



مخابر الدراسات والبحوث  
في القانون والأسرة  
والتنمية الإدارية

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف - المسيلة

فرقة بحث "حماية الفضاء السيبراني من الهجمات الإلكترونية"

وبالتنسيق مع مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية

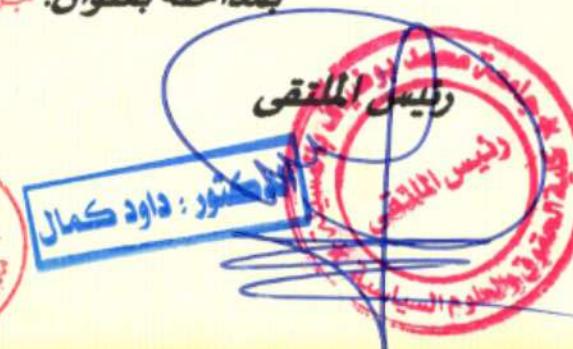
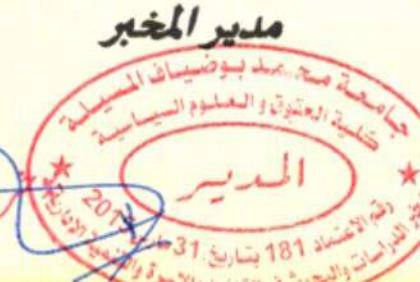
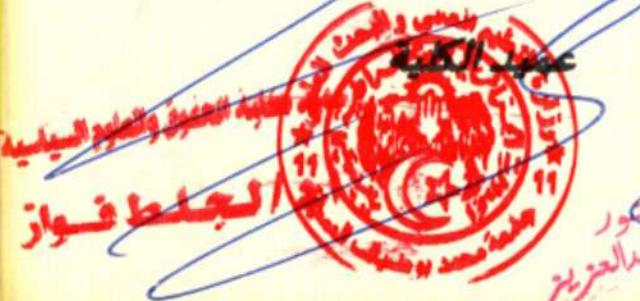


كلية الحقوق والعلوم  
السياسية

## شهادة تقدير

يشهد عميد كلية الحقوق والعلوم السياسية بجامعة محمد بوضياف بالمسيلة بأن: د/ عبد الغني حجاب - جامعة المسيلة قد شارك(ت) في أشغال الملتقى الوطني حول: "الجرائم السيبرانية ومقتضيات السيادة والأمن الوطنيين: الآثار، التداعيات واستراتيجيات المواجهة" المنظم من قبل فرقة بحث "حماية الفضاء السيبراني من الهجمات الإلكترونية" وبالتنسيق مع مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية. يوم 15 ديسمبر 2024 حضوريا وعن بعد.

بمداخلة بعنوان: جرائم الفضاء الإلكتروني وتأثيرها على الأمن القومي



فرقة بحث "حماية الفضاء السيبراني من الهجمات الالكترونية"  
و بالتنسيق مع  
مخبر الدراسات والبحوث في القانون والأسرة والتنمية الادارية  
  
برنامج الملتقي الوطني الموسوم :  
**الجرائم السيبرانية ومقتضيات السيادة والأمن الوطنيين: الآثار، التداعيات  
واستراتيجيات المواجهة**

**Cybercrimes and the Requirements of National Sovereignty and Security: Impacts, Consequences and Confrontation Strategies**

المجمع تنظيمه حضوريا وعن بعد يوم الاحد 15 ديسمبر 2024

قاعة المحاضرات مولود بدبار

التوقيت: 16:20-9:00

**الجلسة الافتتاحية**

رابط الجلسة الافتتاحية:

التوقيت	البرنامج
9.05-9.00	تلاؤة آيات بينات من الذكر الحكيم
9.10-9.05	النشيد الوطني
9.20-9.10	كلمة رئيس الملتقى: د. كمال داود
9.30-9.20	كلمة السيد عميد كلية الحقوق والعلوم السياسية: أ.د. لجلط فواز
9.40-9.30	كلمة السيد مدير جامعة المسيلة: أ.د. بودلاعة عمار

التوقيت: 11.30-09.40

**الجلسة الرئيسية الحضورية: برئاسة: أ. ضريفي نادية**

**رابط الجلسة الرئيسية:**

الرقم	الاسم ولقب	عنوان المداخلة	مؤسسة الانتماء	التوقيت
1	أ.د. دحية عبد اللطيف أ.د. لدغش سليمة	الإستراتيجية العربية للأمن السيبراني كآلية للتنظيم القطاع السيبراني في المنطقة العربية	المсиئة الجلفة	09.50-09.40
2	د. محمد بوضياف	خطوات إعداد إستراتيجية مواجهة الجرائم السيبرانية	المسيئة	10.00-09.50
3	أ.د. قسمية محمد	مكافحة الجرائم السيبرانية في التشريع الدولي والجزائري	المسيئة	10.10-10.00
4	د. دراج عبد الوهاب ط. د. عماري بلال	آليات مواجهة الجريمة السيبرانية الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحة أنماذجها	المسيئة	10.20-10.10
5	د. عمارة عمارة	الإجراءات الخاصة لمواجهة الجريمة السيبرانية و الوقاية منها: المساس بأنظمة المعالجة الآلية للمعطيات أنماذجا	المسيئة	10.30-10.20
6	د. مراد يرمش	أثر الجريمة الالكترونية على حقوق الملكية الفكرية	المسيئة	10.40-10.30
7	د. تاهي مصطفى ط. د. مروان قرابسي	فهم تعرض الأمن القومي في الجزائر للمخاطر السيبرانية و سبل الوقاية منها	المسيئة	10:50-10.40
8	د. زبيري عبد الله د. لعجال عفيفة	تعزيز الوعي الأمني مقاربات بديلة لمواجهة التهديدات و المخاطر	المسيئة	11.00-10.50
9	أ.د. ضريفي نادية د. لعجال مني	اليات مكافحة الجرائم السيبرانية	المسيئة	11:10-11:00
10	د. زروقي مرازقة د. حشاني فاطمة الزهراء	الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والأفاق المستقبلية	جامعة المسيئة	11:20-11:10
11	د. كمال داود	آثار السيادة السيبرانية على الحقوق الرقمية	المسيئة	11:30-11:20

