المجرم الإلكتروني ـ الدّوافع والأنماط

د. عبير علي حسين الورفلي ـ قسم القانون – جامعة ليبيا المفتوحة

الملخّص :

لقد أفرز التّطور الهائل لتقنية المعلومات والاتصالات طائفة جديدة من الجُناة تختلف سماتهم ودوافعهم عن غيرهم من الجُناة المتعارف عليهم في علم الإجرام .

فبرزت من ذلك أهمية الدراسة التي سعت لفهم أنماط ودوافع وسمات المجرم الإلكتروني ، والتي ستُتيح لصانعي السياسات العقابية من وضع آليات وقائية وعقابية لمنع الجناة من تنفيذ انشطتهم الإجرامية ، وحماية المصالح العامة في المجتمع . ومن منطلق ذلك ظهرت عدة تساؤلات من أبرزها : ما المقصود بالمجرم الإلكتروني. وهل هناك خصائص أو سمات خاصة يتميز بها عن غيره من الجناة. وما هي أبرز الدوافع و العوامل الكامنة وراء سلوكهم الإجرامي؟ . وأمام هذه التساؤلات وباستخدام المنهج الوصفي توصلت الدراسة إلى عدة نتائج لعل من أبرزها : إن التزايد المتسارع للأنشطة المتنوعة عبر شبكات الاتصال أضحى من الطبيعي أن يُشكل المجرم الإلكتروني النسبة الأكبر بين المستخدمين لها، وإن اختلفت سماتهم ودوافعهم وأسباب ارتكاب جرائمهم والتي خلصت الدراسة أن أغلبها إما كان لأسباب تتعلق بالتفاعلات الاجتماعية للمستخدمين أو لأسباب تتعلق بعدم القدرة على ضبط النفس أو التكوين النفسي والاهتمام والمعرفة والمهارات المختلفة. كما أظهرت الدراسة أن أنماط المجرم الإلكتروني تنوعت واختلفت وفقًا للغايات المرجوة من الأنشطة الإجرامية .

ABSTRACT

The tremendous development of information and communication technology has produced a new class of offenders whose characteristics and motives differ from other offenders known in criminology. Hence the importance of the study, which sought to understand the patterns, motives, and characteristics of the cybercriminal, which will allow punitive policy makers to develop preventive and punitive mechanisms to prevent perpetrators from carrying out their criminal activities, and to protect public interests in society. Based on this, several questions arose, perhaps the most prominent of which is: What is meant by cybercriminal? Are there special features that distinguish it from other offenders? And what are the most prominent motives and factors behind their criminal behavior. Faced with these questions and using the descriptive approach, the study reached several results, perhaps the most prominent of which are: The rapid increase in various activities across communication networks has become natural for the cybercriminal to constitute the largest percentage among its users, even if their

characteristics, motives, and reasons for committing their crimes differ, and the study concluded that most of them were either For reasons related to the social interactions of users or for reasons related to the inability to self-control or psychological formation, interest, knowledge and various skills. The study also showed that the patterns of the cybercriminal varied and differed according to the desired goals of the criminal activities.

المقدمـــــــــة :

لقد صاحب نشـــوء الفضاء الإلكتروني الجديد ، تحولا نوعيًّا طـــرأ على مستويات الطلب في خدمات الإنترنت باعتبارها المنفذ التجاري القادر على تعزيز اقتصاديات البلدان وتيسير إنجاز المعاملات المالية والمصرفية والحكومية للجماهير من جهة، ومن جهة أخـــرى إخراجها عن كونها أداة للتعلم والبحث والاتصال والتواصل الاجتماعي إلى أداة للتنظيم والقيادة والتهديد، ثم إلى حاضنات مثالية لنمو الجناة ليسوا كالجناة وجرائم ليست كالجرائم، تعتمد على المعرفة التقنية والهندسة الاجتماعية والأسلحة الرقمية أمام هذا التحول والنمو المطرد للمكاسب المحتملة من ارتكاب الجرائم الإلكترونية وانخفاض احتمالية الكشف عنها والعقاب عليها شجع بعض المستخدمين لتقنية المعلومات في ارتكاب أشكال مختلفة من الجرائم الالكترونية وإن كانت الدوافع والأسباب تختلف، وهذا بدوره خلق طائفة جديدة من الجناة تختلف دوافعهم وسماتهم عن ما تعارف عليه في علم الإجرام وصفات المجرم التقليدي .

تكتسي دراسة شخصية المجرم الإلكتروني أهمية بالغة من حيث فهم سماته وأنماطه ودوافعه، والتي ستُمكّن صانعي السياسات العقابية من وضع آليات وقائية وعقابية لمنع الجناة من تنفيذ أُنشطتهم الإجرامية ، وحماية المصالح العامة في المجتمع .

إشكالية الدراســـــة:

انعكاسًا لأهمية الدراسة برزت عدّة تساؤلات من أهمها : ما المقصود بالمجرم الإلكتروني؟ وهل هناك خصائص أو سمات خاصة يتميز بها عن غيره من الجناة؟ وما هي أبرز الدوافع والعوامل الكامنة وراء سلوكهم الإجرامي؟ .

أهداف الدراسة:

تهدف الدراسة إلى ما يلي :

1- تحديد منضبط لمفهوم المجرم الإلكتروني وخصائصه .

2- فهم الأسباب الدافعة لارتكاب المجرم الإلكتروني للجريمة الإلكترونية .

3- ضبط أنماط المجرمين الإلكترونيين .

منهجية الدِّراسة :

بالنظر لطبيعة الدِّراسة التي تهدف إلى رصد مفهوم المجرم الإلكتروني و فهم دوافعه والعوامل الكامنة وراء سلوكه الإجرامي ، فقد اعتمدت الدراسة على المنهج الوصفي، وذلك من خلال وصف الظاهـــرة ومحاولة فهمها انطلاقا من العوامل المؤدية إليها، خاصّة وأن المنهج الوصفي يتعدّى حدود فهم الظاهرة إلى محاولة رصدها ومعرفة العوامل المحيطة بها وكذلك علاقتها بالمتغيرات الأخرى، وصولا إلى تحديد منضبط لأنماط المجرم الإلكتروني.

خطـــــــــــة الدراسة:

وبناءً على ما تقدم ستقسم الدراسة إلى مطلبين ، سيتناول المطلب الأول البحث في ماهية المجرم الإلكتروني وأبرز سماته، في حين يتناول المطلب الثاني الدوافع والعوامل الكامنة وراء الظاهرة الإجرامية وأنماط المجرم الإلكتروني.

المطلب الأول ـ ماهيـــــة المجرم الإلكترونـــــــي وسماته :

الفرع الأول ـ تعريف المجرم الإلكتروني:

غالبًا ما يُشـــــار إلى مرتكبي الجرائـــم الإلكترونية بشـــكل عام بالمتسللين إلا أن استخدام مصطلح " الهاكر"(1) للتعَريف بمرتكبي هـــذه الجرائـــم قد بدأ في الستينات من القرن الماضي لوصف خـــبراء البرمجيات والأجهزة ذوي النية الحسنة ، فعلى الرّغم من قدرتهم الفائقة على الاختراق إلا أنهم لا يقومون به لغرض الإيذاء وإنما نتيجة لشعورهم الذاتي بالأمـــن والحرية المطلقة في العالم الافتراضي، ومع كلّ ذلك فقد اسْتُخدِم هذا المصطلح في الأونـــة الأخيرة وبشكل كبير للإشارة إلى خبراء الحاسوب المهرة الذين يتطلعون إلى الوصول بشكل غير قانوني إلى الأنظمة والبيانات (2)،

وانطلاقا من ذلك فقد عُـــرّف المجـــرم الإلكتروني بأنّـــه : " كلّ فرد يستخدم الحاسوب أو الشبكات أو غيرها من المهارات للوصول غير المصرح به إلى الأنظمة أو الشبكات لارتكاب الجرائم" (3)، أم هـــو " كلّ من لديه القدرة على تحويل لغته إلى لغـة رقميـة وتخزينهـا، واسترجاعها باستخدام الحاسوب الإلكتروني الرقمي وملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل أو امتناع مما يُحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محليًّا أو دوليًّا "(4)، كما عرّفه بعضهم بأنه " المجرم المتخصص ذو المهارات العالية والحرفية ، وصاحب المستوى العالي من التعليم "(5) ، ويضيف أخرون بأنه : " الشّـــخص الذي يمارس شـــكلًا من أشـــكال النشاط غير القانوني باستخدام أجهزة الحاسوب أو غيرها من التقنيات الرقمية مثل الإنترنت" (6).

الفرع الثاني ـ سمات المجـــرم المعلوماتـــي : اختلف الباحثـــون في تحـــديد صفات المجرم الإلكتروني ، فذَهب بعضهم (7) إلـــى القـــول بأنهم ليســـوا دائما مجموعة من النوابغ الذين لا يمـــكن التنبؤ بهم أو معرفتهم ، فإذا كان هذا النمط موجود بالفعل إلا أن النمط السائد هو المجرم الذي تربطه بالمجني عليه صلة ما والتي غالبًا ما تكون صلة وظيفية. في حين يرى أخرون أنَّ المجرم الإلكتروني وإن كان يتميز ببعض السِّمات الخاصة إلا أنه لا يخرج في النهاية عن كونه مرتكبًا لفعل إجرامي يتطلب توقيع العقاب عليه، فكلَّ ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب سماتها من جرائم ذوي الياقات البيضاء(8)، فهم من ناحية يتمتعون بدرجة من العلم و المعرفة ما تجعلهم يتفقون بشكل عام مع مجرمي الياقات البيضاء ، وإن اختلفوا معهم في أنهم لا ينتموا إلى مهنة يرتكبون من خلالها الفعل بل إنهم أيضًا لا ينظرون إلى سلوكهم باعتباره جريمة أو فعل يتنافى مع الأخلاق (9).

وعليه يمكن القول إن المجـرم الإلكتروني يتميز بمجموعة من الخصائص لعل من أبرزها(10):

1- **المهارات التقنيـــة :** تُشـــير الغالبية العظمى من الجرائـــم الإلكترونيـــة التي تم تحليلها إلى أنها لا تنطوي على مهارات أو تقنيات معقـــدة شأنها في ذلك شأن القطاع الشـــائع من مستخدمي الحاسوب .وبصفة عامة تتسم نسبة 65 % من جميع الجرائم الإلكترونية بالسهولة في تحقيقها ، في حين تتطلب نسبة13 % مســـتوى من المهارات المتوسطة ، أما النسبة الباقية 22% تتطلب الإلمام بالمهارات التقنية بشكل دقيق للغاية(11)، كما أثبتت بعض الدراسات (12) أنّ مستويات التعليم بين مرتكبي الجريمة الإلكترونية تعتبر أعلى من مرتكبي الجرائم التقليدية ، حيث خلصت الدراســـة التي تناولت تحليل أنشطة بعض مجرمي المعلومات أنّ نسبة 28 % من المشتبه فيهم بارتكاب جريمة الإلكترونية قد " تلقوا تعليمًا جامعيًا، مقارنة مع 8 % من الجناة المتورطين في جميع الجرائم.، وعلى نحو مماثل، خلُصت الدِّراسة المعنية بالقرصنة إلى أن أكثر من نصف عدد القراصنة قد تلقوا تعليمًا جامعيًّا (13)، وعلى الرغـــم من ذلك فقد خلُصت الدراســـة التي أعدتها شركـــة (BAE Detica) أنه من المرجح أن الاكتساب الاصطناعي للمهارات التقنية وذلك من خلال الأدوات الخبيثة، ومنها (ZeuS أو Butterfly Bot) قد أدّى إلى التحول من الملامـــح التقليدية للمهارات العالية للإجرام الرقمي إلى تجمع أوسع بكثير من الأفـــراد (14).

