

حوكمة الإنترنت هي مجموعة القواعد والمعايير والمبادئ التي تحكم استخدام الإنترنت و قد أعطت القمة العالمية لمجتمع المعلومات تعريفاً لحوكمة الإنترنت على النحو التالي: " إدارة الإنترنت هي تطوير وتطبيق الحكومات والقطاع الخاص والمجتمع المدني ، و تشمل قضايا حوكمة الإنترنت (IG) بشكل عام مواضيع ثلاث هي الوصول المفتوح إلى عمليات الحوكمة و أمن واستقرار الشبكة و الإدارة المسؤولة لموارد الإنترنت الهامة. و تعتبر حوكمة الإنترنت عملية تتيح ال تحكم والإدارة والتنظيم لشبكة الإنترنت والخدمات المرتبطة بها. وهي تشتمل على الأسس والمبادئ والإجراءات والآليات التي تحدد كيفية توزيع السلطات والمسؤوليات بين مختلف الأطراف ذات الصلة فيما يتعلق بإدارة الإنترنت، وتشمل حوكمة الإنترنت تأييد السياسات والقوانين التي تحكم استخدام الإنترنت وتحديد الحقوق والواجبات المتعلقة بها. يهدف مفهوم حوكمة الإنترنت إلى تحقيق التوازن بين حماية حرية الوصول والتعبير وحماية الأمن السبراني والخصوصية والملكية الفكرية. وتشتمل على الحوكمة الإلكترونية المختلفة مثل حوكمة نطاقات الإنترنت وتوزيع عناوين ال IP، وإدارة الأمان والخصوصية والحقوق الرقمية والحقوق الإنسانية على الإنترنت وغيره. تعد حوكمة الإنترنت مهمة بشكل خاص في ضوء الزيادة المستمرة في استخدام الإنترنت وأهميتها الحيوية في حياتنا اليومية، وذلك يستلزم وضع إطار عمل واضح وملائم لحمايتها وتطويرها بشكل مستدام. وترتبط حوكمة الإنترنت بالأمن السبراني للدول، بل على الأقل بيئة تتوفر على الحماية ويسودها النظام وهو الأمر الحاصل في العالم الافتراضي والتي قد تكون موضع عملات تسلل أو تعديلات أو تعطى أو حتى انقطاع، ويعرف الأمن السبراني من طرف الإتحاد الدولي للاتصالات بأنّه ((مجموع الأدوات والسياسات ومفاهيم الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والآليات الضمان وتكنولوجيات التي استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمسؤولين. وتشتمل على أصول المؤسسات والمسؤولين أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و / أو المحفوظة في البيئة السبرانية ويسعى الأمن السبراني إلى تحقيق خصائص أمن أصول المؤسسة والمسؤولين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السبرانية وتضمن أهم أهداف العام للأمن السبراني: التيسر، وتوفير الاتصالات المشفرة. وفقاً للمرجع العالمي للمعهد القومي للمخابرات والتكنولوجيا NIST بالولايات المتحدة الأمريكية حول تقويم المخاطر والأداء في الأمن السبراني 10، يشتمل الأمن السبراني خمسة مكونات رئيسية هي: الحماية (Protect) وهي القدرة ثم الاستجابة (Respond) وهي القدرة على التعامل مع الهجمات الإلكترونية المكتشفة واتخاذ الإجراءات اللازمة لمعالجتها. والشبكات المتأثرة بالهجوم الإلكتروني بسرعة وفعالية. اللازم للحماية السيبرانية 11. و يهدف الأمن السبراني إلى ضمان أمن البيئة السيبرانية في الأنظمة المعلوماتية، وهو نظام قد يشمل أصحاب المصلحة الذين ينتمون إلى العديد من منظمات القطاعين العام والخاص، باستخدام مكونات متنوعة وأساليب مختلفة لتحقيق الأمن أما بالجزائر، لذلك فقد تم إنشاء منظومة وطنية للأمن الأنظمة المعلوماتية موضوعة لدى وزارة الدفاع الوطني، كما أنه تشتمل على التنظيم لإعداد الاستراتيجية الوطنية للأمن الأنظمة المعلوماتية وتنسيق تنفيذ هذه الاستراتيجية. فضلا عن "إبداء رأي متطابق في أي مشروع من صياغة التشريعي أو تنظيمي" ذي صلة بهذا الموضوع. تعتبر مؤسسة عمومية ذات طابع إداري وتتمتع بالشخصية المعنوية والاستقلالية المادية، على غرار "اقتراحات كفاءات اعتماد مزودي خدمات التدقيق في مجال أمن هذا النوع من الأنظمة و"السهر على جمع وتحليل وتقويم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاس تخلاص المعلومات الملائمة التي تساهم إلى حد كبير. و بمقتضى ذات المرسوم والرئيسي، فإن الوكالة "مؤهلة لطلب أي وثيقة أو معلومة مفيدة للقيام بالمهام الموكلة إليها من الهيئات تعيين مسؤولهم المكلف بأمن الأنظمة المعلوماتية" في أجل أقصاه سنة ابتداء من نشر المرسوم وفي الجريدة لأنه يحدد الحد الأدنى من المتطلبات المتعلقة بالأمن، زائدة على ذلك، مع التركيز على تدريب وتوعية المسؤولين بخدمات المخاطر التي تنطوي عليها، والتقييم الدوري للضوابط من أجل ضمان الرضا والمسئولية للمتطلبات الأمنية و