مناقشة 11:40-11:30

رابط الجلسة الأولى عن بعد: <https://meet.google.com/aas-ksdu-pvz>

التوقيت	مؤسسة الاتصال	عنوان المداخلة	الاسم ولقب	الرقم
13.10-13.00	جامعة سعيدة	الجريمة المعلوماتية و مقتضيات الأمن الرقمي	د.بلعابد عيدة د.سليماني جميلة	1
13.20-13.10	المركز الجامعي النعامة	مفهوم الجرائم السيبرانية (التعريف النشأة و التطور)	ط.د. قارة عبد الحق	2
13.30-13.20	جامعة المدية	التداعيات المباشرة وغير المباشرة للجريمة السيبرانية على السيادة و الأمن الوطنيين	ط.د بن زهرة السعيد	3
13.40-13.30	المسلة	اختصاص القطب الجنائي في الجرائم السيبرانية	د. حلطاش عمر	4
13.50-13.40	المسلة	تطور النظام القانوني للجريمة الإلكترونية	د.حمريط النواري	5
14.00-13.50	المسلة	الجهود الإقليمية لمكافحة الجريمة السيبرانية	أ.د السعيد براج د.كشيدة الطاهر	6
14.10-14.00	المسلة	الجريمة السيبرانية في منظور القانون الدولي العام	د. بوعون نضال د. لخضر حميزة عبد الله	7
14.20-14.10	الوادي	آليات مكافحة الجريمة السيبرانية في التشريع الجزائري	ط. د.دحماني رشيد	8
14:30-14:20	المسلة برج بوعربيرج	تحديات الأمن السيبراني في ظل ثورة لذكاء الاصطناعي -قراءة في واقع التجربة الجزائري-	د. لرقط الحسين د. مومن رضوان	9
14.40-14.30	المسلة	إجراءات التحقيق الخاصة بالجرائم السيبرانية	د. الوافي السعيد	10
14:50-14:40	المسلة	الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني	د.زيتوني عادل د. بوضياف الخير	11
15:00-14:50	جامعة تونس	الجريمة السيبرانية الأفاق والتحديات	ط.د زكري عبد المجيد	12
15:10-15:00	سوق أهراش	الجرائم السيبرانية مفهومها وأنواعها	د.عيساوي الساسي د.غول أمينة	13
15.20-15.10	جامعة المسلة	جرائم الفضاء الإلكتروني وتأثيرها على الأمن القومي	د.عبد الغني حجاب ط.جلود وسام	14
15:30-15:20	المسلة	المعالجة التشريعية للتحديات السيبرانية في التشريع الجزائري و التشريع المقارن	ا. العمارة عبد الرزاق	15
15:40-15:30	جامعة تبزي وزو	استراتيجيات المواجهة والتصدي للجريمة السيبرانية: آليات الوقاية والمكافحة	ط.د.تيزراوي نعيمة	16

مناقشة 16:00 -15:50

رابط الجلسة الثانية عن بعد: [meet.google.com/nmm-cdax-hzd](https://meet.google.com/nmm-cdax-hzd)

الرقم	الاسم واللقب	عنوان المداخلة	مؤسسة الانتماء	التوقيت
1	د. عيدلي حمزة ط. ددورا فاطمة	نحو تفعيل تكنولوجيا الذكاء الاصطناعي في مجال الوقاية والتحري عن جرائم الفساد دراسة مقارنة	المسللة	13.10-13.00
2	د. قاوي السعيد	السيادة السيبرانية و الرقمنة الوطنية و سبل تعزيزها	المسللة	13.20-13.10
3	د. لعازقة حمزة	فعالية تحليل السلوك الإجرامي السيبراني بين تطبيقات الذكاء الاصطناعي والاستخبارات المفتوحة المصدر	سطيف 2	13.30-13.20
4	د. صبيحي شهيناز	الذكاء الاصطناعي كآلية لمواجهة الجريمة السيبرانية	الشلف	13.40-13.30
5	د. بن جامع حنان	المواجهة القانونية لجريمة الابتزاز الإلكتروني في التشريع الجزائري	سكنكدة	13.50-13.40
6	د رابعي ابراهيم	النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال	المسللة	14.00-13.50
7	ط. دبركانة محمد ط. د. مقدم مختار	آليات مكافحة الجريمة الإلكترونية على المستوى الدولي والوطني	المركز الجامعي النعامة	14.10-14.00
8	د. خوجة اسامي	السيبرانية منطقة تغلغل العرب الخفية وبسط القوة في ظل الالفية الثالثة	المسللة	14.20-14.10
9	د. فراحتية اكرم د. بوعكار خليل	الجريمة السيبرانية بين الحداثة و حتمية التقني	المسللة	14:30-14:20
10	أ. د عطوي خالد	الفضاء السيبراني و السيادة: علاقة تأثير و تأثر	المسللة	14.40-14.30
11	د. بويعسي حسام الدين د. محمدى اسمهان	التحولات الأمنية الجديدة في ظل التطور الرقمي:الجزائر أنموذجا آليات الحماية والوقاية	المسللة	14:50-14:40
12	د. برابح حمزة	مكافحة الجريمة السيبرانية في إطار منظمة الأمم المتحدة	المسللة	15:00-14:50
13	د صغير يرم عبد المجيد ط. دقيرزة حليم	في كيفية حماية الخصوصية الوطنية من الجريمة العابرة للأوطان	المسللة	15:10-15:00
14	د. بن النوي زبیر	الاثبات في الجريمة السيبرانية	المسللة	15.20-15.10
15	د. رشيد مسعودي	مقترن لهندسة إستراتيجية أمنية تشابكية لمواجهة التهديدات الاتجائية للإجرام السيبراني على منظومة الأمن الوطني في الجزائر	المسللة	15:30-15:20
16	د. بلهمدي ابراهيم	رقمنة المرافق العمومية بين تقديم الخدمة وتهديدات الجرائم السيبرانية	جامعة المسللة	15:40-15:30
17	د. بوعكة الكاملة	الحماية القانونية للأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي على ضوء القانون 18-07	جامعة المسللة	15:50-15:40
18	د. قمرة النذير	جريمة الاعتداء على الخصوصية في التشريع الجزائري	جامعة المسللة	16:00-15:50

مناقشة 16:30-16:20

الجلسة الختامية

قراءة التوصيات واختتم الملتقى

## جرائم الفضاء الإلكتروني وتأثيرها على الأمن القومي

### Cybercrime and its impact on national Security

ط (\*) وسام جلود

جامعة محمد بوضياف - المسيلة - الجزائر

djeloud.wissam@gmail.com

د عبد الغني حجاب

جامعة محمد بوضياف - المسيلة - الجزائر

Abdelghani.hadjab@univ-msila.dz

تاريخ القبول: ×/×/×

تاریخ الارسال: اليوم/الشهر/السنة

ملخص:

تعتبر جرائم الفضاء الإلكتروني قضية معقدة تتجاوز مجالات إدارة المخاطر في تكنولوجيا المعلومات وإنفاذ القانون تفرض تكلفة ثقيلة على المجتمعات وتضعف الأمن الاقتصادي الوطني ومع ذلك، ثبت أن الهياكل الحالية لمواجهة التهديد غير كافية. لذا، من الضروري أن تستثمر الدول في تدابير الأمان السيبراني القوية والتعاون الدولي لمكافحة هذا التهديد المتزايد.

**الكلمات المفتاحية:** الأمن السيبراني؛ الفضاء الإلكتروني؛ إدارة المخاطر؛ الأمن الوطني.

**Abstract:**

Cybercrime is a complex issue that transcends the areas of risk management in information technology and law enforcement that imposes a heavy cost on societies and weakens national economic security. It is therefore imperative that countries invest in strong cybersecurity measures and international cooperation to combat this growing threat.

**Keywords:** cybersecurity; cyberspace; risk management; national security

\*المؤلف المرسل: د. عبد الغني حجاب

## مقدمة

أصبح الفضاء الإلكتروني - وهو فرع من تطور الكمبيوتر وتقنيات الاتصالات الرقمية - في العقود الأخيرة جزءاً لا يتجزأ من حياتنا. فالحوسبة دورها في تحسين وتبسيط العمليات المتعلقة بالعمل والتعلم والترفيه لا يقدر بثمن، وتأثر فعلياً على كل مجال من مجالات المساعي البشرية.

