

قاموس مصطلحات البيئة الرقمية

Digital Environment lexcon

الإصدار الأول
ديسمبر 2024



نبذة عن قاموس مصطلحات حماية الرقمية للعملية الانتخابية

قاموس مصطلحات حماية الرقمية للعملية الانتخابية هو أداة مهمة أعدتها المفوضية الوطنية العليا للانتخابات وشركاؤها، ويتضمن عدد (46) مصطلحًا أساسيًا يتعلق بحماية المعلومات والعمليات الانتخابية في العصر الرقمي. يهدف هذا القاموس إلى توضيح المفاهيم الأساسية التي تتعلق بالمعلومات المضللة والأمن السيبراني، وحماية البيانات، والتقنيات المستخدمة في العملية الانتخابية، مما يساهم في تعزيز الفهم العام حول كيفية حماية الانتخابات من التهديدات الرقمية.

يعتبر هذا القاموس أداة تعليمية قيمة للجهات المعنية، بما في ذلك الأحزاب السياسية، والكيانات الانتخابية، والمترشحين، بالإضافة إلى وسائل الإعلام ومنظمات المجتمع المدني. من خلال توفير تعريفات واضحة ودقيقة، يساهم القاموس في تعزيز الوعي حول أهمية حماية المعلومات في العملية الانتخابية، مما يساعد على بناء ثقة أكبر في النظام الانتخابي.

كما أن القاموس يعكس الجهود المستمرة للمفوضية الوطنية العليا للانتخابات وشركائها في مواجهة التحديات الرقمية، ويعزز من قدرة المجتمع على التصدي للمخاطر المرتبطة بالانتخابات في العصر الرقمي. من خلال فهم المصطلحات الأساسية، يمكن لجميع المعنيين اتخاذ خطوات فعالة لضمان نزاهة الانتخابات وحمايتها من التهديدات.

الإصدار الأول
ديسمبر 2024

1

إغلاق الإنترنت

يشير إلى قطع الاتصالات القائمة على الإنترنت بشكل متعمد عن سكان محددين أو مناطق محددة أو وسائل وصول معينة. قد تقوم الحكومات أو كيانات تعمل نيابة عنها ببعض الإغلاقات لعرقلة الوصول إلى أنظمة المعلومات والاتصالات عبر الإنترنت. يمكن أن تشمل الإغلاقات حظرا كاملاً لاتصال الإنترنت أو قيود مستهدفة على شبكات أو خدمات محددة، مثل وسائل التواصل الاجتماعي أو تطبيقات المراسلة.

Internet Shutdowns

refer to the intentional disruption of internet-based communications for a specific population, location, or mode of access.

Governments or entities acting on their behalf may implement shutdowns to intentionally impede access to online information and communication systems. Shutdowns can involve complete blockages of internet connectivity or targeted restrictions on specific networks or services, such as social media or messaging apps.

2

اختراق البيانات

يشير إلى أي حادث أمني يتمكن من خلاله الأطراف غير المصرح لها من الوصول إلى معلومات حساسة أو سرية، بما في ذلك البيانات الشخصية ويحظر عليها تقييد قدرة الفرد على الاتصال بالإنترنت لأسباب غير معقولة.

Data Breach

refers to any security incident where unauthorized parties gain access to sensitive or confidential information, including personal or and are prohibited from unreasonably limiting an individual's ability to connect to the internet.

3

البيانات الشخصية

تشير إلى أي معلومات تتعلق بشخص حي يمكن تحديده بطريقة مباشرة أو غير مباشرة. وعندما يتم جمع ودمج أجزاء مختلفة من المعلومات التي تؤدي إلى التعرف المحتمل على شخص معين، فإنها مجتمعة تشكل بيانات شخصية لذلك الشخص.

Personal Data

refers to any information that pertains to a living individual who can be identified directly or indirectly. When various pieces of information are gathered and combined, leading to the potential identification of a specific person, they collectively constitute personal data.

4

البصمة البيومترية

هي وسيلة تحقق تعتمد على الخصائص البيولوجية والفريدة للفرد، مثل بصمات الأصابع، قزحية العين، أو ملامح الوجه، لتأكيد الهوية.

Biometric authentication

is a verification method that relies on an individual's unique biological characteristics, such as fingerprints, iris patterns, or facial features, to confirm identity.

