المحاضرة 14: الاستراتجيات الجزائرية لتحقيق الأمن السيبراني.

مقدمة:

أصبح الامن السيبراني في العمر الرقمي أحد أعمدة السيادة الوطنية ومكونا لا ينفصل عن مفاهيم الأمن القومي التأمل، فالدول لم تعد تهدد فقط عبر حدودها الجغرافية، بل عبر فضائها الرقمي، وبناها التحتية.

في هذا السياق، شرعت الجزائر خلال السنوات الاخيرة في بلورة مقاربة الاستراتيجية تدريجية للأمن السيبراني، تستند إلى حماية الدولة والاقتصاد، ومواجهة التهديدات السيبرانية المتنامية، مع مراعاة الخصوصيات السياسية والقانونية والاجتماعية الوطنية.

وتهدف هذه المحاضرة إلى تحليل الاستراتجيات الجزائرية لتحقيق الأمن السيبراني من خلال تفكيك مرتكزاتها، وآليات تنفيذها، وتقييم فعالياتها، واسنشراف أفاق تطويرها مستقبلا.

أولا: الإطار المفاهيمي والاستراتيجي للامن السيبراني

1-مفهوم الاستراتيجية في مجال الامن السيبراني.

الاستراتيجية السيبرانية في خطة وطنية شاملة تهدف إلى

- حماية الفضاء الرقمي الوطني.
- ضمان استمرارية الخدمات الحيوية.
- مواجهة التهديدات السيبرانية الداخلية والخارجية.

2-الامن السيبراني في العقيدة الامنية الجزائرية.

يندرج الأمن السيبراني ضمن:

- الأمن الوطني الشامل.
- الأمن المعلوماتي.
- الأمن الإعلامي.
- الأمن الإقتصادي.

وتعتمد الجزائر مقاربة وقائية تقوم على التحكم، الحماية، الردع، والاستجابة.

3-دوافع تبني استراتيجية سيبرانية وطنية.

- تسارع الرقمنة.
- توسع الإدارة الإلكترونية.
- تنامي الجرائم الالكترونية.
- تصاعد الحرب المعلوماتية.
- حماية الاستقرار المجتمعي.

ثانيا: الإستراتيجية الجزائرية لحماية البنى التحتية الرقمية.

1-مفهوم البنى التحتية المعلوماتية الحرجة

تشمل:

- شبكات الاتصالات.
- الانظمة البنكية.
- الطاقة والمياه.
- النقل.
- الإعلام والإتصال.

2-مرتكزات الاستراتيجية الجزائرية.

أ- الوقاية السيبرانية

- تامين الأنظمة الحكومية.
- اعتماد الأنظمة الحماية والحدة.
- تقليل نقاط الضعف التقنية.

ب- الاستجابة للحوادث

- تطوير آليات التدخل السريع.
- احتواء الأضرار الرقمية.
- استعادة الأنظمة.

ج- استمرارية الخدمة

- ضمان عدم تعطيل تعطيل المرافق الحيوية.
- خطط الطوارئ الرقمية.

3- السيادة الرقمية كخيار استراتيجي.

- التحكم في المعطيات الوطنية.
- تقليص التبعية التكنولوجية.
- حماية البيانات السيادية.

ثالثا: الاستراتيجية القانونية والمؤسساتية للأمن السيبراني.

1- الإطار القانوني للأمن السيبراني في الجزائر.

تعتمد الإستراتيجية الجزائرية على:

- قوانين مكافحة الجرائم الالكترونية.
- تشريعات حماية الأنظمة المعلوماتية.
- قوانين حماية المعطيات الشخصية.
- تنظيم الإعلام الرقمي.
- تحطيم الإعلام الرقمي.

2- البعد المؤسساتي

أ- دور الدولة:

- التنسيق بين القطاعات.
- وضع السياسات العمومية الرقمية.
- الاشراف على الامن السيبراني.

ب- المقاربة التشاركية.

- إشراك المؤسسات العمومية.
- اشراك المتعاملين الاقتصاديين.
- التعاون مع الجامعات ومراكز البحث.

