الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف -المسيلة

فرقة بحث "حماية الفضاء السيبراني من الهجمات الالكترونية"

وبالتنسيق مع مخبر الدراسات والبحوث في القانون والأسرة والتنمية الادارية

كلية الحقوق والعلوم السياسية

مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية

شهادة مشاركة

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 الالكترونية" وبالتنسيق مع مخبر الدراسات والبحوث في القانون والأسرة والتنمية الادارية. يوم 15 ديسمبر 2024 حضوريا وعن بُعد.

بمداخلة بعنوان: جرائم الفضاء الالكتروني و تأثيرها على الأمن القومي

عميد الكلية

الجلط فواز

مدير المخبر

الدكتور

عبد العزيز

رئيس الملتقى

الدكتور: داود كمال

وزارة التعليم العالي والبحث العلمي
كلية الحقوق والعلوم السياسية
جامعة محمد بوضياف المسيلة

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

فرقة بحث"حماية الفضاء السيبراني من الهجمات الالكترونية"

وبالتنسيق مع

مخبر الدراسات والبحوث في القانون والأسرة والتنمية الادارية

برنامج الملتقى 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

المزمع تنظيمه حضوريا وعن بعد يوم الاحد15ديسمبر2024

قاعة المحاضرات مولود بديار

التوقيت: 16:20-9:00

الجلسة الافتتاحية

رابط الجلسة الافتتاحية:

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

الجلسة الرئيسية الحضورية: برئاسة : أ. ضريفي نادية التوقيت: 09.40- 11.30

رابط الجلسة الرئيسية:

الرقم	الاسم واللقب	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	المسيلة الجلفة	09.50-09.40
2	د. محمد بوضياف	خطوات إعداد إستراتيجية مواجهة الجرائم السيبرانية	المسيلة	10.00-09.50
3	أ.د قسمية محمد	مكافحة الجرائم السيبرانية في التشريع الدولي والجزائري	المسيلة	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 و الاتصال و مكافحتها أنموذجا	المسيلة	10.20-10.10
5	د. عمارة عمارة	الإجراءات الخاصة لمواجهة الجريمة السيبرانية و الوقاية منها: المساس بأنظمة المعالجة الآلية للمعطيات أنموذجا	المسيلة	10.30-10.20
6	د. مراد يرمش	أثر الجريمة الالكترونية على حقوق الملكية الفكرية	المسيلة	10.40-10.30
7	د.تاهمي مصطفى ط.د مروان قرابسي	فهم تعرض الأمن القومي في الجزائر للمخاطر السيبرانية و سبل الوقاية منها	المسيلة	10:50-10.40
8	د .زبيري عبد الله د. لعجال عفيفة	تعزيز الوعي الأمني مقاربات بديلة لمواجهة التهديدات و المخاطر	المسيلة	11.00-10.50
9	ا.د ضريفي نادية د. لعجال منى	اليات مكافحة الجرائم السيبرانية	المسيلة المسيلة	11:10-11:00
10	د. زروقي مرزاقة د. حشاني فاطمة الزهراء	الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والافاق المستقبلية	جامعة المسيلة	11:20-11:10
11	د. كمال داود	اثار السيادة السيبرانية على الحقوق الرقمية	المسيلة	11:30-11:20