2- **مجرم غير عنيف:** ينتمي الإجرام الإلكتروني في أغلبه إلى إجرام ذوي الياقات البيضاء ، وهذا النوع من الإجرام لا يستلزم مقدارا من العنف للقيام به (15).

3- مجرم متكّيف اجتماعيًّا : المجرم الإلكتروني ووفقا للواقع هو شخص اجتماعي بطبعه قادر على التكيف في بيئته الاجتماعية، ولا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل إن ذكاءه يدفعه للتكيف مع المجتمع، و كلما ازداد تكيفه مع المجتمع كلما زادت خطورته الإجرامية.

4- الميل إلى ارتكاب الجرائم : يتميز مرتكبو الجرائم الإلكتروني بفرط في النزعة الإجرامية والميل إلى ارتكاب الجرائم.

كما يُسهم وجود المجرم في الانترنت في جماعة إجرامية إلى التأثير في قدرته العقلية وسرعة اكتسابه المهارة التقنية التي تدفعه إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى أعلى معدلات المهارة التقنية المتمثلة في إثبات قدرته على القيام بالدور الرئيس في تنفيذ الجريمة (16) .

5- الميل إلى التقليد- :يبلغ الميل إلى التقليد أقصاه حينما يتواجد الفرد داخل الجماعة، إذ يكون عندئذٍ أسهل وأسرع انسياقا لتأثير غيره عليه ، ويظهر ذلك في مجال الجريمة الإلكترونية من خلال محاولة الفرد تقليد غيره بالمهارات الفنية التي لديه مما يؤدي لارتكابه للجريمة (17)، ولعل ذلك يرجع إلى عدم اتزان شخصية المجرم الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصّلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط به، وينتهي به الأمر إلى التقليد وارتكاب الجريمة .

6- معرفة مسرح الجريمة : فالجُناة عادة يمهدون لارتكاب جرائمهم بالتعرف على المحيط الذي تمارس فيه جرائمهم حتّى لا يواجهون بوقائع مادية من شأنها إفشال أفعالهم أم الكشف عنهم، وتُميز المعرفة بمفهومها السابق مجرمي تقنية المعلومات حيث يستطيع المجرم الإلكتروني أن يكوِّن تصورًا كاملا لجريمته ، ويرجع ذلك إلى أنّ المسرحَ الذي يمارس فيه الجريمة الإلكترونية هو نظام الحاسب الآلي ، فالفاعل يستطيع أنْ يمارسَ نشاطه على أنظمة مماثلة لتلك التي يستهدفها، وذلك قبل تنفيذ جريمته، حيث يدرك المجرمون على سبيل المثال أنّ العديد من الشركات الصغيرة والمتوسطة تستخدم أجهزة محمولة ذات الحد الأدنى من الأمان لإجراء الأعمال وقد تم تدريبها على اختراق هذه الأجهزة (18).

7- السّلطة : يتمتع أغلب مجرمي تقنية المعلومات بسلطة مباشرة أو غير مباشرة على المعلومات محل الجريمة الإلكترونية ، و تتمثل هذه السلطة في الشفرة

الخاصة بالدخـــول إلى أنظمة المعلومات ، التي تمنح الفاعل مزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحـــو أو تعديل المعلومات التي تحتوي عليها، كما يمكن أن تتمثل السلطة في الحق في استعمال الحاسب الآلي أم إجراء بعض التعاملات أم مجرد الدخول إلى الأماكن التي تحتوي على أنظمة الحاسبات الآلية، كما يمكن أن تكون السلطة التي يتمتع بها الجاني غير حقيقية، كما هو الحالة في استخدام شفرة الدخول الخاصة بشخص آخر (19).

المطلب الثاني – دوافـــع المجـــرم الإلكترونـــي وفئاتهم :

الفرع الأول : دوافع المجرم الإلكتروني-

تختلف الأسباب الكامنة وراء أية جريمة مهما كان نوعها وطبيعتها، وعلى الرغم من التطورات المتلاحقة في مجال البحوث والدراسات في علم الإجرام والجريمة وعلم النفس الجنائي؛ إلا أنّ الباحثين في هذا المجال لا زالوا يواجهون الصعوبات في تحديد العوامل الدافعة لارتكاب الجرائم بأشكالها المختلفة، فبالإضافة إلى العوامل الاجتماعية والبيئية ، ترتبط سمات الشخصية الفردية للمجرم الإلكتروني ارتباطًا وثيقًا بالسلوك غير القادر على التكيف. حيث تشير نتائج بعض الدراسات (20) إلى أن سمات الشخصية الفردية التي تُسهم في الإجرام الإلكتروني هـــي :

- السيكوباتية.
- ضعف ضبط النفس.
- المزاج الصعب.

ونظـــرًا لاختـــلاف الأســـباب الكامنـــة وراء السلوك الإجرامـــي للمجـــرم الإلكترونـــي ستُقسم العوامل إلى عوامل داخلية (فردية واجتماعية) ، وعوامل خارجية.

1- العوامل الداخلية :

1.1- الدوافع الشخصية.

1.1.1 البحث عن التقدير: يُثير اخـــتراق بعض المتسللين لنظم المعلومات الإلكترونية الشعور بالإنجاز والتحدي ، ويرتبط هذا أيضًا بحقيقة أن مجرمي المعلومات الالكترونية منافسون بطبيعتهم ، كما يبحثون من خلال أفعالهم إلى الاعتراف بهم (21). ويحبون التحدي الذي تجلبه أفعالهم، فالمجرم الإلكتروني يعتبر نشاطه الإجرامي بمثابة إنجاز ذاتي حققه وهو عمل خارق يستدعي عليه الثناء والحمد من المحيطين به في مجال الجرائم الالكترونية، فهو بلا شكّ بطل خارق (22) .

2.1.1 ضبط الذات المنخفض : ينطلق تفسير هذا الدافع من النظرية العامة في السلوك الطائش (23)، التي تؤكد أن احتمالية انخراط الأفراد في فعل إجرامي يحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض (24). وقد عرّف كل من (**جتفردستون وهيرشي**) السلوك الطائش بأنّه (كلّ فعل يقوم على القوّة والخداع لتحقيق الرغبات الذاتية) (25). وعليه فإنّ السلوك الطائش يُعدّ مظهرًا من مظاهر الضبط الذاتي المنخفض، فالدوافع لارتكاب السلوك الطائش ليست متغيرة، وذلك لأنَّ كل فرد قد يندفع لتحقيق مصالحه الشخصية بما في ذلك السلوك الطائش، فالسلوك الطائش يُعدّ عملاً سهلاً وقد يحقِق المصالح الخاصة بسرعة وسهولة من دون بذل أي جهد(26). إنّ توفر صفة الضبط الذاتي المنخفض مع وجود الفرصة لارتكاب السلوك الطائش يعدان عاملين مؤثّرين في ارتكاب السلوك الإجرامي ، وقد أرجع كلّ من جتفردستون وهيرشي الاختلاف بين المجرمين وغيرهم إلى الاختلافات في مستوى ضبط الذات(27).

وفي ذات الإطار ترى بعض الدراسات (28) أنه في ضوء تفاعل نظرية التعليم الاجتماعي والنظرية العامة للجريمة فإنّ هؤلاء الأشخاص الذين يعانون من عدم ضبط النفس قد يبحثون بنشاط عن أشخاص آخرين مماثلين لهم ويتجمعون معهم في البيئة الافتراضية بالطريقة نفسها كما هو الحال في العالم الحقيقي. ففي الفضاء السيبراني، يمكن أنْ تحدثَ هذه العملية في إطار زمني قصير بشكل كبير وبامتداد جغرافي أوسع من ذلك بكثير.

3.1.1 مواجهة التحدّي التقني : لطالما تم تحديد التحدي التقني على أنه الدافع الأكبر لارتكاب الجرائم الإلكترونية. إذ يميل مرتكبو الجرائم الالكترونية إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة، وقد تكون الرغبة في إثبات الذات وتحقيق انتصار شخصي على الأنظمة المعلوماتية من بين الدوافع الذهنية أو النمطية لارتكاب الجريمة(29) فالمجرم الإلكتروني حينما يشعر بقهره للأنظمة المعلوماتية يحقق نوعا من الانتصار النفسي الذي يدفعه للشعور بالفرح والسرور نتيجة لارتكابه هذه الافعال(30) .

4.1.1 الفضول : الفضول قوة عقلية لا تقاوم ، فهي تدفع الناس إلى معرفة المجهول والتحكم فيما لا يمكن السيطرة عليه ، أو تدمير ما تم إنشاؤه ، وإفساد التنظيم ، سواء في الأبعاد الكلية أم الدقيقة، وتعد أنظمة المعلومات بُعدًا تطور جزئيًا في ظل ديناميكيات الفضول البشري وتم تهديدها جزئيًا بواسطة هذه القوة (31) ، إن أغلب الأنشطة الإلكترونية غير القانونية هي في الواقع نتاج طلب المعرفة والسعي لفهم أنظمة

المعلومات بشكل أفضل (32)، ولتحقيق هذه الغاية يستخدم المتسللون الأجهزة والبرامج بشكل مشروع أم غير مشروع . إن هذا الشعور بالفضول والسعي للبحث عن المعلومة هو في واقع الأمر حالة نفسية مزاجية يعيشها مرتكب الجريمة الإلكترونية أثناء بحثه، كما وأن وصوله إلى معرفة جديدة ستشعره بالرضا النفسي والطمأنينة (33) .

2.1 الدوافـــــــــــع الاجتماعيـــــــــة .

1.2.1 البطـــالة : ترتبط مختلف أنواع الجرائم وفق الدراسات السوسيولوجية مباشرة بمظاهر البطالة والظروف الاقتصاديّة الصعبة، خاصّة على مستوى الفئات العمريّة الشابة التي تلجأ الى النشاط الاجرامي الإلكتروني، ولذلك يعتقد بعض الباحثين أن البطالة تُعدّ من العوامل الدافعة للمجرم الإلكتروني، لتبرير سلوكه الإجرامي من منطلق أنه يعيش في بطالة ، مما يحول دون شعوره بالندم جراء ما يقوم به بل إنّ كثيرين منهم يشعرون بالفخر والاعتزاز نتيجة ما قاموا به والذي يُعدّ إنجازًا في مسيرته المعلوماتية(34) .