رابعا–الاليات والجيود الامنية الجزائرية لمواجية التهديدات السيبرانية:

في ظل التطور التكنولوجي المتسارع وتزايد الاعتماد على الأنظمة الرقمية في جميع مناحي الحياة، أصبحت الأمن السيب ارني واحدة من أبرز التحديات التي تواجه الدول في القرن الحادي والعشرين. وتشكل التهديدات السيبرانية خط اًر حقيقياً يهدد الأمن القومي، والاقتصاد الوطني، وسرية المعلومات الحساسة، واستمرارية الخدمات الحيوية مثل الطاقة، والصحة، والبنوك، والتواصل.

برزت الحاجة إلى بناء قدرات وطنية شاملة للتصدي لهذه التهديدات عبر مجموعة من الإجراءات الاستباقية والردود الفعلية التي تشمل: وضع التشريعات اللازمة، وإنشاء الهيئات المتخصصة، وبناء الكوادر المؤهلة، وتعزيز التعاون الدولي، ونشر الوعي المجتمعي ومن هنا سندرج بعض من القوانين والمراسيم المتعلقة بالجهود الوطنية في مواجهة التهديدات السيبرانية .

1- الهيئات المكلفة بالأمن السيبراني:

تُعتبر الهيئات المكلفة بالأمن السيبراني الركيزة الأساسية لحماية الفضاء الرقمي الوطني، من خلال وضع الآليات والإجراءات الوقائية والردية لمواجهة التهديدات الإلكترونية المتزايدة. وتتنوع مهام هذه الهيئات بين وضع الاستراتيجيات الوطنية، ومراقبة تنفيذها، واعتماد المعايير التقنية، والتدخل في حالات الطوارئ السيب ارنية. وتعمل هذه المؤسسات بتنسيق عضوي مع مختلف القطاعات الحيوية لضمان أمن الأنظمة المعلوماتية وسلامة البيانات ودعم استمرارية الخدمات الأساسية للدولة ومن بين هذه الهيئات هي الوكالة الوطنية لتطوير الرقمنة، والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، والمجلس الوطني لأمن الأنظمة المعلوماتية.

أ- الوكالة الوطنية لتطوير الرقمنة:

عالج المشرع الجزائري احكام الوكالة الوطنية لتطوير الرقمنة بموجب القانون 317/19 المتضمن انشاء الوكالة الوطنية لتطوير الرقمنة.

تُعد الوكالة الوطنية لتطوير الرقمنة الذراع التنفيذي المسؤول عن دعم ومواكبة عملية التحول الرقمي في مختلف قطاعات الدولة. وتهدف إلى تعزيز استخدام التقنيات الحديثة وتطوير البنية التحتية الرقمية لبناء اقتصاد رقمي مبتكر ومستدام. كما تلعب الوكالة دوًار محورًيا في إعداد السياسات والبرامج الخاصة

بالرقمنة،

وتقديم الدعم الفني واللوجستي للإدارات العمومية والهيئات المحلية لرفع كفاءة الخدمات الرقمية وجودتها.

ب- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال:

عالج المشرع الجزائلاي احكام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

رغم تركيزه على قطاع الاتصالات، إلا أنه يشترط على مزودي الخدمات ضمان الأمان والحماية من التهديدات السيبرانية.

- يلزم الشركات باتخاذ الإجراءات اللازمة لحماية المستخدمين والمعلومات .

ت- السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

عالج المشرع الجزائري احكام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب القانون 07/18 بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:

- هو أول تشريع شامل ينظم مجال الجرائم الإلكترونية في الجزائر.
- يحدد الجرائم المرتكبة ضد أنظمة المعالجة الآلية للمعطيات.
- يتضمن عقوبات على جرائم الاختراق، الاحتيال الإلكتروني، والتدخل غير المشروع في البيانات.
- ساهم في تأسيس إطار قانوني لمكافحة الجرائم السيبرانية.

