الأمن السيبراني وتحديات الذكاء الاصطناعي

فيصل مبارك الراشدي
طالب بسلك الدكتوراه، كلية العلوم القانونية والاقتصادية والاجتماعية عين السبع بالدار البيضاء
المغرب

Abstract

Despite the emergence of artificial intelligence and the vast potential and opportunities it offers in various fields and areas, it also carries numerous risks that threaten the stability of countries and their economic transactions, and rarely leads to chaos and disorder in various public and private institutions and organizations. Therefore, it must be dealt with with some caution. While it carries many positives on many levels, its risks are also significant. Therefore, it is necessary to strengthen the cybersecurity system to mitigate the threats that artificial intelligence may pose.

ملخص:

مع ظهور الذكاء الاصطناعي وما يتيحه من إمكانيات وفرص كبيرة في شتى المجالات ومختلف الميادين، إلا أنه يتضمن مخاطر عديدة تهدد استقرار الدول ومعاملاتها الاقتصادية ويندر بحدود فوضى واضطراب في مختلف المؤسسات والمنظمات العامة والخاصة، لذلك يستوجب التعامل معه بشيء من الحذر، فإن كان يحمل معه إيجابيات كثيرة على مستويات عدة، فإن مخاطره، كذلك، كبيرة، وعلى هذا الأساس يجب تعزيز منظومة الأمن السيبراني للحد من التهديدات التي قد يحملها الذكاء الاصطناعي.

مقدمة:

الأمن السيبراني هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. التي تهدف عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية. وبالتالي فالأمن السيبراني هو حماية الأفراد والمؤسسات والأنظمة من حالات الاختراق الرقمي أو الدخول الغير مصرح به أو التهديدات الأمنية الخطيرة، والتي قد تؤثر على خصوصية البيانات والمعلومات لاسيما الحساسة. فالهدف الأساسي وراء ظهور الامن السيبراني هو ظهور ما يعرف بالهجمات الرقمية الخطرة أو الفيروسات المنيعة وفيها يتم الهجوم على الأنظمة الرقمية الخاصة بالأفراد أو المنشأة والسيطرة على ما تمتلكه من بيانات حساسة، وخضوعها لعمليات الابتزاز والسرقة. وجراء الخسائر الفادحة التي تسببها هذه الهجمات، ظهر الأمن السيبراني، لا بهدف الدفاع أو الحماية فقط من الهجمات الحاسوبية الضارة، بل أيضًا من أجل القيام بالهجوم المتعمد والذي يتم فيه اكتشاف الثغرات الموجودة في النظام والعمل على إصلاحها فور اكتشافها .

ومع الاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات وشبكة الإنترنت في العصر الحديث من قبل الحكومات والشركات والمؤسسات والأفراد، ولاسيما القطاعات الحيوية مثل القطاع المالي وقطاعات الطاقة لتقديم خدمات فعالة وعالية الجودة والكفاءة، وما يحمله الفضاء الإلكتروني في طياته من فرص وإمكانيات التوسع في المستقبل؛ إلا أن طبيعة الفضاء الإلكتروني – غير المقيدة بأي حدود — تتيح لبعض الجهات فرصًا لاختراق بيانات الأفراد والشركات وإلحاق الضرر بهم، لذا أصبح الحفاظ على سلامة أفراد المجتمع وشبكات البنية التحتية أحد أكبر التحديات العالمية التي تواجه جميع الدول.

وقد بادرت الدول على توظيف الذكاء الاصطناعي في مختلف مجالات الحكم والإدارة في إطار ما يعرف بالحكومة الإلكترونية، وما ينتج عنها في مجال الوظيفة العامة تحت اسم "الإدارة الذكية" التي باتت مطلباً أساسيا للارتقاء بطرق إدارة المرافق العامة؛ لأننا نعيش عصرا فريدا من نوعه، من خلال سرعة الأحداث التي تواكبها سرعة التقنيات وثورة في الرقميات، وهو ما أدى إلى تغير مجالات العمل حيث تواجه إدارة الموارد البشرية تحديات جديدة يجب معالجتها مع ضمان النمو الأمثل وتطوير جودتها. ولا شك أن تطبيق تقنية الذكاء الاصطناعي في الإدارة العامة[1].