وبمجرد أن أصبحت الإنترنت ذات طابع تجاري منذ عام 1988، سرعان ما تحولت إلى الدعامة الأساسية للفضاء الإلكتروني، مما وفر وصولاً غير مكلف وفوري إلى العديد من مصادر المعلومات، وتبادلها، والعمل المشترك لمسافات طويلة

إن آثار جرائم الفضاء الإلكتروني على الأمن القومي مستمدة من الطريقة التي تستخدم بها العناصر المعادية للتكنولوجيا. تقترح هذه المداخلة دراسة موجهة لمعنى جرائم الفضاء الإلكتروني وتأثيرها على الأمن القومي، دون التركيز على التقييمات النقدية الواسعة النطاق للأضرار التي تسببها الجرائم الإلكترونية. وهو يتضمن لمحات عن التعاون بين المجرمين والجريمة المنظمة والمنظمات المعادية، ويناقش تسويق قدرات الاستطلاع والهجوم السيبراني، التي أصبحت ممكنة بفضل التقنيات المتقدمة باستمرار ونمو السوق السوداء في خدمات تكنولوجيا المعلومات في الوقت الحالي،

لا تعد الجرائم الإلكترونية ذات أهمية كبيرة خارج مجالات إدارة مخاطر تكنولوجيا المعلومات وإنفاذ القانون. ومع ذلك، تحدد هذه المداخلة شرطين منفصلين حيث يمكن أن تصبح الجريمة السيبرانية تهديداً كبيراً للأمن القومي.

يرتفع الطلب العام على الأمن السيبراني بما يتناسب مع الاعتراف المتزايد بهذا التهديد. ومن غير المتوقع أن ينخفض هذا الطلب. إن مسؤولية الدولة في توفير الأمن لمواطنيها لا يمكن أن يقف عند عتبة حد الفضاء السيبراني.

## 1. ظاهرة الجرائم الإلكترونية

تسمح الحوسية بتقسيم المهام إلى وحدات صغيرة وتحقيق اللامركزية في المعالجة؛ تتيح الشبكات الوصول العالمي إلى المعلومات والتركيز على المعرفة كمنتج قيم. يتم تطبيق التقنيات الحوسية لتغيير وتعزيز كفاءة العمليات الإبداعية والعملية في كل جانب من جوانب الحياة.

هناك تساؤلات عن الجديد في الجريمة السيبرانية فيما إذا كانت مجرد ظاهرة قديمة تستخدم أدوات جديدة، والتعرif المقترن للجريمة السيبرانية هو: "استخدام الفضاء السيبراني لأغراض غير قانونية، مع استغلال ميزات الفضاء السيبراني الفريدة، مثل السرعة والفورية؛ والتشغيل عن بعد؛ والتشويش والتعتيم، مما يجعل من الصعب تحديد العملية والمشغل." ويستمر النقاش حول الجرائم الإلكترونية. منذ أكثر من عقد من الزمان.

يحاول معظم الباحثين تحليل الجريمة السيبرانية باعتبارها ظاهرة فريدة من نوعها. يصنفها (ماجد يار) وفقاً للمهدف المستهدف: الممتلكات أو الأشخاص أو الدولة.

ويميز (Shinder) (Cross) بين أنواع الجرائم وفقاً لمستوى العنف المعنى: "الجرائم العنيفة والجرائم العنيفة المحتملة، والجرائم غير العنيفة (كتجارة المخدرات وغسيل الأموال)، والجريمة التي لا يزال ينظر إليها على أنها تقع ضمن فئة ذوي الياقات البيضاء<sup>1</sup> (اقتحام أجهزة الكمبيوتر، والسرقة، والاحتيال).

ووفقاً لـ(وول)، فإن الجرائم السيبرانية هي "تحويل السلوك الإجرامي أو الضار بواسطة التكنولوجيا الشبكية". لقد تطورت نتيجةً لتطور الحوسية والفضاء الإلكتروني وما ترتب على ذلك من فرص جديدة للحصول على المعلومات أو تعطيلها أو التلاعب بها لتحقيق مكاسب. ويصنف وول أيضاً الجرائم الإلكترونية إلى ثلاثة فئات: الجريمة التي تنطوي على سلامنة أنظمة الكمبيوتر ونظام عملها (القرصنة)؛ جرائم استغلال الفضاء الإلكتروني (الاتصالات المشفرة بين المجرمين)؛ والجرائم التي تنطوي على محتويات معلوماتية محوسية (سرقة الأسرار، ونشر محتويات ضارة).

<sup>1</sup> عمال الياقات البيضاء [بالإنجليزية](#) White-collar Workers : هو مصطلح غربي يطلق على أولئك الناس الذين يقومون بعمل «ذهني» مكتبي مثل [المديرين](#) والمختصين، وهم بذلك يتميزون عن أصحاب الياقات الزرقاء (Blue-collar Workers) (pink-collar worker)، كما يطلق مصطلح آخر وهو أصحاب الياقات الوردية للعمال الذين يعملون في أعمال خدمة الزبائن.

لا يوجد شيء فريد أو جديد في الكثير من الجرائم الإلكترونية كالتحرش، الاحتيال، الدعاية غير القانونية، المواد الإباحية، السرقة، غسل الأموال والتجسس، وما إلى ذلك، باستثناء استخدام الفضاء الإلكتروني.

ولكن هناك مستوى آخر من الجريمة لا يمكن أن يوجد بدون الفضاء السيبراني: البريد العشوائي والنقر الاحتيالي، وأنواع مختلفة من البرامج الضارة، وشبكات أجهزة الكمبيوتر المقيدة (botnets)، وسرقة الهوية الرقمية، والتمويه وتشفير البيانات والاتصالات، والانتهاكات المحسوبة لأنظمة الآمنة ذات القيمة العالية. المرافق والتجسس التلقائي طويل الأمد في المنظمات الآمنة - مما يحرمها من السيطرة على الملكية الفكرية.-

يستغل مجرمو الإنترنت القيمة المتزايدة للبيانات الرقمية بجميع أشكالها، والطرق القانونية والقضائية التي تتعامل بها البلدان المختلفة مع الفضاء الإلكتروني.

لقد كانت الجريمة دائماً ظاهرة اجتماعية منتشرة على نطاق واسع، وتجمع التفسيرات الجنائية بين الدافع والفرصة والعديد من دوافع السلوك الإجرامي جوهريه ولا يتم تحديدها إلا من خلال تحديد التكلفة والفوائد.

ليس هناك من الأسباب ما يجعلنا نعتقد أن زيادة استخدام هذه التكنولوجيا أو تلك من شأنه أن يغير السلوك البشري. ولذلك ليس من المستغرب أن يستخدم الناس الفضاء الإلكتروني أيضاً لتحقيق احتياجاتهم وتحقيق أهدافهم في الأنشطة المشروعة كالدراسة والترفيه والتعليم والعمل.

يعتمد المبدأ الكلاسيكي لعلم الجريمة على مفهوم الاختيار الحر والتقييم العقلاني للمكاسب المتوقعة مقابل خطر العقوبة؛ وعلى هذا فإن الدافع إلى ارتكاب الجريمة هو قرار اقتصادي عقلاني. ويحلل الاقتصاديون وعلماء النفس والسلوك البشري - بما في ذلك السلوك الإجرامي - باعتباره مشتقاً من التحليل العقلاني للتکاليف والفوائد.

