MINISTÈRE
DES ARMÉES
ET DES ANCIENS
COMBATTANTS

Liberté
Égalité
Fraternité

ANNALES DU CONCOURS

Accès au grade de secrétaire administratif spécialisé de classe normale de la DGSE

Épreuve d'admissibilité :
spécialité arabe

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

Session 2025 (2nde session)

MINISTÈRE
DES ARMÉES
ET DES ANCIENS
COMBATTANTS

Liberté
Égalité
Fraternité

2ème épreuve d'admissibilité

Spécialité "langue : arabe"

Épreuve constituée d'une série de six à neuf questions à réponse courte portant sur le programme de la spécialité « Langue : arabe ».
Les réponses sont rédigées, permettant ainsi de juger des qualités rédactionnelles du candidat.

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

Durée : 3 heures - coefficient 2

CONCOURS EXTERNE

POUR L'ACCÈS AU GRADE DE SECRÉTAIRE ADMINISTRATIF SPÉCIALISÉ DE CLASSE NORMALE

SESSION 2025

Epreuve d'admissibilité : **Spécialité : langue arabe**

Épreuve consistant à répondre à une série de questions à réponses courtes portant sur la spécialité « langue arabe ». Il est demandé au candidat de proposer des réponses rédigées.

L'utilisation du dictionnaire bilingue est autorisée (à l'exception de tout dictionnaire électronique).

Durée : 3 heures ; coefficient 2

الأسئلة

1. اشرح مفهوم السيادة السيبرانية كما ورد في النصوص, (نقطتين) (2 points)
2. بيّن التحديات التي تواجهها الدول في الحفاظ عليها.((نقطتين).(2 points)
3. عدّد إيجابيات وسلبيات الفضاء الرقمي (٤ نقاط).(4 points)
4. اشرح كيف غيّر الفضاء السيبراني مفهوم السيادة التقليدي. (نقطتين)(2 points)
5. بيّن العلاقة بين تطور التكنولوجيا والرهانات الجيوسياسية الجديدة التي تواجهها الدول في الفضاء السيبراني مركزا على النقاط التالية: (٦نقاط).(6 points)

- الفضاء السيبراني كساحة صراع جديدة
- التكنولوجيا والتهديدات الجديدة
- الهيمنة الرقمية كأداة نفوذ جيوسياسي

6. ترجم الى الفرنسية الفقرة التالية: (٤ نقاط)(4 points)

في ظل تسارع التحول الرقمي، باتت الدول تواجه تحديات امنية جديدة، حيث لم تعد الحروب تقتصر على الميدان العسكري التقليدي، بل انتقلت الى الفضاء السيبراني، مما يستدعي تطوير أدوات جديدة لحماية السيادة الوطنية.

SOMMAIRE

Document n°1 (pages 1 à 3)

الأمن السيبراني مفهومه وتاريخه

19/9/2024

Document n° 2 (pages 4 à 6)

عصر الفضاء السيبراني والسيادة الوطنية

مركز النهرين للدراسات الاستراتيجية

تاريخ النشر18-04-2023

احمد طارق خالد

Document n° 3 (pages 7 à 9)

السيادة الرقمية.. عندما يرتهن مصير دول بكبسة زر – الإخبارية

فريق التحرير 14أغسطس 2025

النص الأول

Document 1

الأمن السيبراني مفهومه وتاريخه

19/9/2024

مقدمة

الأمن السيبراني -ويسمى أيضا أمن الكمبيوتر- وسيلة لحماية البرمجيات وأجهزة الحاسوب والشبكات، وهو مجموعة من الإجراءات المتخذة لمواجهة الهجمات والاختراقات السيبرانية وما ينتج عنها من أخطار. ظهر مع بداية الحرب الباردة وتطور مع ثورة الإنترنت وأنظمة الحاسوب، وصار وسيلة أمنية وحربية دولية أساسية ضد أي هجوم سيبراني. هذا الاخير يشكل خطرا أمنيا على الأفراد والمؤسسات والدول، فقد يستعمل لسرقة البيانات والاحتيال والوصول غير القانوني إلى بيانات مالية أو طبية أو عسكرية أو أمنية سرية، أو حتى التلاعب في أنظمة أجهزة إلكترونية عن بعد وتوجيهها بأهداف سياسية بقصد التسبب بضرر مادي، كتفجير أجهزة عن بعد أو تعطيل أنظمة.

وعليه يهدف الأمن السيبراني إلى حماية 5 أنواع من المعدات والأنظمة الأساسية، هي : أمن البنية التحتية (الاتصالات والنقل والطاقة وغيرها) وأمن الشبكات وأمن السحابة وأمن إنترنت الأشياء (الأجهزة الذكية المرتبطة بالإنترنت) وأمن التطبيقات.

مفهوم الأمن السيبراني

الأمن السيبراني مفهوم معقد يحمل الكثير من المعاني والتعريفات، ورغم اختلافها فإنها تتفق على وظيفته العامة تقريبا.

وحسب الاتحاد الدولي للاتصالات فالأمن السيبراني هو "مجموعة من الأدوات والسياسات والمفاهيم الأمنية ونهج إدارة المخاطر والإجراءات والتدريب، وغيرها من التكنولوجيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المؤسسات من المخاطر الأمنية ذات الصلة في البيئة السيبرانية".

وتعرفه وكالة الأمن السيبراني وأمن البنية التحتية الأميركية (سي آي إس إيه) بأنه "فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام الإجرامي، ويمثل ممارسة ضمان سرية المعلومات وسلامتها وتوافرها."

وتعرفه الموسوعة البريطانية بأنه "حماية نظم الحوسبة والمعلومات من الأضرار والسرقة والاستخدام غير المصرح به."

بداية ظهوره

ظهر الأمن السيبراني مع نهاية الحرب الباردة، وظهور مصطلح حرب الإنترنت أو الحرب السيبرانية، التي جاءت مع بداية اعتماد الدول على أجهزة الكمبيوتر في مؤسساتها وتطوير وحدة المعالجة المركزية في هذه الأجهزة، التي دخلت في عمل المؤسسات والحكومات وحتى في الحياة اليومية، واقتصر دور الأمن السيبراني في الفترة الأولى على الحماية من الفيروسات والبرمجيات الخبيثة.

وفي عام 1983، طوّر معهد ماساتشوستس للتقنية نظام اتصالات يعتمد على التشفير، أصبح أساسا لتطوير تقنيات الأمن السيبراني الحديثة.

وشكل ظهور الإنترنت ثورة نوعية في حياة البشرية، إذ بدأ استخدامه في المجالين الأمني والعسكري وتسابقت الدول في تطويره مع مطلع تسعينيات القرن العشرين، حتى سميت تلك الفترة بـ"الحرب السيبرانية الباردة" أو "سباق التسلح السيبراني"، وظهرت حينئذ هجمات التصيد الاحتيالية "فيشينغ" والتجسس الإلكتروني و"الهجوم الموزع لحجب الخدمة" (دي دي أو إس).

وظهرت الحاجة دوليا إلى وجود قوة غير مادية إلى جانب القدرات العسكرية والاقتصادية، فبدأت الدول تولي اهتمامها بالقوة السيبرانية لتأثيرها على المستويين المحلي والدولي.

ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي، واعتبار عدد من الباحثين الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، ظهرت الحاجة لتوفير ضمانات أمنية، خاصة مع بداية ظهور التهديدات والجرائم السيبرانية مع دخول القرن الـ21.

ودخل الأمن السيبراني ضمن حقل الدراسات الأمنية، وظهرت تقنيات متطورة مثل التشفير والأمان السحابي والكشف عن التهديدات بالذكاء الاصطناعي، ومع ذلك فإن الهجمات السيبرانية مجال معقد وسريع التطور، مما يستلزم استجابات أمنية سريعة تضاهي وتيرة نموه السريع.

كيف يعمل الأمن السيبراني؟

تعتمد المؤسسات على متخصصي الأمن السيبراني لتنفيذ إستراتيجيات الحماية. ويقيّم هؤلاء الخبراء المخاطر الأمنية التي قد تواجه أنظمة الحوسبة والشبكات ومخازن البيانات والتطبيقات والأجهزة المتصلة. ثم يضعون إطارا شاملا للأمن السيبراني ويطبقون تدابير الحماية اللازمة داخل المؤسسة.

وتعتمد مؤسسات الأمن السيبراني عدة مبادئ أساسية في عملها، الأول مبدأ "انعدام الثقة"، الذي يتطلب مصادقة صارمة ومراقبة مستمرة لجميع المستخدمين والتطبيقات. الثاني تحليلات السلوك لمراقبة الأنشطة غير المعتادة في نقل البيانات والتنبيه بشأنها.

كما تعتمد المؤسسات على أنظمة كشف التسلل لتحديد الهجمات بسرعة باستخدام تعلم الآلة. إضافة إلى التشفير السحابي لحماية البيانات المخزنة عبر تشفيرها، باستخدام خدمات للتحكم في مفاتيح التشفير.

أنواع وأشكال الهجمات السيبرانية

من أبرز التقنيات المستعملة في الهجمات السيبرانية:

- البرمجيات الخبيثة:

برامج ضارة تنشأ بهدف توفير الوصول غير المصرح به لأطراف ثالثة، إلى معلومات حساسة أو تعطيل عمل البنية التحتية الحيوية وأنظمة العمل الأساسية. ومثالا عليها: أحصنة طروادة وبرامج التجسس والفيروسات.

- الذكاء الاصطناعي:

تقنية سريعة التطور تستخدم لإنشاء هجمات سيبرانية أكثر تعقيدا وقوة، مما يجعل من الصعب اكتشافها والتصدي لها، ويمكن استخدامها لإنشاء برامج ضارة أكثر ذكاء يمكنها التهرب من تقنيات الأمان التقليدية، كما يمكن أيضا استخدام الذكاء الاصطناعي لإنشاء هجمات تستهدف البنية التحتية الحيوية، مثل شبكات الطاقة أو نظم النقل.

- التصيد الاحتيالي:

تهديد سيبراني يستخدم تقنيات الهندسة الاجتماعية لخداع المستخدمين وكشف معلوماتهم الشخصية. فقد يرسل المهاجمون رسائل إلكترونية تزعم أنها من جهة موثوقة، وتدعو المستخدمين للنقر على روابط، أو إدخال بيانات بطاقة الائتمان على صفحات ويب وهمية. ويمكن عبرها أيضا تنزيل مرفقات ضارة تثبت برامج خبيثة على الأجهزة.

- التهديدات السيبرانية للصحة الرقمية:

قد تستهدف أجهزة الرعاية الصحية أو نظم السجلات الطبية، وذلك لأنها حساسة للغاية ويمكن استخدامها لأغراض ضارة، مثل الابتزاز أو التجسس أو حتى إلحاق الضرر الجسدي.

- هجمات التحكم في الطائرات المسيرة:

أصبح استهداف الطائرات المسيرة أو أنظمة التحكم فيها محط اهتمام متزايد، وقد تتسبب هذه الهجمات بأضرار جسيمة، بما في ذلك تعطيل الطائرات أو سرقة البيانات أو حتى إسقاطها.

النص الثاني

Document 2

عصر الفضاء السيبراني والسيادة الوطنية

مركز النهرين للدراسات الاستراتيجية

تاريخ النشر18-04-2023

احمد طارق خالد

لم يعد مفهوم السيادة الوطنية المطلقة دقيقاً مع ظهور الفضاء السيبراني في أواخر تسعينيات القرن الماضي، وسيطرة الشركات متعددة الجنسيات على قطاع الانترنيت والاتصالات، وتحول الدول نحو العولمة والحكومات الالكترونية، حيث دخل الفضاء السيبراني كبعد جديد يضاف الى ابعاد السيادة الوطنية البر والبحر والجو، ويعتبر ذو طابع استراتيجي لما له من تأثير اجتماعي واقتصادي وسياسي لامركزي يعيد مفهوم السيادة الوطنية وسيطرة الدولة على حدودها بشكل كامل.

الفضاء السيبراني

اختلفت التعاريف للفضاء السيبراني من وجهة نظر المنظمات والدول لتتقاطع بمفهوم واحد، على ان الفضاء السيبراني هو مجال عالمي يتكون من شبكات مترابطة فيما بينها من خلال البنى التحتية لتكنولوجيا المعلومات والاتصالات. وتشمل شبكات الانترنيت والاتصالات وأنظمة الحاسوب والأنظمة الخاصة بوحدات التحكم للمنظومات والمعدات والمحطات، ويتكون من ثلاثة عناصر : العنصر المادي ويشمل أجهزة الحاسوب والخوادم والشبكات بأنواعها والاقمار الصناعية. العنصر التقني من أنظمة وبرمجيات وخوارزميات والعنصر الأخير البشري العامل عليها. ويدار هذا الفضاء من قبل الدول المالكة للتكنولوجيا إضافة الى الشركات العابرة للحدود التي أصبحت كيانا ينافس الدول من حيث الاقتصاديات والإدارة وعدد المواطنين (المستخدمين).

إيجابيات الفضاء السيبراني

- التواصل والتقارب الاجتماعي بين العالم الخارجي داخل نطاق واحد عبر منصات مواقع التواصل وفتح افاق المعرفة وحرية التعبير.
- تنشيط الاقتصاد العالمي والتجارة الالكترونية التي دخلت بشكل كبير في الآونة الأخيرة وظهور العملات الرقمية.
- الخدمات المصرفية (البطاقات الالكترونية) والسياحية (حجز الطيران والفنادق) التي تسهل الحياة على الانسان
- التعليم الالكتروني والجامعات الرقمية لما لها من دور كبير في نشر العلم والتعليم، إضافة الى كونها طريقة فاعلة في استمرار الحياة في الظروف الحرجة مثل الكوارث والحروب والجائحات.