فالذكاء الاصطناعي يسهل التواصل بين الأشخاص والآلات وتبادل المعلومات، مما يسهل تصنيع المنتجات وتعزيز الكفاءة في العمليات. مع تقدم التكنولوجيا أصبحت المعايير السابقة التي حددت الذكاء الاصطناعي قديمة. على سبيل المثال، الأجهزة التي تحسب الوظائف الأساسية أو تتعرف على النص من خلال التعرف البصري على الأحرف لم تعد تُعتبر تجسيدًا للذكاء الاصطناعي، نظرًا لأن هذه الوظيفة أصبحت الآن مفروغًا منها كوظيفة كمبيوتر متأصلة[2].

كما أن الذكاء الاصطناعي يتطور باستمرار لإفادة العديد من الصناعات المختلفة. يتم توصيل الآلات باستخدام نهج متعدد التخصصات يعتمد على الرياضيات وعلوم الكمبيوتر واللغويات وعلم النفس والمزيد. وغالبًا ما تلعب الخوارزميات دورًا مهمًا جدًا في بنية الذكاء الاصطناعي، حيث تُستخدم الخوارزميات البسيطة في التطبيقات البسيطة، بينما تساعد الخوارزميات الأكثر تعقيدًا في تأطير الذكاء الاصطناعي[3].

ويهدف الذكاء الاصطناعي إلى مساعدة القدرات البشرية على اتخاذ قرارات متقدمة ذات عواقب بعيدة المدى. هذا هو الجواب من الناحية الفنية. من منظور فلسفي يمتلك الذكاء الاصطناعي القدرة على مساعدة البشر على عيش حياة ذات مغزى أكبر خالية من العمل الشاق، والمساعدة في إدارة الشبكة المعقدة للأفراد والشركات والدول.

وكما استفاد الكثير من الشركات المصنعة من مبادئ الإدارة، من المتوقع أن يشكل الذكاء الاصطناعي خطوة عظيمة إلى الأمام في مجال تعزيز الإنتاجية. فدمج الذكاء الاصطناعي في الإدارة يعتبر المفتاح السحري لنظم رشيدة ومستقرة، ويسودها الرضا العام من الجماهير على أداء حكومته[4].

ومع ظهور الذكاء الاصطناعي وما يتيحه من إمكانيات وفرص كبيرة في شتى المجالات ومختلف الميادين، إلا أنه يتضمن مخاطر عديدة تهدد استقرار الدول ومعاملاتها الاقتصادية ويندر بحدود فوضى واضطراب في مختلف المؤسسات والمنظمات العامة والخاصة، لذلك يستوجب التعامل معه بشيء من الحذر، فإن كان يحمل معه إيجابيات كثيرة على مستويات عدة، فإن مخاطره، كذلك، كبيرة، وعلى هذا الأساس يجب تعزيز منظومة الأمن السيبراني للحد من التهديدات التي قد يحملها الذكاء الاصطناعي.

الإشكالية:

ما هي نوعية التحديات التي يحملها الذكاء الاصطناعي؟ وكيف يمكن للأمن السيبراني من الحد منها؟

خطة البحث:

المحور الأول:

المحور الثاني:

المحور الأول: الإطار النظري للدراسة

أولا: مفهوم الأمن السيبراني

هناك العديد من التعريفات التي قدمت لمفهوم الأمن لسيبراني، حيث يُعرف بأنه: "مجموعة من الإجراءات المتخذة في مجال الدفاع صد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة."

وما ذهب إليه الكاتبان " Pekka & Martti في كتابهما الموسوم " Cyber " حيث اعتبرا أن الأمن السيبراني: "عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة."

بينما عرفه إدوارد أمورسو " Amoroso" بأنه: وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة."

