداء علي حقوق النسخ، وبرمجيات الحاسوب، وكذلك الإعتداء علي براءات الإختراع.

فشبكة الإنترنت - بوصفها نتاج المعلوماتية - كأداة للربط والاتصال مختلف شعوب العالم، تشكل أداة لارتكاب الجريمة، أو تكون محلا لها. وذلك بإساءة استخدامها، واستغلالها علي نحو غير مشروع.

المحور الثالث : حجم الجريمة السيبرانية :

يرتبط حجم الجريمة السيبرانية ارتباطا وثيقا لا يقبل التجزئة، بتقدم الشعوب في استخدام تكنولوجيا الحاسوب والإنترنت إذ كلما زاد ذلك، كلما كان مؤشرا رئيسيا علي زيادة حجم الجريمة السيبرانية، أي علاقه هنا علاقة طردية، وقد تسبب ظهور الإنترنت في تفاقم حالات و أشكال الهجوم علي البنية التحتية.

وتعد الجريمة جزءا لا يتجزأ من سلوك الإنسان غير القويم في المجتمع بصرف النظر عن درجة ثقافته وتطوره الاقتصادي و العلمي وتسعي كل دولة جاهدة إلى وضع حدود للحد منها، ورغم ذلك فإن مؤشرات الإحصائية تفيد بزيادة ارتفاع معدلاتها خاصة بعد التقدم التقني الذي يشهده العالم ، حيث أفرز التطور التكنولوجي لاسيما في الدول المتقدمة ظهور جرائم جديدة تختلف عن الجرائم التقليدية في أطرافها ومكانها وموضوعها وأساليب ارتكابها .

ونظرا لوقوع الجرائم السيبرانية في نطاق تقنية متقدمة وأنها تتزايد يوما بعد يوم وأن مجالات وقوعها كثيرة ومخاطرها عديدة نظرا لطبيعة استخدامها في المعاملات الاقتصادية و المالية و الوطنية و الدولية والاعتماد عليها في تسيير شئون الحياة اليومية بالنسبة للأفراد والشئون العامة بالنسبة للحكومات، شأن ذلك أن يضيف أبعادا غير مسوقة علي الخسائر والأضرار التي تنجم عن هذه الجرائم ويدل علي ذلك أن الخسائر المادية الناجمة عن هذه الجرائم ضخمة جدا.

ولدى الحديث عن واقع ونطاق ظاهرة الجرائم السيبرانية يتعين ابتداء أن ندرك أنه ليس ثمة دراسات إحصائية شاملة، وليس ثمة أكثر من تقديرات تتباين دقتها تبعا لقدرة الجهات القائمة على إنجاز مثل هذه الدراسات ومدى موضوعيتها، وفي هذا النطاق فإن هناك فرقا حقيقيا بين دراسات الجهات غير الربحية وبين المؤسسات التجارية التي غالبا ما تكون دراسات موجهة لغرض ما فتجيء النتائج معبرة عن هذا التوجه وعلي الرغم من ذلك فإن تقدير حجم الجريمة السيبرانية وما يترتب عليها من خسائر ليس بالأمر اليسير.

وكما أن كثيرا من هذه الدراسات قد استقت هذه الحالات من مصادر قد لا يكون موثوقاً بها في كثير من الحالات خاصة كتلك التي يتم نشرها في الصحف و المجلات . حتى إننا نجد أن نفس الحالة قد أشار إليها أكثر من باحث بطرق مختلفة، ويصبح الوصول إلي الحقيقة الواقعة أمرا عسيرا.

وتعكس لنا الإحصائيات النادرة في مجال ظاهرة الإجرام السيبراني، حقيقة مؤلمة تكاد تكون أقرب إلى الخيال وهي أن هذه الظاهرة المستحدثة للإجرام لن تتوقف عن الازدياد وتظل من جهة أخرى تفوق بعشرين مرة نظيرتها في مجال السطو المسلح. ويقدر الخبراء أن الخسائر الناجمة عن تخريب الشبكة

المعلوماتية بأضعاف ما يسببه انهيار مبنى، أو قصف منشأة، أو تفجير جسر أو اختطاف طائرة، إذ تفيد المعلومات أن انقطاع الكوابل البحرية التي تربط أوروبا بالشرق الأوسط في نهاية شهر يناير عام ٢٠٠٨ م، والانقطاع الذي حدث بالقرب من ساحل دبي وخليج عمان خلف خسائر تقدر بمئات الملايين من الدولارات تكبدها قطاع الاتصالات والتعاملات الإلكترونية.

وعلى الرغم من عدم وجود إحصائيات دقيقة في الوطن العربي بالنسبة لحجم الجرائم السيبرانية، إلا أن هذا لا ينفي وجودها وانتشارها وخطورتها.