سلبيات الفضاء السيبراني

- يحتوي على كم هائل من البيانات مما يجعلها سلاحا خطيرا بيد الدول والشركات والمنظمات والجماعات الإرهابية.
- الجرائم الالكترونية والابتزاز الالكتروني والاحتيال التي تزداد مع انتشار الفضاء السيبراني وزيادة عدد المشتركين.
- دول الظلام، استخلاص من مسمى الانترنت المظلم الذي ينشط فيه الإرهاب السيبراني، واستخدام العملات الرقمية المشفرة لغسل الأموال والدفع للمجرمين لتأمين ما يحتاجه المشتري من ممنوعات، او لتأدية خدمات إجرامية.
- الحروب السيبرانية والإرهاب الالكتروني.
- تجارة المخدرات والسلاح والاتجار بالبشر إضافة الى سرقة الملكية الفكرية.
- تحكم الشركات متعددة الجنسيات بملايين البشر من خلال مواقعها وفرض القيود التي قد تخالف وسياسة بعض الدول.

الفضاء السيبراني والسيادة الوطنية

دخل الفضاء السيبراني كبعد من ابعاد هيمنة الدولة وركن من اركان قوتها العسكرية، إضافة الى البر والبحر والجو والفضاء، لما له من تأثير كبير في إدارة المعركة والتأثير في العدو. إضافة الى القوة الاقتصادية والدبلوماسية والاجتماعية التي تقوي من مكانة الدولة بين دول العالم وتجعلها لاعبا مؤثرا على الصعيد المحلي والإقليمي والدولي، إذ لم تعد تقاس الدول بحجم المساحة وتعداد السكان وحجم الترسانة العسكرية وتكنولوجيا الأسلحة التقليدية، بل على مدى تطورها في المجال السيبراني وسيطرتها على فضائها السيبراني..

ان مفهوم السيادة السيبرانية للدولة يعتمد على محورين أساسيين :

1. مسؤولية الحكومات عن الهجمات الإلكترونية التي تنطلق من أراضيها، كونها تقع تحت سيادة الدولة. فالسيادة "تمنح حقوقاً للدول وتفرض عليها التزامات، وفقاً إلى محكمة العدل الدولية. وتاليا، يُفترض أن تتحكم الدول في بنيتها التحتية الإلكترونية ومنع استخدامها عن قصد أو عن غير قصد لإلحاق الضرر بالجهات الحكومية وغير الحكومية خارج حدود الدولة. وبناءً عليه، تخضع الدولة ومواطنيها ممن شاركوا في الهجمات الإلكترونية لنطاق السيادة السيبرانية.
2. مسؤولية الحكومات عن فضائها السيبراني وامن بنيتها التحتية وامن مواطنيها من الهجمات الداخلية والخارجية، ومقدرتها على صد الهجمات والاستجابة للأحداث السيبرانية والاجراء الاستباقي في الحروب السيبرانية. اضافة الى التعافي بعد الهجمات والعودة للعمل بأقل الخسائر وأسرع وقت.

اعتمدت بعض الدول مثل الصين على قوانين خاصة بالتعامل مع الانترنيت لحماية سيادتها من التدخل الخارجي من خلال بناء شبكاتها المحلية والسيطرة على بنيتها التحتية والبرمجيات والتطبيقات الخاصة بها

أضف إلى ذلك جدار الحماية العظيم للصين الذي يراقب نشاط مواطنيها في الفضاء السيبراني من خلال تطبيقات الذكاء الصناعي وخوارزمياته المعقدة في مراقبة المحتوى وحظر المواضيع المناهضة للحكومة. كذلك ا استخدام محركات بحث خاصة بها مثل Baidu وبرنامج التواصل WeChat مع سيطرتها شبه الكاملة على شركات صينية دولية مثل علي بابا وتيك توك وغيرها من شركات التواصل الاجتماعي .

كما اعتمدت بعض الدول مثل الاتحاد الأوروبي قوانين ومعاهدات تحمي بيانات مواطنيها وخصوصيتهم. وتوسعت هذه الاتفاقيات لتشمل دول خارج الاتحاد، وانطلاقة لدول أخرى لسن القوانين الخاصة بخصوصية بيانات مواطنيها على الفضاء السيبراني العالمي وتنظيم فضائها السيبراني بشكل لا يتعارض مع المبدأ العام للأنترنيت وحرية التدفق الحر للمعلومات وحرية التعبير.

الاستنتاج

جغرافياً، هناك حدود معروفة لكل دولة، ولكن في عصر الثورة التقنية والمعلوماتية الحديثة لا يوجد حدود رقمية دولية، مما جعل الأمن السيبراني أحد أهم ركائز منظومة الأمن القومي لأغلب دول العالم. وذلك بسبب أن معظم الدول باتت تخشى على سيادتها من التهديدات الجديدة ذات الطبيعة السيبرانية.

لذلك لزم الأمر بتعديل استراتيجيات وسياسات وتشريعات التحول الرقمي والخصوصية بما يتناسب ويتوافق مع مصلحة الدول الوطنية والإقليمية والدولية، إضافة الى بناء مراكز وطنية للأمن السيبراني مسؤولة عن إدارة الفضاء السيبراني وتنظيمه وحماية الدولة من الهجمات الداخلية والخارجية، ووضع الخطط والتنبؤ والاستعداد لهذه الهجمات والية التعافي منها، وتوظيف هذا الفضاء لتعزيز المكانة الدولية في المجال السياسي والاقتصادي والاجتماعي، وبناء القدرات الوطنية العاملة في هذا المجال والتثقيف ونشر الوعي والمواطنة الرقمية من اجل بناء مجتمع واع وآمن ومحصن رقميا .

النص الثالث

Document 3

السيادة الرقمية.. عندما يرتهن مصير دول بكبسة زر – الإخبارية

فريق التحرير 14أغسطس 2025

يشهد العالم تحولات تكنولوجية ورقمية متسارعة تدفع كبرى الدول إلى مواكبة أحدث التطورات في مختلف المجالات، لا سيما تلك المتعلقة بالأمن السيبراني والدفاع والاقتصاد.

ويتوقع الخبراء أن ما يعرف بـ"السيادة الرقمية" القائمة على أدوات الأمن السيبراني والذكاء الاصطناعي ستكون هي القوة المسيطرة على العالم، خصوصا مع بروز إستراتيجيات تعتمدها الدول للتصدي للمخاطر الأمنية والعسكرية والاقتصادية.

في هذا التقرير سنبرز واقع السيادة الرقمية في ظل الحروب الراهنة، وكيف تتحكم الاستخبارات السيبرانية بمصير سياسات الدول واقتصاداتها.

معركة وجود

في النصف الأول من القرن العشرين، شهد العالم حروبا كانت قائمة على قوة الهجمات النارية والمعدات العسكرية الثقيلة، من مدافع ودبابات وطائرات وقنابل استهدفت الأرض وملايين البشر وغيرت مجرى التاريخ.

أما اليوم، فنحن أمام نوع جديد من الصراعات غير التقليدية التي تعتمد على التكنولوجيا والرقمنة، حيث باتت الحروب الرقمية والهجمات السيبرانية أدوات رئيسية تستخدمها الدول لتحقيق أهداف إستراتيجية على المستويات السياسية والعسكرية والاقتصادية.

يرى المتخصص في الذكاء الاصطناعي والتحول الرقمي المهندس *قاسم دنش* أن السيادة الرقمية لم تعد ترفا فكريا أو ملفا تقنيا، بل أصبحت خط الدفاع الأول للأمن القومي وقدرة الدول على الصمود في مواجهة الحروب الحديثة التي تتخذ شكلا اقتصاديا بالدرجة الأولى، وتتقاطع مع الفضاء السيبراني بشكل مباشر.