وفي التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام ٢٠١١-٢٠١٠ عُرف الأمن السيبراني بأنه: "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلي وتقنيات يمكن استخدامها لحماية البيئة السيبرانية[5].

وقدمت وزارة الدفاع الأمريكية "البنتاغون" تعريفاً دقيقاً لمصطلح الأمن السيبراني، فاعتبرته جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات التخريب التجسس والحوادث."

ويمكن تعريف الأمن السيبراني، ايضاً بأنه أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت. وعليه؛ فهو المجال الذي يتعلق بإجراءات ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقسى وأسوأ الأحوال، ويرتبط هذا الأمن، ارتباطاً وثيقاً، بأمن المعلومات، فالوصول إلى هذه الأخيرة، أو بثها أو الاطلاع عليها والمتاجرة بها، أو تشويهها واستغلالها، هو ما يقف غالب الأحيان، وراء عمليات الاعتداء على الشبكات وعلى الإنترنت شكل أكثر.

ومن هنا فإن على الأنظمة الإلكترونية الاعتماد على المعلومة، حقيقة لا لبس فيها، والتي تفرض اعتماداً على التي تُعالجها والحديث عن الأمن، ويستدعي تعريف الخطر، أي التهديد الذي يتعرض له النظام، إضافة إلى نقاط الضعف، أو الثغرات التي تعتريه، ومن ثم الإجراءات

المفروض اتخاذها، لدفع الخطر، فالتهديد هو نوع الأعمال العدائية، التي يمكن أن تمارس ضد النظام، بينما نقاط الضعف هي مستوى الانكشاف على هذا التهديد، في سياق معين، والإجراءات التي يفترض اتخاذها[6].

ثانيا: مفهوم الذكاء الاصطناعي

الذكاء الاصطناعي هو قفزة نوعية وفريدة في عالم البرمجيات وصيحة تكنولوجية ومعلوماتية غزت جميع مجالات الحياة، وهو فرع من الفروع الحديثة التابع لعلوم الكمبيوتر، ويتمثل هدفه الأساسي في بناء آلات ذكية قادرة على أداء المهمات المعقدة حتى ولو تطلب حلها ذكاء بشريا. ويعتبر الذكاء الاصطناعي واحدا من أنجع الحلول للنهوض بأداء الإدارة، وتحقيق التنمية المستدامة بأهدافها المختلفة، وفي خضم الثورة الصناعية الرابعة والتي يبرز فيها الذكاء الاصطناعي كأحد أهم أركانها الذي بدأت بعض الدول تتنافس في دراسته وتطويره والاعتماد عليه في مختلف الاستخدامات، فقد أصبح دمج الذكاء الاصطناعي من أجل تحسين أداء الإدارة بما يتوافق مع مختلف الإمكانيات والتوقعات في التنمية الاقتصادية والاجتماعية، فلم يعد الذكاء الاصطناعي مجرد خيال علمي فقط بل هو المستقبل.

يسهّل الذكاء الاصطناعي التواصل بين الأشخاص والماكينات وتبادل المعلومات، مما يسهل تصنيع المنتجات وتعزيز الكفاءة في العمليات. وكما استفاد الكثير من الشركات المصنعة من مبادئ الإدارة، من المتوقع أن يشكل الذكاء الاصطناعي خطوة عظيمة إلى الأمام في مجال تعزيز الإنتاجية. فدمج الذكاء الاصطناعي في الإدارة يعتبر المفتاح السحري لنظم رشيدة ومستقرة، ويسودها الرضا العام من الجماهير على أداء حكومته[7].

وفي هذا المنحى، يأتي للذكاء الاصطناعي لتعزيز جمع البيانات ومعالجتها وتحسين نمذجة المخاطر من خلال استخراج أنماط معقدة من حجم متزايد من البيانات الجغرافية المكانية ودعم اتصالات الطوارئ الفعّالة. وسيقوم الفريق المتخصص الجديد بتحليل حالات الاستعمال ذات الصلة للذكاء الاصطناعي لتقديم تقارير تقنية ومواد تعليمية مرتبطة بها تتناول هذه الأبعاد الرئيسية الثلاثة لإدارة الكوارث الطبيعية. وستتناول دراسة اتصالات الطوارئ التي سيضطلع بها الفريق الجوانب التقنية والاجتماعية والديمغرافية لهذه الاتصالات لضمان أن تعود بالفائدة على جميع الناس المعرضين للخطر[8].