2.2.1 الدافـــع المادي : نتيجة لمشكلات البطالة – والتي تمت الإشارة إليها فيما سبق - وغياب التوعية بأمن المعلومات، والقوانين الرادعـــة للجرائم الإلكترونية أصبح المجرمون الإلكترونيون يفكرون في طرائق جديدة للاحتيال والنَّصب عبر الإنترنت، ومع انتشار Script Kiddies ، والمواقع وقيامها بتعليم طرائق الاحتيال وأساليبه ، ومنتديات ومدونات المبرمجين والمطورين والمخترقين باللغة العربية، أصبح الأمر أكثر انتشارًا، وأصبح المجرمون المحليون يستهدفون المستخدمين في منازلهم، ومواقع التجارة الإلكترونية، والمصارف والشركات المصرفية، وشركات الأعمال الصغيرة نظرًا لانعدام الوعي بأمن المعلومات(35).

إنّ الحاجة إلى تحقيق الربح المادي السريع دفع المجرم الإلكتروني إلى استخدام التقنية واستغلالها في بيـــع المعلومات والجوسسة التي أسهمت في تطـــور سوق المعلومات باختراق الأنظمة والبيانات الخاصة بالدول والهيئات والمؤسسات ، وقد ذهب بعض الباحثين (36) إلى القول بأن الدافع المادي يُعدّ المُحّرك الأول والأساسي لأية جريمة إلكترونية في ظل عصر المعلومات. فحســـب بعض الدّراســـات (37) أنّ 43%من حالات الغش المعلن عنه قد بوشـــرت من أجل اختلاس أموال، 23% من أجل سرقة المعلومات، و19% مثلت أفعال إتلاف في حين أن 15% شكلت جرائم سرقة، أي: استعمال غير المشـــروع لأجل تحقـــيق منافع شخصية.

3.2.1 الانتقام : كثيرا ما يلجأ المجرم الإلكتروني إلى ارتكاب جريمته انتقامًا من ضحياه لعدة أسباب قد تكون شخصية أو مهنية كمحاولة تشويه سمعتهم من خلال نشر معلوماتهم الشخصية السرية ، أو التلاعب بالبرامج المعلوماتية الخاصة بالشركات التي كان يعمل بها المجرم بُغية إخفاء البيانات أو إتلافها.

إنّ شخصية المجرم الإلكتروني لها دور في تحديد البُعد الانتقامي لديه ، وتحديد إدراكاته للموقف الذي يحصل على مستواه الشخصي والذي يدفعه للانتقام على الرغم من أنه لا يستحق كل ما فعله، لذا فالتصورات والإدراكات التي تميز المجرم الإلكتروني هنا تدفعه لسلوك انتقامي حفاظا على ذاته التي يتصور أنها تعرضت للمساس من قِبل المجني عليه ممّا يدفعه لارتكاب السلوك الإجرامي لإعادة الاعتبار لنفسه **(38)**.

4.2.1 النشاط الروتيني : أن التغيرات في أنشطة الناس الروتينية، كاستخدام الإنترنت وشبكات التفاعل الاجتماعي مثل (الفيس بوك)، والمواقع الإلكترونية وغيرها قد خلقت فرصًا للجناة مع وجود أهداف قيّمة وسهلة في الحيز الفضائي مع غياب الرقابة ، وهذا ما ذهب إليه كلّ من كوهين و فيلسون حيث يرون أنه " من المرجح أن تحدث الجريمة عندما تتلاقى ثلاثة عوامل هي: الجاني المتحفز (Motivated offender) والهدف المناسب (suitable targets) وغياب الرقابة (absence of capable guardians)"(39).

5.2.1 **نظرية التعلم الاجتماعي :** على الرغم من ندرة الأبحاث التي تدعم دور نظرية التعلم الاجتماعي في أنشطة الجريمة الإلكترونية ، غير أنّ بعض الدراسات أظهرت وجود تفاعل بين التحكم الذاتي والتعلم الاجتماعي على عينات من طلاب المدارس الإعدادية أو الثانوية من الشباب الذين لا تزال مستويات ضبط النفس لديهم قابلة للانحراف. ومع ذلك تؤكد ذات الدراسات أنه يمكن للبالغين التأثر أيضا بالتعلم الاجتماعي والارتباط التفاضلي بالأصدقاء المنحرفين ، ويرجع ذلك أساسًا إلى زيادة تواجدهم عبر الإنترنت**(40)**.

2- الدوافع الخارجية .

1.2 الضغوط العامة : قد تلعب العوامل الاجتماعية والاقتصادية دورًا مهمًا في زيادة الجريمة الإلكترونية ، حيث يمكن أن يؤدي الضغط على مؤسسات القطاع الخاص لخفض الإنفاق وخفض مستويات التوظيف على سبيل المثال إلى وجود ثغرات في مجال الأمن، وإتاحة الفرص للكشف عن نقاط الضعف التي تعتري تكنولوجيا المعلومات والاتصالات ، فإجبار الشركات على توظيف متعاقدين من خارج الشركة أو

توظيف عمالة مؤقتة ، أو أن يصبح الموظفون في حالة استياء من خفض أجورهم ، أو الخوف من فقد الوظيفة ، كلها عوامل قد تزيد من الأعمال الإجرامية الفردية و من نفوذ الجماعات الإجرامية المنظمة عبر المطلعين على شؤون الشركة.(41)، ولقد عبرّت بعض الشركات المتخصصة في الأمن السيبراني، بأنّ أحد التهديدات المحتملة أثناء فترات التراجع الاقتصادي تتمثل في الموظفين السابقين الذين قد تم تسريحهم لوجود فائض من العمالة، كما ذكرت أن زيادة أعداد العاطلين عن العمل، أو تزايد أعداد الطلبة الخرجين الذين يعملون في وظائف غير مناسبة ولديهم مهارات حاسوبية يشكلون أحد الموارد الجديدة للجرمية المنظمة(42).

الدوافع السياسية (الإيدولوجيـــــة) : ظهر مصطلح هاكتيفيزم Hactivisme من خلال دمـــج مصطلحين هما : الهاكرز (Hakers) والنشاط (Activisme) وذلك على يد مجموعة (Cult of the Dead Cow) سنة 1994م ، ويقصد به استعمال الإنترنت لأجل أغراض ونشاطات سياسية، وعادة ما يكون دوافع هذه المجموعات (Les Activistes) سياسيًّا أو أيديولوجيًا ، ويظهر في كل أشكال الإعتداءات الإلكترونية التي تسعى إلى تعطيل المواقع التي تدعوا للعنصرية ، مع الدفاع عن مبادئ احترام الحرية الإنسانية ، فعادة ما يُعتبر أفراد ومعتنقو هذا التوجيه أنفسهم بمثابة الشخصية الروائية (روبن هود) ويطلقون على أنفسهم (روبن هود شبكة الإنترنت) فهم يتولون الدفاع عن الفئة الضعيفة داخل البيئة الإلكترونية(43) ، وتعتبر منظمة (أنونيموس Anonymos) من أشهر هذه الجماعات التي تتولى المنطلق الأيدلوجي في اعتداءتها المعلوماتية ، حيث يظهر أفرادها بأقنعة شخصية ويتولون مهمة الدفاع عن الحق في الإعلام عبر شبكة الإنترنت، ويرفعون شعارات "الحرية على شبكة الإنترنت" و " شبكة الإنترنت للجميـــع" ، وهو ما يفسرون به حمالاتهم العدائية على مختلف الأنظمـة المعلـوماتيـة التي تهـدد هـذه المبادئ كهجماتهـم سنـة 2010 م الـتي أطلقـوا عليهـا اسـم : (operation pay Back) التي استهدفـت الأنظمة المعلوماتية المخصصة لمواجهة تبادل الملفات الموسيقية ومقاطع الفيديو، وهو ما حدث ضـد الأنظمـة بالحكومـة الأمريكيـة سنة 2012م بعـد غلقها لموقـع (Mega Upload)(44)، كما قد يؤدي الهجوم السبراني بناء على دوافع سياسية إلى نتائج وخيمة تأخذها حكومات الدول المتقدمة على محمل الجدّ خاصة تلك التي تعتمد في بنيتها التحتية على المعلومات. وقد لوحظ ذلك مؤخرًا في فرنسا حيث ضغط الرئيس (إيمانويل ماكرون) من أجل تحقيق إسرائيلي في برنامج التجسس NSO ، الذي يُزعم أنه استخدم لاستهدافه و 50000 من

كبار الشخصيات، ووفقًا لتقارير الصحف أعرب ماكرون عن قلقه من إصابة هاتفه وهواتف معظم وزرائه ببرنامج Pegasus وهو برنامج قرصنة طورته شركة المراقبة الإسرائيلية NSO Group ، الذي يمكّن مشغلو البرنامج من استخراج الرسائل والصور ورسائل البريد الإلكتروني ، وسجل المكالمات وتنشيط مستويات الصوت سرا من الاجهزة المصابة. كما تعرض حزب ماكرون – أيضًا - لهجوم إلكتروني في عام 2017 عندما ننشرت أكثر من 20 ألف رسالة بريد إلكتروني تنتمي إلى حملته الانتخابية على الإنترنت(45)، وهناك عدد لا يحصى من الأمثلة الأخرى لأنواع مماثلة من الهجمات ، مثل اختراق حساب عمدة تامبا على Twitter في عام 2019 ، قبل أسبوعين من انتخابات بلدية تامبا. قام أحد القراصنة بخرق حساب بوب بوكهورن ، ونشر من خلاله مجموعة متنوعة من التغريدات المسيئة التي تحتوي على تعليقات عنصرية ، ومواد إباحية للأطفال ، والتهديد بقنبلة ضد مطار تامبا الدولي والتحذير من هجوم صاروخي باليستي وارد. وفي مارس 2018 م تم تسريب مئات رسائل WhatsApp بين النواب البريطانيين الذين يناقشون خروج بريطانيا من الاتحاد الأوروبي إلى وسائل الإعلام ، مما كشف العديد من الخلافات والأسرار(46).

3.2 الدوافع الإرهابية : قد يتحول الدافع الأيدلوجي إلى دافع جهادي من خلال شبكة الإنترنت التي يمكن أن تأوي مواقع خاصة بالجماعات الإرهابية ، حيث تمارس نشاطاتها من خلال التحريض على القتل والتمرد والعصيان المدني، وتهدف إلى ترويع المواطنين والأفراد من خلال نشرها لصور وأفلام عن كيفية صنع المتفجرات والقنابل والإشادة بأعمالها الإجرامية ، كما أنها عادة ما تستهدف النظم المعلوماتية للحكومات بغرض تعطيلها وتدميرها(47) .

كما يلعب الدافع الإرهابي دورًا بارزًا في الجريمة الإلكترونية خاصة في دول الشرق الأوسط وشمال أفريقيا، حيث يُستخدم الإنترنت من الجماعات الجهادية كوسيلة للاتصال و الهجوم على أعدائه، كما يُعدّ الصراع العربي الإسرائيلي والبطالة والمشاكل السياسية من العوامل الدافعة إلى زيادة ما يُعرف بالجهاد الإلكروني، ناهيك عن الاستخدام السياسي للأوعية الرقمية للإنترنت الاجتماعي وآخرها استخدامات شبكات التواصل الاجتماعي فيما أطلق عليه احتجاجات الربيع العربي، والذي أخذ شكلًا آخر في غسل عقول قطاعات عريضة من المستخدمين العرب في ظل غياب الوعي والعمق الفكري والممارسة السياسية بمفاهيمها الحقيقية. ونشأ ما يعرف باسم(الجهاد على الإنترنت)، أو ما أطلق عليه الغرب بـ Jihad Online بالإضافة

إلى هؤلاء الذين يطرحون أنفسهم كمستخدمين لتقنيات الاختراق لمهاجمة النظم السياسية العدائية لهم كما هو الحال في "الجيش السوري الإلكروني "، حيث يستخدم الجهاديون مواقعهم كآلة فعالة للدعاية لأفعالهم وأيضًا لاستقطاب آخرين للمساندة والاشراك في حروبهم الإلكترونية، كما تستخدم هذه المواقع في جمع التبرعات باسم الجهاد، والحصول على معلومات من المستخدمين والأعضاء، وتقوم بعض مواقع الجهاد على شبكة الإنترنت بتجميع وتحليل معلومات عن الزوار والمستخدمين لاستقطابهم(48).

