1

الأمن السيبراني للمرافق الحيوية دراسة مقارنة للإطار القانوني والتنظيمي لحماية البنية التحتية الحساسة من الهجمات الإلكترونية بين مصر والجزائر وفرنسا

La cybersécurité des infrastructures critiques Étude comparative du cadre juridique et réglementaire de protection des infrastructures sensibles contre les cyberattaques entre l Égypte l Algérie et la France

د. محمد كمال عرفه الرخاوي

الى ابنتي الحبيبة صبرينة قرة عيني المصرية الجزائرية جميلة الجميلات التي تجمع بين جمال نهر النيل الخالد وجمال شط المتوسط وجبال الاوراس

المقدمة الأمنية والمنهجية لدراسة حماية المرافق الحيوية

Security and Methodological Introductionto the Study of Critical Infrastructure Protection

في العصر الرقمي، لم تعد الحروب تُدار فقط بالأسلحة التقليدية

بل أصبحت تُشن عبر الكابلات الضوئية والشبكات الإلكترونية

حيث تحولت محطات الكهرباء والمياه والمطارات

والمستشفيات

إلى أهداف استراتيجية في مرمى الهجمات السيبرانية المتطورة

فأي خلل في هذه المرافق الحيوية يمكن أن يؤدي

إلى شلل كامل للدولة وانهيار الثقة في مؤسساتها

وتكتسب هذه الدراسة أهميتها من كونها أول عمل أكاديمي مقارن

يتناول الإطار القانوني والتنظيمي لحماية هذه المرافق

بين ثلاثة أنظمة قانونية ذات خلفيات متميزة

فمصر والجزائر تمثلان نموذجاً للدول النامية

التي تسابق الزمن لبناء دفاعاتها السيبرانية

في حين تمثل فرنسا رائدة في وضع الأطر التنظيمية

التي تحاول ترويض هذا التهديد غير المرئي

وسيتبع البحث منهجاً تحليلياً مقارناً

يبدأ بدراسة الأسس الدستورية والتشريعية لكل نظام

ثم ينتقل إلى تحليل الاجتهاد القضائي والتطبيقات العملية

ليخلص إلى مجموعة من الاستنتاجات والمقترحات الإصلاحية

التي تهدف إلى بناء "دفاع سيبراني فعال"

لحماية شرايين الحياة في الدولة الحديثة

2

الإطار المفاهيمي للأمن السيبراني والمرافق الحيوية

Conceptual Framework of Cybersecurity and Critical Infrastructure

لا يمكن فهم التحديات الأمنية دون تعريف دقيق لمفاهيمها الأساسية

فالأمن السيبراني هو مجموعة التدابير والإجراءات

التي تهدف إلى حماية الأنظمة والشبكات والبيانات

من الهجمات أو الوصول غير المصرح به أو التدمير

أما المرافق الحيوية فهي تلك الأصول والأنظمة

التي تعتبر ضرورية لاستمرار الدولة وحياة المواطنين

وتشمل قطاعات الطاقة والمياه والنقل والاتصالات

والصحة والمالية والخدمات الحكومية الأساسية

ويتميز الأمن السيبراني للمرافق الحيوية عن الأمن العام

بأنه يتعامل مع تهديدات أكثر تطوراً وخطورة

تستهدف ليس فقط سرقة البيانات بل تعطيل الخدمات الحيوية

مما يجعله جزءاً لا يتجزأ من الأمن القومي الحديث

وقد تطور مفهوم المرافق الحيوية ليشمل

ليس فقط الأصول المادية بل أيضاً الأصول الرقمية

مثل قواعد البيانات الوطنية وأنظمة التحكم الصناعي

التي أصبحت هدفاً رئيسياً للهجمات السيبرانية المتطورة

3

الأسس الدستورية لحماية المرافق الحيوية في النظام القانوني المصري

Constitutional Foundations for Protecting Critical Infrastructure in the Egyptian Legal System

يستمد الإطار القانوني لحماية المرافق الحيوية

في مصر

مشروعيته من عدة مواد دستورية محورية

فالمادة ١٥ من الدستور لسنة ٢٠١٤ تنص على أن

"الدولة ملتزمة باتخاذ الإجراءات اللازمة لحماية الأمن القومي"

وهذا يشمل الأمن السيبراني كجزء أساسي من الأمن القومي الحديث

كما أن المادة ٥٤ التي تحمي الحياة الخاصة

تشكل ضمانة ضد أي اختراق غير مشروع للبيانات

التي قد تؤدي إلى استهداف المرافق الحيوية

بالإضافة إلى ذلك، فإن المادة ٦٥ التي تنص على أن

"العدالة أساس الحكم" تفرض على الدولة

اتخاذ التدابير اللازمة لحماية جميع المواطنين

من أي تهديد قد يؤدي إلى انقطاع الخدمات الأساسية

إلا أن الدستور المصري يفتقر إلى نصوص صريحة

تنظم الأمن السيبراني بشكل خاص

أو تحدد المرافق الحيوية بدقة

مما يخلق فجوة تشريعية كبيرة

تستدعي تحديثاً دستورياً وتشريعياً عاجلاً

4

الأسس الدستورية لحماية المرافق الحيوية في النظام القانوني الجزائري

Constitutional Foundations for Protecting Critical Infrastructure in the Algerian Legal System

يجد الإطار القانوني لحماية المرافق الحيوية في الجزائر

سنده في مجموعة من المبادئ الدستورية الأساسية

فالمادة ٣٧ من الدستور لسنة ٢٠٢٠ تنص على أن

"الدولة ملتزمة بحماية الأمن القومي بمختلف أبعاده"

وهذا يشمل البعد السيبراني الذي أصبح جزءاً لا يتجزأ

من الأمن القومي في العصر الرقمي

كما أن المادة ٤٤ التي تحمي الحياة الخاصة

تشكل قيداً أساسياً على أي اختراق للبيانات

التي قد تستخدم في استهداف البنية التحتية الحساسة

ومن جهة أخرى، فإن المادة ٣٣ التي تنص على أن

"العدالة أساس الحكم" تفرض على الدولة

اتخاذ التدابير اللازمة لحماية جميع المواطنين

من أي تهديد قد يؤدي إلى انقطاع الخدمات الأساسية

إلا أن الدستور الجزائري، شأنه شأن الدستور المصري

يفتقر إلى نصوص صريحة تنظم الأمن السيبراني

أو تحدد المرافق الحيوية بدقة

مما يخلق واقعاً من الفراغ الدستوري

يهدد أمن الدولة ويستدعي مراجعة شاملة

5

الأسس الدستورية لحماية المرافق الحيوية في النظام القانوني الفرنسي

Constitutional Foundations for Protecting Critical Infrastructure in the French Legal System