ويوصف الذكاء الاصطناعي بأشد العبارات دلالة، وهي قدرته على تحريك عجلة التفكير نحو المستقبل، وإمكانية توظيف العمليات التحليلية في تقييم الفعل البشري الذي تتخلله الإرهاصات المستقبلية واستلاب الماضي وحالة اللاشعور المفضية إلى خلخلة المعيار المادي الذي تقوم عليه الحضارة. إنّ الفعل الأداتي للآلة تشكلت معه مفاهيم قاصرة حول الأدائية التي يراد للآلة القيام بها، إلى جانب تحديد الكيف والزمان الخاصين بها، وعلى هذا تنبري الخطورة في تمييز التهديد الحاصل عن "فعل الذكاء الاصطناعي" مقابل "الاستغلال الوحشي للآلة" في استحالة الاستخدامات الرشيدة للذكاء الاصطناعي بالمطلق، بعيدا عن التشوّهات التي يفرضها الهلع المستمر منه.

المحور الثاني: دور الأمن السيبراني في الحماية من مخاطر الذكاء الاصطناعي

شهدت الآونة الأخيرة تطورًا ملحوظًا في التكنولوجيا الحديثة واجتاح العصر الرقمي تقنيات جديدة لا مثيل لها ومن أبرزها الذكاء الاصطناعي الذي أصبح يستخدم في كافة المجالات حيث يمتلك الكثير من المميزات التي حلت العديد من المشكلات البشرية ولكن بالرغم من ذلك أن أنه يمتلك العديد من السلبيات التي تشكل مخاوف أمنية وأخلاقية بسبب استخدامه السيء من قبل بعض الناس، لذا يجب الحذر عند استخدام هذه التقنية من قبل الأفراد والشركات.

فالذكاء الاصطناعي هو عبارة عن مجموعة من التقنيات مدموجة معًا ظهرت حديثاً وهي تحاكي الذكاء البشري لها القدرة على حل المشكلات بطريقة ذكية ومختصرة، كما يقوم بأداء الكثير من المهام من خلال جمع البيانات ثم استخدامها لاتخاذ القرار، مما أنه يقوم بتحديث نفسه من خلال المعلومات التي يجمعها.

لم يظهر الذكاء الاصطناعي فجأة بل هو امتداد لتطور مجموعة من التقنيات مع بعضها البعض، لتظهر لنا تقنية جديدة تحاكي ذكاء الإنسان في اتخاذ القرارات بشكل سريع، وقد استفاد منه البشر منذ الظهور الأول له في الكثير من الأمور سواء في التعليم أو في الصناعة، من تطوير برامج مفيدة على الإنترنت، وما زالت التطويرات مستمرة للذكاء الاصطناعي كل يوم.

بالرغم من أن الذكاء الاصطناعي فاد البشر كثيراً إلا أنه يطوي داخله الكثير من المخاطر والتحديات التي لا يمكن السيطرة عليها فيما بعد، ويجب عليك كمهتم بهذه التقنية الحذر من سلبياتها، ومن هذه السلبيات ما يلي:

التأثير على سوق العمل حيث ظهرت البطالة بكثرة في الآونة الأخيرة خاصة بعد أن حل الذكاء الاصطناعي وبرامجه محل البشر في الكثير من الوظائف الرقمية مثل الكتابة وتعديل الصور، وكتابة البيانات وغيرها من الوظائف الأخرى.

زيادة تكاليف الإنتاج حيث تحتاج برامج وأجهزة الذكاء الاصطناعي إلى تطوير مستمر وكذلك تتطلب صيانتها الكثير من الجهد والمال.