5

التعقب السيبراني

ينطوي على استخدام الإنترنت أو وسائل الاتصال الإلكترونية الأخرى لتعقب فرد أو مجموعة أو منظمة.

Cyber Stalking

involves the use of the internet or other electronic means to stalk or harass an individual, group, or organization.

البيانات الشخصية

لتأكد من صحة الحقائق المذكورة في نص مكتوب، مقالة إخبارية، خطاب، إلخ. في منظومة المعلومات الحالية، يتطلب الانتشار المتزايد للمعلومات الكاذبة أو المضللة فحصاً يقطاً ومنهجياً للادعاءات لضمان نشر محتوى دقيق وصحيح. هذا أمر بالغ الأهمية بشكل خاص في العمليات الانتخابية، حيث يكون للمعلومات المضللة والكاذبة تأثير كبير. تلعب مبادرات التحقق من الحقائق دوراً رئيسياً في الحفاظ على سلامة العمليات الديمقراطية، ورفع مستوى وعي الناخبين، وحماية مصداقية مصادر المعلومات.

Personal Data

refers to the process of checking that all the facts in a piece of writing, a news article, a speech, etc., are correct. In today's information landscape, the growing prevalence of false or misleading information requires a vigilant and systematic examination of claims to ensure the dissemination of accurate and truthful content. This is particularly crucial in electoral processes, where the potential impact of dis/misinformation is substantial. Fact-checking initiatives play a key role in upholding the integrity of democratic processes, fostering an informed electorate, and safeguarding the credibility of information sources.

التسويق الماكر

هو إخفاء راعي أو صاحب رسالة أو منظمة ما، كأن تكون سياسية أو دينية، لجعل المحتوى يبدو كما لو أنه نشأ أو دعم من قبل مشاركين حقيقيين. بحيث، من خلال إنشاء واجهة دعم شعبية تبدو حقيقية، تمكّن الكيانات السياسية من أن تخدع الجمهور.

Astroturfing

is the practice of hiding the sponsors of a message or organization, e.g., political, religious, etc., to make it appear as though it originated from and/or is supported by grassroots participants. By creating a façade of genuine grassroots support, political entities can deceive the public.

8

التشهير السيبراني (تشويه السمعة عبر الإنترنت)

هو نشر الافتراءات بشكل غير دقيق أو بشكل مؤذٍ عبر الوسائط الإلكترونية. يمكن أن يتضمن ذلك نشر بيانات كاذبة أو معلومات مدمرة يتم نشرها من خلال القنوات الرقمية، مما يشكل تهديداً للسمعة.

Cyber Libel (Online Defamation)

involves inaccurately, or injuriously written defamation triggered via electronic means. This can include false statements or damaging information disseminated through digital channels, posing reputational risks and legal challenges to individuals or entities.

9

التعلم الآلي

ينطوي على استخدام وتطوير أنظمة الحاسوب القادرة على التعلم والتكيف دون تعليمات صريحة. يتم ذلك من خلال تطبيق خوارزميات ونماذج إحصائية لتحليل البيانات واستخلاص استنتاجات من الأنماط الموجودة في البيانات.

Machine Learning

Involves the use and advancement of computer systems capable of learning and adapting without explicit instructions. This is achieved through the application of algorithms and statistical models to analyze data, drawing inferences from patterns in data.

10

التعقب السيبراني

ينطوي على استخدام الإنترنت أو وسائل الاتصال الإلكترونية الأخرى لتعقب فرد أو مجموعة أو منظمة.

Cyber Stalking

involves the use of the internet or other electronic means to stalk or harass an individual, group, or organization.

11

التحذير المسبق

يشير إلى مواجهة المعلومات الكاذبة المحتملة عن طريق تحذير الناس منها قبل نشرها. وهو أسلوب تتبعه مختلف المؤسسات بما في ذلك شركات التكنولوجيا والمنظمات غير الربحية والجهات الحكومية، لتحصين الأفراد ضد المزاعم الكاذبة حول الانتخابات والصحة العامة ومواضيع حساسة أخرى.

Pre-bunking

refers to the practice of countering potential misinformation by warning people against it before it is disseminated. It is an approach adopted by various entities, including tech companies, non-profit, and government agencies, to inoculate individuals against false claims about elections, public health, and other sensitive topics.