مناقشة 11:40-11:30

الجلسة الأولى عن بعد: برئاسة : د. بوعون نضال التوقيت: 13.00- 16.00

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

الرقم	الاسم واللقب	عنوان المداخلة	مؤسسة الانتماء	التوقيت
1	د.بلعابد عيدة د.سليماني جميلة	الجريمة المعلوماتية و مقتضيات الأمن الرقمي	جامعة سعيدة	13.10-13.00
2	ط.د. قارة عبد الحق	مفهوم الجرائم السيبرانية(التعريف النشأة و التطور)	المركز الجامعي النعامة	13.20-13.10
3	ط.د بن زهرة السعيد	التداعيات المباشرة وغير المباشرة للجريمة السيبرانية على السيادة و الأمن الوطنيين	جامعة المدية	13.30-13.20
4	د. حططاش عمر	اختصاص الاقطاب الجزائية في الجرائم السيبرانية	المسيلة	13.40-13.30
5	د.حمربط النواري	تطور النظام القانوني للجريمة الالكترونية	المسيلة	13.50-13.40
6	أ.د السعيد برابح د.كشيدة الطاهر	الجهود الإقليمية لمكافحة الجريمة السيبرانية	المسيلة	14.00-13.50
7	د. بوعون نضال د. لخضر حمينة عبد الله	الجريمة السيبرانية في منظور القانون الدولي العام	المسيلة	14.10-14.00
8	ط . د دحماني رشيد	آليات مكافحة الجريمة السيبرانية في التشريع الجزائري	الوادي	14.20-14.10
9	د. لرقط الحسين د. مومن رضوان	تحديات الأمن السيبراني في ظل ثورة لذكاء الاصطناعي –قراءة في واقع التجربة الجزائري-	المسيلة برج بوعريريج	14:30-14:20
10	د. الوافي السعيد	اجراءات التحقيق الخاصة بالجرائم السيبرانية	المسيلة	14.40-14.30
11	د.زيتوني عادل د. بوضياف الخير	الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني	المسيلة	14:50-14:40
12	ط.د زكري عبد المجيد	الجريمة السيبرانية الأفاق والتحديات	جامعة تونس	15:00-14:50
13	د.عيساوي الساسي د.غول أمينة	الجرائم السيبرانية مفهومها و أنواعها	سوق أهراس	15:10-15:00
14	ط.د.جلود وسام د.عبد الغني حجاب	جرائم الفضاء الالكتروني و تأثيرها على الأمن القومي	جامعة المسيلة	15.20-15.10
15	ا. لعمارة عبد الرزاق	المعالجة التشريعية للتهديدات السيبرانية في التشريع الجزائري و التشريع المقارن	المسيلة	15:30-15:20
16	ط.د.تيزراوي نعيمة	استراتيجيات المواجهة و التصدي للجريمة السيبرانية: آليات الوقاية و المكافحة	جامعة تيزي وزو	15:40-15:30

مناقشة 15:50- 16:00

الجلسة الثانية عن بعد: برئاسة د. مسعودي رشيد التوقيت: 13.00 – 16.10

رابط الجلسة الثانية عن بعد: meet.google.com/nnm-cdax-hzd

الرقم	الاسم واللقب	عنوان المداخلة	مؤسسة الانتماء	التوقيت
1	د.عبدلي حمزة ط.ددوارة فاطمة	نحو تفعيل تكنولوجية الذكاء الاصطناعي في مجال الوقاية و التحري عن جرائم الفساد دراسة مقارنة	المسيلة	13.10-13.00
2	د.قاوي السعيد	السيادة السيبرانية و الرقمنة الوطنية و سبل تعزيزها	المسيلة	13.20-13.10
3	د.لعزازقة حمزة	فعالية تحليل السلوك الإجرامي السيبراني بين تطبيقات الذكاء الاصطناعي و الاستخبارات 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 الالكترونية في التشريع الجزائري	سكيكدة	13.50-13.40
6	د رابعي ابراهيم	النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال	المسيلة	14.00-13.50
7	ط. د.بركانة محمد ط.د مقدم مختار	آليات مكافحة الجريمة الالكترونية على المستوى الدولي و الوطني	المركز الجامعي النعامة	14.10-14.00
8	د . خوجة اسامة	السيبرانية منطقة تغلغل الحرب الخفية وبسط القوة في ظل الالفية الثالثة	المسيلة	14.20-14.10
9	د. فراحتية اكرم د. بوعكاز خليل	الجريمة السيبرانية بين الحداثة و حتمية التقنين	المسيلة	14:30-14:20
10	أ . د عطوي خالد	الفضاء السيبراني و السيادة : علاقة تأثير و تأثر	المسيلة	14.40-14.30
11	د. بوعيسي حسام الدين د. محمدي اسمهان	التحولات الامنية الجديدة في ظل التطور الرقمي: الجزائر أنموذجا آليات الحماية و الوقاية	المسيلة	14:50-14:40
12	د. برابح حمزة	مكافحة الجريمة السيبرانية في اطار منظمة الامم المتحدة	المسيلة	15:00-14:50
13	د صغير بيرم عبد المجيد ط.دقيزة حليم	في كيفية حماية الخصوصية الوطنية من الجريمة العابرة للأوطان	المسيلة	15:10-15:00
14	د. بن النوي زبير	الاثبا ت في الجريمة السيبرانية	المسيلة	15.20-15.10
15	د. رشيد مسعودي	مقترح لهندسة إستراتيجية أمنية تشابكية لمواجهة التهديدات الاتماثلية للإجرام السيبراني على منظومة الأمن الوطني في الجزائر	المسيلة	15:30-15:20
16	د.بلمهدي ابراهيم	رقمنة المرافق العمومية بين تقديم الخدمة وتهديدات الجرائم السيبرانية	جامعة المسيلة	15:40-15:30
17	د. بوعكة الكاملة	الحماية القانونية للأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي على ضوء القانون 07-18	جامعة المسيلة	15:50-15:40
18	د.قمرة النذير	جريمة الاعتداء على الخصوصية في التشريع الجزائري	جامعة المسيلة	16:00-15:50