4.2 دافع التجسس والمنافسة: يتضمن التجسس الإلكتروني استخدام تكنولوجيا المعلومات والاتصالات (ICT) من قبل مجرمي المعلومات أو المنظمات الإجرامية لتحقيق بعض المنافع الاقتصادية أو المكاسب الشخصية ؛ كما قد يُرتكب أيضًا من قبل جهات فاعلة حكومية ، أو مجموعات ترعاها الدولة أو تديرها الدولة ، أو جهات أخرى تعمل نيابة عن الحكومات ، وتسعى إلى الوصول غير المصرح به إلى الأنظمة والبيانات في محاولة لجمع المعلومات الاستخبارية عن أهدافها من أجل تعزيز أمنها القومي ، أو زيادة القدرة التنافسية الاقتصادية ، أو القوة العسكرية(49) .

وفي إطار ذلك استهدف برنامج التجسس (Flame) أنظمة الكمبيوتر الحكومية للولايات المتحدة حيث قام بجمع المعلومات بما في ذلك تشغيل كاميرات الويب والميكروفونات للأنظمة المصابة عن بُعد ، وأخذ لقطات شاشة لشاشات الأنظمة المصابة ،كما قام بنقل واستقبال البيانات والأوامر عبر البلوتوث وغيرها(50)، هذا واستهدف برنامج آخر يُدعى (Gauss) الحكومة لذات الأغراض حيث تم تصميمه لجمع البيانات حول اتصالات الشبكة ومحركات الأقراص وعمليات النظام والمجلدات ، وإصابة محركات الأقراص ببرامج التجسس لجمع المعلومات من الأنظمة الأخرى ، وترحيل هذه المعلومات مرة أخرى إلى خادم تحت سيطرة أولئك الذين نشروا البرامج الضارة(51). كما استخدم الجناة أداة أخـــرى للتجسس الإلكتروني تتمثل في الهندسة الاجتماعية ، حيث يخدع الجاني الهدف لإفشاء المعلومات أو القيام بعمل آخر. أسلوب الهندسة الاجتماعية الذي تم استخدامه في العديد من حوادث التجسس الإلكتروني هو التصيد بالرمح ، والذي يتضمن إرسال رسائل بريد إلكتروني تحتوي على مرفقات أو روابط مصمّمة لخداع المتلقي للنقر على المرفقات أو الروابط (52).

كما قد يلجأ الجناة إلى ارتكاب الجرائم الإلكترونية بدافع المنافسة غير العادلة حيث تقوم بعض الشركات بالهجمات الإلكترونية ضد منافسيها لتشويه سمعتها مما يُسفر عنه

تراجع المنافسين في الأسواق المالية وزيادة حصة الشركات المهاجمة . كما أنها تقوم في إطار هجومها على سرقة أسرار العمل وحقوق الملكية الفكرية ، وقد ينجم عن هذه الهجمات إنهيار اقتصادي ومالي لبعض المؤسسات الضحية(53) .

5.2 دوافع لشن الحرب الإلكترونية : ظهرت مع بداية التسعينيات من القرن الماضي دوافع إجرامية تهدف إلى شن هجمات مدمرة لأنظمة المعلومات وأُطلِقَ عليها الحرب الإلكترونية ، وقد نادى مؤيدوها من المنظمات الإجرامية السيبرانية (Legion of the Underground) إلى شن الحرب على بعض الدول انتقامًا منها لإنتهاكها لحقوق الإنسان ، وقد أدانت مجموعات آخرى من القراصنة هذا العمل العدواني ، كما دعت منظمة Cyberwafare خلال السنوات الأخيرة من القرن الحادي والعشرين إلى شن هجمات إلكترونية بهدف الدعاية للحرب الإلكترونية ، وكان أغلبها في دول شرق آسيا ، وقد سعت الدول المعنية إلى اتخاذ كافة الاحتياجات الأمنية اللازمة ومراقبة أنظمة المعلومات لديها خوفا من احتمال إساءة استخدام أجهزة الحواسيب والشبكات الرقمية**(54).**

6.2 دوافع مكافحة الحوسبة: لا شكَّ أن لثورة المعلومات الرقمية العديد من المؤيدين لما لها من مزايا إلا أن ذلك لا يمنع من وجود بعض المعارضين والمشككين في عملية تطور الحوسبة وتقنية الشبكات ؛ لذلك فقد وصف هؤلاء الهجمات التي يقوم بها القراصنة ضد تقنية المعلومات بأنها احتجاجات مبررة وعمل مشروع ضد أعداء البيئة أو المجتمع بشكل عام ، ويمثل Unabomber أحد القراصنة المعارضين لتقدم التكنولوجية المعلوماتية وقد أفاد " أن هذا التقدم أدى إلى وجود متطلبات غير مرغوب فيها من قبل الأشخاص، وأن الناس يمكن أن يُوقفوا هذا الوضع لاستعادة حياتهم الأكثر بساطة وسهولة بالقرب من الطبيعة"**(55)** ، وقد قام بعض المؤيدين لهذه النظرية في جميع انحاء العالم بتدمير عدد من أجهزة الحاسوب للاحتجاج على المجتمع الرقمي الذي بات في اعتقادهم يُسيطر على حياة الإنسان وقدراته الطبيعية، في الواقع يعتقد البعض أن هؤلاء لم يكونوا قراصنة في الفضاء السيبراني بقدر كونهم قاذفة قنابل تقليدية في مجتمع حقيقي**(56)**.

7.2 دوافع التسويق : تقوم بعض الشركات المنتجة لبرامج الحماية ضد الفيروسات إلى زرع فيروسات وبرامج مدمّرة في الحواسيب التي تم تحميلها بالبرامج الخاصة بالحماية ، والغاية من ذلك إجبار المستخدمين على شراء الإصدارات الحديثة التي تم تطويرها من ذات الشركة لبرامج مكافحة الفيروسات ؛

وذلك بهدف زيادة حصتهم في الأسواق وبيع منتجاتهم الخاصة**(57)**، ومن أبـــرز أشـــكال البرامـــج الخبيثة التي تطلقها بعض الشـــركات ما يُعرف بملفات تعريف الارتباط ، ففي حالات التســـويق الخبيث تصيب بعض مواقع الويب أجهزة حاسوب المستخدمين برموز ضارة كما تقوم بتوجيه مستخدمي الأجهزة المصابة لزيارة مواقع الويب الخاصة بهم بشكل متكرر والدفع مقابل تنظيف الحاسوب، كما يُعدّ التلاعب في متصفح الويب إحدى عمليات الاختطاف التي تتحكم في الصفحة الرئيسة ، أو حتى المتصفح بالكامل ، ويتم توجيهها فقط إلى مواقع الويب الخاصة بالجناة**(58)**.

8.2- **الدوافـــع المتعلقة بالتوظيف :** لا شك أن أنشـــطة القرصنة من الجرائم الإلكترونية ، غير أن المخترق الناجح عادة ما يحظى بالإعجاب لمهاراته وبالتالي الحصول على وظيفة جيدة الأجر كخبير حاسوب أو حتى مدير أمان. وهذا فعلا ما حظي به **روبرت تي موريس** الذي ابتكر برنامج Morris Worm في عام 1988 ، حيث أصاب حوالي 6000 جهاز حاسوب وتسبب في خسائر تراوحت بين 200 إلى 53000 ألف دولار. وفي الوقت الحالي كتب على موقع الويب الخاص به: "أنا في مختبر MIT لعلوم الحاسوب والذكاء الاصطناعي ...." **(59)**، ولا يقتصر فعل القرصـــنة على مجرد محاولة الحصول على وظيفة جيدة ، فقد يسعى المتسللون أو القراصنة إلى اختراق الحواجز الأمنية لشركات معينة بغرض الانتقام من أصحاب العمل لعدم تقديمهم عرض بالوظيفة، وهذا ما قام به Skeeve Stevens حيث ألحق أضرارًا جسيمة بشركة AUSNET ، وهي شركـة إنترنت رفضـت توظيفه، ولقد قام باختراق 1225 بطاقة ائتمان وعرض رسالة على الصفحة الرئيسة للشركة في أبريل 1995 ، قائلاً: "AUSNET شبكة مثيرة للاشمئزاز ... ويجب إغلاقها**(60)**.

9.2 دوافـــع غير واضحـــة : إذا كان لبعض الجناة دوافع لارتكاب الجريمة الإلكترونية فإن بعضهم الآخر لا تدفعه لارتكاب الجريمة أي دوافـع محددة ، ومن المستحيل معرفتها مـن خـلال وقائـع الجريمـة . ففـي قضيـة State v. Moning على سبيل المثال ، استخدم المتهم أحد حواسيب مراكز تقديم خدمات الإنترنت للوصول إلى قاعدة البيانات لإجراء استعلام عن إدانة سابقة تتعلق بالمخدرات عن أحد معارفه بعد أن طبع نسخة من المعلومات ، سلم الضحية النسخة المطبوعة. وبهذا أصبح الضحية على علم بسلوك الجاني وأبلغ عن وصوله غير المصرح به ، ولم تتضح الدوافع الرئيسة للجاني**(61)**.

من خلال ما تقدم يمكن القول أن دوافع المجرم الإلكتروني تختلف وفقا للعوامل المحيطة به بين دفعٍ وجذبٍ . فتارةً يندفع نحو الجريمة لأسباب شخصية كعدم ضبط النفس أو المغالاة في حبّ النفس والظهور أمام غيره بالمهارة والتفوق المعرفي بتقنية المعلومات ، أو لأسباب تتعلق بتحقيق فائدة سياسية أو مادية أو اقتصادية .