12

التصيد عبر الإنترنت

من خلال الردود المزجة على المحتوى أو التعليقات عبر الإنترنت بهدف تشتيت الانتباه. يتسبب هذا السلوك في تحويل الانتباه بعيداً عن القضايا الجوهرية، مما يخلق بيئة على الإنترنت فوضوية تعيق الحوار البناء والمشاركة.

Trolling

is characterized by disruptive responses to online content or comments. This behavior, diverting attention away from substantive issues, potentially creates a chaotic online environment hindering constructive discourse and engagement.

13

التلاعب بوسائل الإعلام

هو ممارسة متعددة الجوانب تنطوي على صياغة استراتيجية الروايات من قبل الأطراف المعنية، باستخدام تقنيات مثل المغالطات المنطقية والتلاعب والخداع الصريح. يمتد التلاعب في كثير من الأحيان إلى كبت المعلومات أو وجهات النظر

13

المعارضة، أو تحويل الانتباه، أو تسبب الانسحاب، وكل ذلك يمكن أن يؤثر على الرأي العام ويؤثر على الديناميكيات السلوكية. تشمل أنشطة التلاعب بوسائل الإعلام نشر الأخبار الزائفة، بما في ذلك الأخبار الزائفة المبنية على النوع الاجتماعي، والمعلومات السيئة، والمعلومات الخاطئة.

Media Manipulation

is a multifaceted practice that involves the strategic crafting of narratives by partisans, employing techniques such as logical fallacies, manipulation, and outright deception. The manipulation often extends to suppressing opposing information or viewpoints, diverting attention, or inducing disengagement, all of which can shape public opinion and impact behavioural dynamics. Media manipulation activities include disinformation, including gender-based disinformation, mal-information, and misinformation.

14

التدخل الأجنبي والتلاعب في المعلومات

يشمل سلوكاً، غالباً غير قانوني، ويشكل تهديداً للقيم الأساسية أو له القدرة على التأثير سلباً على الإجراءات المستقرة والعمليات السياسية. يتضمن هذا السلوك التلاعب المتعمد والمنسق، ويشمل الممثلين الحكوميين أو غير الحكوميين داخل وخارج حدودهم.

Foreign Information Manipulation and Interference (FIMI)

encompasses predominantly non-illegal conduct that poses a threat to, or has the potential to adversely affect, fundamental values, established procedures, and political processes. This manipulative behaviour is intentional and coordinated, involving actors who may be either state or non-state entities, along with their proxies within and beyond their borders.

15

التدخل الأجنبي والتلاعب في المعلومات

هو استخدام الشخص هوية غير هويته الحقيقية لأغراض خبيثة. تمتد هذه الممارسة إلى ما هو أبعد من الدوافع المالية لتشمل أعمالاً خبيثة تستهدف التحرش والتهديد والتخويف للضحايا.

Foreign Information Manipulation and Interference (FIMI)

encompasses predominantly non-illegal conduct that poses a threat to, or has the potential to adversely affect, fundamental values, established procedures, and political processes. This manipulative behaviour is intentional and coordinated, involving actors who may be either state or non- state entities, along with their proxies within and beyond their borders.

16

التضليل

هو نشر متعمد ومخفي المعلومات الكاذبة، بما في ذلك بث الشائعات، بهدف التأثير على ال أري العام أو تشويش الحقيقة. في سياق العمليات الانتخابية، يمكن أن تشير حملات التضليل/ نشر المعلومات الكاذبة الشك وتخلق الارتباك، وتهدد بشكل محتمل شرعية الانتخابات.

Disinformation

is the intentional and covert spread of false information, including the planting of rumours, with the aim of influencing public opinion or obscuring the truth. In the context of electoral processes, disinformation campaigns can sow doubt, create confusion, and potentially undermine the legitimacy of elections.

17

التحذير المسبق

يشير إلى مواجهة المعلومات الكاذبة المحتملة عن طريق تحذير الناس منها قبل نشرها. وهو أسلوب تتبعه مختلف المؤسسات بما في ذلك شركات التكنولوجيا والمنظمات غير الربحية والجهات الحكومية، لتحصين الأفراد ضد المزاعم الكاذبة حول الانتخابات والصحة العامة ومواضيع حساسة أخرى.

Pre-bunking

refers to the practice of countering potential misinformation by warning people against it before it is disseminated. It is an approach adopted by various entities, including tech companies, non-profit, and government agencies, to inoculate individuals against false claims about elections, public health, and other sensitive topics.