مناقشة 16:20-16:30

الجلسة الختامية

قراءة التوصيات واختتام الملتقى

جرائم الفضاء الإلكتروني وتأثيرها على الأمن القومي

Cybercrime and its impact on national security

د عبد الغني حجاب
جامعة محمد بوضياف –المسيلة - الجزائر
Abdelghani.hadjab@univ-msila.dz

ط (*) وسام جلود
جامعة محمد بوضياف –المسيلة - الجزائر
djeloud.wissam@gmail.com

تاريخ الارسال : اليوم/الشهر/السنة	تاريخ القبول : ××/××/××

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 الأمن 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 جزءًا لا يتجزأ من حياتنا. فالحوسبة دورها في تحسين وتبسيط العمليات المتعلقة بالعمل والتعلم والترفيه لا يقدر بثمن، وتؤثر فعليًا 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 لمحة عن التعاون بين المجرمين والجريمة المنظمة والمنظمات المعادية، ويناقش تسويق قدرات الاستطلاع والهجوم السيبراني، التي أصبحت ممكنة بفضل التقنيات المتطورة 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 تهديدًا كبيرًا 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 الحوسبة بتقسيم المهام إلى وحدات صغيرة وتحقيق اللامركزية في المعالجة؛ تتيح الشبكات الوصول العالمي إلى المعلومات والتركيز على المعرفة كمنتج قيم. يتم تطبيق التقنيات المحوسبة 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،[1] والتعريف المقترح للجريمة السيبرانية هو: "استخدام الفضاء السيبراني لأغراض غير قانونية، مع استغلال ميزات الفضاء السيبراني الفريدة، مثل السرعة والفورية؛ والتشغيل عن بعد؛ والتشفير 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) وفقًا للهدف المستهدف: الممتلكات أو الأشخاص أو الدولة.[2]

ويميز (Shinder) و(Cross) بين أنواع الجرائم وفقًا لمستوى العنف المعني: "الجرائم العنيفة والجرائم العنيفة المحتملة، والجرائم غير العنيفة (كتجارة المخدرات وغسيل الأموال)، والجريمة التي لا يزال يُنظر إليها على أنها تقع ضمن فئة ذوي الياقات البيضاء[2] (اقتحام أجهزة الكمبيوتر، والسرقة، والاحتيال).3

ووفقًا لـ(وول)، فإن الجرائم السيبرانية هي "تحويل السلوك الإجرامي أو الضار بواسطة التكنولوجيا الشبكية". لقد تطورت نتيجة لتطور الحوسبة والفضاء الإلكتروني وما ترتب على ذلك من فرص جديدة للحصول على المعلومات أو تعطيلها أو التلاعب بها لتحقيق مكاسب. ويصنف وول أيضًا الجرائم الإلكترونية إلى ثلاث فئات: الجريمة التي تنطوي على سلامة أنظمة الكمبيوتر ونظام عملها (القرصنة)؛ جرائم استغلال الفضاء الإلكتروني (الاتصالات