يتسبب الذكاء الاصطناعي في ضعف المهارات البشرية بسبب الاعتماد المفرط على التكنولوجيا مما يصبح الإنسان أكثر كسلًا بعد أن وكّل الكثير من الأعمال إلى الروبوتات، وهذا بالطبع سوف يقتل الإبداع تدريجياً.

ظهور المخاطر الأخلاقية حيث يحتاج الذكاء الاصطناعي إلى جمع الكثير من البيانات والمعلومات الشخصية مما أدى إلى انعدام الخصوصية مع احتمالية استخدام هذه المعلومات الشخصية بطريقة غير أخلاقية ضد الأشخاص.

انعدام الإبداع؛ فبالرغم من أن الذكاء الاصطناعي ينجز الكثير من المهام إلا أنه لن يستطيع محاكاة العقل البشري، وإن اعتماد البشر عليه سوف يمحي الإبداع البشري بشكل تدريجي.

إلحاق أضرار كبيرة ببعض الأشخاص أو الشركات، أو الدول، مثل تشويه السمعة عن طريق التلاعب بالصور أو نشر معلومات شخصية فاضحة.

ظهور مخاطر أمنية، حيث يستخدم البعض الذكاء الاصطناعي في شن هجمات إلكترونية واختراق المعلومات السرية وهذا ما يعرف بالقرصنة السيبرانية.

كما ظهرت الكثير من المخاطر التي يعكسها الذكاء الاصطناعي على البشر والمجتمع ككل، حيث يظهر تأثيره السلبي بشكل واضح على البشر في ظهور البطالة، وانعدام الخصوصية، والاعتماد الكامل على التكنولوجيا مما أدى إلى اندثار الإبداع البشري، وأثر أيضاً على العلاقات البشرية حيث قل الاحتكاك بين البشر من ذي قبل بسبب الاعتماد على العمل من المنزل من خلال عدة برامج وعدم وجود حاجة للذهاب إلى الشركات والتواصل مع الآخرين، كما أن الشركات نفسها تعتمد على الأجهزة بشكل كبير.

يؤثر الذكاء الاصطناعي على المجتمع بشكل سلبي وبشكل خطورة كبيرة على المستوى السياسي والصحي والاجتماعي، والاقتصادي، وبالنسبة إلى تأثيره على المجتمع فيكمن في هذه النقاط:

يؤثر على الأمن العام خاصة في الجهات الحكومية التي تستخدم هذه التقنية حيث يقوم بجمع كمية كبيرة من المعلومات والبيانات والتي قد يتم اختراقها في أي من قبل المحتلين مما يشكل تهديدا للأمن القومي.

يؤثر على اقتصاد المجتمع حيث تتطلب هذه البرامج تحديثًا مستمراً وتكلفة عالية لصيانتها مما يضعف الاقتصاد وفي نفس الوقت يقلل من فرص العمل للأشخاص مما يزيد من معدل البطالة.

عند استخدام الذكاء الاصطناعي في مجال الصحة فإن ذلك يؤثر على السلامة العامة حيث يتم استخدام هذه التقنية في الأجهزة الطبية وفي حالة حدوث خطأ بسيط فإن ذلك يهدد سلامة المرضى.

بالإضافة إلى ذلك فإن للذكاء الاصطناعي يضعف من العلاقات الإنسانية ويقلل من احتكاك البشر ببعضهما البعض في أماكن العمل، حيث استغنى الكثير من الناس بالأجهزة والحاسوب، والهواتف، واستغلالها في العمل، واتخاذ القرارات دون حاجة إلى التعامل مع الآخرين، وهذا عامل كبير في ضعف الترابط والانفكاك بين البشر9.