18

التزييف العميق

تشير إلى صورة أو تسجيل تم تعديله والتلاعب به بشكل مقنع لتشويه صورة شخص ما وتصويره وكأنه يفعل أو يقول شيئاً لم يفعله أو ولم يقله أصلاً. يكتسب التعريف أهمية متزايدة، خاصة في الساحة الانتخابية، حيث تمتد آثار التلاعب المتطورة إلى ما هو أبعد من مجرد نشر معلومات مضللة.

Deep Fake

refers to an image or a recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said. The definition gains heightened relevance.

19

التمييز الرقمي

يشير إلى نوع من التمييز يتم فيه اتخاذ قرارات آلية من قبل الخوارزميات، تعتمد بشكل متزايد على تقنيات الذكاء الاصطناعي مثل التعلم الآلي، وتعامل بشكل غير عادل أو غير أخلاقي أو مختلف مع المستخدمين عبر الإنترنت استناداً إلى بياناتهم الشخصية، مثل الدخل والتعليم والجنس والعمر والعرق والدين.

19

Digital Discrimination

refers to a form of discrimination in which automated decisions taken by algorithms, increasingly based on AI techniques like Machine Learning, treat online users unfairly, unethically, or just differently based on their personal data, such as income, education, gender, age, ethnicity, religion.

20

الحقوق الرقمية

هي حقوق شرعية وقانونية تسمح للأفراد بالوصول إلى واستخدام وإنشاء ونشر الوسائط الرقمية أو الوصول واستخدام الحواسيب والأجهزة الإلكترونية الأخرى وشبكات الاتصالات. تتعلق الحقوق الرقمية بحماية وأداء الحقوق القائمة 'غير الرقمية' مثل حق الخصوصية وحرية التعبير، في سياق التقنيات الرقمية، وخاصة الإنترنت.

Digital Rights

are human and legal rights allowing individuals to access, use, create and publish digital media or to access and use computers, other electronic devices, and telecommunication networks. Digital rights relate to the protection and realization of existing 'offline' rights, such as the right to privacy and freedom of expression, in the context of digital technologies, especially the internet.

21

الخوارزمية

تطبق على وسائل التواصل الاجتماعي وتشير إلى مجموعة من القواعد والتعليمات الرياضية التي تقوم بفرز وتصنيف وتركيز المحتوى المتاح على المنصة للمستخدمين استناداً إلى احتمالية إعجابهم به والتفاعل معه. ومن الممكن لأنظمة التزكية الخوارزمية، والتي صممت لاقتراح محتوى جديد يتناسب مع ما يفضله الشخص، أن تكون قنوات لنشر المعلومات الكاذبة. ويمكن لآليات الفرز والتصنيف المنهجية إعطاء الأولوية للمحتوى المضلل أو الحساس، على الرغم من أنها تستهدف تعزيز مشاركة المستخدم، ولو بشكل غير مقصود، مما يضخم الروايات الضارة والكاذبة.

21

Digital Rights

applied to the field of social media, indicate a mathematical set of rules and instructions that systematically sorts, filters, and recommends platform content for users based on how likely they are to like and interact with. Algorithmic recommender systems, designed to suggest new content tailored to individual preferences, can become conduits for disinformation. The systematic sorting and filtering mechanisms, while aimed at enhancing user engagement, may inadvertently prioritize sensational or misleading content amplifying false and harmful narratives.

22

الحكومة الإلكترونية

هي استخدام وكالات الحكومة لتقنيات المعلومات (مثل الشبكات الواسعة النطاق و الإنترنت والحوسبة المتنقلة) التي يمكن أن تغير العلاقات مع المواطنين والأعمال وفروع الحكومة الأخرى. يمكن أن تخدم تلك التقنيات مجموعة متنوعة من الأغراض المختلفة: تحسين تقديم الخدمات الحكومية للمواطنين، وتحسين التفاعل مع الأعمال والصناعة، وتمكين المواطنين من الوصول إلى المعلومات، أو إدارة الحكومة بشكل أكثر كفاءة. يمكن أن تشمل الفوائد الناتجة عن ذلك الأمر تقليل الفساد، وزيادة الشفافية وزيادة الراحة ونمو الإيرادات و/أو تقليل التكاليف.

