محاضرة الثالثة عشرة- واقع الأمن السيبراني في الجزائر وتهديدات الاختراقات:

تسعى الدولة إلأ بناء منظومة وطنية للحماية الرقمية، في مقابل تصاعد التهديدات السيبرانية التقنية وغير التقنية.

أولا-الإطار المفاهيمي والمؤسساتي للأمن السيبراني في الجزائر.

1- تعريف الأمن السيبراني:

يقصد بالأمن السيبراني في الجزائر مجموعة السياسات والاجراءات التقنية والقانونية والتنظيمية الرامية إلى:

- حماية الانظمة المعلوماتية الوطنية.
- تامين الشبكات الحكومية والخاصة.
- مكافحة الجرائم الالكترونية.
- ضمان سيادة الدولة الرقمية

2- تطور الاهتمام بالامن السيبراني في الجزائر:

يشهد الامن السيبراني تقدما ملحوظا نتيجة

- انتشار الخدمات الإلكترونية الحكومية,
- توسع الإعلام الرقمي ومنصات التواصل الاجتماعي.
- تزايد الهجمات السيبرانية العابرة للحدود.

3- الاطار المؤوسساتي:

من أبرز الفاعلين في المجال الأمن السيبراني

- ✓ القطاعات الوزارية المعنية بالرقمنة.

- ✓ الهيئات التقنية المختصة بأمن المعلومات.
- ✓ المصالح الامنية.
- ✓ المتعاملون في مجال الاتصالات.
- ✓ المؤسسات الإعلامية الرقمية.

ثانيا: واقع التحول الرقمي والجاهزية السيبرانية في الجزائر

1- **التحول الرقمي في الجزائر:** عرفت الجزائر خطوات مهمة في مجال الرقمنة، رقمية الإدارة العمومية، ورقمية العدالة، تطوير الدفع الإلكتروني، رقمية القطاع البنكي، توسيع الخدمات الحكومية عبر الإنترنيت.

2- **الجاهزية السيبرانية:** رغم التقدم المسجل، لا تزال الجاهزية السيبرانية تعاني من تفاوت في مستوى الحماية بين القطاعات.

- ضعف التنسيق بين الفاعليين.
- محدودية ثقافة الأمن الرقمي.

3- **التهديدات السيبرانية التي تواجه الجزائر**

أ- **التقنية:** وتشمل

- الاختراقات الالكترونية.
- هجومات حجب الخدمات (DDOS).
- البرمجيات الخبيثة.
- سرقة البيانات.

ب-**الاقتصادية:**

- استهداف المؤسسات المالية.
- الاحتكار الالكتروني.
- سرقة المعطيات البنكية.

ت-**الإعلامية والمعلوماتية**

- التضليل الإعلامي.
- الحرب المعلوماتية.
- استغلال الفضاء الرقمي للتاثير على الرأي العام.

ث-**المرتبطة بالعنصر البشري**

- ✓ ضعف التكوين.
- ✓ الهندسة الاجتماعية.
- ✓ الإهمال وسوء استعمال الأنظمة.

رابعا: التحديات القانونية التقنية والبشرية.

1- القانونية:

- تطور الجرائم الرقمية أسرع من التشريعات.
- صعوبة الإثبات الرقمي.
- الطابع العابر للحدود للجريمة السيبرانية.

2- التقنية:

- قدم بعض البنى التحتية.
- الاعتماد على حلول أجنبية.
- نقص مراكز الرصد والاستجابة.

3- البشرية:

- ✓ نقص الكفاءات المتخصصة.
- ✓ هجرة العقول.
- ✓ ضعف برامج التكوين المتخصصة.

<u>توصيات:</u>

- ➢ إنشاء هيئة وطنية موحدة للأمن السيبراني.
- ➢ تعزيز التنسيق بين القطاعات.