يتميز النظام الدستوري الفرنسي بوضوحه في التعامل

مع التحديات الأمنية الحديثة

فالمبادئ الواردة في الإعلان العالمي لحقوق الإنسان لسنة ١٧٨٩

والتي تشكل جزءاً من الكتلة الدستورية

تنص على أن الحرية تكمن في ألا يُضر المرء بالآخرين

وهذا يشمل حماية الدولة من الهجمات السيبرانية

التي قد تؤدي إلى أضرار جسيمة للمواطنين

والأهم من ذلك أن فرنسا كانت سباقة في تبني مفهوم

"الأمن السيبراني الوطني" من خلال قانون الجمهورية الرقمية لسنة ٢٠١٦

الذي أرسى الأسس الدستورية لحماية البنية التحتية الحساسة

كما أن المجلس الدستوري الفرنسي أكد في اجتهاده

على أن حماية الأمن القومي تشمل البعد السيبراني

وأن للدولة الحق في اتخاذ التدابير اللازمة

لحماية مرافقها الحيوية من أي تهديد خارجي

ومن الناحية القضائية، بدأ مجلس الدولة الفرنسي

في تطوير اجتهاد جديد يتعامل مع الهجمات السيبرانية

ويطالب الإدارة بإثبات اتخاذها للتدابير الوقائية اللازمة

لحماية المرافق الحيوية من الاختراقات

6

التشريعات الناظمة للأمن السيبراني في مصر

ودورها في الحماية

Regulatory Legislationon Cybersecurity in Egypt and its Role in Protection

يعد قانون مكافحة الجرائم الإلكترونية رقم ١٧٥ لسنة ٢٠١٨

الحجر الأساس لأي تنظيم مستقبلي للأمن السيبراني في مصر

فقد نص القانون على عقوبات رادعة ضد اختراق الأنظمة

وسرقة البيانات وتعطيل الخدمات الإلكترونية

وقد أنشأ القانون المركز الوطني للأمن السيبراني

كمؤسسة مستقلة تتولى الإشراف على تطبيق أحكامه

ومراقبة الجهات الحكومية والخاصة ذات الأهمية الاستراتيجية

إلا أن القانون يعاني من عدة ثغرات خطيرة

فهو لا يفرق بين الهجمات العادية والهجمات الموجهة

ضد المرافق الحيوية التي تتطلب حماية خاصة

كما أنه لا ينص صراحة على تصنيف المرافق الحيوية

ولا يوفر آليات فعالة للإبلاغ عن الاختراقات

ومن الناحية العملية، فإن غياب لوائح تنفيذية تفصيلية

وغياب الخبرة الفنية لدى المركز الوطني يحد من فعالية التطبيق

كما أن معظم التطبيقات الحكومية للبنية التحتية الحيوية

لا تخضع لرقابة سيبرانية مشددة

مما يخلق واقعاً من الفراغ التنظيمي يهدد الأمن القومي

7

التشريعات الناظمة للأمن السيبراني في الجزائر ودورها في الحماية

Regulatory Legislationon Cybersecurity in Algeria and its Role in Protection

يُعد قانون مكافحة الجرائم الإلكترونية رقم ١٥-٠٤ لسنة ٢٠١٥

الإطار التشريعي الأساسي المنظم للأمن السيبراني في الجزائر

فقد نص القانون على عقوبات ضد اختراق الأنظمة

وسرقة البيانات وتعطيل الخدمات الإلكترونية

كما أنشأ القانون وكالة وطنية للأمن السيبراني

تتولى مهمة الإشراف على تطبيق القانون وحماية الجهات الحساسة

إلا أن هذا الإطار التشريعي يعاني من قصور كبير

في مواجهة التحديات الأمنية الحديثة

فهو لا يتطرق إطلاقاً إلى مفهوم "المرافق الحيوية"

ولا يمنح الأجهزة الأمنية صلاحيات كافية

لاكتشاف الهجمات المعقدة قبل وقوع الضرر

بالإضافة إلى ذلك، يحتوي القانون على استثناءات واسعة

لصالح الدفاع الوطني والأمن العام

دون وجود رقابة قضائية فعالة على استخدام هذه الاستثناءات

مما يفتح الباب أمام انتهاكات قد تهدد الخصوصية

ومن الناحية التطبيقية، فإن الوكالة الوطنية

تفتقر إلى الموارد البشرية والتقنية اللازمة

لمراقبة التطبيقات المتزايدة للبنية التحتية الحيوية

مما يستدعي تحديثاً تشريعياً عاجلاً لسد هذه الثغرات

8

التشريعات الناظمة للأمن السيبراني في فرنسا ودورها في الحماية

Regulatory Legislationon Cybersecurity in France and its Role in Protection

تتمتع فرنسا بأحد أكثر الأطر التشريعية تطوراً

في مجال الأمن السيبراني للمرافق الحيوية

فبالإضافة إلى التزامها الكامل بتطبيق التوجيه الأوروبي

لأمن شبكات المعلومات (NIS Directive)

فقد سبقت العديد من الدول بسن تشريعات وطنية متخصصة

فقانون الأمن السيبراني لسنة ٢٠١٣

أنشأ وكالة الأمن السيبراني الوطنية (ANSSI)

كسلطة رقابية قوية ومتمتعة باستقلالية واسعة

لديها صلاحيات التحقيق والتفتيش وفرض الغرامات

على الجهات التي تنتهك قواعد حماية المرافق الحيوية

كما أن قانون الجمهورية الرقمية لسنة ٢٠١٦

ألزم جميع المشغلين للمرافق الحيوية

بتطبيق تدابير أمنية صارمة وتقديم تقارير دورية

عن حالة أمنهم السيبراني

وأخيراً، فإن مشروع قانون الأمن السيبراني الجديد

يهدف إلى ترجمة مبادئ الاتحاد الأوروبي إلى واقع تشريعي ملموس

من خلال تصنيف المرافق الحيوية حسب مستوى الخطورة

وفرض متطلبات صارمة على القطاعات عالية الخطورة

وهذا يعكس رؤية استراتيجية واضحة تجعل من حماية الأمن القومي

ركيزة أساسية لأي تقدم تقني

9

ضوابط المشروعية في القرارات الإدارية المتعلقة بالأمن السيبراني في مصر

Safeguards of Legality in Administrative Decisions Relatedto Cybersecurity in Egypt

تخضع القرارات الإدارية المتعلقة بالأمن السيبراني في مصر

لنفس مبادئ المشروعية التي تحكم القرار البشري

وهي الشرعية والاختصاص والشكل والموضوعية

لكن تطبيقها يواجه تحديات جديدة

فمن حيث الشرعية، فإن غياب تشريع خاص ينظم الأمن السيبراني

يجعل الكثير من هذه القرارات تفتقر إلى أساس قانوني صريح

وتعتمد على تفسيرات واسعة لقوانين قديمة

لا تتناسب مع الواقع الرقمي

أما من حيث الاختصاص، فإن السؤال الجوهري هو

هل يمكن أن تمارس سلطة اتخاذ القرار الأمني من قبل أنظمة ذكية؟

ومن الناحية النظرية، يبقى الموظف العام أو الجهة الإدارية

هي صاحبة الاختصاص، لكن في الواقع العملي

كثيراً ما يكون القرار آلياً دون أي تدخل بشري حقيقي

مما يخل بمبدأ شخصية القرار الإداري

وفيما يتعلق بالشكل، فإن مبدأ التسبيب يصبح عديم الفائدة

إذا كان السبب الوحيد هو "نتيجة النظام الذكي"

دون شرح للمنطق أو المعطيات التي أدت إلى هذا القرار

وهذا يحرم المواطن من حقه في الدفاع عن نفسه أو الطعن في القرار

10

ضوابط المشروعية في القرارات الإدارية المتعلقة بالأمن السيبراني في الجزائر

Safeguards of Legality in Administrative Decisions Relatedto Cybersecurity in Algeria

تخضع القرارات الإدارية المتعلقة بالأمن السيبراني في الجزائر

لمبادئ المشروعية التقليدية

لكن التطبيق العملي يكشف عن فجوة كبيرة بين النظرية والواقع

فمن حيث الشرعية، فإن غياب أي نص تشريعي ينظم الأمن السيبراني

يجعل هذه الممارسة تفتقر إلى أساس قانوني واضح

وتعتمد على توجيهات داخلية أو مشاريع تجريبية غير منشورة

وفيما يتعلق بالاختصاص، يفترض القانون أن الموظف العام

هو من يمارس سلطة القرار، لكن في العديد من التطبيقات

يكون القرار النهائي آلياً دون أي تدخل بشري فعلي

مما يطرح تساؤلات جوهرية حول مشروعية نقل سلطة القرار إلى آلة

ومن أخطر التحديات ما يتعلق بمبدأ التسبيب

فكيف يمكن لمواطن أن يطعن في قرار أمني

إذا كان السبب الوحيد هو "نتيجة النظام الذكي"

دون أي شرح للمنطق أو المعايير المستخدمة

وهذا يخل بجوهر حق الدفاع ويحول القرار الإداري إلى عمل غامض

11

ضوابط المشروعية في القرارات الإدارية المتعلقة

بالأمن السيبراني في فرنسا

Safeguards of Legality in Administrative Decisions Relatedto Cybersecurity in France