الفرع الثاني ــ أنماط المجرم الإلكتروني

بوجه عام يمكن القول إن المجرم الإلكتروني الذي أطلق عليه اسم المتسلل ينقسم في البيئة الافتراضية إلى عدة أقسام لعل من أبرزها:

1 – الهاكـــــرز hackers : أُطِلقت كلمة هاكر على مجموعة من المبرمجين الأذكياء الذين كانوا يتحدون الأنظمة المختلفة ويحاولون اقتحامها، وليس بالضرورة أن يكون ذلك بقصد ارتكاب جريمة ، فهم يرون أن نجاحهم في الاختراق يُعتبر نجاحًا لقدراتهم ومهارتهم، إلا أن القانون يرى خلاف ذلك حيث عدّهم جناة لدخولهم إلى أنظمة غير مصرح بها. ومن المعروف أنهم عند اقتحامهم لهذه الأنظمة هم في الواقع يمتحنون قدراتهم دون أن يفصحوا عن هُوياتهم الحقيقية، ولقد استغل بعظهم هذه القدرات لارتكاب أفعال إجرامية كتدمير المعلومات ومسحها أو التجسس و سرقة المعلومات أو الأموال **(62)**.ولذلك فقد ذهبت بعض الشركات مثل مايكروسوفت لحماية أنظمتها إلى تعيين هؤلاء الهاكرز بمرتبات مُجزية تكون مهمتهم محاولة اختراق أنظمتها المختلفة والعثور على أماكن الضعف فيها، واقتراح سبل الوقاية اللازمة من الأضرار التي قد يتسبب فيها قراصنة الحاسوب، وبهذه الطريقة اكتسب الهاكر الكثير من الإيجابيات. إلا أن المسمى الأساسي ظل واحدًا ، وقد أصبحت كلمة **"هاكر"** تُطلق على المبرمج ذي القدرات الخاصة التي يستخدمها في الصواب كما يمكن أن يستخدامها في الخطأ**(63)**. وينقسم الهاكرز إلى ثلاث فئات هي -

1.1 قراصنة القبعة البيضاء White Hat Hacker هو كل مخترق للحواسيب بصورة أخلاقية و يمكن القول بأنه كلّ خبير بأمن الحواسيب ونظم المعلومات، ويختص غالبًا بالاختراق الاختباري بصورة ممنهجة لضمان أمن نظم المعلومات في الشركات أو الهيئات، وهذا النوع من القرصنة يُطلق عليه في البيئة الرقمية أو تقنية المعلومات بالـقرصنة الأخلاقية التي تنصب على الأشخاص الذين تتعارض قِيَمهم الأخلاقية مع انتهاك أنظمة الحواسيب الأخرى حيث يركز القرصان ذو القبعة البيضاء على حماية الأنظمة (64). ومن المعروف أن هؤلاء المخترقين قد يعملون منفردين أو في جماعات كما هو الحال في جماعة النمور أو الفرق الحمراء(65).

2.1 قراصنة القبعة السوداء Black hat hacker : هم مجرمون يقتحمون شبكات الحاسوب لأغراض إجرامية، فقد يقومون بإصدار برامج ضارة تعمل على تدمير الملفات أو احتجاز أجهزة الحاسوب كرهائن أو سرقة كلمات المرور وأرقام بطاقات الائتمان والمعلومات الشخصية الأخرى، وعلى الرغم من أن القرصنة قد أصبحت أداة رئيسة لجمع المعلومات الاستخبارية للحكومات ، إلا أنه لا يزال من الشائع أن يعمل قرصان القبعة السوداء بمفرده أو مع منظمات إجرامية أخرى لأغراض مادية .

ويُمثل Wanna Cry ransomware أحد البرامج الضارة الذي تم إصداره في مايو 2017 حيث تمكن في غضون الأسبوعين الأولين من إطلاقه ، على إصابة ما يقارب عن 400.000 جهاز حاسوب في 150 دولة (66)، وتُعدّ القرصنة Black Hat مشكلة عالمية ، كما أنها تمثل إحدى أكبر التحديات التي تُواجهها أجهزة تطبيق القانون خاصة أن هؤلاء القراصنة غالبًا ما يتركون أدلة وراءهم (67).

3.1 قراصنة القبعات الرمادية Gray Hat Hacker : هم أشخاص غامضون يقفون في منطقة محايدة بين قراصنة القبعة البيضاء والسوداء ، فقد تجدهم في بعض الأحيان يُقدمون المساعدة في حماية أمن الشبكات والمعلومات وفي أحيان أخرى تكون الشبكة المعلوماتية ضحيتهم في الواقع هم لا يقومون بالاختراق لأغراض خبيثة أو لمصلحة شخصية، بل لزيادة خبرتهم في الاختراق واكتشاف الثغرات الأمنية ، ويرى كثيرون أن عالم أمـــن تكنولوجيا المعلومات هو عالم أبيض وأسود، ومع ذلك فإن قراصنة القبعة الرمادية يلعبون دورًا بارزًا في البيئة الأمنية، ولعل أكثر الأمثلة شيوعًا على ذلك ما يقدمه قرصان القبعة الرمادية حيث إنه وباختراقه لأنظمة شبكة المعلومات يستطيع كشف الثغرات الأمنية وبالتالي نشر الوعي العام بوجود هذه المشكلة؛ لذلك يرى الخبراء أن الاختلاف بين قرصان القبعة البيضاء وقرصان القبعة الرمادية هو أن الأخير يستغل الثغرة علنًا ، مما يسمح لقراصنة القبعة السوداء بالاستفادة منها، وعلى النقيض من ذلك فإنْ قرصان القبعة البيضاء قد يقوم بنفس النشاط إلا أنه يكون لغرض تنبيه الشركة بتلك الثغرات، دون الإعلان عن النتائج (68).

2- الكراكـــــر cracker : هو مصطـــلح قديم يُســـــتخدم لوصف شخص ما اخترق أنظمة الحاسوب ، أو تجاوز كلمات المرور أو التراخيص في برامج الحاسوب، وذلك لأغراض تتعلق بتحقيق الربح أو التدمير أو مجرد التحدي، وقد عرّف بعضهم الكراكر بأنه " كل فرد يحاول الوصول إلى أنظمة الحاسوب دون إذن، وهم غالبًا ما يكونون ضارين على عكس المتسللين ولديهم العديد من الوسائل المتاحة لاقتحام أنظمة

الحواسيب." (69)، عادة ما يستفيد هؤلاء الأشخاص من مهاراتهم في نُظم المعلومات للحصول على منافع مالية أو بغرض إلحاق أضرار بالأفراد و المنظمات. إن هجوم الكراكر على الموقع الإلكترونية قد تتنوع بين الضربات الصغيرة و بين الإرهاب الإلكتروني ضد الحكومات . في الواقع أن هـــؤلاء هم جنود الحرب المعلوماتية وأعدادهم تتزايد باستمرار مع وتيرة الحرب الاقتصادية للمعلومات ، وتجدر الإشارة هنا أن الساحة العربية لا تخلو من المخترقين الإلكترونيين (الكـــراكر)، بل إن الساحة العربية تشهد صراعاتٍ إلكترونية تأخذ أغلبها صور هجمات على المحتوى أكثر منها على أنظمة التشغيل العربي الإلكتروني، كما تتسم الممارسات العربية في الاختراق الإلكتروني على الإنترنت بطبيعة فردية، أو بأسلوب مجموعات العمل الصغيرة تعمل بأساليب أو باسم وشعارات المجموعات العالمية الأكثر خطورة على الإنترنت، كما أنّ النشاط العربي في هذا الشأن، بات يأخذ منحىً سياسيًا كمهاجمة بعض الأنظمة السياسية الحاكمة والمواقع الحكومية، أو دينية، واستخدام رسائل البريد الإلكترونـــي ذات المضمون الديني للاستيلاء على بيانات شخصية أو فتـــح أبواب خلفية في أنظمة تشغيل الحواسيب أو غير ذلك من الأساليب، بالإضافة إلى مناحي عقائدية وإرهابية وإجرامية ذات طبيعة اقتصادية (70).

3- مخـــترقـــو شـــبكات الاتصال PHREAKER(71) : ينطـــبق بشكل خاص على الأفراد المتخصصين في اختراق الهواتف والشبكات الدولية، وظيفتهم الرئيسة هي التنصت على الهواتف عن طريق قطع بعض خطوط الشبكة. غالبًا ما تسمح لهم هذه المهارات بالهروب من أجهزة تطبيق القانون، ويكون هدفهم من ذلك إما المتعة أو كسب الأموال، فالعديد منهم هم مجرمون في الواقع ، لأنهم يقتطعون باختراقهم تكلفة فواتير هواتفهم ويستمرون في سرقة الشبكات بطريقة أكثر هدوءًا، ومع ظهور الإنترنت وانخفاض تكلفة الاتصالات بات هذا الفعل يتناقص، على الرغم من محاولة هؤلاء المخادعين لمواجهة تحدي اختراق شبكات الهواتف(72).

4- **مطـــاردو الانترنت** : **Cyberstalking**: يتم تعريف المطـــاردة عبر الإنترنت على أنها اتصال متكـــرر غير مرغوب فيه، أو مضايقة من قبل شخص ما من خلال الاتصالات الإلكترونيـــة عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي أو الرسائل النصية، لقد أضحت المطاردة عبر الإنترنت من المشكلات العالمية، فوفقًا لمركز **بيو** للأبحاث ، تعرض 41٪ من الأمريكيين للمضايقة من قبل مطارد عبر الإنترنت ، كما شهد ما يقارب (66٪) من الأشخاص حول العالم لمضايقات عبر

الإنترنت (73)، وتشمل خصائص هــذه المضايقات القذف والتشهير والتهديدات ورسائل البريد الإلكتروني المخترقة وســرقة الهُوية، وفي الواقع أن تطور الأجهزة الرقمية وإنشاء منصات الوسائط الاجتماعية ترتّب عنها ارتفاع حالات المطاردة عبر الإنترنت بشكل كبير والتي غالبًا ما يؤدي نموها إلى تسهيل العثور على الهوية الرقمية لشخص ما وكشفها بما في ذلك موقعه واهتماماته وشبكاته الشخصية، فيقوم الملاحقون عبر الإنترنت بالاتصال بالضحايا أو متابعتهم بشكل متكرر عبر الإنترنت، كما يُمكن أن تتضمن المطاردة عبر الإنترنت أفعالًا خفية ، مثل التعليق العلني على محادثات وسائل التواصل الاجتماعي ، أو الأعمال العدوانية العلنية ، مثل: إرسال رسائل تهديد للضحية أو لعائلتها وأصدقائها. وقد أظهرتِ الدِّراسات أن أغلب ضحايا المطاردة عبر الإنترنت هم من الإناث، ففي الولايات المتحدة ، "تمت مطاردة امرأة واحدة من كلّ 12 امــرأة ورجــل واحــد من كلّ 45 رجلًا عبر الإنترنت في وقت ما من حياتهم."(74).

كما تتسم إجراءات ضبط المطارد عبر الإنترنت بالصعوبة؛ وذلك لكون المطارد يقوم بجمع المعلومات حول ضحيته بشكل خفي كما أنه لا توجد آثار مرئية يسهل ملاحقتها على وسائل التواصل الاجتماعي ، خاصة أنّ بعضَ المطاردين قد يكونون من المقربين للضحية كأصدقاء سابقين أو أزواج منفصلين ، أو حتى أزواج يستخدمون تقنيات المطاردة عبر الانترنت لتحقيق أهدافٍ واقعيةٍ.