---

[1]

[2] **عمال الياقات البيضاء** بالإنجليزيةWhite-collar Workers : هو مصطلح غربي يطلق على أولئك الناس الذين يقومون بعمل «ذهني» مكتبي مثل المديرين والمتخصصين، وهم بذلك يتميزون عن أصحاب الياقات الزرقاء (Blue-collar Workers) الذين يقومون بعمل يدوي ميداني كالعمال، كما يطلق مصطلح آخر وهو أصحاب الياقات الوردية (pink-collar worker) للعمال الذين يعملون في أعمال خدمة الزبائن.

المشفرة بين المجرمين)؛ والجرائم التي تنطوي على محتويات معلوماتية محوسبة (سرقة الأسرار، ونشر محتويات ضارة).

ويصنف الجدول الملحق1 الجريمة على أساس الدور الذي يلعبه الحاسوب في ارتكاب الجريمة، وهو موقف مماثل لما اعتمدته الاتفاقية الأوروبية بشأن الجرائم الإلكترونية.

//////////////

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 المحوسبة للأنظمة 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 دائما ظاهرة اجتماعية منتشرة على نطاق واسع، وتجمع التفسيرات الجنائية بين الدافع والفرصة والعديد من دوافع السلوك الإجرامي جوهرية 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 أيضًا 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 للتكاليف 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 المحوسبة، 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 أيضًا سرقة البنوك. على سبيل المثال، يعد استخدام شبكات الروبوت التي تضم عشرات الآلاف من أجهزة الكمبيوتر الشخصية لسرقة تفاصيل الهوية إلى المواقع المصرفية والتي يتم استخدامها بعد ذلك لسرقة مبالغ صغيرة من المال، أمرًا شائعًا جدًا. ونظراً لمشكلة تحديد هوية المجرم في الفضاء السيبراني، فإن فرص تحديد هوية المجرم ضئيلة.[1]

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 لمجرمي الإنترنت. ولكن على الرغم من ذلك، فإن المخاطر المادية المباشرة لا تزال أقل بكثير بالنسبة للمجرم السيبراني مقارنة بالمجرم "التقليدي". كما أن خطر العقوبة القانونية سابقا كان أقل أيضًا، نظرًا لأن النظام القضائي كان ينظر عمومًا إلى الاحتيال عبر الإنترنت على أنه جريمة غير عنيفة من نوع "ذوي الياقات البيضاء". وكان يتم التعامل معه وفقًا لذلك.

2. نطاق الجرائم الإلكترونية والأضرار اللاحقة

عادة 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 بتخزين قاعدة بيانات مكونة من ألف إدخال قد تم اختراقه؛ لنفترض أيضًا أن قاعدة البيانات غير مشفرة وأن الإدخالات مكتوبة بنص عادي. بحيث يمثل كل إدخال بطاقة ائتمان صالحة، بما في ذلك جميع المعلومات اللازمة 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 قادرون على تقدير القيمة المالية للمعلومات التي يتم الوصول إليها بشكل كامل؟ هل يستطيع اللص تقييم القيمة الحقيقية 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 تنوعًا من المجيبين الذين يقدمون تقديراتهم الخاصة لعدد الحوادث وقيمة الأضرار، ولكنها أيضًا طريقة تحتوي على بعض العيوب الخطيرة التي تقلق علماء الاجتماع والإحصائيين. ثانيًا، في غياب بيانات كافية، يستخدم الباحثون الأساليب الإحصائية لاستخلاص التقييمات من البيانات الجزئية. 2

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 تقدير الضرر، ويبدو حتى الآن أن التقييمات النقدية التي نشأت عن الاستخدام الفج للأساليب الإحصائية لتقديم الافتراضات على أساس بيانات غير كافية تميل إلى المبالغة. بالإضافة إلى مسائل موثوقية طرق البحث ومصداقية مصادر المعلومات ومدى ملاءمة المنهج الإحصائي لهذا النوع من البحث.