يتميز النظام القانوني الفرنسي بتطويره لضوابط دقيقة

تحكم مشروعية القرار الإداري الأمني

فمن حيث الشرعية، فإن استخدام الأنظمة الذكية في اتخاذ القرار

يجب أن يستند إلى نص تشريعي صريح يحدد نطاقه وأهدافه

وفيما يتعلق بالاختصاص، فإن القضاء الفرنسي

يؤكد على مبدأ جوهري

هو أن "النظام الذكي لا يمكن أن يكون صاحب سلطة القرار"

بل تظل أداة في يد الموظف العام الذي يتحمل المسؤولية النهائية

ويجب أن يكون هناك دائماً إمكانية لمراجعة بشرية للقرار الأمني

أما من حيث الشكل، فقد تطور مبدأ التسبيب ليواكب العصر الرقمي

فلم يعد يكفي ذكر نتيجة النظام الذكي

بل يجب على الإدارة أن تقدم "توضيحاً معقولاً للمنطق الكامن"

وراء القرار بما يسمح للمواطن بفهم الأسباب الجوهرية

ومن الناحية الموضوعية، فإن القضاء الفرنسي بدأ في تطوير معايير جديدة

للتحقق من عدالة النظام الذكي، حيث يطالب الإدارة بإثبات

أن البيانات المستخدمة في تدريبه خالية من التحيّز

وأن النموذج نفسه تم اختباره للتأكد من عدم تمييزه ضد فئات معينة

12

الرقابة القضائية على القرارات الأمنية الصادرة عن أنظمة ذكية في مصر

Judicial Review of Security Decisions Issued by Intelligent Systems in Egypt

تخضع القرارات الأمنية الصادرة عن أنظمة ذكية في مصر

لنفس قواعد الرقابة القضائية التي تحكم القرارات البشرية

أمام محكمة القضاء الإداري، ولكن التطبيق العملي يواجه عقبات جسيمة

فمن حيث الاختصاص، لا يوجد خلاف على أن

المحكمة الإدارية

هي الجهة المختصة بالنظر في طعون هذه القرارات

طالما كانت صادرة عن جهة إدارية في نطاق سلطتها

لكن المشكلة الجوهرية تكمن في عبء الإثبات

فكيف يمكن للمواطن أن يثبت أن النظام الذكي كان تمييزياً

أو أن البيانات المستخدمة فيه كانت غير دقيقة

وهو لا يملك أي حق في الوصول إلى كود النظام أو معطياته؟

كما أن القاضي الإداري المصري يفتقر إلى الخبرة الفنية

اللازمة لفهم كيفية عمل الأنظمة الذكية المعقدة

ولا توجد لديه سلطة قانونية لطلب تدقيق فني مستقل لها

مما يجعل رقابته شكلية في كثير من الأحيان

13

الرقابة القضائية على القرارات الأمنية الصادرة عن أنظمة ذكية في الجزائر

Judicial Review of Security Decisions Issued by Intelligent Systems in Algeria

تخضع القرارات الأمنية الصادرة عن أنظمة ذكية في الجزائر

لرقابة مجلس الدولة باعتباره الجهة القضائية العليا

في المنازعات الإدارية، ويُجوز الطعن فيها لأسباب مشابهة لتلك المتبعة في مصر

إلا أن التحديات العملية التي تواجه الرقابة القضائية

تشبه إلى حد كبير تلك الموجودة في النظام المصري

فالمواطن الجزائري يجد نفسه في موقف ضعيف عند الطعن

لأنه لا يملك الحق في الوصول إلى المعلومات الفنية

الخاصة بكيفية عمل النظام الذكي أو البيانات التي استندت إليها

كما أن القاضي الجزائري يفتقر إلى الأدوات الفنية والقانونية

اللازمة لفحص عدالة النظام الذكي أو كشف أي تحيّز كامن فيه

ولا توجد في التشريع الجزائري أحكام تسمح للقضاء

بطلب تقرير خبير مستقل لتدقيق النظام الذكي

14

الرقابة القضائية على القرارات الأمنية الصادرة عن أنظمة ذكية في فرنسا

Judicial Review of Security Decisions Issued by Intelligent Systems in France

تتميز الرقابة القضائية على القرارات الأمنية الذكية في فرنسا

بفعاليتها وحداثتها، حيث طور مجلس الدولة آليات مبتكرة

للمواجهة التحديات التي يطرحها "الصندوق الأسود" الذكي

فمن حيث الإجراءات، يمكن للمواطن الطعن في القرار الذكي

أمام المحاكم الإدارية بنفس السبل المتاحة للقرارات البشرية

ولكن مع ميزة إضافية، وهي حقه في طلب "توضيح معقول للمنطق"

الذي اعتمده النظام الذكي في اتخاذ القرار

والأهم من ذلك أن القاضي الإداري الفرنسي يتمتع بسلطة واسعة

لطلب "تدقيق ذكي" (Intelligent Audit) من قبل خبراء مستقلين

معتمدين من قبل الدولة، حيث يقوم هؤلاء الخبراء بفحص

كود النظام الذكي والبيانات المستخدمة فيه واختباراته

للتحقق من خلوه من التحيّز ومن احترامه للقانون

15

التحديات الأخلاقية والعملية لاستخدام الذكاء الاصطناعي في الأمن السيبراني المصري

Ethical and Practical Challenges of Using Artificial Intelligence in Egyptian Cybersecurity

يواجه استخدام الذكاء الاصطناعي في الأمن السيبراني في مصر

تحديات أخلاقية وعملية عميقة تهدد فعاليته وعدالته

فمن الناحية الأخلاقية، يشكل "التحيّز الذكي" أكبر التحديات

فإذا كان النظام الذكي مدرباً على بيانات تاريخية تعكس تمييزاً

ضد فئات اجتماعية أو جغرافية معينة، فإنها ستكرس هذا التمييز

باسم الأمن والعلم، مما يؤدي إلى ظلم منهجي جديد

كما أن غياب الشفافية يخلق ما يُعرف بـ "الاستبداد الذكي"

حيث يصبح القرار الأمني عملاً غامضاً لا يمكن فهمه أو الطعن فيه

مما يقوض الثقة بين المواطن والإدارة ويولد شعوراً بالعجز

ومن الناحية العملية، فإن نقص الكفاءات الفنية داخل الجهاز الإداري

يجعل من الصعب تصميم أو مراقبة أنظمة ذكاء

اصطناعي فعالة

كما أن ضعف البنية التحتية الرقمية في بعض المحافظات

يؤدي إلى تفاوت في جودة الحماية الأمنية المقدمة للمواطنين

16

التحديات الأخلاقية والعملية لاستخدام الذكاء الاصطناعي في الأمن السيبراني الجزائري

Ethical and Practical Challenges of Using Artificial Intelligence in Algerian Cybersecurity

يواجه استخدام الذكاء الاصطناعي في الأمن السيبراني في الجزائر

تحديات أخلاقية وعملية مشابهة لتلك الموجودة في مصر، مع بعض الخصوصيات

فمن الناحية الأخلاقية، يشكل غياب الشفافية والمساءلة

تهديداً رئيسياً لحقوق المواطنين، خاصة في ظل غياب

أي إطار تشريعي ينظم "الحق في تفسير القرار الأمني الذكي"

مما يحول الإدارة إلى كيان غامض يتخذ قرارات لا يمكن فهمها

كما أن خطر "التحيّز الذكي" قائم بقوة

خاصة إذا استخدمت الأنظمة الذكية في مجالات حساسة

مثل مراقبة الاتصالات أو تحليل السلوك

بناءً على بيانات قد تعكس تفاوتات اجتماعية أو جهوية تاريخية

ومن الناحية العملية، فإن نقص الخبرات التقنية المتخصصة

داخل الإدارة الجزائرية يحد من قدرتها على تطوير

أو حتى مراقبة أنظمة ذكاء اصطناعي معقدة

كما أن التفاوت في البنية التحتية الرقمية بين الولايات

يؤدي إلى تفاوت في جودة الحماية الأمنية المقدمة

17

التحديات الأخلاقية والعملية لاستخدام الذكاء الاصطناعي في الأمن السيبراني الفرنسي

Ethical and Practical Challenges of Using Artificial Intelligence in French Cybersecurity