5- الحاقـــــدون أو The Insider: يغلب على هـــذه الطائفة عدم توفـــر أهداف وأغراض الجريمة المتوفرة لدى الفئات المتقدمة، فهم لا يسعون إلى اثبات القدرات التقنية أو المهارات الحاسوبية، ولا إلى مكاسب مادية أو سياسية، بل هم في الواقع مدفُعون برغبات الانتقام والثأر ضد أصحاب العمل السابقين، أو تصرفات المنشأة المعنية معهم عندما لا يكونون موظفين فيها، وهـــم بهذا ينقســمون إما إلى مستخدمين للنظام بوصفهم موظفين أم مشتركين أم علـــى علاقة بالنظام محل الجريمة، وإلى غرباء عن النظام يتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم (75)، في الحقيقة أن أعضاء هذه الفئة لا يتسمون بالمعرفة التقنية الاحترافية، ومع ذلك تجدهم يسعون للوصول إلى كافة عناصر المعرفة المتعلقة بأفعالهم التي يرغبون في ارتكابها، وتغلب على أنشطتهم من الناحية التقنية استخدام البرامج الضارة وتخريب النظام أو إتلاف المعطيات ، أو نشاط إنكار الخدمة وتعطيل النظام ، أو الموقع المستهدف إن كان من مواقع الإنترنت(76). هذا وتتميز أنشطتهم بسهولة ضبطها والكشف عنها لتوفر الظروف والعوامل المساعدة لذلك. وعلى الرغم من عدم خطورة هذه الفئة من

المجرمين مقارنة بالفئات المتقدمة؛ إلا ان ذلك لا يمنع من أن تكون الأضرار التي تنجم عن أنشطتهم جسيمة وقد تُلحق خسائر فادحة بالمؤسسات المستهدفة(77).

6- مجرمو التشفير Cypher Punks (78): يُقصد بالتشفير في الأمن الإلكتروني تحويل البيانات من تنسيق قابل للقراءة إلى تنسيق مشفّر. حيث لا يمكن قراءة البيانات المشفرة أو معالجتها إلا بعد فكّ تشفيرها، ويُعدُّ التشفير من أيسر الطرائق وأهمها لضمان عدم سرقة معلومات نظام الحاسوب أو قراءتها من جانب شخص يريد استخدامها لأغراض ضارة، كما يُستخدم تشفير البيانات لتأمينها على نطاق واسع من قبل المستخدمين الأفراد والشركات الكبيرة لحماية معلومات المستخدم المرسلة بين المستعرض والخادم، وقد تشمل تلك المعلومات أي شيء من بيانات الدفع إلى المعلومات الشخصية، ويتم استخدام برنامج تشفير البيانات المعروف أيضًا باسم خوارزمية التشفير أو التشفير فحسب، لتطوير مخطط تشفير لا يمكن اختراقه نظريًّا إلا بقوة حوسبية هائلة، ولذلك تسعى هذه الفئة من المجرمين إلى محاولة فكّ تشفير البيانات إما رغبة منها لتحدي جدار الحماية وفكّ التشفير عن البرامج والبيانات أو لسرقة البيانات بسبب رغبة جهات ضارة في بيع المعلومات أو استخدامها في سرقة الهوية، إذ يمكن لمجرمي التشفير فكّ التشفير عن البيانات لسرقة معلومات كافية، يمكنهم استخدامها للوصول إلى حسابات آمنة أو إصدار بطاقات ائتمان باستخدام اسم الضحية أو استخدام هوية الضحية بطريقة أخرى لصالح أنفسهم، كما يمكن لمجرمي التشفير إرسال فيروسات برامج الفدية (79) ، حيث يتم تشفير البيانات الخاصة بالضحية **أو** نظام التشغيل نفسه ، وذلك بغرض الحصول على منافع مادية مقابل فك تشفير البيانات، كما تستخدم المنظمات الإجرامية بشكل متزايد أدوات الاتصال المشفرة وتواصل البحث عن طرائق الاستفادة من أحدث التقنيات للتهرب من التحقيقات. وتعتمد السلطات القضائية وأجهزة تنفيذ القانون بشكل متزايد على البيانات الرقمية لمتابعة هذه التحقيقات، وغالبًا ما تكون هذه البيانات مشفرة ويصعب الوصول إليها بشكل قانوني، يمنح التشفير المجرمين والإرهابيين أداة قوية لإخفاء أنشطتهم الإجرامية التي يقومون بها بمنأى عن أجهزة تطبيق القانون، حيث يجعل من المستحيل على هذه الأجهزة الحصول على الأدلة اللازمة للإدانة أو المعلومات الاستخباراتية الحيوية التي تساعدهم في التحقيقات الجنائية. كما يؤدي التشفير إلى إحباط كلّ عمليات اعتراض الاتصالات ، التي لعبت دورًا مهمًا في تجنب الهجمات الإرهابية وفي جمع المعلومات حول تهديدات محتملة عبر الوطنية بما في ذلك الإرهاب وتهريب المخدرات والجريمة المنظمة(80)، لمساعدة

الممارسين على التعامل مع هذه التحديات ، نشـــرت Eurojust و Europol في يوليو 2021م التقرير الثالث لوظيفة المرصد حول التشفير، يشارك التقرير رؤى حول التشفير في سياق القضايا العابرة للحدود مع التركيز على عنصرين رئيسين هما : الحالات التي يكون فيها فكّ التشفير ينصب على الأداة التي يستخدمها المجرمون والتي تُعدّ المحور الرئيس للتحقيقات الجنائية ، وعندما تكون الاتصالات المشفرة بين المجرمين مطلوبة كدليل في التحقيقات، كما يكشف التقرير – أيضًا - الحاجة إلى إيجاد وسائل قانونية لفكّ تشفير الاتصالات الإلكترونية ، وقَبول الأدلة التي تم الحصول عليها من الأجهزة التي تم فكّ تشفيرها ، ومشاركة هذه البيانات مع أجهزة تنفيذ القانون الأخرى في سياق القضايا المتعلقة بالجرائم العابرة للحدود **(81)**.

7- لصـــــوص الهُويـــــة Identity Theft (82): يُستخدم مصطلح سرقة الهوية للتعبير عن الأشخاص الذي ينتحلون صفة شخصًا آخر بهـــدف تحقيق مكاسب مادية أو غير ذلك، وعندما يتم ذلك عبر الانترنت يُطلق عليه سرقة الهوية عبر الإنترنت، حيث يسعى المجرم في هذه الفئة الحصول على البيانات الشخصية الخاصة بالضحية ســـــواء من بطاقات الائتمان أم معلومات رخصة القيادة بغرض استخدامها للحصـول على منافع شخصية **(83)**، وتُعدّ سرقة الهوية من أقدم الجرائم الإلكترونية ، وقد اكتسبت مكانةً بـــارزةً خلال الســـنوات الأولى للإنترنت ، حيث استفاد هـــؤلاء المجرمـــون من تقنيات القرصنة الأســـاسية قبل تعديل البيانات والاستفادة من الاحتيال الأساسي في الهوية للكشف عن المعلومات المطلوبة، كما تقدمت هذه الممارسة في النطاق والتقنية بسبب التقدم في الحوسبة ، كما يمكن للعديد من لصوص الهوية اختراق قاعدة بيانات الحكومات والشركات لسرقة عدد كبير من الهويات والمعلومات الشخصية**(84)**. فوفقا لشبكة Digital journal ، ينفـق الأمريكيون أكثر من 3,5 مليار دولار سنويًا على خدمات حماية الهوية ، كما أكّد مكتب إحصائيات وزارة العدل الأمريكية أن 17.6 مليون مواطن أمريكي قد تعرضوا لسرقة الهوية خلال سنة 2014م ، كما تسببت سرقة الهوية في ضياع 16 مليار دولار من 15 مليون مستخدم خلال سنة 2017م**(85)**. في الواقع أن أسباب ازدياد معدلات سرقة الهوية بدرجة كبيرة يرجع في الأساس لاستعداد المستخدمين لمشاركة بياناتهم الشخصية عبر الإنترنت، سواء كان ذلك عبر مواقع شبكات التواصل الاجتماعي أم عبر تقديم هذه المعلومات إلى المصارف أم شركات البيع بالتجزئة عبر الإنترنت.

8- صغار السن kiddies: طائفة صغار السِّن ، أو كما يسميهم بعضهم ، صغار نوابغ المعلوماتية ، ويصفهم بأنهم " الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية"(86) فإنّ من بينهم في الحقيقة فئة لا تزال دون سنّ الأهلية مولعين بالحوسبة والاتصال، وقد تعددت أوصافهم في الدِّراسات الاستطلاعية والمسحية ، وشاع في نطاق الدّراسات الإعلامية والتقنية وصفهم بمصطلح المتلعثمين الدّال حسب تعبير الأستاذ توم فورستر، على " الصغار المتحمسين للحاسوب، بشعور من البهجة، دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب"(87). ويثير مجرمو الحوسبة عن هذه الطائفة جدلا واسعا، ففي الوقت الذي كَثُر الحديث فيه عن مخاطر هذه الفئة على الأقل بمواصلتها العبث بالحواسيب ، ظهرت دراسات ومؤلفات تدافع عن هذه الفئة لتخرجها من دائرة الإجرام إلى دائرة العبث ، وأحيانا البطولة (88) وعلى الرغم من افتقار هذه الفئة إلى خبرة القراصنة، إلا أنهم يُشكلون خطرًا على الشركات الصغيرة حيث تُسبب البرامج الضارة التي يرسلها هؤلاء المجرمون أضرارًا كبيرة لهذه الشركات ، ومن أبرز الأمثلة على ذلك ما قام به بعض هؤلاء العابثين في مايو 2000م ، عندما قاموا بإرسال رسالة من البريد إلكتروني بعنوان "ILOVEYOU" تم حقنها ببرنامج فايروس الدودة الضارة، وقد تسبب هذا الاختراق اليسير في خسائر تُقدر بعشرات المليارات من الدولارات في الإنتاجية والبيانات ، حتى أنه قد تم إغلاق أنظمة البريد الإلكتروني مؤقتًا للبنتاغون والبرلمان البريطاني ووكالة المخابرات المركزية الأمريكية(89).

الخاتمة :

صحيح أنّ شبكات الاتصال الإلكتروني وحدها لا تصنع الإجرام ، وأن الجريمة هي نتاج إرادة وأدوات يحرّكها دافع الجناة لارتكاب أنشطة إلكترونية غير قانونية أو غير أخلاقية، ولذلك فإنّ تكنولوجيا الاتصالات والمعلومات والإنترنت إنما هي وسيلة تتيح مجموعة غير متناهية من الأدوات المجردة، والانتقاء من هذه الأدوات مرهون بمحصلة النتائج المستهدفة ونتائج استخداماتها مرتبط بالممارسة الإلكترونية نفسها للمستخدمين إنّ فهم شخصية المجرم الإلكتروني تقتضي النظر إليها نظرة شمولية تُحيط بتباين الأصناف ووقوع كلّ صنف أمام مجموعة من المؤثرات الداخلية والخارجية – التي ذُكرت آنفًا - ، ومدى تفاعلها مع بعضها البعض لتدفع المجرم إلى ارتكاب جرائمه، وإن كانت حتمية العلاقة بين هذه العوامل والجريمة ليست مطلقة، بل تُنبئ عن الاحتمال فقط قد يتحقق بارتكاب الفعل وقد لا يقع إطلاقًا.

نعتقد أن المقاربة التي يجب أن تُعتمد أمام أنماط المجرم الإلكتروني ومدى خطورته هي تغليب دور التدابير العلاجية والوقائية خاصة لفئة صغار السن ، أما باقي الفئات فردعها يبقى مرهونا بمستوى وقدرة الأجهزة القضائية والتشريعية على مواكبة المستوى التقني والأساليب الإجرامية المبتكرة.