ويشير المسؤولون في السلطات من واقع خبراتهم إلى فن إعداد الاستبيان حول سجلات جرائم السيبرانية لا تظهر الرقم الحقيقي حول الاعتداءات. وبصفة عامة يختلف هذا الرقم باختلاف الجرائم فمنها ما يصل إلى علم السلطات العامة بصورة شبه دائمة كالاغتداء على الموظفين العموميين وجرائم الدم، ومنها ما لا يصل إلى علمها إلا نادراً كالجرائم الماسة بالعرض وتنتمي الجرائم السيبرانية إلى النوع الثاني أكثر حيث يرتفع الفارق بين الحجم الحقيقي للجريمة وبين ما هو مسجل بالإحصائيات . بل إنه يمكن القول إن الجرائم السيبرانية تعد من أكثر الجرائم التي تعاني من مشكلة الرقم الأسود. فمصطلح الهيئة المظلمة أو الجريمة السوداء أو الرقم الأسود الذي يستخدمه علماء الإجرام لكي تشير إلى الجرائم التي لم يتم الإبلاغ عنها، قد تم تطبيقه على جرائم السيبرانية التي لم تكتشف.

و ترجع صعوبة تقدير حجم الجريمة السيبرانية إلى عدة أسباب هي :

أولاً: هناك فئة قليلة من الجرائم التي تصل إلى علم السلطات، ولما كان من الممكن إعطاء وصف دقيق للأنواع المتعددة من الجرائم السيبرانية المرتكبة فإنه قد ثبت استحالة إعطاء رؤية دقيقة ومقبولة من امتداد الجريمة وأضرارها والتعدد الحالي للعدوان الإجرامي.

ثانياً : التكنولوجيا المعقدة لقدرة التخزين العالية والمدمجة في الحاسوب والسرعة التي يعمل بها من خلال إتصاله بالإنترنت، يؤكد كل ذلك صعوبة إمكان اكتشاف جرائم السيبرانية.

ثالثاً : في الغالب ليس هناك تدريب كاف للمحققين لمواجهة المشكلات البيئية المعقدة لمعالجة البيانات.

رابعاً: عدم وجود تعريف متفق عليه يقف عائقاً أمام الدراسات الإحصائية التي تهدف إلى بيان حجم هذه الجريمة، وكما أنه يخلق بدوره عقبة أخرى، إذ يجعل من المستحيل المقارنة بين الإحصائيات الصادرة عن الدول المختلفة؛ حيث إن تحديد ما يعد جريمة سيبرانية يختلف من دولة إلى أخرى.

خامسا: العديد من الضحايا ليس لديهم خطط بديلة رداً على ما تحدثه الجرائم السيبرانية؛ وذلك لإحجام الضحايا عن التبليغ عن الجرائم السيبرانية بمجرد اكتشافهم لها.

فإن هذا الإحجام يرتبط بأمرين: فبعض الضحايا لا يكون من صلاحياتهم بث المعلومات حول نشاطهم خشية الدعاية المضادة، أو الإحراج العام، أو خسارة الشهرة، أو السمعة. والبعض الآخر يخشون خسارة المستثمرين لديهم أو الثقة العامة اقتصاديا، وفي نفس الوقت تمسكا أمام الآخرين بفعالية نظام الأمن لديها.

سادسا: لا تمثل إحصاءات الجريمة السيبرانية المسجلة لدى الشرطة أساسا سليما لإجراء مقارنات عبر الوطنية، على الرغم من أن هذه الإحصاءات غالبا ما تكون هامة لرسم السياسات على المستوى الوطني. يرى ثلثي الدول أن أنظمتها غير كافية لإحصاءات الشرطة في تسجيل الجريمة السيبرانية. وترتبط سجلات الشرطة للجريمة السيبرانية مع مستويات الدولة التنموية وقدرة الشرطة المتخصصة.

فلا يمكن تقدير أفعال الإجرام السيبراني؛ وذلك بسبب ردود الأفعال السلبية لضحايا هذه الأفعال ويبقى سكوت وسلبية هؤلاء الضحايا خير معين لمرتكبي هذه الأفعال. ولقد اقترح بعض الخبراء أن هذه الأسباب ذات تأثير واضح في كشف الجرائم السيبرانية.

وخلاصة القول إن الجرائم السيبرانية هي ظاهرة إجرامية تفرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، وهي في تطور مستمر لا يتوقف، ناهيك عن أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعو الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية، والثقافية، والأمنية .

تم بحمد الله الإنتهاء من شرح المحاضرة الثالثة
مع تمنياتي بالتوفيق د. أسماء رويحي