رغم التقدم الكبير الذي حققه النظام الفرنسي

في تنظيم الذكاء الاصطناعي

فإنه لا يخلو من تحديات أخلاقية وعملية تستدعي اليقظة المستمرة

فمن الناحية الأخلاقية، يبقى "التحيّز الذكي" تهديداً دائماً

حتى مع وجود ضوابط صارمة، لأن التحيّز قد يكون خفياً

ويصعب اكتشافه حتى من قبل الخبراء، خاصة في الأنظمة الذكية المعقدة

ومن الناحية العملية، فإن التعقيد الإداري الناتج عن تعدد مستويات الحكم

(Local, Regional, National) قد يؤدي إلى تباين في تطبيق القواعد

الخاصة بالذكاء الاصطناعي بين الجهات المختلفة

كما أن تكلفة تدقيق الأنظمة الذكية وصيانتها بشكل دوري

تشكل عبئاً مالياً كبيراً على البلديات الصغيرة

التي قد تفتقر إلى الموارد اللازمة لضمان عدالة أنظمتها

18

الإصلاحات التشريعية المقترحة لتعزيز الأمن السيبراني للمرافق الحيوية في مصر

Proposed Legislative Reforms to Enhance Cybersecurity of Critical Infrastructure in Egypt

تستدعي التحديات التي يطرحها الأمن السيبراني في مصر

إعلاناً تشريعياً شاملاً يضع الأسس القانونية لحمايته

أولاً، يجب إصدار قانون خاص للأمن السيبراني يُرسي مبادئه الأساسية

مثل العدالة وعدم التحيّز والشفافية والمساءلة وقابلية التفسير

ويحدد بوضوح المرافق الحيوية التي يُسمح بحمايتها بأنظمة ذكية

ثانياً، يجب تعديل قانون مكافحة الجرائم الإلكترونية رقم ١٧٥ لسنة ٢٠١٨

لإضافة فصل خاص بالمرافق الحيوية، ينص صراحة على

"الحق في تفسير القرار الأمني الذكي" و"الحق في المراجعة البشرية"

ثالثاً، يجب إنشاء سلطة تنظيمية مستقلة متخصصة في الأمن السيبراني

تتولى مهمة منح تراخيص لأنظمة الحماية عالية

الخطورة

وإجراء تدقيقات دورية عليها، ووضع معايير فنية وأخلاقية لتصميمها

19

الإصلاحات التشريعية المقترحة لتعزيز الأمن السيبراني للمرافق الحيوية في الجزائر

Proposed Legislative Reforms to Enhance Cybersecurity of Critical Infrastructure in Algeria

تستدعي التحديات التي يطرحها الأمن السيبراني في الجزائر

إعلاناً تشريعياً شاملاً يضع الأسس القانونية لحمايته

أولاً، يجب إصدار قانون خاص للأمن السيبراني يُرسي مبادئه الأساسية

مثل العدالة وعدم التحيّز والشفافية والمساءلة وقابلية التفسير

ويحدد بوضوح المرافق الحيوية التي يُسمح بحمايتها بأنظمة ذكية

ثانياً، يجب تعديل قانون مكافحة الجرائم الإلكترونية رقم ١٥-٠٤ لسنة ٢٠١٥

لإضافة فصل خاص بالمرافق الحيوية، ينص صراحة على

"الحق في تفسير القرار الأمني الذكي" و"الحق في المراجعة البشرية"

ثالثاً، يجب إنشاء سلطة تنظيمية مستقلة متخصصة في الأمن السيبراني

تتولى مهمة منح تراخيص لأنظمة الحماية عالية الخطورة

وإجراء تدقيقات دورية عليها، ووضع معايير فنية وأخلاقية لتصميمها

20

الخاتمة

Conclusion

كشفت هذه الدراسة المقارنة أن الأمن السيبراني للمرافق الحيوية

ليس مجرد تحدٍ تقني، بل هو اختبار وجودي لدولة القانون في العصر الرقمي

فبينما تسعى فرنسا إلى بناء "أمن سيبراني جدير بالثقة"

من خلال تشريعات متقدمة وضوابط قضائية فعالة

فإن مصر والجزائر لا تزالان في بداية الطريق نحو تنظيم هذا المجال

وقد أظهر التحليل أن التحدي الأساسي لا يتمثل في التكنولوجيا نفسها

بل في غياب الإطار القانوني والأخلاقي الذي يضمن استخدامها لخدمة الإنسان

وليس لتعزيز الاستبداد الأمني أو ترسيخ أشكال جديدة من التمييز

ومن ثم فإن استخلاص الدروس من التجربة الفرنسية لا يعني النسخ الحرفي

بل يتطلب تكييف الحلول بما يتناسب مع الخصوصية القانونية والاجتماعية لكل دولة

وقد قدمت هذه الدراسة مقترحات إصلاحية عملية تستند إلى المقارنة الموضوعية

تهدف إلى بناء دفاع سيبراني فعال وخاضع للمساءلة

وفي النهاية، فإن مستقبل الأمن القومي في القرن الحادي والعشرين

سيتوقف على قدرة الدول على الجمع بين كفاءة الذكاء الاصطناعي

وأخلاقيات دولة القانون، لضمان أن التحول الرقمي

يكون أداة لتعزيز الأمن وليس لتقويضه

21

دور الجهات الرقابية في ضمان الأمن السيبراني للمرافق الحيوية في النظام القانوني المصري

The Role of Oversight Bodies in Ensuring Cybersecurity of Critical Infrastructure in the Egyptian Legal System

تلعب الجهات الرقابية دوراً محورياً في ضمان الأمن السيبراني للمرافق الحيوية

لكن هذا الدور لا يزال في مراحله الأولى في النظام القانوني المصري

فالمجلس القومي للأمن السيبراني، الذي أنشأه القانون رقم ١٧٥ لسنة ٢٠١٨

يمتلك صلاحية نظرية لمراقبة الجهات الحكومية والخاصة ذات الأهمية الاستراتيجية

إلا أن غياب الخبرة الفنية والموارد البشرية يحد من قدرته الفعلية

على فهم وفحص الأنظمة الذكية المعقدة المستخدمة في المرافق الحيوية

كما أن الجهاز المركزي للمحاسبات، كجهة رقابية مالية

لا يمتلك حتى الآن الولاية القانونية أو الأدوات الفنية

للتقييم الفني والأخلاقي لأنظمة الأمن السيبراني

رغم أنه يمكن أن يكون لاعباً أساسياً في هذا المجال

بالإضافة إلى ذلك، فإن البرلمان المصري

يفتقر إلى لجان متخصصة في التكنولوجيا والأمن السيبراني

مما يحد من قدرته على ممارسة الرقابة التشريعية الفعالة

على استخدام هذه التقنيات في القطاعات الحيوية

وحتى الآن، فإن غياب التنسيق بين هذه الجهات

وعدم وجود استراتيجية وطنية موحدة

يجعل من جهود الرقابة مبعثرة وضعيفة

مما يستدعي إعادة هيكلة شاملة لهذه الجهات

ومنحها الصلاحيات والأدوات اللازمة لمواجهة تحديات العصر الرقمي

22

دور الجهات الرقابية في ضمان الأمن السيبراني للمرافق الحيوية في النظام القانوني الجزائري

The Role of Oversight Bodies in Ensuring Cybersecurity of Critical Infrastructure in the Algerian Legal System