ويأتي دور الأمن السيبراني في الحماية من مخاطر الذكاء الاصطناعي من خلال عدة جوانب وفيما يأتي أبرزها: يشمل كافة الأمور المرتبطة بحماية البيانات من المهاجمين المختصين في سرقة المعلومات والتسبب بالضرر، إذ يمكن أن تكون هذه البيانات حساسة، أو معلومات حكومية وصناعية، أو معلومات شخصية، أو بيانات تعريف شخصية، أو حقوق ملكية فكرية. يُشكّل وجود برامج الأمن السيبراني وآليات الدفاع الإلكترونية وسيلة متطورة ذات أهمية كبيرة في حماية البيانات وخدمة مصلحة الجميع، إذ يعتمد جميع أفراد المجتمع على البُنية التحتية الحيوية كالمستشفيات، ومؤسسات الرعاية الصحية، وبرامج الخدمات المالية التي يجب المحافظة عليها. تقليل مخاطر الهجمات الإلكترونية على الصعيد الفردي، إذ يمكن أن تتسبب هذه الهجمات إلى تعرض الأفراد لسرقة هوياتهم وابتزازهم، وبالتالي إحداث أضرار وخيمة في حياة الأفراد[10].

خاتمة:

أصبح الأمن السيبراني مطلبا ضروريا لكل الدول دون استثناء، لأنه يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية من خلال الإنترنت، فهو إذن حماية الحواسيب المكتبية أو المحمولة من أي نوع من الهجمات والاختراقات والتهديدات التي تحدث عن طريق السيرفرات والحواسيب الأخرى وشبكة الإنترنت بشكل عام، ويعمل مختصو الأمن السيبراني على ضمان عدم السماح لأحد غير مصرح له بالدخول والوصول إلى المعلومات، فالمارقون الذين يمارسون الجرائم الإلكترونية يقومون بنشر الفيروسات أو ينسخون المعلومات السرية والهامة أو يعدلون ويحرفون في معلومات مهمة أو حتى يبثوا معلومات غير صحيحة على مواقع مهمة، وذلك عندما يكون الأمن السيبراني ضعيفًا ويحتاج لتقوية، بالتالي فإن مهمة هذا النوع من الأمن تكمن في حماية الحاسب كله من المصادر الخارجية.

الهوامش:

[1] تهامه سميح موسى الجعافرة، الذكاء الاصطناعي ودوره في إدارة الموارد البشرية في البلديات 2023، مجلة العلوم الإنسانية والطبيعية، تاريخ النشر: 2023/02/01م تاريخ القبول: 2023/01/21

[2] Autor, David H., David Dorn, Lawrence F. Katz, Christina Patterson, and John Van Reenen,(2017)The Fall of the Labor Share and the Rise of Superstar Firms," CEPR Discussion Paper No. DP12041, May 2017b. As of October 11, 2017: https://ssrn.com/abstract=2968382

[3] حمد، احمد يوسف حافظ (2013)) النشر الالكتروني ومشروعات المكتبات الرقمية والدور العربي في رقمنة وحفظ التراث العربي. القاهرة، دار النهضة للنشر والتوزيع. مصر

[4] أمنيه سالم، إدارة الأزمات والتخطيط الاستراتيجي، المكتب العربي للمعارف، 2015، ص12

[5] فارس العمارات، ابراهيم محمد الحمامصة، الأمن السيبراني (المفهوم وتحديات العصر)، دار الخليج للنشر والتوزيع، 2022، ص 16 وما بعدها.

[6] نفس المرجع السابق، ص17

[7] أمنيه سالم، إدارة الأزمات والتخطيط الاستراتيجي، المكتب العربي للمعارف، 2015، ص12

[8] نورة محمد عبدالله العزام، دور الذكاء االصطناعي في رفع كفاءة النظم الإدارية لإدارة الموارد البشرية بجامعة تبوك، جامعة سوهاج، 2020، ص5

[9] حياة حسين، الفضاء الإلكتروني وتحديات الأمن العالمي، مجلة العلوم القانونية والسياسية، المجلد 1، العدد 1، الجزائر، ابريل 2021 ص 94

[10] سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي: الولايات المتحدة الأمريكية نموذجاً، رسالة ماجستير، جامعة محمد بوضياف بالجزائر، كلية الحقوق والعلوم السياسية، 2017. ص 96