وأضاف، خلال حديثه للجزيرة نت، *"إن معركة السيادة الرقمية هي معركة وجود، فمن يملك السيطرة على فضائه الرقمي يملك القدرة على حماية اقتصاده وفرض إرادته وتأمين أمنه القومي في زمن الحروب الاقتصادية والميدانية معا، والقوة اليوم باتت تقاس بقدر ما تملك من سيطرة على البيانات والفضاء السيبراني تماما كما كانت تقاس سابقا بما تملكه من أرض وسلاح."*

من جهتها، نشرت الجمعية الفرنسية للمعلومات سلسلة من المقابلات، من بينها مقابلة مع *لودوفيك مي* مدير برنامج الأمن السيبراني لدى وكالة البرمجة التابعة للمعهد الوطني الفرنسي للبحث في علوم الحوسبة

والرياضيات التطبيقية(INRIA) ، طرحت خلالها تأثير الذكاء الاصطناعي على مختلف القطاعات المهنية، ولا سيما مجال الأمن السيبراني.

وقد أبرزت المقابلة الدور المتصاعد للذكاء الاصطناعي في تطوير أدوات وتقنيات الحماية والدفاع، بالإضافة إلى تركيزها الشديد على تداعيات هذه التقنية وأن هذا التطور يتطلب وجود مراكز بيانات ضخمة ذات استهلاك عال للطاقة من أجل جمع البيانات بما يؤثر بشكل مباشر على البيئة والمناخ، بالإضافة إلى التحديات التي يفرضها هذا التطور على أمن الأنظمة الرقمية.

الاستخبارات السيبرانية

وفي تعليقه على أبرز الإستراتيجيات التي تعتمدها الدول للتصدي لمخاطر السيادة الرقمية على المستويات الأمنية والعسكرية والاقتصادية، قال المهندس دنش إن الدول الكبرى اليوم تبني جيوشا سيبرانية موازية للجيوش التقليدية المعتادة ومجهزة بأحدث أدوات الدفاع والهجوم الرقمي مع أنظمة إنذار مبكر لحماية البنى التحتية الحيوية من شبكات كهرباء ومياه ومنظومات اتصال ونقل وصولا إلى الأنظمة العسكرية نفسها.

وفي ظل هذه التحديات، يتعين على الدول أن تسنّ تشريعات صارمة لحوكمة البيانات وحمايتها من التسرب أو السيطرة الخارجية مع توطين مراكز البيانات والخدمات داخل الحدود الوطنية، ويؤكد دنش أن *"هذا تحدّ كبير أمامها وأن عليها بناء تحالفات رقمية مع الدول الصديقة لخلق شبكات تقنية آمنة."*

كما أكد المهندس دنش أن الاستقلالية التقنية على المستوى الاقتصادي باتت ضرورة وجودية، من خلال تطوير أنظمة دفع رقمية وطنية وحلول مالية داخلية قادرة على العمل حتى في حال قطع الدولة عن المنظومات العالمية، وحماية سلسلة الإمداد التكنولوجية وضمان امتلاك المكونات الحساسة من دون الخضوع لابتزاز أو حصار رقمي.

استثمار القوى العظمى في النظم المعلوماتية

وأوضحت بيانات رسمية نشرها موقع المنظمة العالمية للملكية الفكرية " ويبو "بتاريخ 2 يونيو/حزيران 2025 أن الإنفاق العالمي على البرمجيات بلغ ما يقارب 700 مليار دولار أميركي سنة 2024.

ووفقا لمؤشرات قاعدة البيانات "إس آند بي غلوبال" لعام 2024، فإن إجمالي إنفاق الولايات المتحدة على البرمجيات بلغ 368.52 مليار دولار أميركي، والصين 61.77 مليار دولار، وألمانيا 22.23 مليار دولار.

كما بلغ إنفاق المملكة المتحدة على القطاع نحو 20.32 مليار دولار، وفرنسا 19.28، وإيطاليا 14.24، وكندا 14.03، واليابان 13.16، ويقدر إجمالي إنفاق الاتحاد الأوروبي بما يقارب 118 مليار دولار أميركي.

وأنفقت روسيا الاتحادية ما يقارب 1.6 تريليون روبل (نحو 20 مليار دولار أميركي) على استبدال أنظمة البرمجيات الأجنبية بالمحلية، وخلال الثلاث سنوات الأخيرة نما سوق البرمجيات لديها بنسبة 40%، وبلغ نحو 5 تريليونات روبل روسي (ما يعادل نحو 62 مليار دولار أميركي)، وفقا لما ذكره موقع"إي تي ورلد" الروسي.

هل تسيطر الرقمنة على حروب العصر الحديث؟

أما عن إمكانية الاعتماد الكلي على الذكاء الاصطناعي في الحروب الحديثة، فقد اعتبر المهندس دنش أنه لن يحدث في المدى القريب، لأن الحروب لا تزال تحتاج إلى مزيج بين القدرات التقليدية والذكية .واستدل على ذلك باستمرار الاعتماد على معدات عسكرية ثقيلة، ودمجها، بدلا من الاستغناء عنها، مع أنظمة تحكم ذكية عن بعد، بحيث أصبحت تدار هذه المنظومات بكبسة زر لكن تحت إشراف بشري محكم.

وأضاف أن الدول تدرك أن الذكاء الاصطناعي يمنحها سرعة ودقة تفوق قدرات البشر في جمع المعلومات وتحليلها وتنفيذ العمليات، ولكنه يحمل مخاطر عالية إذا تُرك القرار النهائي للآلة من دون رقابة بشرية.

لهذا، يتجه العالم اليوم، بحسب المتخصص بالذكاء الاصطناعي، نحو "العسكرة الذكية المراقبة" وهي أنظمة هجينة تمزج بين القوة المادية التقليدية والقدرة الذكية مع بقاء الإنسان في دائرة اتخاذ القرار النهائي.

MINISTÈRE
DES ARMÉES
ET DES ANCIENS
COMBATTANTS

Liberté
Égalité
Fraternité

Copies ayant obtenu la meilleure note

Spécialité langue : arabe

L'administration n'a volontairement pas corrigé les imperfections de fond et de forme dans les copies communiquées ci-après.

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

© EXATECH

Année : 2025

Concours : SAS EXTERNE

Épreuve : Spécialité : Langue arabe

Consignes :

- *Ne pas signer la composition et ne pas y apporter de signe distinctif*
- *Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens*
- *N'effectuer aucun collage ou découpage de sujets ou de feuilles*
- *Ne joindre aucun brouillon*

(1) مفهوم الأمن السيبراني « السيادة السيبرانية »

مع انتشار الفضاء المعلوماتي في الآونة الأخيرة، وازدياد المخاطر والتحديات التي تشكلها صعوبة تناقل المعلومات على مستوى الأفراد وكذلك الأنظمة والدول، فإنه ذلك أصبح يشكل صعوبة من العبء على الأنظمة لإيجاد حلول ومقترحات تكنولوجية وكذلك قانونية لتنظيم وإدارة كل ما يتعلق بتبادل وتناقل المعلومات.