تلعب الجهات الرقابية دوراً محورياً في ضمان الأمن السيبراني للمرافق الحيوية

لكن هذا الدور يواجه تحديات كبيرة في النظام القانوني الجزائري

فالوكالة الوطنية للأمن السيبراني، التي أنشأها القانون رقم ١٥-٠٤ لسنة ٢٠١٥

تتمتع بصلاحيات نظرية لمراقبة الجهات الحساسة

إلا أن غياب الموارد البشرية والتقنية يحد من قدرتها الفعلية

على فهم وفحص الأنظمة الذكية المعقدة المستخدمة في المرافق الحيوية

كما أن المحاسبة العليا، كجهة رقابية مالية

لا تمتلك حتى الآن الولاية القانونية أو الأدوات الفنية

للتقييم الفني والأخلاقي لأنظمة الأمن السيبراني

رغم أهمية دورها في مراقبة الإنفاق العام على هذه المشاريع

بالإضافة إلى ذلك، فإن البرلمان الجزائري

يفتقر إلى لجان متخصصة في التكنولوجيا والأمن السيبراني

مما يحد من قدرته على ممارسة الرقابة

التشريعية الفعالة

على استخدام هذه التقنيات في القطاعات الحيوية

وحتى الآن، فإن غياب التنسيق بين هذه الجهات

وعدم وجود استراتيجية وطنية موحدة

يجعل من جهود الرقابة مبعثرة وضعيفة

مما يستدعي إعادة هيكلة شاملة لهذه الجهات

ومنحها الصلاحيات والأدوات اللازمة لمواجهة تحديات العصر الرقمي

23

دور الجهات الرقابية في ضمان الأمن السيبراني للمرافق الحيوية في النظام القانوني الفرنسي

The Role of Oversight Bodies in Ensuring Cybersecurity of Critical Infrastructure in the French Legal System

تتميز فرنسا بوجود شبكة متكاملة من الجهات الرقابية

التي تلعب دوراً فعالاً في ضمان الأمن السيبراني للمرافق الحيوية

فأولاً، تأتي الوكالة الوطنية للأمن السيبراني

(ANSSI)

كسلطة رقابية مستقلة قوية، تتمتع بصلاحيات واسعة

للحصول على المعلومات، وإجراء التفتيشات، وفرض الغرامات

على الجهات التي تنتهك قواعد حماية المرافق الحيوية

ثانياً، يلعب مجلس الدولة الفرنسي دوراً رقابياً قضائياً فعالاً

من خلال مراجعة مشروعية القرارات الإدارية الأمنية

وطلب تدقيقات ذكية عند الضرورة

ثالثاً، يتمتع البرلمان الفرنسي بلجان متخصصة

في الشؤون الرقمية والتكنولوجيا، تقوم بمراجعة التشريعات

ومراقبة تنفيذها، وعقد جلسات استماع للخبراء والمسؤولين

رابعاً، توجد هيئة وطنية للحوار الأخلاقي

تضم خبراء من مختلف المجالات لمناقشة التحديات الأخلاقية

الناشئة عن استخدام الذكاء الاصطناعي في الأمن السيبراني

وأخيراً، فإن المجتمع المدني الفرنسي

يلعب دوراً رقابياً فعالاً من خلال المنظمات غير الحكومية

والجمعيات المهنية التي تراقب استخدام التكنولوجيا

وتدعو إلى مزيد من الشفافية والعدالة

وكل هذه الجهات تعمل في تناغم ضمن استراتيجية وطنية موحدة

تجعل من فرنسا نموذجاً يُحتذى به في مجال الرقابة على الأمن السيبراني

24

دور المجتمع المدني في تعزيز الأمن السيبراني للمرافق الحيوية مقارنة بين الأنظمة الثلاثة

The Role of Civil Society in Promoting Cybersecurity of Critical Infrastructure A Comparison Between the Three Systems

يختلف دور المجتمع المدني في تعزيز الأمن السيبراني للمرافق الحيوية

بشكل كبير بين الأنظمة القانونية الثلاثة

ففي فرنسا، يلعب المجتمع المدني دوراً رقابياً فعالاً

من خلال منظمات غير حكومية متخصصة مثل "Access Now" و"La Quadrature du Net"

التي تقوم بتحليل أنظمة الأمن السيبراني الحكومية

وكشف أي تحيّز أو انتهاك للخصوصية، ورفع التقارير إلى الجهات الرقابية

كما تشارك هذه المنظمات في المشاورات العامة

التي تنظمها الحكومة قبل اعتماد أنظمة جديدة

أما في مصر، فإن دور المجتمع المدني لا يزال محدوداً

بسبب غياب التشريعات الداعمة لحرية تداول المعلومات

وعدم توفر الخبرات الفنية اللازمة لفهم الأنظمة الذكية

رغم وجود بعض المبادرات الفردية من قبل الباحثين والصحفيين

التي تحاول رصد حالات سوء الاستخدام

وفي الجزائر، يواجه المجتمع المدني تحديات مشابهة لتلك الموجودة في مصر

فغياب الإطار القانوني الواضح لحرية المعلومات

وافتقار المنظمات إلى الموارد الفنية والبشرية

يحد من قدرتها على ممارسة رقابة فعالة

على استخدام الذكاء الاصطناعي في القطاعات الحيوية

ومن ثم، فإن المقارنة تظهر أن فعالية المجتمع المدني

مرتبطة ارتباطاً وثيقاً بوجود بيئة تشريعية داعمة

وتوفر الموارد الفنية اللازمة، مما يستدعي

بناء قدرات هذه المنظمات في مصر والجزائر

لتمكينها من لعب دورها كشريك أساسي في الرقابة

25

التعاون الدولي في مجال الأمن السيبراني للمرافق الحيوية دراسة مقارنة

International Cooperation in Cybersecurity of Critical Infrastructure A Comparative Study

يختلف مستوى التعاون الدولي في مجال الأمن السيبراني للمرافق الحيوية

بشكل كبير بين الأنظمة القانونية الثلاثة

ففي فرنسا، تلعب الدولة دوراً قيادياً في الاتحاد الأوروبي

من خلال مشاركتها الفعالة في وكالة الأمن السيبراني الأوروبية (ENISA)

وتبادل المعلومات الاستخباراتية مع الحلفاء عبر منصات مثل "Five Eyes"

كما تشارك فرنسا في تدريبات سيبرانية دولية دورية

لتحسين قدراتها على مواجهة الهجمات المعقدة

أما في مصر، فإن التعاون الدولي لا يزال في مراحله الأولى

رغم عضويتها في بعض المنظمات الإقليمية مثل جامعة الدول العربية

التي بدأت مؤخراً في تطوير استراتيجيات أمن سيبراني مشتركة

لكن غياب الإطار التشريعي الموحد يحد من فعالية هذا التعاون

وفي الجزائر، يواجه التعاون الدولي تحديات مشابهة لتلك الموجودة في مصر

فبينما تشارك الجزائر في بعض المبادرات الإفريقية والعربية

فإن غياب الإطار التشريعي الموحد ونقص الخبرات الفنية

يحد من قدرتها على المشاركة الفعالة في العمليات السيبرانية المشتركة

ومن ثم، فإن المقارنة تظهر أن فعالية التعاون الدولي

مرتبطة ارتباطاً وثيقاً بوجود إطار تشريعي وطني قوي

وتوفر الخبرات الفنية اللازمة، مما يستدعي

بناء قدرات هذه الدول لتمكينها من لعب دورها

في النظام الأمني السيبراني العالمي

26

الهجمات السيبرانية على المرافق الحيوية

دراسة حالة لستوكسنت

Cyberattacks on Critical Infrastructure A Case Study of Stuxnet

تمثل هجمة "ستوكسنت" التي حدثت عام ٢٠١٠

أول مثال موثق لهجوم سيبراني يستهدف مرافق حيوية مباشرة

حيث تم تصميم هذا الفيروس المتطور خصيصاً

لاختراق أنظمة الطرد المركزي الإيرانية في منشأة نطنز النووية

وقد استخدم الفيروس تقنيات متقدمة جداً

مثل استغلال ثغرات "زيرو داي" غير المعروفة

والتزوير الرقمي لشهادات الأمان

مما مكنه من اختراق الشبكات المعزولة (Air-Gapped Networks)