إن مجموعة الظروف الخارجية المتغيرة باستمرار قد تشجع الجرائم السيبرانية؛ ويحدث هذا عندما يحدد شخص ما قيمة المكاسب المحتملة ويقدر التكلفة - خطر العقوبة - على أنها أقل من هذا المكسب.

إن الجمع بين زيادة الاتصال الرقمي في شكله الحالي غير الآمن، وبين القيمة المتزايدة للبيانات المحسوبة، يؤدي إلى موقف ترتفع فيه الدوافع الخارجية للسلوك الإجرامي.

على الرغم من أن الدول المتقدمة أنشأت آليات منظمة لإنفاذ القانون، إلا أن استجابات الدول لم تواكب وتيرة التغيرات التكنولوجية في الفضاء السيبراني. وخير مثال على ذلك هو سرقة البنك "التقليدي" مقارنة بالسرقة السيبرانية. في عمليات السطو على البنوك التقليدية، يجب إخضاع الترتيبات الأمنية حيث من المحتمل حدوث مواجهة مع الحراس المسلحين. وحتى لو نجحت عملية السطو نفسها، فإن السلطات ستلاحق اللصوص لسنوات قادمة.

مع تطور الفضاء الإلكتروني، أصبح استغلال نقاط ضعفه يشمل أيضاً سرقة البنوك. على سبيل المثال، يعد استخدام شبكات الروبوت التي تضم عشرات الآلاف من أجهزة الكمبيوتر الشخصية لسرقة تفاصيل الهوية إلى الواقع المصرفية والتي يتم استخدامها بعد ذلك لسرقة مبالغ صغيرة من المال، أمراً شائعاً جداً. ونظراً لمشكلة تحديد هوية الجرم في الفضاء السيبراني، فإن فرص تحديد هوية الجرم ضئيلة.

وتدرك المؤسسات المالية جيداً المخاطر التي تهدد مصالحها التجارية، وتتخذ - بالتعاون مع الهيئات التنظيمية - خطوات لحماية نفسها، والاستثمار في أمن تكنولوجيا المعلومات لتقليل المخاطر إلى أدنى حد ممكن. نطاق الفرص المتاحة لمجري الإنتربت. ولكن على الرغم من ذلك، فإن المخاطر المادية المباشرة لا تزال أقل بكثير بالنسبة للمجرم السيبراني مقارنة بال مجرم "التقليدي". كما أن خطر العقوبة القانونية سابقاً كان أقل أيضاً، نظراً لأن النظام القضائي كان ينظر عموماً إلى الاحتيال عبر الإنتربت على أنه جريمة غير عنيفة من نوع "ذوي الياقات البيضاء". وكان يتم التعامل معه وفقاً لذلك.

## 2. نطاق الجرائم الإلكترونية والأضرار اللاحقة

عادةً ما يتم دراسة ظاهرة الجرائم السيبرانية من وجهات نظر متنوعة: قانونية (التشريعات والعقوبات)، أو جنائية (الدافع والتنظيم)، أو اقتصادية (الحوافز والقيمة)، أو فنية (البيانات).

إن نطاق الضرر المحتمل كبير. لنفترض أن جهاز الكمبيوتر الذي يقوم ب تخزين قاعدة بيانات مكونة من ألف إدخال قد تم اختراقه؛ لنفترض أيضاً أن قاعدة البيانات غير مشفرة وأن الإدخالات مكتوبة بنص عادي. بحيث يمثل كل إدخال بطاقة ائمان صالحة، بما في ذلك جميع المعلومات الازمة لاستخدامها (الرقم والرمز وتاريخ انتهاء الصلاحية والاسم الكامل ورقم الهوية وعنوان حامل البطاقة، بالإضافة إلى المعلومات المصرفية الخاصة بجهة إصدار البطاقة). في هذا السيناريو يرى اللص صورة كاملة وحقيقية للمعلومات الموجودة في الملف. ولكن حتى في ظل هذه الظروف المثالية، هل نحن قادرؤن على تقدير القيمة المالية للمعلومات التي يتم الوصول إليها بشكل كامل؟ هل يستطيع اللص تقييم القيمة الحقيقة للمعلومات المسروقة بشكل صحيح؟

جهود البحث والتطوير الطويلة – يميل الضحية إلى تحديد الحد الأقصى للربح الذي يود تحقيقه عند الانتهاء من عملية البحث والتطوير والتصنيع والتسويق على أنه ضرر. تعتبر المسوحات، وهي وسيلة مناسبة لتوضيح الظواهر التي يصعب ملاحظتها، هي الطريقة الرئيسية للتعرف على نطاق الضرر. تسمح المسوحات للباحثين بالوصول إلى مجموعة أكبر وأكثر تنوعاً من المجيبين الذين يقدمون تقديراتهم الخاصة لعدد الحوادث وقيمة الأضرار، ولكنها أيضاً طريقة تحتوي على بعض العيوب الخطيرة التي تقلق علماء الاجتماع والإحصائيين. ثانياً، في غياب بيانات كافية، يستخدم الباحثون الأساليب الإحصائية لاستخلاص التقييمات من البيانات الجزئية.

وتؤثر مشاكل القياس على كل جانب من جوانب النقاش الدائر حول الفضاء الإلكتروني، وخاصة محاولات مساعدة المناقشة من خلال قياس الضرر من الناحية النقدية. هناك صعوبة متأصلة في تقيير الضرر، ويبدو حتى الآن أن التقييمات النقدية التي نشأت عن الاستخدام الفج لأساليب الإحصائية لتقديم الافتراضات على أساس بيانات غير كافية

تميل إلى المبالغة. بالإضافة إلى مسائل موضوعية طرق البحث ومصداقية مصادر المعلومات ومدى ملاءمة المنهج الإحصائي لهذا النوع من البحث.

هناك أيضاً مشكلة أخرى. غالباً ما تتضمن التقديرات النقدية مكونات غير مباشرة للضرر: سواء كان ذلك على سمعة المنظمة الضحية، أو التأثير السلبي على سلوك المستهلك مع آثار على الاقتصاد الكلي، أو قضايا الأضرار، أو التأمين، أو النفقات المصاحبة، أو غيرها.

تظل بعض الأسئلة الأساسية لفهم هذه الظاهرة دون إجابة. هل يعقل تقييم الضرر على أساس الاستخدام؟ وماذا عن تكلفة الأمن والعودة إلى الأداء الطبيعي؟

إن الصورة التي تم الحصول عليها من المصادر المعتادة أقل من المصداقية، والضرر الناجم عن التقييمات المتضخمة من شأنه أن يؤدي إلى رد فعل مضاد يتمثل في الفشل في أخذ قوة الجريمة السيبرانية على محمل الجد بما فيه الكفاية. إن إقامة المناقشة حول الجرائم الإلكترونية على تقديرات الأضرار المالية ينتقص من المناقشة العقلانية والذكية والمستنيرة حول مشكلة القدرة على صياغة السياسة العامة المناسبة.

### 3. التعاون بين المجرمين والمنظمات الإرهابية

كما أن التفاعل بين المجرمين المحترفين والجريمة المنظمة من ناحية، والمنظمات الإرهابية من ناحية أخرى، ليس ظاهرة جديدة. وحتى لو نظرنا فقط إلى الواقع، فإننا نرى أن مثل هذا التعاون يسبب الضرر على المستوى الوطني

#### 1.3. إعادة النظر في معنى الجرائم السيبرانية

إن أي فحص حالى للجريمة السيبرانية يكشف عن تعاون تجاري مماثل. في السنوات الأخيرة، حيث ظهرت سوق سوداء للخبراء الفنيين و"رعاة" الروبوتات، لتطوير وتوفير الأدوات والخدمات التقنية مقابل ثمن. على الرغم من أن تقديرات الأضرار المالية المعتادة مبالغ فيها إلى حد كبير.