هناك أيضًا مشكلة أخرى. غالبًا 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.

إعادة النظر في معنى الجرائم السيبرانية

إن أي فحص حالي 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 ويفتقر إلى موارد البحث والتطوير يجد أسلحة الفضاء الإلكتروني (مجموعات أدوات البرامج الضارة) متاحة للتنزيل من الإنترنت، وعادةً ما يكون ذلك مقابل دفع مبلغ يتراوح بين عشرات إلى عدة آلاف من الدولارات. إن المعرفة منتج لا ينضب، وهي "سلعة غير منافسة" بالنسبة للاقتصاديين. لكن الانطباع السائد بأن الفضاء

الإلكتروني يسهل جني الأرباح الضخمة من المؤسسات الإجرامية لم يغب عن عالم الجريمة المنظمة.34

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 عادةً دون تعطيل عملها الطبيعي. وعادةً 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.[1]323

والظاهرة الأحدث هي التهديد المستمر المتقدم (APT) والمعروفة أيضًا باسم الهجوم التكيفي المستمر3 (APA) وهو عبارة عن أسلحة معقدة ومتعددة المراحل من الفضاء الإلكتروني لغرض الهجمات السرية المستمرة. لا يعمل المهاجم إحصائيًا على نطاق واسع لاستغلال نقاط الضعف المعروفة؛ وبدلا من ذلك فإن الهدف محدد بشكل جيد. يستخدم المهاجم مجموعة من الأدوات المخصصة. وتتكون 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 أذونات 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. وبمجرد تحديد اللاعبين الرئيسيين، يتم بذل جهد متضافر لسرقة بيانات اعتمادهم وإصابة أجهزة الكمبيوتر الخاصة بهم.

تتمثل إحدى الطرق في التصيد الاحتيالي، أو إدخال أداة الوصول عن بعد (RAT) عن طريق بريد إلكتروني من مرسل موثوق به محتوى ذي صلة، وبالتالي يتمكن من تجاوز آليات تصفية البريد العشوائي باستخدام المعلومات الشخصية المجمعة. يسمح فتح البريد الإلكتروني بإدخال (حصان طروادة) في نقطة نهاية موثوقة داخل شبكة الشركة الخاصة

بالمؤسسة، وبالتالي الوصول إلى المزيد من الموارد الداخلية. في الجرائم العادية، 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 جزئيًا إلى التغلب على أنظمة الدفاع المصممة لمنع تسرب المعلومات. أثناء الهجوم، يقوم المهاجمون بإجراء اختبارات لتحديد حدود استجابة النظام وعادةً ما يقومون بتكييف طرق التسلل للمعلومات المسروقة. يتم تقسيم البيانات إلى حزم صغيرة، مموهة داخل الاتصالات المشروعة، وبالتالي تتسرب عبر النظام دون إثارة الدفاعات. 34

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

لقد نجح الفنيون 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، والمجرمون، 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. .35

على مر السنين، شهد النموذج العديد من التحولات؛ والكلمة المعبرة الحالية لها هي "الحوسبة السحابية". المبرر الاقتصادي للنموذج واضح: من الآن فصاعدا، 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 قُدر نطاق السوق العالمية لهذا النوع من خدمات الكمبيوتر بمبلغ 14.5 مليار دولار في عام 2012. 3

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 مجرمًا إلكترونيًا قد انخفض. لم يعد من الضروري أن يمتلك الشخص الكفاءة لتطوير الأدوات والأساليب لاختراق أجهزة الكمبيوتر بنفسه. إن البنية التحتية التكنولوجية اللازمة لاختراق أجهزة الكمبيوتر واستخدامها بشكل غير مصرح 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. 3

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 البنى التحتية الحيوية (CIP) هي القضية الأكثر أهمية في مجال أمن الفضاء الإلكتروني، والسوق السوداء للأسلحة السيبرانية تجعل الحاجة إليها أكثر إلحاحا. 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 تتوسع لتتجاوز الدول والمنظمات الإرهابية المعروفة لتشمل أي عنصر قادر على شراء الخدمات التجارية المتاحة لـ DarkMarket.