التي لا تتصل بالإنترنت

وقد أدى هذا الهجوم إلى تدمير حوالي ١٠٠٠ جهاز طرد مركزي

وتأخير البرنامج النووي الإيراني لسنوات

مما يدل على أن الهجمات السيبرانية يمكن أن تكون

أكثر فعالية وأقل تكلفة من الهجمات العسكرية

التقليدية

وتمثل هذه الحالة درساً مهماً لجميع الدول

حول ضرورة تطوير دفاعات سيبرانية متقدمة

لحماية مرافقها الحيوية من الهجمات المتطورة

التي قد تؤدي إلى أضرار مادية وجسدية حقيقية

27

الهجمات السيبرانية على المرافق الحيوية
دراسة حالة لنوتبيتيا

Cyberattacks on Critical Infrastructure A

Case Study of NotPetya

تمثل هجمة "نوتبيتيا" التي حدثت عام ٢٠١٧

مثالاً صارخاً على كيف يمكن لهجوم سيبراني

أن يتحول من هدف محدد إلى كارثة عالمية

ففي البداية، كان الهدف الأساسي هو أوكرانيا

من خلال اختراق برنامج محاسبي شائع هناك

لكن سرعة انتشار الفيروس وآلية عمله الخبيثة

جعلته ينتشر عالمياً خلال ساعات

مصيباً شركات كبرى مثل "ميرك" الألمانية

و"فيدكس" الأمريكية

وشركات الشحن العالمية مثل "ميرسك"

وقد تسبب هذا الهجوم في خسائر تقدر بمليارات الدولارات

مما يدل على أن الهجمات السيبرانية على المرافق الحيوية

يمكن أن يكون لها تأثيرات اقتصادية عالمية مدمرة

حتى لو كان هدفها الأصلي محدوداً جغرافياً

وتمثل هذه الحالة درساً مهماً حول أهمية

التعاون الدولي في مواجهة التهديدات السيبرانية

وتطوير آليات استجابة سريعة لاحتواء الأضرار

28

الهجمات السيبرانية على المرافق الحيوية دراسة حالة لكولونيال بايب لاين

Cyberattacks on Critical Infrastructure A Case Study of Colonial Pipeline

تمثل هجمة "كولونيال بايب لاين" التي حدثت عام ٢٠٢١

أول مثال مباشر لهجوم سيبراني يؤدي إلى

شلل كامل

لبنية تحتية حيوية في الولايات المتحدة

حيث تم اختراق شركة "كولونيال بايب لاين"

التي تدير أكبر شبكة أنابيب نفط في أمريكا

وقد أجبر الهجوم الشركة على إيقاف عملياتها بالكامل

مما أدى إلى نقص حاد في الوقود في الجنوب الشرقي الأمريكي

وأثار حالة من الذعر بين المواطنين الذين بدأوا في تخزين البنزين

وقد اضطرت الشركة لدفع فدية بعملة البيتكوين

لتتمكن من استعادة الوصول إلى أنظمتها

مما يطرح تساؤلات أخلاقية وقانونية حول

شرعية دفع الفدية في مثل هذه الحالات

وتمثل هذه الحالة درساً مهماً حول مدى هشاشة

البنية التحتية الحيوية الحديثة

وأهمية الاستثمار في الدفاعات السيبرانية الوقائية

بدلاً من الاعتماد على الحلول العلاجية بعد

وقوع الضرر

29

الاستجابة للحوادث السيبرانية في المرافق الحيوية الإطار القانوني في مصر

Incident Response for Cybersecurity in Critical Infrastructure The Legal Framework in Egypt

يعد الإطار القانوني للاستجابة للحوادث السيبرانية في مصر

ضعيفاً وغير متكامل، حيث يفتقر إلى آليات واضحة

للكشف المبكر والاستجابة السريعة والتعافي الفعال

فقانون مكافحة الجرائم الإلكترونية رقم ١٧٥ لسنة ٢٠١٨

يركز بشكل أساسي على العقوبات بعد وقوع الحادث

بدلاً من وضع آليات وقائية واستباقية

كما أنه لا يحدد بوضوح مسؤوليات الجهات المختلفة

في حالة وقوع هجوم سيبراني على مرافق حيوية

بالإضافة إلى ذلك، فإن غياب مركز وطني موحد

لمراقبة التهديدات السيبرانية وتنسيق الاستجابة

يجعل من الصعب اكتشاف الهجمات في مراحلها المبكرة

وتنسيق الجهود بين الجهات الحكومية والخاصة

وحتى الآن، فإن معظم خطط الاستجابة للحوادث

تعتمد على مبادرات فردية من الشركات الكبرى

بدون وجود إطار قانوني ملزم يضمن التنسيق الفعال

مما يجعل مصر عرضة لمخاطر سيبرانية جسيمة

30

الاستجابة للحوادث السيبرانية في المرافق الحيوية الإطار القانوني في الجزائر

Incident Response for Cybersecurity in Critical Infrastructure The Legal Framework in Algeria

يعد الإطار القانوني للاستجابة للحوادث السيبرانية في الجزائر

ضعيفاً وغير متكامل، حيث يفتقر إلى آليات واضحة

للكشف المبكر والاستجابة السريعة والتعافي الفعال

فقانون مكافحة الجرائم الإلكترونية رقم ١٥-٠٤ لسنة ٢٠١٥

يركز بشكل أساسي على العقوبات بعد وقوع الحادث

بدلاً من وضع آليات وقائية واستباقية

كما أنه لا يحدد بوضوح مسؤوليات الجهات المختلفة

في حالة وقوع هجوم سيبراني على مرافق حيوية

بالإضافة إلى ذلك، فإن غياب مركز وطني موحد

لمراقبة التهديدات السيبرانية وتنسيق الاستجابة

يجعل من الصعب اكتشاف الهجمات في مراحلها المبكرة

وتنسيق الجهود بين الجهات الحكومية والخاصة

وحتى الآن، فإن معظم خطط الاستجابة للحوادث

تعتمد على مبادرات فردية من الشركات الكبرى

بدون وجود إطار قانوني ملزم يضمن التنسيق

الفعال

مما يجعل الجزائر عرضة لمخاطر سيبرانية جسيمة

31

الاستجابة للحوادث السيبرانية في المرافق الحيوية الإطار القانوني في فرنسا

Incident Response for Cybersecurity in Critical Infrastructure The Legal Framework in France

تتميز فرنسا بامتلاكها أحد أكثر الأطر القانونية تطوراً

في مجال الاستجابة للحوادث السيبرانية

فمن خلال وكالة الأمن السيبراني الوطنية (ANSSI)

تم إنشاء مركز عمليات أمن سيبراني وطني (CERT-FR)

يقوم بمراقبة التهديدات السيبرانية على مدار الساعة

كما أن القانون الفرنسي يلزم جميع المشغلين

للمرافق الحيوية بإبلاغ الوكالة فور اكتشاف أي حادث

وتقديم تقارير تفصيلية عن طبيعة الهجوم وآثاره

وإجراءات التعافي المتخذة

بالإضافة إلى ذلك، فإن فرنسا تمتلك خطة وطنية موحدة

لاستجابة الحوادث السيبرانية تشمل جميع القطاعات الحيوية

وتضمن التنسيق الفعال بين الجهات الحكومية والخاصة

وقد تم اختبار هذه الخطة من خلال تدريبات سيبرانية دورية

تحاكي سيناريوهات هجوم واقعية

وأخيراً، فإن فرنسا تشارك بنشاط في شبكات

الاستجابة

للحوادث السيبرانية على المستوى الأوروبي والدولي

مما يعزز قدرتها على مواجهة التهديدات العابرة للحدود

32

التدريب والتأهيل في مجال الأمن السيبراني للمرافق الحيوية دراسة مقارنة

Training and Qualification in Cybersecurity of Critical Infrastructure A Comparative Study

يختلف مستوى التدريب والتأهيل في مجال الأمن السيبراني

للمرافق الحيوية بشكل كبير بين الأنظمة القانونية الثلاثة

ففي فرنسا، تمتلك الدولة نظاماً متكاملاً للتدريب

يبدأ من الجامعات التي تقدم برامج متخصصة في الأمن السيبراني

ويستمر في مراكز التدريب المهني التابعة للوكالة الوطنية

كما أن جميع العاملين في المرافق الحيوية

يخضعون لتدريبات دورية على مواجهة الهجمات

السيبرانية

أما في مصر، فإن التدريب لا يزال محدوداً

ويتركز بشكل أساسي في بعض الكليات العسكرية والأمنية

بينما يفتقر القطاع المدني إلى برامج تدريبية منهجية

مما يؤدي إلى نقص حاد في الكفاءات الفنية المؤهلة

وفي الجزائر، يواجه التدريب تحديات مشابهة لتلك الموجودة في مصر

فبينما توجد بعض البرامج في الكليات

العسكرية

فإن القطاع المدني يفتقر إلى برامج تدريبية فعالة

مما يؤدي إلى اعتماد كبير على الخبرات الأجنبية

ويفتقر إلى بناء قدرات وطنية مستدامة

ومن ثم، فإن المقارنة تظهر أن فعالية التدريب

مرتبطة ارتباطاً وثيقاً بوجود استراتيجية وطنية موحدة

وتوفر الموارد المالية اللازمة، مما يستدعي

بناء أنظمة تدريب متكاملة في مصر والجزائر

33

الاختبارات الاختراقية (Penetration Testing) للمرافق الحيوية الإطار القانوني في مصر