الهوامـــــــش:

[1] - يعود الفضل في استخدام مصطلح الهاكر إلى كاتب الخيال العلمي الكندي وليم جيسون وعادة ما يطلق لفظ الهاكر الأمن لمستخدم الحاسوب الذي يكون غرضه الدخول غير المصرح به في أنظمة الحاسوب لإرضاء الشعور الداخلي بالنجاح . ينظر في ذلك .

[2] Dr.Yusuf Perwej, Syed Qamar Abbas, Jai Pratap Dixit, Dr. Nikhat Akhtar, Anurag Kumar Jaiswal. A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, 2021, 9 (12), pp.669-710.

[3] Wesley Chai - Linda Rosencrance,hacker, May 2021.Available at; https://www.techtarget.com/searchsecurity/definition/hacker

[4] خالد ممدوح إبراهيم ، جرائم المعلوماتية ، الإسكندرية : دار الفكر الجامعي ، 2009م، ص 26 . وينظر أيضًا أيمن عبد الله فكري ، جرائم نظم المعلومات ، القاهرة: دار الجامعة الجديدة للنشر ، 2007م ، 74 .

[5] مصطفى يوسف كافي ، جرائم الفساد وغسيل الأموال ، والإرهاب الإلكتروني ، المعلوماتية ، الأردن: مكتبة المجمع العربي للنشر والتوزيع، الطبعة الأولى ، 2014م ص 165 .

[6] John Sammons, Michael Cross, in The Basics of Cyber Safety, 2017, Available at; https://www.sciencedirect.com/topics/computer-science/cybercriminals

[7] Cornwall (Hugo), Datatheft, Computer Fraud, Industrial Espionage and Information Crime, Heinemann: London 1987, p 134. see also, Matthew Edwards,Emma Williams,Claudia Peersman,Awais Rashid,Characterising Cybercriminals: A Review, university of bristol , bristol cyber security group,February 16, 2022, pp 9 , 14 .

[8] جرائم ذوي الياقات البيضاء مصطلح يطلق على الجرائم غير العنيفة والمرتكبة لدوافع مالية من قبل رجال الأعمال وأصحاب النفوذ. في علم الجريمة عرّف المتخصص بعلم الاجتماع إدوين سذرلاند المصطلح لأول مرة في عام 1939 بأنه " جريمة يرتكبها فرد من ذوي الطبقات الاجتماعية العليا وله مكانة مرموقة في نطاق مهنته ، وتشمل جرائم ذوي الياقات البيضاء :الاحتيال والرشوة والاختلاس والجرائم الإلكترونية وانتهاك حقوق الطبع وغسيل الأموال وانتحال الشخصية والتزييف". ينظر لمزيد من المعلومات :

Edwin Hardin Sutherland, white collar criminality, American sociological review, vol 5, Feb, 1940, number 1, pp4, 5.

[9] Suthreland (Edwin H) , « White-collar criminality", Geis (Gilbert) (ed), in White collar criminal: The Offender in Business and the Professions, Atherton press, 1968.

10 Parker (Donn B) Fighting computercrime – A new Farmework for Protecting Information, john Wiley & sons, Inc., 1998 .p 136

[11] Report on Attack Kits and Malicious Websites; Fortinet, 2013. Fortinet 2013 Cybercrime Report – Cybercriminals Today Mirror Legitimate Business Processes; and Trend Micro, 2012.

12ينظر مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، دراسة شاملة عن الجريمة السيبرانية ، 2013م ، منشورات الأمم المتحدة ، ص 50 وما بعدها .

13 وجدت الدراسة المعنية بالقرصنة HPP على سبيل المثال :أن المهارات الفنية لدى القراصنة تعتبر كالتالي : مستوى منخفض (21%) مستوى متوسط (32%) مستوى عالي (22%) ، مستوى خبير متمرس (24%) .ينظر لمزيد من المعلومات . المرجع السابق نفسه .

14 Camryn Mottl, Why are Cyber Criminals More Likely to Target Small to Midsize Businesses?, Aug 19, 2016 9:00:00 AM, Available at: https://www.coretech.us/blog/why-criminals-target-small-businesses

15طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني لحماية المعلومات، الإسكندرية: دار الجامعة الجديدة للنشر ، 2009 ، ص176 وما بعدها.

16 أيمن عبد الحفيظ، الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية، (د ب)، (د ن)، ص34 .

17 محمد الحبشة ، إشكالية إثبات الجرائم الإلكترونية؛ وعقوبة اختراق المواقع الالكترونية وماهي آليات اثبات الجرائم المعلوماتية طبقا للقانون، نشرت بتاريخ 9 مايو، 2020م على الموقع الالكتروني: https://ae.linkedin.com/pulse/

18 أيمن عبد الحفيظ ، المرجع السابق ، ص34 .

19 شيخة حسين الزهراني، الطبيعة القانونية للهجوم السيبراني وخصائصه، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 1 ، يونيو 2020م ، ص 781 وما بعدها .

20 ذياب موسى البداينة ، الجرائم الإلكترونية :المفهوم والأسباب، ورقة مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية 2014م، عمان –الاردن، منشور على الموقع الالكتروني :

https://www.researchgate.net/publication/328064682

21 Camryn Mottl, 6 Motivations of Cyber Criminals, Mar 3, 2022 11:15:00 AM. Available at: https://www.coretech.us/blog/6-motivations-of-cyber-criminals

22 Xingan Li, A Review of Motivations of Illegal Cyber Activities. Criminology & Social Integration Journal Vol. 25 No. 1 2017, .p112 .

23 هي إحدى النظريات العامة للجريمة والتي قال بها ميشيل جتفردسون وترافيس هيرشي، والتي تعني أن التنشئة غير المناسبة، وغير المكتملة للفرد، تؤدي إلى ضبط الذات المنخفض، وهذا يؤدي إلى السلوك الطائش، وغيره من الأفعال المحظورة.

24 Gottfredson, M. R. and Hirschi, T. (1990). A General Theory of Crime, California: Stanford University Press, p11.

25 المرجع السابق نفسه.

26 ذياب البداينة، وأخرين ، العلاقة بين مستوى ضبط الذات المنخفض والسلوك الطائش لدى طلبة المدارس في الأردن .مجلة العلوم الإنسانية والاجتماعية، جامعة الشارقة ، العدد 16 ، سنة 2010م ، ص 23 وما بعدها .

27 اقتحم متسلل يبلغ من العمر 17 عامًا موقعًا رسميًا للموارد البشرية ، وشوه الصفحة الرئيسية للموقع، كما قام بنسخ القرص الصلب للخادم ، ودمر قرصًا كبيرًا يحتوي على كمية كبيرة من البيانات. كما قام شخص أخر وخلال إجازته المرضية في المنزل ، بالتسلل إلى مواقع الويب الخاصة بالمخترقين ، وقام بتحميل بعض برامج القرصنة. ثم وجد بعض المواقع على شبكة الإنترنت بها ثغرات أمنية وتطفل عليها. في البداية ، أرسل رسائل إلى مديري مواقع الويب هذه ، يخبرهم فيها أن مواقع الويب الخاصة بهم بها ثغرات. دون تلقي أي رد ، غضب وقام بتشويه بعض مواقع الويب هذه. لمزيد من المعلومات ينظر

Yan, W. and Zhang, Y. 6 November 2001. Xinjiang's First Cybercrime 17-Year-Old Hacker Arrested,Beijing Youth Daily. Available at: https://www.sixthtone.com/users/1010167/beijing+youth-daily

28 نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الأردن، بدون سنة ، ص44 - 45

29 عادل يوسف عبد النبي الشكري ، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، مجلد 1 ، العدد 7 ، 2008م ، ص 111 - 132 .

30 قام أحد القراصنة بإنشاء برنامج حصان طروادة يسمى IPXSRV ، وسيطر على 60.000 جهاز كمبيوتر. لقد أنشأ شبكة بوت نت ، والتي كانت عبارة عن "مجموعة من أجهزة الكمبيوتر المخترقة التي يتحكم فيها نفس الدخيل ، وغالبًا [باستخدام] برامج التحكم عن بعد أو خدمات محادثة الإنترنت . حيث قام المتسلل بلشن هجوم رفض الخدمة ضد موقع ويب للموسيقى لمدة ثلاثة أشهر قبل أن تكتشفه الشرطة، وقد كشفت التحقيقات أن المتسلل كان يبحث عن فرصة لتجربة قوة برنامج طروادة الخاص به ، واختار موقع الويب هذا كهدف لهجوم رفض الخدمة. ونتيجة لذلك ، تم تعطيل الموقع لمدة ثلاثة أشهر . لمزيد من المعلومات ينظر .

NTOKO NTONGA RENE,UNDERSTANDING CYBER CRIMES AS PRACTICE IN CAMEROON, Article published on the website:
file:///C:/Documents%20and%20Settings/New%20user/My%20Documents/Downloads/SSRN-id3835231.pdf.

31 مراجعة لدوافع الأنشطة السيبرانية غير القانونية ، مرجع سابق ، ص 112 وما بعدها .

32 أفاد كلّ من جوردان وتايلور في أن دافع كيفن ميتنيك ، أشهر المتسللين على الإطلاق ، هو اكتساب المعرفة والسعي إلى فهم أفضل لأنظمة المعلومات. لمزيد من المعلومات ينظر .

Jordan, T. and Taylor, P. A. "Sociology of Hackers", Sociological Review, vol 46 number 4, 1998 p.81

33 صابر بحري وآخر ، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية ، مجلة الدراسات في سيكولوجية الإنحراف ، الجزائر ، مجلد 6 ، العدد 1، سنة 2021م ، ص 49 وما بعدها .

34 د. وديعة الأميوني ، الجريمة الرقمية كيف نكافحها؟ مقال منشور بتاريخ 2021م على الموقع الالكتروني : https://www.annahar.com/arabic/section/140

35 رامي وحيد منصور ، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها ، البحرين: منشورات مجلس التعاون لدول الخليج العربي ، الأمانة العامة ، 2016م، ص 163

36 ليليا عين سويه وآخر ، وعي مستخدم شبكة الانترنت بالجرائم الإلكترونية ، مجلة مفاهيم للدراسات الفلسفية والانسانية المعمقة ، جامعة زيان عاشور ، الجزائر، العدد الخامس، 2019م، ص 52.

37 محمد أمين الرومي، الكمبيوتر والانترنت ، الإسكندرية: دار المطبوعات الجامعية، 2003م، ص 24 .

38 صابر بحري وآخر ، مرجع سابق ، ص 52 وما بعدها.

39 Felson, M. and Clarke, R.V. (1998) Opportunity Makes the Thief. Police Research Series Paper 98, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate. London: Home Office. Available at: http://www.homeoffice.gov.uk/rds/prgpdfs/fprs98.pdf

40 Thomas E Dearden, Katalin Parti, Cybercrime, Differential Association, and Self-Control: Knowledge Transmission ThroughOnline Social Learning.Center for Peace Studies and Violence Prevention at Virginia Tech. For more details see the website:

https://vtechworks.lib.vt.edu/bitstream/handle/10919/106589/Dearden.Parti.AJCJ.PROOF.pdf?sequence=5

41 BAE Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012.

[42] المرجع السابق نفسه .