ومع ذلك، عندما يكون هناك استثمار مستمر ترعاه الدولة في البحث والتطوير، فإن القدرات التكنولوجية المتاحة بشكل علني في السوق تتخلف 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.

نحو إدراك مسؤولية الدولة عن الأمن السيبراني

لابد من توضيح معنى ظاهرة الجرائم السيبرانية للباحثين وصانعي السياسات - للأسباب المذكورة سابقا- إذ لا تُوفر تقييمات الأضرار المالية أساسًا واقعيًا ثابتًا 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 وانتهاك الخصوصية والابتزاز والتجسس الاقتصادي والإضرار بالملكية الفكرية كلها أمور منتشرة على نطاق واسع وتضر ببعض المواطنين والمنظمات. ورغم أن التقييمات النقدية تبدو مبالغ فيها، فإن تطور الفضاء الإلكتروني يزيد من أعداد الضحايا المحتملين ويوسع سبل ارتكاب الجرائم ضد المواطنين والجماعات. ونظراً لتزايد الوعي بالمشكلة والزيادة الفعلية في الجرائم السيبرانية، فإن الدولة مطالبة بشكل معقول باتخاذ خطوات لتوفير الأمن 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 مواطنيها، ويتعين عليها أن تعمل على تقليل الأضرار التي تلحق بهم. ويجب 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 يُطرح 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 منخفضا نسبيا،

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 ومأمونة.

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

تعمل هيئات الإنفاذ السيادية على أساس قانوني وطني. وسيتعين على البنى التحتية تخصيص المزيد من الموارد لمنع الجرائم السيبرانية والتحقيق فيها ومعاقبة مرتكبيها. 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 المجلس 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.

أولا، 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 تُفقد فعليًا، بل تُسرق 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 تتحول مناقشة هذه القضية بوضوح من التركيز على الاقتصاد وأمن البيانات والقانون إلى حوار أمني 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 صفراً: 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 وفقًا لمعايير مختلفة وبيعها لعملاء السوق السوداء.[1]

يتم عادة إدخال برامج تجسس في عدد من المواقع 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 تتسبب 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 يدعي المرء أن المواطنين غير مدركين لأمن البيانات؛ وأن وسائل الإعلام غير مسؤولة وتضخّم حدثًا هامشيًا بشكل مبالغ فيه، مما يؤدي إلى زرع الذعر؛ وأن أصحاب مواقع الويب كانوا مهملين أو حتى مهملين إجراميًا في فشلهم في تأمين البيانات التي بحوزتهم؛ وأن الدولة أهملت خلق بيئة 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، المسؤولة 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، وزيادة وعي 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 التنصل من مسؤوليتها تجاه المواطنين. لكن لا شيء يعفي سلطات الدولة من الاستجابة لمختلف مطالب المواطنين وإجراء تغييرات قانونية وتنظيمية لزيادة أمن البيانات على المواقع التجارية. سيؤدي الفشل في تنظيم وإنفاذ القانون والنظام في الفضاء السيبراني إلى تمكين مجموعة من الجرائم السيبرانية من الازدهار، إلى حد إيجاد تهديدات حقيقية 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 تهديدًا 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 تضخيمها باستمرار. ومع ذلك، لا يمكن التغاضي عن الخطر المحتمل الكبير الذي تنطوي عليه الجرائم السيبرانية.

يوضح التحليل الوارد في هذه المقالة أن مجموعة كبيرة من الجرائم الإلكترونية لا تمثل في الواقع تهديدًا للأمن القومي. إن الظواهر مثل السرقة والتجسس الصناعي والاحتيال والمحتويات الضارة وجرائم الكراهية وتدمير المواقع الإلكترونية 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 اللازمة للحد من المخاطر وجعل الأمر أكثر صعوبة على مجرمي الإنترنت للعمل في هذا المجال.