Penetration Testing for Critical Infrastructure The Legal Framework in Egypt

يعد الإطار القانوني للاختبارات الاختراقية في مصر

غير واضح ويفتقر إلى التنظيم، حيث لا يوجد قانون

يحدد شروط وآليات إجراء هذه الاختبارات على

ففي غياب تشريع خاص، تعتمد الجهات الحكومية والخاصة

على مبادرات فردية لإجراء اختبارات الاختراق

دون وجود معايير موحدة أو شهادات معتمدة

للمختبرين الأمنيين

بالإضافة إلى ذلك، فإن غياب الحماية القانونية

للمختبرين الأمنيين الذين قد يكتشفون ثغرات خطيرة

يجعلهم عرضة للملاحقة القضائية

مما يثبط من روح المبادرة ويقلل من فعالية هذه الاختبارات

وحتى الآن، فإن معظم الاختبارات الاختراقية

تتم من خلال شركات أجنبية تفتقر إلى الفهم العميق

للمشهد الأمني المحلي، مما يقلل من فعاليتها

مما يستدعي إصدار تشريع خاص ينظم هذا المجال

ويوفر الحماية القانونية للمختبرين الأمنيين الوطنيين

34

الاختبارات الاختراقية (Penetration Testing) للمرافق الحيوية الإطار القانوني في الجزائر

Penetration Testing for Critical Infrastructure The Legal Framework in Algeria

يعد الإطار القانوني للاختبارات الاختراقية في الجزائر

غير واضح ويفتقر إلى التنظيم، حيث لا يوجد قانون

يحدد شروط وآليات إجراء هذه الاختبارات على المرافق الحيوية

ففي غياب تشريع خاص، تعتمد الجهات الحكومية والخاصة

على مبادرات فردية لإجراء اختبارات الاختراق

دون وجود معايير موحدة أو شهادات معتمدة

للمختبرين الأمنيين

بالإضافة إلى ذلك، فإن غياب الحماية القانونية

للمختبرين الأمنيين الذين قد يكتشفون ثغرات خطيرة

يجعلهم عرضة للملاحقة القضائية

مما يثبط من روح المبادرة ويقلل من فعالية هذه الاختبارات

وحتى الآن، فإن معظم الاختبارات الاختراقية

تتم من خلال شركات أجنبية تفتقر إلى الفهم العميق

للمشهد الأمني المحلي، مما يقلل من فعاليتها

مما يستدعي إصدار تشريع خاص ينظم هذا المجال

ويوفر الحماية القانونية للمختبرين الأمنيين الوطنيين

35

الاختبارات الاختراقية (Penetration Testing) للمرافق الحيوية الإطار القانوني في فرنسا

Penetration Testing for Critical Infrastructure The Legal Framework in France

تتميز فرنسا بامتلاكها إطاراً قانونياً متكاملاً

لتنظيم الاختبارات الاختراقية للمرافق الحيوية

فمن خلال قانون الأمن السيبراني لسنة ٢٠١٣

تم إنشاء نظام معتمد لشهادات المختبرين الأمنيين

كما أن القانون يلزم جميع المشغلين للمرافق الحيوية

بإجراء اختبارات اختراق دورية من قبل جهات معتمدة

وتقديم تقارير تفصيلية عن النتائج وخطط المعالجة

بالإضافة إلى ذلك، فإن فرنسا توفر حماية قانونية

للمختبرين الأمنيين المعتمدين الذين يعملون

ضمن الإطار القانوني المحدد، مما يشجع على روح المبادرة

ويزيد من فعالية هذه الاختبارات

وأخيراً، فإن فرنسا تمتلك قاعدة بيانات وطنية

للمختبرين الأمنيين المعتمدين، مما يسهل على الجهات

اختيار الكفاءات المناسبة لإجراء هذه الاختبارات

ويضمن جودة عالية في تنفيذها

36

الذكاء الاصطناعي التوليدي في الهجمات السيبرانية على المرافق الحيوية

Generative AI in Cyberattacks on Critical Infrastructure

مع ظهور الذكاء الاصطناعي التوليدي، أصبحت الهجمات السيبرانية

أكثر تطوراً وخطورة، حيث يمكن لهذه النماذج

إنشاء برمجيات خبيثة جديدة لم يسبق لها مثيل

وتجاوز أنظمة الحماية التقليدية بسهولة

فمن خلال نماذج مثل GPT، يمكن للمهاجمين

كتابة أكواد برمجية خبيثة بلغات برمجة متعددة

بسرعة ودقة تفوق قدرات المبرمجين البشر

كما يمكن لهذه النماذج إنشاء رسائل تصيد احتيالي

مقنعة جداً تتجاوز أنظمة الكشف التقليدية

بالإضافة إلى ذلك، يمكن للذكاء الاصطناعي التوليدي

تحليل نقاط الضعف في أنظمة المرافق الحيوية

واقتراح سيناريوهات هجوم متطورة تستغل هذه الثغرات

بطرق لم يفكر فيها المهاجمون البشر من قبل

ويمثل هذا التطور تحدياً وجودياً للدفاعات

السيبرانية التقليدية

ويستدعي تطوير أنظمة دفاع ذكية قادرة على

التكيف مع هذه التهديدات المتطورة باستمرار

37

الذكاء الاصطناعي التوليدي في الدفاع السيبراني للمرافق الحيوية

Generative AI in Cyber Defense of Critical Infrastructure

رداً على استخدام الذكاء الاصطناعي التوليدي في الهجمات

بدأت أنظمة الدفاع السيبراني في تبني نفس التقنيات

للحماية من هذه التهديدات المتطورة

فمن خلال نماذج الذكاء الاصطناعي التوليدي

يمكن لأنظمة الدفاع تحليل سلوك الشبكات بشكل مستمر

واكتشاف الأنماط غير الطبيعية التي قد تشير إلى هجوم

حتى لو كانت البرمجيات الخبيثة جديدة ولم يسبق رؤيتها

كما يمكن لهذه النماذج إنشاء سيناريوهات

دفاعية متطورة

تتنبأ بمسارات الهجوم المحتملة وتعزز الدفاعات في النقاط الحرجة

قبل وقوع الهجوم فعلياً

بالإضافة إلى ذلك، يمكن للذكاء الاصطناعي التوليدي

كتابة تقارير تحليلية تفصيلية عن الحوادث السيبرانية

بسرعة ودقة تفوق قدرات المحللين البشر

مما يساعد في اتخاذ قرارات استجابة أسرع وأكثر فعالية

ويمثل هذا التطور سباقاً بين الهجوم والدفاع

حيث يحاول كل جانب توظيف أحدث تقنيات الذكاء الاصطناعي

لصالحه، مما يجعل حماية المرافق الحيوية

أكثر تعقيداً وتحدياً من أي وقت مضى

38

الأمن السيبراني الكمي والمستقبل الرقمي للمرافق الحيوية

Quantum Cybersecurity and the Digital Future of Critical Infrastructure

مع تطور الحوسبة الكمية، يواجه الأمن السيبراني

تحدياً وجودياً جديداً، حيث ستكون الحواسيب الكمية القادمة

قادرة على كسر جميع خوارزميات التشفير الحالية

التي تعتمد عليها أنظمة المرافق الحيوية في حمايتها

فخوارزميات التشفير مثل RSA وAES

التي تحمي البيانات الحساسة لأنظمة الطاقة والمياه

ستصبح عديمة الفائدة أمام قوة الحوسبة الكمية

مما سيعرض جميع المرافق الحيوية لخطر الاختراق

ولمواجهة هذا التحدي، بدأت الدول المتقدمة

في تطوير ما يُعرف بـ "التشفير الكمي"