أي شخص يفضل العمل بمفرده ويفتقرب إلى موارد البحث والتطوير يجد أسلحة الفضاء الإلكتروني (مجموعات أدوات البرامج الضارة) متاحة للتتزيل من الإنترنت، وعادة ما يكون ذلك مقابل دفع مبلغ يتراوح بين عشرات إلى عدة آلاف من الدولارات. إن المعرفة المنتج لا ينضب، وهي "سلعة غير منافسة" بالنسبة للاقتصاديين. لكن الانطباع السائد بأن الفضاء

الإلكتروني يسهل جنـي الأرباح الضخمة من المؤسسات الإجرامية لم يغـب عن عالم الجريمة المنظمة.

لقد أدى النمو في قوة الحوسبة والإنترنت في كل مكان إلى إنشاء أداة جديدة للجرائم الإلكترونية واسعة النطاق: شبكة الروبوتات. هذه عبارة عن مجموعة من أجهزة الكمبيوتر المتصلة بالإنترنت والتي تم اختراق دفاعاتها بواسطة البرامج الضارة وتم التنازل عن التحكم لطرف ثالث ضار قادر على التحكم عن بعد.

ويتم استغلال أجهزة الكمبيوتر هذه عند الطلب عادة دون تعطيل عملها الطبيعي. وعادة ما يصيب مجرمو الإنترنت أجهزة الكمبيوتر المتصلة بالإنترنت ببرامج ضارة عن طريق استغلال الثغرات الأمنية المعروفة التي فشل المستخدمون ومسؤولو النظام في التعامل معها. في عام 2007، قدرت شركة McAfee أن حوالي 5% من جميع أجهزة الكمبيوتر الشخصية المتصلة بالإنترنت كانت أسيرة لشبكة الروبوتات.

والظاهرة الأحدث هي التهديد المستمر المتقدم (APT) والمعروفة أيضا باسم الهجوم التكيفي المستمر (APA) وهو عبارة عن أسلحة معقدة ومتعددة المراحل من الفضاء الإلكتروني لغرض الهجمات السرية المستمرة. لا يعمل المهاجم إحصائيا على نطاق واسع لاستغلال نقاط الضعف المعروفة؛ وبدلاً من ذلك فإن الهدف محدد بشكل جيد. يستخدم المهاجم مجموعة من الأدوات المخصصة. وت تكون هذه الهجمات من عدة مراحل ويمكن أن تستمر لأشهر أو حتى سنوات. يبدأ المهاجم بجمع المعلومات الاستخبارية حول الهيكل التنظيمي للهدف، وتحديد الأشخاص الذين يحملونه. مناصب عليا مع أدوات الوصول إلى المعلومات الحساسة. يتم جمع المعلومات الشخصية عادة عن طريق الاستخبارات مفتوحة المصدر (OSInt): بالوصول إلى المعلومات العامة والمعلومات الشخصية المشتركة على الشبكات الاجتماعية ووسائل الإعلام الإخبارية. وب مجرد تحديد اللاعبين الرئيسيين، يتم بذل جهد متضاد لسرقة بيانات اعتمادهم وإصابة أجهزة الكمبيوتر الخاصة بهم.

تتمثل إحدى الطرق في التصيـد الاحـتيـالي، أو إدخـال أداـة الوـصول عنـ بـعد (RAT) عن طـريق بـريد إـلكـتروـني من مرـسل موـثـوق بـه مـحتـوى ذـي صـلـة، وبـالتـالي يـتمـكـن من تـجاـوز آـليـات تصـفيـة البرـيد العـشوـائي باـسـتـخدـام المـعـلومـات الشـخـصـية المـجـمـعـة. يـسمـح فـتح البرـيد إـلكـتروـني بإـدخـال (حـصـان طـروـادـة) في نقطـة نـهاـية موـثـوقـة دـاخـل شبـكة الشـركـة الخـاصـة

بالمؤسسة، وبالتالي الوصول إلى المزيد من الموارد الداخلية. في الجرائم العادلة، بمجرد إتمام الوصول، يتحرك المهاجم العادي بسرعة لاسترداد المعلومات القيمة واستخدامها.

ومع ذلك، ليس هذا هو الحال مع هجوم APA. فالغرض هنا هو الوصول السري على المدى الطويل، وتجاهل الإغراءات المالية المباشرة. يستمر الهجوم لفترة طويلة، ويرجع ذلك جزئياً إلى التغلب على أنظمة الدفاع المصممة لمنع تسرب المعلومات. أثناء الهجوم، يقوم المهاجمون بإجراء اختبارات لتحديد حدود استجابة النظام وعادة ما يقومون بتكييف طرق التسلل للمعلومات المسروقة. يتم تقسيم البيانات إلى حزم صغيرة، مموهة داخل الاتصالات المشروعة، وبالتالي تتسرب عبر النظام دون إثارة الدفاعات.

تطلب APA جمع معلومات استخباراتية منهجية وتحطيم وقدرات التكيف والصبر لتنفيذ مهمة طويلة المدى. في المقابل، فإن الضرر الذي يلحق بـ APA له نطاق مختلف من المنظور الاقتصادي.

لقد نجح الفنانون في تطوير واستخدام أدوات برمجية للتحكم في عشرات الآلاف من أجهزة الكمبيوتر، مما أدى في الواقع إلى إنشاء خدمة ذات قيمة اقتصادية. ومن حيث الطلب، فقد وجد العديد من العملاء – المتسللون الآخرون، والمحققون الخاصون، وال مجرمون، ومنظمات التجسس، والمنظمات الإجرامية العابرة للحدود الوطنية – استخدامات مختلفة للمنتج. وقد أدى ذلك إلى إنشاء نموذج "البرمجيات كخدمة" (CaaS)، وهو نظير السوق السوداء لـ "البرمجيات كخدمة" (SaaS) الذي خدم صناعة تكنولوجيا المعلومات منذ عام 2001.

على مر السنين، شهد النموذج العديد من التحولات؛ والكلمة المعبرة الحالية لها هي "الحوسبة السحابية". المبرر الاقتصادي للنموذج واضح: من الآن فصاعداً، لم يعد العميل بحاجة إلى شراء أجهزة الكمبيوتر من أجل استخدام خدمات الكمبيوتر؛ يمكنه ببساطة شراء الخدمة المحددة التي يحتاجها من كبار المشغلين واستخدامها عبر الاتصالات القياسية. وقد قدر نطاق السوق العالمية لهذا النوع من خدمات الكمبيوتر بمبلغ 14.5 مليار دولار في عام 2012.