وتظهر التجارب السابقة أن العناصر المعادية تقوم بتجنيد الخبرات الإجرامية لتحقيق أهداف عملياتية. وبسبب وتيرة التطورات التكنولوجية، فإن القدرات المتقدمة لتكنولوجيا 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 أيضًا 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 أنواعًا 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 يتكبده المواطنون والمنظمات والدول، فلا يزال يتعين على الدولة أن تستجيب للفرص والتحديات التي يفرضها الواقع عندما يتكشف. ومع الدخول المستمر للفضاء السيبراني في كل مناحي الحياة، فمن الآمن أن نفترض أن المطالب على الدولة لضمان الأمن الشخصي والوطني في الفضاء السيبراني سوف تنمو أيضًا. 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 نقاشًا عامًا ومعاركًا سياسية ومعاملة قانونية طويلة الأمد.

ثانيا، 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 عبئا ثقيلا للغاية على سلطات الأمن الوطني. تقدم المنظمات الإجرامية السيبرانية الموارد والبنى التحتية وحتى خدمة العملاء بتكلفة معقولة. وهذا سوق

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

ونظرًا 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. ويتعين 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 الأكاديمية والعامة والأمنية، وذلك لتوفير الأمن السيبراني الوطني والشخصي للدولة ومواطنيها.

1 P. N. Grabosky, « Virtual Criminality : Old Wine in New Bottles ? » Social &Legal Studies, 10, no. 2 (2001) : 243-49.
2. Majid Yar, Cybercrime and Society : Crime and Punishment in the Information Age(London : SAGE Publications, 2006).
3. D. L. Shinder and M. Cross, Scene of the Cybercrime (Burlington, MA :Syngress, 2008).
4. David S. Wall, Cybercrimes : The Transformation of Crime in the Information Age(Cambridge : Polity, 2007), p. 10.
5. A. Alkaabi, G. M. Mohay, A. J. McCullagh, and A. N. Chantler, « Dealing withthe Problem of Cybercrime, » Conference Proceedings of 2nd InternationalICST Conference on Digital Forensics & Cyber Crime, October 4-6, 2010.
6. 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.
7. A botnet is a collection of internet-connected computers whose defenseshave been breached and control ceded to a malicious party gaining distancecontrol and using these computers' capabilities. A botnet is commonly usedfor sending spam, attacking DDoS, and continuous data theft. See https://www.checkpoint.com/products/anti-bot-software-blade/anti-bot-softwareblade-landing-page.html.
8. Asymmetric key cryptography is the basis of the RSA algorithm developedby Leonard Adelman, Adi Shamir, and Ron Rivest, and presented publiclyin 1978. Its patent expired in 2000. PGP (Pretty Good Privacy) developedby Phil Zimmermann in 1991 was the first software to allow free use ofstrong encryption using this method. The

common web security standards(HTTPS, TLS/SSL, SSH, Bitcoin) are employing the same public key
9. Cryptography principle.9 Richard M. Ryan and Edward L. Deci, « Intrinsic and Extrinsic Motivations :Classic Definitions and New Directions, » Contemporary EducationalPsychology 25, no. 1 (2000) : 54-67.10
10. R. Piquero and Stephen G. Tibbetts, eds., Rational Choice and CriminalBehavior : Recent Research and Future Challenges (New York : Routledge, 2002).