ولأنه الإطار الأكبر من المعلومات يقع في جانب أنظمة الدول وقطاعاتها، فإنه ذلك يُعتبر بشكل رئيس سيادة الدولة، في أي حالة من اختراقه أو سرقة بيانات تتضمن ما يمس سلامة وأمن الدولة على كافة الأصعدة.

ولذا فإنه الفضاء السيبراني يُعد حقلاً واسعاً ورحباً نرى فيه صور من صفحات الدول على دول أخرى ليس بالقوة العسكرية فقط كما كان سابقاً، وإنما صورة من التبادل أو امتلاك مفاتيح معلوماتية تشكل وسيلة ضغط أو معادلة للطرف الآخر المخترق.

لذلك فإنه حماية الدولة لنظامها المعلوماتي - وهو أمنها في الأساس - يتجلى في صورة حفاظها على سيادتها.

ولذا يمكننا القول أن السيادة السيبرانية للدولة تقوم على ركيزتين:

(1) أنه الحكومات هي التي يقع على عاتقها المسؤولية عن أي هجمات إلكترونية تنظم من أراضيها - نظام سيادتها -، لأنه مفهوم السيادة يمنح للدول حقوقاً ويفرض عليها التزامات، وفقاً للنظام القانوني الذي نصت عليه محكمة العدل الدولية.

إضافة إلى ذلك، تحكم الدول والحكومات في بنيتها التحتية الإلكترونية - وهو أمر مفترض - بحيث أن يمنع استخدام تلك البنى التحتية عن قصد أو دونه في إحداث أي ضرر أو تهديد للجهات والأجهزة الحكومية وغير الحكومية خارج حدود الدولة

وبناءً على ذلك، فهي تُخضع ذاتها - أي الدولة بأجهزتها - وكذا مواطنيها لأي مسؤولية حال صدور أي هجمات الكترونية منهم أو ضدهم، وهذه صورة السيادة السيبرانية للدولة.

2) القدرة والمسؤولية من الدولة على توفير الحماية وأمن البنية التحتية وفضائها السيبراني من أي صورة تهديد داخلي أو خارجي، وقدرتها على صد الهجمات والعودة للعمل بأقل الخسائر وأسرع وقت، وهو ما يشكل الثقة في القدرة على التصرف وحماية الأمن المعلوماتي، مما يصير دلالة دامغة على حماية سيادة الدولة لذاتها.

2) التحديات التي تواجه الدول في الحفاظ على السيادة السيبرانية

رغم أن العديد من الدول خاصة الدول الكبرى دخلت في مجال التنافس الكبير الذي يشكل سباقاً للزمن في الوصول إلى امتلاك أكبر قدر من مفاتيح السيطرة على أمنها الرقمي - السيبراني -، وهذا التسابق في الوسائل هو الذي يدلل على تلك الصورة الجلية للسيادة من عدمها، فإننا نلاحظ أن دولاً كالصين مثلاً قد ابتكرت آلية تطبيق للقيام بحساب خوارزميات البرمجيات المستخدمة من الأفراد والأجهزة لديها لرقابة الفضاء المعلوماتي وحمايته من الاختراق، وهي آلية تسعى بها للحد من أي وسيلة تقوّض أمنها السيبراني، إضافة إلى سعيها الدؤوب في السيطرة على الشركات ووسائل التواصل كالتيك توك وغيره الذي يتضمن قاعدة عريضة من المستخدمين، تحرص على أن يكون مملوكاً لها وليس لندّ لها مثل أمريكا التي يمتلك رجال أعمالها شبكات أخرى كـ إكس وفيسبوك «ميتا» التي تضم في بوتقتها العديد من الشبكات.

لذا، فإن التحدي الأكبر للدول، رغم وجود الحدود التي تحدد شكل الدول برياً وبحرياً وجوياً، إلا أن التسارع التكنولوجي والصيغ الجديدة في تناقل المعلومات لا يعترف بتلك الحدود، مما يجعل الأمن السيبراني ذاته أحد أعمدة الأمن القومي للدولة، وأمام هذا التحدي الكبير، فإن الدول تسعى لبناء مراكز وطنية للأمن السيبراني تكون مسؤولة عن إدارة الفضاء السيبراني وتنظيمه وحماية الدولة من الهجمات الداخلية والخارجية، ووضع الخطط والتنبؤ والاستعداد لهذه الهجمات وآلية التعافي منها، وتوظيف هذا الفضاء لتعزيز مكانة الدولة «دولياً» في المجال السياسي والاقتصادي والاجتماعي، وتقوم بتعزيز بناء القدرات الوطنية واختيار وتدريب الكفاءات الوطنية العاملة في هذا المجال سعياً لامتلاك القدر الكافي من العمل في هذا الحقل، تنمية وحماية، ونشر الوعي التثقيفي بين المواطنين حول الثقافة الرقمية وسبل الحماية ومواجهة أخطارها، للوصول إلى بناء أساس صلب وقوي لمجتمع آمن ومحصن رقمياً، وهي الصورة التي تشكل السيادة السيبرانية الكاملة بأمن الفرد والجماعة الوطنية.

③ إيجابيات وسلبيات الفضاء الرقمي

تجدر الإشارة إلى أن الفضاء السيبراني « الرقمي » بما يشكله من تحديات للأفراد وكذلك الدول بأجهزتها، فإنه يحمل في طياتها الجانبين، السلبي والإيجابي كالعديد من الوسائل التكنولوجية على وجه الخصوص.

فنرى إيجابيات الفضاء الرقمي كما يلي:

- الصلة والتقارب الاجتماعي بين العالمين الخارجي والداخلي في بوتقة واحدة عبر منصات مواقع التواصل، وفتح مجالات وآفاق المعرفة وكذا حرية التعبير والرأي، حيث لم تقتصر وسائل الاتصال والتعارف على الطرق التقليدية التي توجب المقابلات بالأجساد « فيزيائياً »، وإنما أصبح هناك همزات وصل بين الأطراف وهم في قارات متغايرة، إلى جانب حريات التعبير التي صارت تجعل الناس لا ينتظرون جريدة أو مجلة كي تخبرهم برأي صحفي واحد بوجهة نظر واحدة، وإنما صار التبادل والتعبير بين كافة الناس عبر المنصات والحسابات المختلفة.

- تنشيط الاقتصاد العالمي والتجارة الإلكترونية، فلم يصر الأمر مقتصراً على فكرة الأسواق التقليدية التي تحتاج إلى حجز أماكن ومصروفات، بل إن التجار اليوم وكذا الاقتصاديون يملكون منصات تجارية ويبيعون لبلاد أخرى وأفرادها عبر تلك الحسابات على المساحات الفضائية، بتأجير منصات وامتلاكها، حتى الشركات الكبرى سعت لامتلاك منصات موازية لها على الفضاء الرقمي لكسب عدد أكبر من العملاء، وأصبح باستطاعة أي شخص أن يروج لسلعة أو حرفة يمتلكها عبر منصة ينشئ عليها حساباً خاصاً وهي مسألة عملية وموفرة للمصروفات.
إضافة للعملات الرقمية والمتاجرة بها، وهي صورة من صور المضاربة والتجارة في هيئة تبادلية لتحويل الأموال إلى مجرد أرقام في الحسابات المصرفية.