دعونا نتفحص ظاهرة السوق السوداء من منظور الأمن القومي. إن وجود سوق سوداء للأسلحة السيبرانية، والاستعانة بمصادر خارجية للبحث والتطوير، وخدمات ضمان

الجودة، والدعم الفني يعني أن المستوى المطلوب من المهارات التقنية ليصبح مجرماً إلكترونياً قد انخفض. لم يعد من الضروري أن يمتلك الشخص الكفاءة لتطوير الأدوات والأساليب لاختراق أجهزة الكمبيوتر بنفسه. إن البنية التحتية التكنولوجية الازمة لاختراق أجهزة الكمبيوتر واستخدامها بشكل غير مصحح به هي نفسها، بغض النظر عما إذا كان الاختراق يهدف إلى الربح أو التخريب أو الإرهاب أو التدمير. ويكشف هذا عن خطر آخر: استخدام الأدوات الموجودة للنشاط الإرهابي والإضرار.

فالبنية التحتية الحيوية -بدلاً من أهداف الاحتيال المتوقعة للسرقة والأرباح السريعة- تهدد بالإضرار بالأمن القومي. وبالتالي فإن التطوير المستمر لآليات الجرائم السيبرانية أصبح مشكلة أمنية طبيعية.

تعتبر حماية البني التحتية الحيوية (CIP) هي القضية الأكثر أهمية في مجال أمن الفضاء الإلكتروني، والسوق السوداء للأسلحة السيبرانية تجعل الحاجة إليها أكثر إلحاحاً. يتيح هذا الاستغلال التجاري للقدرات التقنية والتشغيلية إمكانية وصول العديد من الفواعل -بما في ذلك المنظمات الإرهابية الصغيرة وحتى الأفراد المعزولين- إلى موارد قوية ذات تطبيقات محتملة للهجوم السيبراني. وبالتالي فإن المجموعة المرجعية للتهديدات تتسع لتجاوز الدول والمنظمات الإرهابية المعروفة لتشمل أي عنصر قادر على شراء الخدمات التجارية المتاحة *DarkMarket*.

ومع ذلك، عندما يكون هناك استثمار مستمر ترعاه الدولة في البحث والتطوير، فإن القدرات التكنولوجية المتاحة بشكل علني في السوق تختلف بطبيعة الحال عن تلك التي تعمل على تطويرها قوات الأمن ومؤسسات التعليم العالي في أي دولة. ولذلك فإن القدرات المتاحة في السوق ستكون أدنى من تلك المتاحة للمنظمات التي ترعاها الدولة والتي تتمتع بوسائل بحث وتطوير مستقلة، وتتمتع بدعم الدولة من حيث الموارد والتنظيم.

### 2.3. نحو إدراك مسؤولية الدولة عن الأمن السيبراني

لابد من توضيح معنى ظاهرة الجرائم السيبرانية للباحثين وصانعي السياسات - للأسباب المذكورة سابقاً- إذ لا توفر تقييمات الأضرار المالية أساساً واقعياً ثابتاً لفهم المفهوم أو صياغة السياسة. ولذلك، لابد من إعادة تقييم الجرائم السيبرانية لتصميم السياسة الوطنية المناسبة.

وحتى غياب الاتفاق على نطاق الضرر المباشر وغير المباشر الذي تسببه الجرائم السيبرانية، فإنه يؤثر بالتأكيد على كيفية عمل المواطنين والمنظمات والمجتمع ككل. يتضرر المواطنون والشركات الصغيرة بشكل مختلف بسبب الجرائم الإلكترونية. إن البريد العشوائي والاحتيال عبر الإنترنت وسرقة الهوية الرقمية وانهالك الخصوصية والابتزاز والتجسس الاقتصادي والإضرار بملكية الفكرية كلها أمور منتشرة على نطاق واسع وتضرر بعض المواطنين والمنظمات. ورغم أن التقييمات النقدية تبدو مبالغ فيها، فإن تطور الفضاء الإلكتروني يزيد من أعداد الضحايا المحتملين ويتوسّع سبل ارتكاب الجرائم ضد المواطنين والجماعات. ونظراً لتزايد الوعي بالمشكلة والزيادة الفعلية في الجرائم السيبرانية، فإن الدولة مطالبة بشكل معقول باتخاذ خطوات لتوفير الأمان السيبراني الشخصي والمجتمعي والوطني. يشير تزايد التعرض لانتهاكات البيانات والهجمات السيبرانية إلى نمو متناسب في الاهتمام بالمخاطر التي تشكلها الجرائم السيبرانية.

إن الدولة مسؤولة بشكل أساسي عن القانون والنظام وعن سلامة مواطنها، ويتعين عليها أن تعمل على تقليل الأضرار التي تلحق بهم. يجب أن تتطور السياسة على أساس فهم الآثار الواسعة لهذه الظاهرة وإجراء نقاش عام عقلاني ومستنير. وفيما يلي بعض المؤشرات لتطوير مثل هذا النقاش.

إن غالبية الظواهر الشائعة المصنفة على أنها جرائم إلكترونية لا علاقة لها بالأمن القومي. وهنا يطرح سؤال ما هي إذن أهمية نشر الكراهية والتحريض، ونشر الدعاية عبر وسائل التواصل الاجتماعي والبريد العشوائي، وتهكير حسابات الشبكات الاجتماعية، وإنشاء مقاطع فيديو وحملات على الإنترنت مسيئة للجمهور؟ سيكون المواطنون عرضة للخطر في الفضاء الإلكتروني وسيتعرض العديد منهم للتشهير.

عندما يصبح المواطن ضحية جريمة، يتوقع من سلطات الدولة معالجة الجريمة والتعامل معها. لدى سلطات الدولة مجموعة من الأساليب لتحقيق هذه الغاية ويحتاج معنى الأحداث هذا إلى توضيح لتحديد السياسة المناسبة. ولكن من منظور الأمن القومي، من الصعب رؤية الضرر على المستوى الوطني ما دام معدل الجرائم السيبرانية منخفضاً نسبياً، حتى لو كان أعلى من معدل الجرائم التقليدية. ومع ذلك، إذا تطورت الجريمة السيبرانية

لتصبح ظاهرة دائمة وواسعة النطاق، فقد يفقد المواطنون ثقتهم في سلطات الدولة التي تبدو غير متكافئة في توفير بيئة آمنة ومأمومة.

إن التصدي للتحديات الجديدة يتطلب، أولاً وقبل كل شيء، فهما واضحًا لمختلف الظواهر وانعكاساتها وتشعباتها. وتتطلب العمليات وصياغة السياسات وإنفاذها تنظيمًا وتشريعات محدثة. والتشريعات، التي تختلف بحكم تعريفها عن التطورات التكنولوجية، تقع ضمن نطاق السلطة الوحيدة للدولة.

تعمل هيئات الإنفاذ السيادية على أساس قانوني وطني. وسيتعين على البنية التحتية تخصيص المزيد من الموارد لمنع الجرائم السيبرانية والتحقيق فيها ومعاقبة مرتكبها. وعلى الرغم من الطبيعة الدولية للفضاء السيبراني، فإن الدولة هي المصدر الوحيد للمسؤولية عن الأمن الشخصي لمواطنيها. وتعمل المعاهدات الدولية، مثل اتفاقية بودابست التي أقرها مجلس الأوروبي بشأن الجرائم السيبرانية، والمبادرات الجاري تطويرها في الأمم المتحدة، ومنظمة التعاون الاقتصادي والتنمية، والاتحاد الأوروبي، والاتحاد الدولي للاتصالات، على تعزيز التعاون بين السلطات السيادية. وقد يساهم التعاون الدولي في تدعيم السلطات السيادية في مكافحة الجرائم السيبرانية، ولكن المعاهدات الدولية لا يمكن أن تحل محل السياسة السيادية المستقلة.