ث- المجلس الوطني لأمن الأنظمة المعلوماتية:

عالج المشرع الجزائري احكام المجلس الوطني لأمن الأنظمة المعلوماتية، بموجب القانون 05/20 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

يعد المجلس الوطني لأمن أنظمة المعلومات الجهة العليا المكلفة بوضع السياسات والاست ارتيجيات الوطنية في مجال الأمن السيبراني، وتحديد التوجهات العامة لحماية الأنظمة والمعلومات الحساسة. وهو يترأس جهود التنسيق بين المؤسسات العمومية والخاصة لتعزيز القدرات الوطنية في مواجهة التهديدات الرقمية. ويهدف المجلس من خلال مقاربة استباقية وشاملة إلى ضمان أمن cyberspaceودعم الثقة في الخدمات الإلكترونية واستمرارية الأعمال الحيوية للدولة.

2- القوانين الأساسية في مجال الأمن السيبراني:

تُشكل القوانين الأساسية في مجال الأمن السيبراني الإطار التشريعي الضروري لضمان حماية الفضاء الرقمي الوطني وتنظيم استعماله بأسلوب آمن وموثوق. وتهدف هذه النصوص القانونية إلى تحديد الحقوق والواجبات المتعلقة بحماية البيانات والمعلومات الحساسة، ومعالجة المخالفات الإلكترونية، وضبط معايير الأمان المطلوبة للأنظمة المعلوماتية الحيوية. كما تمثل هذه القوانين حاضنة للتعاون بين الجهات العمومية

والخاصة، وتساهم في تعزيز السيادة الرقمية ومواجهة التحديات المرتبطة على الجرائم السيبرانية والهجمات الإلكتروني ويتعلق الامر ب مرسوم تنفيذي رقم 135/16 يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكليها وتنظيمها وسيرها، **و**مرسوم تنفيذي رقم 134/16 يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها، ومرسوم تنفيذي رقم 110/22 يضبط مبادئ تحديد تعريفة خدمات للتصديق الالكتروني.

أ- مرسوم تنفيذي رقم 135/16 يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكيلها وتنظيمها وسيرها:

تُعد السلطة الحكومية للتصديق الإلكتروني هيئة عمومية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والإداري، تُعنى بتنظيم وضمان أمن وموثوقية العمليات الرقمية، خاصّة في مجال التوقيع الإلكتروني والشهادات الرقمية. وتتألف هذه السلطة من هيكل تنظيمي يضم أجهزة إدارية وفنية متخصصة، تتوزع بينها المهام المتعلقة بإصدار الشهادات، والمراقبة، والاعتماد، والرقابة التقنية. ويتم تنظيم سير عملها وفق مبادئ الشفافية والكفاءة، وبما يتماشى مع المعايير الدولية لضمان الثقة في التعاملات الإلكترونية ودعم الاقتصاد الرقمي الوطني.

ب- مرسوم تنفيذي رقم 134/16 يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها:

تُعد السلطة الوطنية للتصديق الإلكتروني الذ ارع التنظيمية والتنفيذية المكلفة بضمان أمن وموثوقية العمليات الرقمية، خاصّة في مجال التوقيع الإلكتروني والخدمات المرتبطة به. وتتمثل مهمتها الأساسية في وضع الأطر التقنية والإدارية اللازمة لتنظيم عمليات إصدار الشهادات الإلكترونية، والرقابة على مزّود الخدمات المعتمدين. ويأتي تنظيم مصالح هذه السلطة وتحديد مهامها وسير عملها بهدف ضمان كفاءة الأداء، وحماية البيانات، وتعزيز الثقة في التعاملات الإلكترونية على المستوى الوطني والدولي.

ت- مرسوم تنفيذي رقم 10/22 يضبط مبادئ تحديد تعريفة خدمات للتصديق الالكتروني:

تُعد تحديد تعريفة الخدمات المتعلقة بالتصديق الإلكتروني أحد الجوانب الأساسية لتنظيم هذا المجال، ويهدف إلى ضمان شفافية الأسعار وعقلنتها بما يخدم المصلحة العامة ويحقق توازًنا بين جودة الخدمة والتكلفة. وتستند هذه التعريفة إلى معايير موضوعية تراعي طبيعة الخدمات المقدمة، وتكاليف الإنتاج، ومتطلبات الأمن السيبراني، بالإضافة إلى قدرة المستخدمين على تحملها. ويساهم تنظيم هذا الجانب في تعزيز الثقة في منظومة التصديق الإلكتروني، ودفع عجلة استخدام الوثائق الرقمية في مختلف المجالات الاقتصادية والإدارية.