- خدمات البنوك وتسهيلات الدفع والشراء عبر البطاقات الإلكترونية « الائتمانية » مما يسهل صور الدفع وعدم الاحتياج إلى الأموال النقدية، وهو أمر فيه حماية لمعرفة خط سير الأموال من حسابات الأفراد - إلى حد ما -، كما أن امتلاك بطاقات المصارف اليوم يشكل وسيلة تسهيل كبرى للأفراد، لحجز الفنادق والمناسبات العديدة كالطيران والمطاعم والملاهي الترفيهية، والتبرع بالأموال وتحويلها لمن يحتاج خاصة إن كان بعيداً، وهي كلها صور من التيسير المحمود الذي قدمه الفضاء الرقمي.

- التعليم، حيث دخل الفضاء الرقمي بشكل واسع في هذا المجال من خلال إنشاء الجامعات الفعلية التي تمتلك مبان ومواقع لها على الأرض، مساحات موازية لها على الفضاء الإلكتروني، فشكل ذلك تسهيلاً كبيراً للطلبة والباحثين الذين يملكون الوصول

لأبحاثهم، كما أنه شكل وسيلة آمنة كما رأينا في جائحة كورونا عام 20 و 21 حيث صارت الوسيلة الوحيدة للتعلم عن بعد من قبل الأساتذة و الطلبة، أو في حالات الحروب و توقف الجامعات و المدارس عن النهج التقليدي في الدراسة.

عطفاً على ما سبق، فإن دخول الفضاء الرقمي في الجانب التعليمي أنشأ أيضاً فكرة التعلم عن بعد. كما سبق. وهو الحصول على قدر من الساعات التعليمية داخل مؤسسة مسجلة ولها موقع الكتروني، ثم اجتياز الاختبارات و الحصول على شهادة بدرجات التعليم المختلفة، مما يشكل صورة من التأثير على الطلاب و الباحثين في الانخراط بالمجال التعليمي في مؤسسة افتراضية ذات موقع على ساحة الكترونية.

كما أنه يتيح الوصول للأبحاث و المصادر المرجعية للأبحاث، فاليوم لست بحاجة أن تذهب مصر أو روسيا للهند أو الصين أو اليابان أو أمريكا للتوصل إلى مرجع في مكتبة هناك، وإنما من خلال ضغطة زر ترتصل إلى مرادك.

أما إذا جئنا لسلبيات الفضاء الرقمي فنرى التالي:

- أنه يعد وعاء ضخماً يحوي في طياته كماً مهولاً من البيانات و المعلومات، مما يشكل تهديداً من الأفراد و الشركات و الدول و المنظمات و الجماعات الخطرة - الإرهابية - من الوصول إلى تلك البيانات، و عنه نسمع عن جميع أنواع عمليات الاختراق و الوصول لبيانات المستخدمين.

- الجرائم الإلكترونية و الابتزاز الإلكتروني و جرائم النصب و الاحتيال التي تزداد من عدد المشتركين على المنصات بالفضاء الرقمي.

- المناطق المظلمة التي تدعى " Dark Web " الإنترنت المظلم، الذي يعد لباب المخلف الأسوء لكل الممنوعات من غسيل أموال و تجارة الأعضاء و الأفراد و السلاح و تأدية خدمات إجرامية من تصفيات و ملاحقات و لذلك سرقة الملكيات الفكرية.

- الحروب السيبرانية و عمليات القرصنة و سرقة البيانات و الإرهاب الإلكتروني.

- تحكم الشركات متعددة الجنسيات بملايين الأفراد من خلال مواقعها و فرض قيود و سياسات تخالف قوانينه و سياسات يعتمدها الدول، بحيث تصير أعمالها غير مشروعة وفقاً لأنظمة تلك الدول.

© EXATECH

Année : 2025

Concours : SAS EXTERNE

Épreuve : Spécialité Langue arabe

Consignes :

- Ne pas signer la composition et ne pas y apporter de signe distinctif
- Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens
- N'effectuer aucun collage ou découpage de sujets ou de feuilles
- Ne joindre aucun brouillon

④ تغيير الفضاء السيبراني لمفهوم السيادة التقليدي

عبر الزمن، كانت فكرة السيادة التي تطورت عبر المفكرين الإنكليز (لوك) و (هوبز) والفرنسيين (مونتسكيو) و (روسو)، تدور حول تلك الهيمنة بالسلطة السياسية على مكونين: الشعب والإقليم، سواء كانت السلطة ديمقراطية أم مستبدة "دكتاتورية"، وهذا التصور جعل التدافع بين الأمم والدول عبر الأزمنة من خلال القوى المعتادة، أي بالتجارب والهجمات المضادة والصراعات الناشئة عن آليات ~~الاقتتال~~ الاقتتال من أسلحة ~~تكر~~ تتطور عبر الأجيال.

إلا أنه اليوم لم يصر الأمر قائماً أو مقتصراً على هذه الفكرة، بل إن الفضاء الرقمي لم يعد مسألة متعلقة بترفيات أو مسائل فرعية على هامش المجتمع، بل صار هو الأساس والركيزة وخط الدفاع الأول في حماية الأمن القومي، حال وصول ونجاح أحد الأطراف في الصراع لامتلاك مفاتيح وهيمنة المعلوماتية بصورة أكبر أو بشكل استباقي عن الطرف الآخر، وأهم عنصر في ذلك هو القطاع الاقتصادي، لذا فإن الدول الكبرى حرصت - وما زالت - على امتلاك قطاعات استخباراتية - تتعلق بالجانب الاقتصادي للوصول إلى صورة مثلى في حماية الميزانيات ورؤوس الأموال وأمن المصارف والتبادلات التجارية وأمن سوق الأوراق المالية - البورصة - كلها أمور من جوهر الأمن القومي لسيادة الدولة، وهو أمر يدار ببرمجيات من خلف الحواسيب دون احتكاكات بأسلحة تقليدية!

فحقيقة أن القوة اليوم لدى الدول تقاس بمدى امتلاك وفرض هيمنة وسيطرة على المعلومات والفضاء السيبراني، على نفس الدرجة التي كانت تقاس به قديماً بما تملكه الأنظمة من عتاد عسكري أو مساحة أرض.

وهذا السياق يستدعي من الدول لحماية أمنها القومي، إنشاء مراكز بيانات ضخمة ذات طاقة عالية من أجل جمع أكبر كمية من البيانات لحماية الأفراد والشركات

وأجهزة الدولة، فهي صورة حديثة للجيوش التقليدية، وهي الجيوش السيبرانية المجهزة بأحدث التقنيات وأدوات الدفاع والهجوم الرقمي، مع أجهزة إنذار مبكر لحماية البنى التحتية الحيوية كشبكات الكهرباء والمياه والانترنت والاتصال والنقل والمواصلات.

كما يساهم التعاون الأمني بين الدول في المجال السيبراني في الوقاية وكذا الحماية من تلك الهجمات، وتبادل بعض أنظمة الحماية التي توفر سبل توفير الأضرار المستقبلية الناجمة عن أي هجمات مضادة.