[43] mohamed chawki - fight cybercrime - edition, france, 2009.p5.see also: Littlejohn Shinder, Michael Cross, Understanding the People on the Scene In Scene of the

Cybercrime (Second Edition), 2008.
https://www.sciencedirect.com/topics/computer-science/cybercriminals

[44] Myriam quemener- Jean Paul pinte - cyber security of economic actors - risk - strategic and legal response - edition paris, france, 2013.p50

[45] Brendan Kotze, Why Politically Motivated Cyber-Attacks Are a Threat to Democracy, 10/jan/2022.
https://www.infosecurity-magazine.com/opinions/politically-motivated-cyber

[46] المرجع السابق نفسه .

[47] تركي بن عبدالرحمن ، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليته، أطروحة دكتوراه، قسم العلوم الشرطية ، جامعة نايف للعلوم الأمنية، (غير منشورة) ، 2009م، ص 165 .

[48] Edna Erez, LL.B., Ph.D.; Gabriel Weimann, Ph.D.; A. Aaron Weisburd, M.A.Jihad, Crime, and the Internet: Content Analysis of Jihadist Forum Discussions, Report'submitted
'to'the'National'Institute'of'Justice'in'fulfillment,Department'of'Justice. Date Published October 2011.pp5.6.
https://www.ojp.gov/ncjrs/virtual-library/abstracts/jihad-crime-and-internet-content-analysis-jihadist-forum

[49] Maras, Marie-Helen. (2016). Cybercriminology. Oxford University Press.

[50] Bencsáth, Boldizsár. (2012). Duqu, Flame, Gauss: Followers of StuxnetRSA Conference Europe 2012.

[51] Zetter, Kim. (2012). Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload. Wired, 9 August 2012.

[52] United Nations Office on Drugs and Crime .Hacktivism, Terrorism, Espionage, Disinformation Campaigns and Warfare in Cyberspace. For more details see the website: https://www.unodc.org/e4j/ar/index.html

[53] Matthew Edwards. et al, Characterising Cybercriminals: A Review, bristol cyber security group , university of bristol , February 16, 2022, pp15-20.

[54] Camryn Mottl, 6 Motivations of Cyber Criminals op. cit .

[55] FBI , The Unabomber, For more details see the website:
https://www.fbi.gov/history/famous-cases/unabomber

[56] من أبرز المؤيدين لهذه الأفكار منظمة (CLODO) ،والتي ظهرت ظهرت في 6 أبريل 1980 خلال دعوى حريق متعمد ضد شركة "Philips Data system" في تولوز. وهي منظمة مناهضة للصناعات التقنية الفرنسية وتسعى لتدمير أجهزة الحاسوب التي تعتبرها أدوات للقمع والسيطرة. وأكدت اللجنة في بيان صحفي أن "هدفنا هو محاربة كل أشكال السيطرة" لمزيد من التفصيل ينظر :
Pierre Drouin, Un signal d'alarme, Le Monde, 11 avril 1980, lire en ligne:
https://www.lemonde.fr/archives/article/1980/04/11/un-signal-d-alarme_2801590_1819218.html

[57] Xingan Li. op. cit .p118.

[58] Jiang, H. and Yu, Z. 1997. Concerning Offence of Creating and Spreading Destructive Computer Program, Jurists, number 5, pp. 18-27.

[59] Kelly, J. X. 2002. Cybercrime - High Tech Crime, JISC Legal Information Service - University of Strathclyde. Retrieved 10 January 2017, from http://www.jisc.ac.uk/legal/index.cfm?name=lis_cybercrime

[60] Anderson, C. 2002. Hacking the Grade, Originally Aired, 3 September 2002. Retrieved 10 January 2017,from
http://www.techtv.com/cybercrime/internetfraud/story/0,23008,3396685,00.htm
[61] Xingan Li. op. cit .p 122 .
[62] Doug Coleman, Four Types of Hackers You Should Know About , 2019. from https://www.roebucktech.com/it-blog/author/dougcoleman/page/6
[63] C. C. Palmer. Ethical hacking, IBM SYSTEMS JOURNAL, VOL 40, NO 3, 2001, pp770
[64] وقد تم أطلاق مصطلح الاختراق الأخلاقي من قبل شركة أي بي إم . لمزيد من التفصيل ينظر:
Knight, William (October 16, 2009). License to hack., InfoSecurity. from https://www.infosecurity-magazine.com/magazine-features/license-to-hack-ethical-hacking
[65] Palmer ،C.C. (2001). "الإختراق الأخلاقي". IBM Systems Journal. 40 (3), pp769
[66] لحسن الحظ ، أصدر خبراء الأمن أدوات فك التشفير في غضون أيام من ظهور WannaCry ، وقد أدى وقت الاستجابة السريع إلى الحد من مدفوعات الابتزاز إلى حوالي 120 ألف دولار - أكثر بقليل من 1 في المائة من المبلغ المحتمل.
[67] What is a Black-Hat hacker?. From;
https://www.kaspersky.com/resource-center/threats/black-hat-hacker

[68] Gray Hat Hacker, : August 9, 2022. From;
https://www.techopedia.com/definition/15450/gray-hat-hacker
[69] Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012. Organised Crime in the Digital Age. Exploring Internet Crimes and Criminal Behaviour. Boca Raton, FL: CRC Press, Taylor & Francis Group.
[70] رامي وحيد منصور ، مرجع سابق ، ص 86 وما بعدها .
[71] مصطلح عامي ودارج، صِيغَ من أجل وصف نشاط الناس الذي يقومون بدراسة أو تجريب أو استكشاف أنظمة الاتصالات، مثل المعدات والأنظمة المتصلة بشبكات الهاتف العمومية. لمزيد من التفصيل يُنظر موسوعة ويكيبيديا على الموقع الالكتروني : https://ar.wikipedia.org
[72] phreaker ,February 1, 2017. Article published on the website;
https://www.techopedia.com/definition/4050/phreaking
[73] What Is Cyberstalking and How to Protect Yourself From Online Stalkers. From;
https://www.avg.com/en/signal/how-to-avoid-cyberstalkers
[74] المرجع السابق نفسه .
[75] سمير شعبان، الجريمة الإلكترونية - مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم - ، مجلة دراسات وأبحاث ، جامعة الجلفة، الجزائر ، العدد 1 سنة 2009م، ص 125 .
[76] Systems Digital Intelligence – the doorway to digital advantage, The Insider Cyber threats, methods and motivations,From;
https://www.baesystems.com/en/cybersecurity/about-us
[77] Doug Coleman, Four Types of Hackers You Should Know About , 2019, From;
https://www.roebucktech.com/it-blog/author/dougcoleman/page/6
[78] سايفربانك يطلق على أي شخص يدعو إلى الاستخدام الواسع النطاق للتشفير القوي وتقنيات مجال تعزيز الخصوصية كمسار للتغيير الاجتماعي والسياسي . وكان التواصل الأساسي للسايفربانكس عن طريق

مجموعات غير رسمية في قائمة البريد الإلكتروني لـ سايفربانكس، وهدفها هو تحقيق الخصوصية والأمان من خلال الاستخدام الاستباقي للتشفير. وقد انخرطت سايفربانكس في حركة نشطة منذ أواخر ثمانينات القرن العشرين. لمزيد من التفصيل يُنظر موسوعة ويكيبيديا على الموقع الالكتروني : https://ar.wikipedia.org/wiki

[79] - قد تصل برامج الفدية إلى جهاز الضحية بعدة طرائق منها، الإصابة من مواقع ضارة أو إضافات خبيثة في التنزيلات أو رسالة البريد العشوائي .أهداف هجمات برامج الفدية تشمل كلٍ من الأفراد والشركات، ولكن لحسن الحظ يوجد عدة إجراءات يمكن اتباعها من أجل الحماية من هجمات برامج الفدية مع البقاء حذرًا وكذلك تثبيت البرامج المناسبة؛ كل هذه أمور مهمة للحفاظ على أمنك وسلامتك. هجمات برامج الفدية عندما تتم تعني إما فقدان البيانات أو إنفاق الكثير من الأموال أو الأمرين معًا. لمزيد من التفصيل ينظر: . إزالة برامج الفدية | فك تشفير البيانات – كيفية قتل الفيروس، مقال منشور على الموقع الالكتروني:

https://me.kaspersky.com/resource-center/preemptive-safety/ransomware-removal

[80] Dorothy E. Denning and William E. Baugh, Jr .Hiding Crimes in Cyberspace, to appear in Information, Communication and Society, Vol. 2, No 3, Autumn 1999, pp 1-23

[81] ومن الأمثلة الحديثة على عمل Eurojust التشغيلي في هذا المجال الدعم الذي قدمته للمحققين والمدعين العامين في قضية SKY ECC. راقب المحققون الاستخدام الإجرامي لأداة خدمة الاتصالات Sky ECC ، مما أدى إلى تكوين رؤى لا تقدر بثمن لمئات الملايين من الرسائل المتبادلة بين المجرمين. وقد أدى ذلك إلى جمع معلومات حاسمة حول أكثر من مائة عملية إجرامية واسعة النطاق مخطط لها ، ومنع الوقائع التي قد تهدد الحياة والضحايا المحتملين.تعد العملية جزءًا أساسيًا من الجهود المستمرة للسلطة القضائية وأجهزة تنفيذ القانون في الاتحاد الأوروبي لتعطيل الاستخدام غير القانوني للاتصالات المشفرة ، بعد فك التشفير الناجح لمنصة اتصالات EncroChat في عام 2020. بعد الكشف عن EncroChat ، غير العديد من المستخدمين إلى منصة Sky ECC الشهيرة. لمزيد من المعلومات ينظر :

European Union Agency for Criminal Justice Cooperation , Dealing with the criminal use of encryption, 2021.

https://www.eurojust.europa.eu/annual-report-2021/securing- vidence/criminal-use-of-encryption

[82] مصطلح سرقة الهوية تم صياغته في عام 1964م، وفقا لقاموس جامعة اكسفورد. لمزيد من التفصيل يُنظر. ذكري المظهر ، سرقة الهوية عبر الإنترنت: نصائح الوقاية والحماية ، مقال منشور على الموقع الالكتروني : https://ar.ioecomp.com

83 المرجع السابق نفسه .

84 سمير شعبان ، مرجع سابق، ص 124 .

[85] سرقة الهوية: الحقائق والأسئلة المتداولة . مقال منشور على الموقع الإلكتروني : https//:me.kaspersky.com.

86 سامي الشـــــوا، الغش المعلوماتي كظاهـــــرة إجرامية مستحدثة ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة،25 - 28 ، أكتوبر . 1993 ص 125 – 126 .

87 Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge,Massachusetts, 1989, P. 104

88 ومن هذه المؤلفات على سبيل المثال،(كتاب خارج نطاق الدائرة الداخلية كيف تعملها؟) لمؤلفه الأمريكي "لبيل لاندريث " . وكتب(الدليل الجديد للمتعثلمين) لمؤلفه" هوجوكوزن"، وكتاب (المتعثلمين-أبطال ثورة الحاسوب) لمؤلفه " ستيفن ليفي". يُنظر . المرجع السابق نفسه.

89 Doug Coleman, Four Types of Hackers You Should Know About , 2019 https://www.roebucktech.com/it-blog/author/dougcoleman/page/6