أولاً، التعاون بين الدول في الساحة الدولية (الفوضوية) غير ممكن إلا على نطاق محدود للغاية وعلى أساس المصالح المشتركة فقط. وربما تكون الديمقراطيات المتقدمة قادرة على صياغة الترتيبات فيما بينها، ولكن الفجوة بينها وبين الأنظمة الأخرى من حيث تعريف التهديد تبدو كبيرة للغاية.

يركز النقاش الأمريكي حول هذه القضية على التجسس الصناعي المستمر على الملكية الفكرية، وهو نتاج البحث والتطوير في القطاعين التجاري والحكومي في الولايات المتحدة. على مر السنين، أصبح كبار الموظفين في مجتمع الأعمال والحكومة يشعرون بالقلق على نحو متزايد إزاء خسارة الميزة الاقتصادية والاستراتيجية العالمية التي تتمتع بها الولايات المتحدة باعتبارها القوة العظمى والقوة العلمية والتكنولوجية الأولى. في الواقع، كلمة "الخسارة" ليست هي الكلمة الصحيحة، لأن المعرفة لا تفقد فعلياً، بل تسرق من خلال عمليات سرقة منهجية ومنظمة تنظيمًا جيدًا وواسعة النطاق برعاية الدولة، والمذنب في نظر الأمريكيين هي

الصين، الدولة العازمة على دفع اقتصادها إلى الأمام. وقوتها العسكرية تتقدم من خلال تقليد أسرار الأبحاث الأمريكية. ومن ثم تحول مناقشة هذه القضية بوضوح من التركيز على الاقتصاد وأمن البيانات والقانون إلى حوار أمريكي شبه قتالي. ومن جانبها، ترفض الصين هذه الادعاءات بشكل قاطع، وتشعر بالقلق إزاء تقويض أسس نظامها من خلال استخدام الإنترنت في الغرب باسم حرية التعبير.

ثانياً، تسمح سلطة وسيادة الدولة داخل حدودها بتعزيز سياسة مستقلة: فالتشريع وإنفاذ القانون لا يعتمدان على الترتيبات الدولية.

توضح الحادثة المعروفة باسم "قضية القرصنة السعودية" كيف يمتد النقاش من أمن البيانات إلى الأمن القومي. في أوائل يناير 2012، نشر شخص يطلق على نفسه اسم OxOmar قائمة تحتوي على المعلومات الشخصية وأرقام بطاقات الائتمان لآلاف المواطنين الإسرائيليين. كانت المعلومات المنشورة قديمة إلى حد كبير، ومن بين 380.000 إدخال، لم يكن سوى بضعة آلاف صالحة. الضرر المباشر الذي لحق بحاملي البطاقات كان صفرًا؛ حيث قامت شركات الائتمان بإلغاء البطاقات وأصدرت بطاقات جديدة. كما أن نطاق المعلومات التي تم الكشف عنها لم يكن استثنائيًا؛ فكل يوم، تتم سرقة الملايين من هذه الإدخالات على الإنترنت. حيث يتم تجميع التفاصيل وفقاً لمعايير مختلفة وبيعها لعملاء السوق السوداء.

يتم عادة إدخال برامج التجسس في عدد من الواقع التجارية، والتي تنقل البيانات المخزنة من قبل مشغلي الموقع مع تجاهل صارخ لأمن البيانات. وعلى الرغم من أن بعض الهجمات كانت تفتقر إلى التعقيد ولم تسبب في أي ضرر حقيقي للأفراد، ولم تحقق أرباح مالية من المعلومات، إلا أن المهاجمين يستخدمونها لنشر الخوف في البلد المستهدف.

يمكن تحليل هذا الحدث بأي عدد من الطرق المختلفة. قد يدعى المرء أن المواطنين غير مدركين لأمن البيانات؛ وأن وسائل الإعلام غير مسؤولة وتضخم حدثاً هامشياً بشكل مبالغ فيه، مما يؤدي إلى زرع الذعر؛ وأن أصحاب موقع الويب كانوا مهملين أو حتى مهملين إجرامياً في فشلهم في تأمين البيانات التي يحوزونها؛ وأن الدولة أهملت خلق بيئه آمنة للتجارة عبر الإنترنت وتأمين البيانات الشخصية. ولكن في أي تحليل فإن النتيجة الحتمية هي أن الأمن

الشخصي والجماعي للمواطنين في الفضاء الإلكتروني يحتاج إلى التحسين. وفي نهاية المطاف، هذا المطلب موجه إلى الدولة، المسئولة عن أمن مواطنيها وسلامتهم.

من الممكن، بل من المرغوب فيه، مناقشة تعريف الظواهر غير المرغوب فيها والإجرامية في الفضاء الإلكتروني، والمستوى المناسب من الأمن، وتقسيم المسؤولية، وزيادةوعي المستخدم، وحدود تدخل الدولة، والمعضلات الأخرى ذات الصلة بالمسألة. في الأنظمة الديمقراطية، يتم توضيح مثل هذه القضايا من خلال الخطاب العام والعملية السياسية. ولا يمكن افتراض أن الطلب على أمن الفضاء الإلكتروني سوف يختفي، أو أن الدولة ستتمكن من التخلص من مسؤوليتها تجاه المواطنين. لكن لا شيء يعفي سلطات الدولة من الاستجابة لمختلف مطالب المواطنين وإجراء تغييرات قانونية وتنظيمية لزيادة أمن البيانات على الواقع التجارية. سيؤدي الفشل في تنظيم وإنفاذ القانون والنظام في الفضاء السيبراني إلى تمكين مجموعة من الجرائم السيبرانية من الإزدهار، إلى حد إيجاد تهديدات حقيقة للأمن القومي: تقديم الخدمة لعناصر معادية تهدف إلى تنفيذ هجمات سيبرانية وزيادة نطاق الجريمة إلى حد المساس بالأمن الشخصي وبيئة الأعمال في البلاد.

### واجهة خطيرة:

إن الجرائم الإلكترونية باعتبارها تهديدا للأمن القومي تستمر في النمو وتتحدى الدول المتقدمة بطرق مختلفة. يتم الحصول على المعلومات الموجودة حول الجرائم الإلكترونية من التقارير الدورية التي تقدمها شركات الاستشارات وتكنولوجيا المعلومات وأمن المعلومات ووكالات إنفاذ القانون. ونظراً للمشاكل الكامنة في تحديد هذه الظاهرة، والاستخدام الخام للأساليب الإحصائية للتحليل الكمي، وإدراج الضرر غير المباشر في التقييمات النقدية، فمن الواضح أن المعلومات الموجودة ليست موثوقة. ويبدو أن التقييمات النقدية يتم تصفيتها باستمرار. ومع ذلك، لا يمكن التغاضي عن الخطير المحتمل الكبير الذي تنطوي عليه الجرائم السيبرانية.

يوضح التحليل الوارد في هذه المقالة أن مجموعة كبيرة من الجرائم الإلكترونية لا تمثل في الواقع تهديدا للأمن القومي. إن الظواهر مثل السرقة والتتجسس الصناعي والاحتيال والمحفوظات الضارة وجرائم الكراهية وتدمير الواقع الإلكتروني ورفض الخدمة وما إلى ذلك من الممكن أن تصبح مشكلة أمن قومي فقط إذا كانت هناك زيادة ملحوظة في حدوثها وكانت

آثارها دائمة. لذلك، حان الوقت الآن لاتخاذ الإجراءات الازمة للحد من المخاطر وجعل الأمر أكثر صعوبة على مجرمي الإنترن特 للعمل في هذا المجال.