(5) العلاقة بين تطور التكنولوجيا والرهانات الجيوسياسية الجديدة التي تواجهها الدول في الفضاء السيبراني

(1) الفضاء السيبراني كساحة صراع جديدة

شكل ظهور الفضاء السيبراني نقطة تحول جوهرية وكبيرة تشبه الثورة الصناعية، حيث ازدادت وتيرة استخدام أجهزة الحواسيب مع نهايات الحرب الباردة بين أمريكا والاتحاد السوفيتي السابق في ثمانينيات القرن الماضي، مما أدخل معادلة جديدة خاصة لدى الأنظمة الكبرى في وسائل السيطرة والهيمنة شيئاً فشيئاً.

وكانت البدايات في عمليات الهيمنة على سوق التجارة والتصدير وإيجاد منصات تتحكم في أسواق المال العالمية، مما شكل صورة من الحروب والتهديدات للأطراف التي صارت تتسابق خطوة بعد أخرى في انتزاع الهيمنة من نظيرتها للوصول إلى مكاسب جديدة، بيانات جديدة تحقق لك مكسباً في الفضاء الرقمي، مما شكل صورة من الفوز وربح مساحة جديدة.

فكما كان في السابق فكرة الهيمنة على الأرض والبحار والجو بالعتاد العسكري، والتسابق في التسليح والتكنولوجيا العسكرية، فإنه يجدر بنا أن نلاحظ الوتيرة السريعة التي قفزت بها التكنولوجيا خاصة في العقدين الأخيرين، حيث وجدنا أن كل شخص اليوم يملك حاسوباً وجوال - موبايل - متنقل، يملك من خلاله شبكة إنترنت، يستطيع الوصول به إلى كم هائل من المعلومات والبيانات التي ترسم ملامح ما وصل إليه هذا التقدم على المستوى الفردي فما بالنا بمستوى الدول.

فأصبحت الدول تسعى لامتلاك أكبر قدر من المساحة في الفضاء السيبراني لتحقيق أكبر قدر من الهيمنة والسعي وراء الوصول إلى الأسبقية في كافة المجالات والتحكم في الأطراف الضعيفة، وإن جاز لنا القول أن هناك من حين لآخر سباق

سباق التسلح بين الدول في المجال العسكري، فإن الأنظمة اليوم تسعى إلى سباق المعلوماتية والوصول إلى التنافس والهيمنة عن طريق الخطوات الاستباقية كما نرى ذلك جلياً في حرب روسيا وأوكرانيا، كما نراه في الظل بين أمريكا والصين فيما يشبه حرب تكسير العظام على النطاق الجيوسياسي من جهة تيوان واليابان حلفاء أمريكا في وجه الصين، أو النطاق الاقتصادي في حرب السيطرة على المنصات الاجتماعية أو سوق الأموال والتجارة.

(2) التكنولوجيا والتهديدات الجديدة

في مواجهة هذا التقدم المتسارع في المساحات الرقمية يتزايد التهديد بشكل كبير، عبر عمليات سرقة واختراق وقرصنة المعلومات مما يشكل تهديداً للدول والأنظمة ولذا فإن الدول تسعى للوصول إلى أقصى قدر من الحماية لأفرادها وشركاتها ومنظماتها من خلال إنشاء هيئات تعكف على استراتيجيات الحماية السيبرانية من خلال خبراء ومتخصصين، حيث يشهد التطور التكنولوجي استخدام برمجيات ضارة وخبيثة تنشأ بهدف الوصول لبيانات طرف ثالث غير مصرح بذلك، وهذا يسمح بالوصول لمعلومات وبيانات، أو يقوم بتعطيل عمل البنية التحتية الحيوية وأنظمة العمل الأساسية، كأحصنة طروادة وبرامج التجسس والفيروسات.

كما أن الذكاء الاصطناعي وتطوره يشكل تحدياً لإنشاء هجمات سيبرانية أكثر تعقيداً وقوة، مما يجعل من الصعب اكتشافها والتصدي لها، ويمكنها من إنشاء برامج ضارة أكثر ذكاءً يمكنها التهرب من تقنيات الأمن التقليدية.

كما أن الهجمات التي تهدد أجهزة الرعاية الصحية أو نظم السجلات الطبية يمكن استخدامها بصور تهدد بإلحاق الضرر الجسدي أيضاً.

إضافة إلى تكنولوجيا الطائرات المسيرة والتحكم فيها، فأصبح استهدافها أو أنظمة التحكم فيها محط اهتمام متزايد، فالهجمات عليها تشكل تهديداً بأضرار جسيمة، بما في ذلك تعطيل الطائرات أو سرقة البيانات أو حتى إسقاطها.

(3) الهيمنة الرقمية كأداة نفوذ جيوسياسي

أصبحت معركة السيادة الرقمية على الساحة الدولية معركة نفوذ ووجود، فلذا تسعى الدول لامتلاك مفاتيح السيطرة على أكبر قدر من المساحة والفضاء المعلوماتي، فمن يملك السيطرة على فضائه الرقمي يملك القدرة على حماية اقتصاده ويفرض كذلك إرادته، ويملك تأمين أمنه القومي في أزمنة الحروب الاقتصادية وكذلك الميدانية أيضاً.

فالقوة اليوم في الواقع تقاس بقدر ما تملك من سيطرة على البيانات والفضاء السيبراني تماماً كقياسها سابقاً بامتلاك الأرض والسلاح.

ولذلك، فإن الدول والقوى العظمى تقوم باستثمارات ضخمة في النظم المعلوماتية للوصول لأكبر قدر من الحماية الكافية لأمنها والسعي لتحقيق توازن على الساحة الجيوسياسية بين الأطراف المتجاذبة على الصعيد الدولي.

⑥ ترجمة النص إلى الفرنسية :

Dans l'accélération de transfer numérique, les pays se sont devenus devant des nouveaux défis sécurités, parce que les guerres n'ont plus resté just comme des guerres traditionnelles mais, elles ont traversé à l'espace cybranie, donc il doit développer des manières et outils modernes pour protéger la souveraineté nationale.

في ظل تسارع التحول الرقمي، باتت الدول تواجه تحديات أمنية جديدة، حيث لم تعد الحروب تقتصر على الميدان العسكري التقليدي، بل انتقلت إلى الفضاء السيبراني مما يستدعي تطوير أدوات جديدة لحماية السيادة الوطنية.

© EXATECH

Année : 2025

Concours : SAS Externe

Épreuve : Langues et Civilisation Arabe

Consignes :

- *Ne pas signer la composition et ne pas y apporter de signe distinctif*
- *Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens*
- *N'effectuer aucun collage ou découpage de sujets ou de feuilles*
- *Ne joindre aucun brouillon*

الأجوبة

1. ان مفهوم السيادة السيبرانية يعتمد على محورين أساسيين، أما الأولى هي أن المسؤوليات (الحكومية) الحكومات عن الهجمات الإلكترونية التي تنطلق من أراضيها، كونها تقع تحت سيادة الدولة. فالسيادة" تمنح حقوقاً للدول وتفرض عليها التزامات، وفقاً إلى محكمة العدل الدولية". وتالياً، يُفترض أن تتحكم الدول في بنيتها التحتية الالكترونية ومنع استخدامها عن قصد أو عن غير قصد للإلحاق الضرر بالجهات الحكومية وغير الحكومية خارج حدود الدولة. وبناءً عليه، تخضع الدولة ومواطنيها ممن شاركو في الهجمات الإلكترونية لنطاق السيادة السيبرانية. وأما الثانية فهنالك مسؤوليات الحكومات عن فضائها السيبراني وامن بنيتها التحتية وامن مواطنيها من الهجمات الداخلية والخارجية، ومقدرتها على صد الهجمات و الاستجابة للأحداث السيبرانية والاجراء الاستباقي في الحروب السيبرانية اضافة الى التعافي بعد الهجمات والعودة للعمل بأقل الخسائر وأسرع وقت.