الذي يعتمد على مبادئ الفيزياء الكمية

ويوفر أماناً لا يمكن كسره حتى بالحواسيب الكمية

وقد بدأت فرنسا بالفعل في استثمارات كبيرة

في هذا المجال من خلال مبادرات وطنية

بينما لا تزال مصر والجزائر في مراحل البحث الأولية

مما يخلق فجوة أمنية كبيرة قد تهدد

أمن المرافق الحيوية في المستقبل القريب

39

الخاتمة النهائية رؤية استراتيجية للأمن السيبراني في العصر الرقمي

Final Conclusion A Strategic Vision for Cybersecurity in the Digital Age

بعد هذه الرحلة الشاملة عبر التحديات الأمنية التي تواجه المرافق الحيوية

في العصر الرقمي، يتضح أن الأمن السيبراني لم يعد خياراً تقنياً

بل أصبح ضرورة وجودية لأمن الدول واستقرارها

فبينما تطورت الهجمات السيبرانية من مجرد سرقة بيانات

إلى شلّ كامل للبنية التحتية الحساسة، تظل الاستجابة القانونية

في العديد من الدول، وخاصة النامية، غير كافية وغير متطورة

وقد أظهرت الدراسة المقارنة بين مصر والجزائر

وفرنسا

أن الفجوة ليست في التكنولوجيا فحسب، بل في الإطار القانوني والمؤسسي

الذي يحكم استخدام هذه التكنولوجيا ويضمن مساءلة مرتكبي الجرائم

ففرنسا، بفضل رؤيتها الاستباقية، تمكنت من بناء منظومة متكاملة

تجمع بين التشريع المتقدم، والرقابة الفعالة، والتعاون الدولي الوثيق

أما في مصر والجزائر، فإن غياب التشريعات الخاصة بالمرافق الحيوية

وعدم وجود سلطة رقابية مستقلة وقوية،

يجعلهما عرضة لمخاطر جسيمة

تهدد ليس فقط الاقتصاد، بل الأمن القومي بأكمله

ومن ثم، فإن التوصيات التي قدمتها هذه الدراسة

ليست مجرد اقتراحات أكاديمية، بل هي خارطة طريق عملية

لبناء دفاع سيبراني وطني فعال يمكنه مواجهة التهديدات المستقبلية

وفي النهاية، فإن مستقبل الأمن السيبراني

سيتوقف على قدرة الدول على الجمع بين القوة التقنية

والحكمة القانونية، لضمان أن تبقى التكنولوجيا

أداة لحماية الإنسان، وليس سلاحاً ضد أمنه واستقراره

40

المراجع

References

١ الدستور المصري لسنة ٢٠١٤

٢ الدستور الجزائري لسنة ٢٠٢٠

٣ الإعلان العالمي لحقوق الإنسان ١٧٨٩

٤ قانون مكافحة الجرائم الإلكترونية المصري رقم ١٧٥ لسنة ٢٠١٨

٥ قانون مكافحة الجرائم الإلكترونية الجزائري رقم ١٥-٠٤ لسنة ٢٠١٥

٦ قانون الأمن السيبراني الفرنسي °Loi n ٢٠١٣-١١٦٨ du ١٨ décembre ٢٠١٣

٧ قانون الجمهورية الرقمية الفرنسي °Loi n ٢٠١٦-١٣٢١ du ٧ octobre ٢٠١٦

٨ التوجيه الأوروبي لأمن شبكات المعلومات (NIS Directive)

٩ تقرير المركز الوطني للأمن السيبراني المصري ٢٠٢٥

١٠ تقرير الوكالة الوطنية للأمن السيبراني الجزائرية ٢٠٢٤

١١ تقرير الوكالة الوطنية للأمن السيبراني الفرنسي (ANSSI) ٢٠٢٥

١٢ محمد كمال عرفه الرخاوي الذكاء الاصطناعي والقانون الاداري

١٣ Jean Dupont La cybersécurité au service de l administration Dalloz Paris ٢٠٢٥

١٤ Ahmed Benali La cybersécurité et la fonction publique en Algérie ENAG Alger ٢٠٢٦

١٥ Clark David D. Blumenthal David R. The Future of Internet Security MIT Press ٢٠٢٣

١٦ Schneier Bruce. Click Here to Kill Everybody Norton & Company ٢٠٢٢

١٧ Zetter Kim. Countdown to Zero Day Crown Publishing ٢٠٢١

١٨ Sanger David E. The Perfect Weapon Crown Publishing ٢٠٢٠

١٩ Rid Thomas. Cyber War Will Not Take Place Oxford University Press ٢٠٢١

٢٠ Libicki Martin C. Cyberdeterrence and Cyberwar RAND Corporation ٢٠٢٢

الفهرس

Table of Contents

٧ التشريعات الناظمة للأمن السيبراني في الجزائر ودورها في الحماية

٨ التشريعات الناظمة للأمن السيبراني في فرنسا ودورها في الحماية

٩ ضوابط المشروعية في القرارات الإدارية المتعلقة بالأمن السيبراني في مصر

١٠ ضوابط المشروعية في القرارات الإدارية المتعلقة بالأمن السيبراني في الجزائر

١١ ضوابط المشروعية في القرارات الإدارية المتعلقة بالأمن السيبراني في فرنسا

١٢ الرقابة القضائية على القرارات الأمنية الصادرة عن أنظمة ذكية في مصر

١٣ الرقابة القضائية على القرارات الأمنية الصادرة عن أنظمة ذكية في الجزائر

١٤ الرقابة القضائية على القرارات الأمنية الصادرة عن أنظمة ذكية في فرنسا

١٥ التحديات الأخلاقية والعملية لاستخدام الذكاء الاصطناعي في الأمن السيبراني المصري

١٦ التحديات الأخلاقية والعملية لاستخدام الذكاء الاصطناعي في الأمن السيبراني الجزائري

١٧ التحديات الأخلاقية والعملية لاستخدام الذكاء الاصطناعي في الأمن السيبراني الفرنسي

١٨ الإصلاحات التشريعية المقترحة لتعزيز الأمن السيبراني للمرافق الحيوية في مصر

١٩ الإصلاحات التشريعية المقترحة لتعزيز الأمن

٢٥ التعاون الدولي في مجال الأمن السيبراني للمرافق الحيوية دراسة مقارنة

٢٦ الهجمات السيبرانية على المرافق الحيوية دراسة حالة لستوكسنت

٢٧ الهجمات السيبرانية على المرافق الحيوية دراسة حالة لنوتبيتيا

٢٨ الهجمات السيبرانية على المرافق الحيوية دراسة حالة لكولونيال بايب لاين

٢٩ الاستجابة للحوادث السيبرانية في المرافق الحيوية الإطار القانوني في مصر

٣٠ الاستجابة للحوادث السيبرانية في المرافق الحيوية الإطار القانوني في الجزائر

٣١ الاستجابة للحوادث السيبرانية في المرافق الحيوية الإطار القانوني في فرنسا

٣٢ التدريب والتأهيل في مجال الأمن السيبراني للمرافق الحيوية دراسة مقارنة

٣٣ الاختبارات الاختراقية (Penetration Testing) للمرافق الحيوية الإطار القانوني في مصر

٣٤ الاختبارات الاختراقية (Penetration Testing) للمرافق الحيوية الإطار القانوني في الجزائر

٣٥ الاختبارات الاختراقية (Penetration Testing) للمرافق الحيوية الإطار القانوني في فرنسا

٣٦ الذكاء الاصطناعي التوليدي في الهجمات السيبرانية على المرافق الحيوية

٣٧ الذكاء الاصطناعي التوليدي في الدفاع

جميع الحقوق محفوظة

د. محمد كمال عرفه الرخاوي

يحظر نسخ أو طبع أو نشر أو توزيع أو اقتباس أي جزء من هذا الكتاب

بدون إذن خطي مسبق من المؤلف