وتظهر التجارب السابقة أن العناصر المعادية تقوم بتجنيد الخبرات الإجرامية لتحقيق أهداف عملياتية. ويسبب وتيرة التطورات التكنولوجية، فإن القدرات المتقدمة لـ تكنولوجيا المعلومات اليوم سوف تصبح في غضون سنوات قليلة سلعاً رخيصة الثمن ومتوفرة في الأسواق. وتجعل السوق السوداء لخدمات الكمبيوتر القدرات المتقدمة متاحة بسهولة. وتؤدي الأدلة إلى تفاقم القلق من وجود تعاون في الفضاء الإلكتروني أيضاً بين العناصر الإجرامية والكيانات المعادية.

وعلى أساس هذا التحليل، يوصى بالتركيز على واجهتين رئيسيتين بين الجريمة السيبرانية والأمن القومي. أولاً، الدولة القومية هي الكيان المسؤول عن السلامة والأمن الشخصي والجماعي لمواطنيها. تسبب الجرائم الإلكترونية أنواعاً مختلفة من الضرر للمواطنين والمنظمات. نطاق هذا الضرر غير واضح وتقديرات الأضرار المختلفة المقدمة في المناقشة غير موثوقة ومبالغ فيها إلى حد كبير. ولكن حتى من دون الاتفاق على نطاق الضرر الذي يتکبده المواطنون والمنظمات والدول، فلا يزال يتغير على الدولة أن تستجيب للفرص والتحديات التي يفرضها الواقع عندما يتكتشف. ومع الدخول المستمر للفضاء السيبراني في كل مناحي الحياة، فمن الأمن أن نفترض أن المطالب على الدولة لضمان الأمن الشخصي والوطني في الفضاء السيبراني سوف تنمو أيضاً. وعلى الرغم من الطبيعة العالمية للفضاء السيبراني، فسوف تضطر الدولة إلى توسيع مشاركتها بشكل كبير. لقد برزت الخطوط العريضة لتدخل الدولة في الفضاء السيبراني في السنوات الأخيرة، وكانت إحدى القضايا الأكثر إثارة للجدل هي القيم المتناقضة للخصوصية والأمن القومي. في النظام الديمقراطي، تتضمن عملية صياغة سياسة حكومية بشأن الجرائم الإلكترونية نقاشاً عاماً ومعاركاً سياسية ومعاملة قانونية طويلة الأمد.

ثانياً، يؤدي تسويق القدرات التقنية والتشغيلية إلى خفض عتبة الدخول إلى ساحة الحرب السيبرانية، وتوسيع نطاق التهديدات المرجعية إلى ما هو أبعد من الدول والمنظمات الإرهابية الكبيرة، ووضع عبئاً ثقيلاً للغاية على سلطات الأمن الوطني. تقدم المنظمات الإجرامية السيبرانية الموارد والبني التحتية وحتى خدمة العملاء بتكلفة معقولة. وهذا سوق

## جرائم الفضاء الإلكتروني وتأثيرها على الأمن القومي

يمكن استغلاله ليس فقط لارتكاب الجرائم لتحقيق مكاسب مالية، بل أيضاً لتنفيذ هجمات مباشرة على الأمن القومي. يعد الدفاع عن البنية التحتية الحيوية ضد تهديدات الفضاء الإلكتروني قضية رئيسية في الأمن السيبراني وتزداد أهميتها نظراً لانتشار المخاطر المحتملة القادرة على الحصول على أسلحة الفضاء السيبراني وتجنيد "مقاتلين" في السوق السوداء للجرائم السيبرانية.

ونظراً لتحليل أهمية الظاهرة وتحديد الواجهات الخطيرة بين الجرائم السيبرانية والأمن القومي، يجب أن يكون التركيز المباشر للدولة على التعامل مع التهديد من أجل منعه من أن يصبح أكثر حدة. ويتبعن على الدولة أن تعمل على تعزيز مشاركتها في خلق أمن الفضاء الإلكتروني، ولكنها لا تستطيع أن تحل المشكلة بمفردها. يتطلب الإدراك الناجح لمسؤولية الدولة عن أمن الفضاء الإلكتروني تعاون جميع الأطراف المعنية في قطاعات الأعمال والقطاعات الأكademie وال العامة والأمنية، وذلك لتوفير الأمن السيبراني الوطني والشخصي للدولة ومواطنيها.

## References:

- «2005 FBI Computer Crime Survey» p.10, [www.fbi.gov/publications/Ccs2005.pdf](http://www.fbi.gov/publications/Ccs2005.pdf)
- «Kaspersky Reveals Price List for Botnet Attacks» July 23, 2009, <http://www.computerweekly.com/news/1280090242/Kaspersky-reveals-price-listfor-botnet-attacks>. It seems that the cost continues to drop. See Plohmann,
- «Norton Study Calculates Cost of Global Cybercrime: \$114 Billion Annually, » [http://www.symantec.com/about/news/release/article.jsp?prid=20110907\\_02](http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02)
- A botnet is a collection of internet-connected computers whose defenses have been breached and control ceded to a malicious party gaining distance control and using these computers' capabilities. A botnet is commonly used for sending spam, attacking DDoS, and continuous data theft. See <https://www.checkpoint.com/products/anti-bot-software-blade/anti-bot-softwareblade-landing-page.html>.
- Abu Dhabi, <http://eprints.qut.edu.au/38894/1/c38894.pdf.6> CoE, « Convention on Cybercrime, » Budapest, 2001, <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm>.
- All high profile cases of cyber espionage, such as « GhOst RAT, » RSA / Dinei Florêncio and Cormac Herley, « Sex, Lies and Cybercrime Surveys, » Microsoft Research, 2012. The study was condensed and appeared as an op-ed piece in Dinei Florêncio and Cormac Herley, « The Cybercrime Wave That Wasn't, » New York Times, April 15, 2012, <https://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasn't.html?>
- EU, Europol, the European Cybercrime Centre (EC3) officially commenced its activities on January 1, 2013, <https://www.europol.europa.eu/ec3.42>
- Gerhards-Padilla, and Leder, Botnets : 10 Tough Questions.33 Jeffrey Carr, November 2, 2011, <http://jeffreycarr.blogspot.com/2011/11/words-matter-dump-apt-for-apa.html>.
- Lockheed-Martin, and « Flame » are examples of an APA.35 Software as a Service : Strategic Backgrounder (Washington, D.C. : Software & Information Industry Association, February 28, 2001), <http://www.siiainc.org/estore/pubs/SSB-01.pdf>.
- McAfee, « Virtual Criminology Report : Organized Crime and the Internet, » December 2007, [www.mcafee.com/us/research/criminology\\_report](http://www.mcafee.com/us/research/criminology_report)
- Office of Cyber Security & Information Assurance in the UK Cabinet Office and BAE Detica, : « The Cost of Cyber Crime, » 2011, <http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crimefull-report.pdf>.
- Wall, Cybercrime, p. 221.13 See for example the GAO-07-705-Cybercrime Report, June 17, 2007, pp. 16-17. <http://www.gao.gov/assets/270/262608.pdf>