2. التحديات للحفاظ عليها استنتج بإعداد بعض الدول مثل الصين على قوانين خاصة بالتعامل مع الانترنت لحماية سيادتها من التدخل الخارجي من خلال بناء شبكتها المحلية والسيطرة على بنيتها التحتية والبرمجيات والتطبيقات الخاصة بها.

أضف إلى ذالك جدار الحماية العظيم للصين الذي يراقب نشاط مواطنيها في الفضاء السيبراني من خلال تطبيقات الذكاء الصناعي وخوارزمياته المعقدة في مراقبة المحتوى وحظر المواضيع المناهضة للحكومة كذالك استخدام محركات بحث خاصة بها مثل Baidu وبرنامج التواصل Wechat مع سيطرتها شبه الكاملة على شركات صينية دولية مثل علي بابا وتيك توك وغيرها من شركات التواصل الاجتماعي.

كما أيضًا هناك دول أخرى مثل الاتحاد الأوروبي أعتمدت على قوانين ومعاهدات تحمي بيانات مواطنيها وخصوصيتهم. وتوسعت هذه الاتفاقات لتشمل دول خارج الاتحاد، وانطلاقة لدول أخرى لسن القوانين الخاصة بخصوصية بيانات مواطنيها على الفضاء السيبراني العالمي وتنظيم فضائها السيبراني بشكل لا يتعارض مع المبدأ العام للأنترنيت وحرية التدفق الحر للمعلومات وحرية التعبير

.3

* إيجابيات الفضاء الرقمي هم التالي:

- يتوقع الخبراء أن ما يعرف بـ "السيادة الرقمية" القائمة على أدوات الأمن السيبراني والذكاء الاصطناعي ستكون هي القوة المسيطرة على العالم، خصوصًا مع بروز استراتيجيات تعتمدها الدول لتصدي للمخاطر الأمنية والعسكرية والاقتصادية.

- يرى المتخصص في الذكاء الاصطناعي والتحول الرقمي المهندس قاسم دنش أن السيادة الرقمية لم تعد ترفًا فكريًا أو ملفًا تقنيًا، بل أصبحت خط الدفاع الأول للأمن القومي وقدرة الدول على الصمود في مواجهة الحروب الحديثة التي تتخذ شكلًا اقتصاديًا بالدرجة الأولى، و تتقاطع مع الفضاء السيبراني بشكل مباشر

* سلبيات الفضاء الرقمي هو كما أبرزت المقابلة الدور المتصاعد للذكاء الاصطناعي في تطوير أدوات وتقنيات الحماية والدفاع، بالإضافة إلى تركيزها الشديد على تداعيات هذه التقنية وأن التطور يتطلب وجود مراكز بيانات ضخمة ذات استهلاك مال للطاقة من أجل جمع البيانات بما يؤثر بشكل مباشر على البيئة والمناخ، بالإضافة إلى التحديات التي يفرضها هذا التطور على أمن الأنظمة الرقمية.

4. غير الفضاء السيبراني مفهوم السيادة التقليدي للإبرازه على الاستراتيجيات التي تعتمد عليها الدول للتصدي لمخاطر السيادة الرقمية على المستويات الأمنية والعسكرية والاقتصادية وبنيانها جيوشًا سيبرانية موازية للجيوش التقليدية المعتادة ومجهزة بأحدث أدوات الدفاع والهجوم الرقمي مع أنظمة إنذار مبكر لحماية البنى التحتية الحيوية من شبكات كهرباء ومياه ومنظومات اتصال ونقل وصولًا إلى الأنظمة العسكرية نفسها.

Voir la bonne version page 4/4

5.

شهد العالم تحولات تكنولوجية ورقمية متسارعة تدفع كبرى الدول إلى مواكبة أحدث التطورات في مختلف المجالات، لا سيما تلك المتعلقة بالأمن السيبراني والدفاع والاقتصاد. لما دفع إخبار الخبراء لنا بأن السيادة الرقمية القائمة على أدوات الأمن السيبراني والذكاء الاصطناعي ستكون هي القوة المسيطرة على العالم، وأضاف المتخصص للإخبار لنا عبر حديثه للجزيرة نت بأن معركة السيادة الرقمية هي معركة وجود، فمن يملك السيطرة على فضائه الرقمي يملك القدرة على حماية اقتصاده وفرض إرادته وتأمين أمنه القومي في زمن الحروب الاقتصادية والميدانية معا، والقوة اليوم باتت تقاس بقدر ما تملك من سيطرة على البيانات والفضاء السيبراني تماما كما كانت تقاس سابقا بما يملكه من أرض وسلاح، وهنا نستذكر استثمار القوى العظمى في النظم المعلوماتية حيث أوضحت بيانات رسمية عبر نشرها موقع "المنظمة العالمية للملكية الفكرية" وبيو بتاريخ 2 يونيو/حزيران 2025 أن الإنفاق العالمي على البرمجيات بلغ ما يقارب 700 مليار دولار أمريكي سنة 2024 هذا ما يوضح لنا أن الدول تدرك أن الذكاء الاصطناعي يمنحها سرعة ودقة تفوق قدرات البشر في جميع المعلومات وتحليلها وتنفيذ العمليات، لهذا يتجه العالم اليوم، بحسب المتخصص بالذكاء الاصطناعي نحو "العسكرة الذكية المراقبة" وهي أنظمة هجينة تمزج بين القوة المادية والتقليدية وقدرتها الذكية مع بقاء الإنسان في دائرة اتخاذ القرار النهائي.

6.

Durant la transformation numérique, les nations sont confrontées à un nouveau défi sécuritaires, les guerres ne se limitent plus au champs de bataille traditionnelle mais se sont deplacés dans le cyperspace, ce qui les incitent à developer des nouveaux/nouvelles affaires afin de proteger la souveraineté nationale.

إيجابيات الفضاء السيبراني

- التواصل والتقارب الاجتماعي بين العالم الخارجي داخل نطاق واحد عبر منصات مواقع التواصل وفتح آفاق المعرفة وحرية التعبير
- تنشط الاقتصاد العالمي والتجارة الالكترونية التي دخلت بشكل كبير في الآونة الأخيرة وظهور العملات الرقمية
- الخدمات المصرفية
- التعليم الالكتروني

السلبيات الفضاء الرقمي

- يحتوي على كم هائل من البيانات مما يجعلها سلاحاً خطيراً بيد الدول والشركات والمنظمات والجماعات الارهابية
- الجرائم الالكترونية والابتزاز الالكتروني والاحتيال التي تزداد مع انتشار الفضاء السيبراني وزيادة عدد المشتركين
- الحروب السيبرانية والإرهاب الالكتروني
- تجارة المخدرات والسلاح والاتجار بالبشر إضافة إلى سرقة الملكية الفكرية