11. The number of infected computers is itself no indication of the network'spower or potential damages. See Daniel Plohmann, Elmar Gerhards-Padilla,Felix Leder, Botnets : 10 Tough Questions (ENISA, 2011).
12. 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.
14. « 2005 FBI Computer Crime Survey, » p.10, www.fbi.gov/publications/ Ccs2005.pdf.15 Melissa E. Hathaway, « Falling Prey to Cybercrime : Implications for Business
And the Economy, » ch. 6, in Securing Cyberspace : A New Domain for National Security (Queenstown : Aspen Institute, February 2012).16 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.
17. « Norton Study Calculates Cost of Global Cybercrime : $114 BillionAnnually, » http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.
18. M. Lesk, « Cybersecurity and Economics, » IEEE Security & Privacy, 9. No. 6 (2011), p. 76 ; Carl Bialik, « A Cybercrime Stat's Nine Lives, » WallStreet Journal, September 26, 2007, http://blogs.wsj.com/numbersguy/acybercrime-stats-nine-lives-194/tab/print/.
19. Dinei Florêncio and Cormac Herley, « Sex, Lies and Cybercrime Surveys, »Microsoft Research, 2012. The study was condensed and appeared asan op-ed piece in Dinei Florêncio and Cormac Herley, « The CybercrimeWave That Wasn't, » New York Times, April 15, 2012, https://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_
R=3&hpw.20Card Verification Code – the secret three-digit code printed on the back of Credit cards, used to verify the validity of the card details when the card isnot being read magnetically.
23. J. Hunt, « The New Frontier of Money Laundering : How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and HowGovernments Are Trying to Stop Them, » Information and CommunicationsTechnology Law 20, no. 2 (2011) : 133-52.
Actors, Motivations, Threats, and Countermeasures, » in Nir Kshetri, ed, The Global Cybercrime Industry : Economic, Institutional and Strategic Perspectives (Heidelberg ; London : Springer, 2010) ; Misha Glenny, Darkmarket :Cyberthieves, Cybercops, and You (New York : Alfred A. Knopf, 2011).

28. Cyber weapons may be categorized by their intended usage : malware -malicious software meant to disrupt the normal workings of a computerizedsystem clandestinely, thereby damaging the process controlled by thatsystem ; spyware – malicious software meant to gather data clandestinelyand sometimes transfer it over the internet ; scanners to identify knownvulnerabilities ; remote and local exploits – to exploit known vulnerabilities ;network sniffers – to eavesdrop on communications ; backdoor tools, Trojanhorses – for distance access and data retrieval.
31. McAfee, « Virtual Criminology Report : Organized Crime and the Internet, »December 2007, www.mcafee.com/us/research/criminology_report; C.Czosseck, G. Klein, and F. Leder, « On the Arms Race around Botnets :Setting up and Taking Down Botnets, » paper presented at the Cyber Conflict (ICCC), 2011 3rd International Conference, June 7-10, 2011.
32. « 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, 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.
34. All high profile cases of cyber espionage, such as « GhOst RAT, » RSA/ Lockheed-Martin, and « Flame » are examples of an APA.35Software as a Service : Strategic Backgrounder (Washington, D.C. : Software & Information Industry Association, February 28, 2001), http://www.siia.net/estore/pubs/SSB-01.pdf.
38. CoE, « Convention on Cybercrime. » Since 2001, the convention has been Ratified by 30 of the 46 signatory nations.
39. T. Maurer, « Cyber Norm Emergence at the United Nations : An Analysis ofthe UN's Activities regarding Cybersecurity, » Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.40 OECD, « Communiqué on Principles for Internet Policy-Making, » June 29, 2011.
41. EU, Europol, the European Cybercrime Centre (EC3) officially commencedits activities on January 1, 2013, https://www.europol.europa.eu/ec3.42 ITU, National Cybersecurity Strategy Guide, September 2011.
43. Mike McConnell, Michael Chertoff, and William Lynn, « China's CyberThievery is National Policy-and Must Be Challenged, » Wall Street Journal,January 27, 2012 ; Richard Clarke, « How China Steals our Secrets, » New YorkTimes, April 2, 2012 ; Nathan Gardels, « Cyberwar : Former Intelligence ChiefSays China Aims at America's Soft Underbelly, » New Perspectives Quarterly27, no. 2 (2010) :15-17 ; Joel Brenner, America the Vulnerable : Inside the NewThreat Matrix of Digital Espionage, Crime, and Warfare (New York : PenguinPress, 2011) ; U.S.-China Economic and Security Review Commission(USCC), 2009 Report to Congress of the U.S.-China Economic and SecurityReview Commission.
44. See Myriam Anna Dunn and Kristian Søby Kristensen, eds., Securing « theHomeland » : Critical Infrastructure, Risk and (In)Security (London : Routledqe,2007).
46. Dump : a stolen credit card or bank account and the associated customerdata. T. J. Holt, and E. Lampke, « Exploring Stolen Data Markets Online :Products and Market Forces, » Criminal Justice Studies 23, no. 1 (2010).