E-Government

is the use by government agencies of information technologies (such as Wide Area Networks, the internet, and mobile computing) that can transform relations with citizens, business, and other branches of government. Such technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can include less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions.

الذكاء الاصطناعي (AI)

ذروة التقدم التكنولوجي، حيث يوفر للكمبيوترات والروبوتات القدرة على تقليد المهام المرتبطة بالكائنات الذكية. تتجاوز قدرات الذكاء الاصطناعي القدرات الإلكترونية التقليدية، وتشمل حل المشكلات المعقدة والتعلم. هنالك تزايد في استخدام التكنولوجيا المتقدمة للذكاء الاصطناعي نشر المعلومات الكاذبة بشكل متعمد، مما يسرع بشكل كبير من انتشار وتضخيم السرد الرقمي في كل مرحلة من مراحل العمليات الانتخابية، بدءاً من قبل الانتخابات وخلالها وبعدها، مما يبرز التهديد المتزايد لتأثير الخوارزميات على تشكيل الحوار الرقمي.

Artificial Intelligence (AI)

represents a pinnacle in technological advancement, providing computers and robots with the ability to mimic tasks associated with intelligent beings. AI's cognitive capabilities extend beyond routine automation, encompassing complex problem-solving and learning. Increasingly employed to intentionally spread disinformation, advanced AI technology significantly accelerates the expansion and amplification of online narratives at each stage of the electoral processes, including before, during, and post elections, highlighting the threatening growing impact of algorithms in shaping digital discourse.

العمليات المؤثرة

تشمل جمع المعلومات الاستراتيجي حول الخصوم وانتشار الدعاية للحصول على ميزة تنافسية. في سياق الانتخابات، يمكن أن تتجسد العمليات المؤثرة كجهود متكاملة لتشكيل الرأي العام من خلال نشر المعلومات الكاذبة والدعاية. يشكل الطابع الخبيث للعمليات المؤثرة تهديداً كبيراً على نزاهة العمليات الديمقراطية، حيث يمكن أن تستغل نقاط الضعف وتؤدي إلى زعزعة الثقة وتشويه الخطاب العام

Influence Operations

involve the strategic collection of information about adversaries and the dissemination of propaganda to gain a competitive advantage. In the context of elections, influence operations can manifest as a concerted effort to shape public perception through the strategic

24

deployment of misinformation and propaganda. The insidious nature of influence operations poses a significant threat to the integrity of democratic processes, as they can exploit vulnerabilities, leading to an erosion of trust and distorted public discourse.

25

المجتمع المعلوماتي

يتميز بالمشاركة الاقتصادية والسياسية والثقافية الكبيرة في إنشاء وتوزيع واستهلاك ودمج وتلاعب المعلومات. وبصورة أكثر انتشاراً، يمكن وصفه بأنه مجتمع يتم فيه اعتماد التكنولوجيا المعلوماتية والحاسوبية على نطاق واسع ومتقدم، مما يعكس مستوى عالي من الوعي والكفاءة في استخدامها وفهمها.

Information Society

Information Society is characterized by the significant economic, political, and cultural engagement in the creation, distribution, consumption, integration, and manipulation of information. In more widespread terms, it can be described as a society where there is a widespread and advanced adoption of information and computer technology, reflecting a high level of awareness and proficiency in their use and understanding.

26

البيانات الشخصية

هي قوة خادعة في العالم الرقمي، تم إنشاؤها إما كبرمجيات أو عن طريق مجموعات من الأفراد لمحاكاة أشخاص حقيقيين على منصات التواصل الاجتماعي. الهدف الأساسي لهذه الحسابات هو التلاعب بالمعلومات، وتسميم المحتوى الأصلي وغمر المساحة الافتراضية بالعديد من المنشورات الكاذبة المميزة بوسوم محددة. تهدف هذه الاستراتيجية إلى تقليل تأثير المنشورات الحقيقية، مما يجعل وسائل التواصل الاجتماعي أداة ضعيفة لفهم الأحداث العالمية.

26

Electronic flies

are a deceptive force in the digital realm, designed either as software or by groups of individuals to mimic real people on social media platforms. Their primary objective is to manipulate information, poisoning authentic content and flooding the virtual space with many fake publications marked by specific hashtags. This strategic tactic aims to diminish the impact of genuine posts, turning social media into a weakened tool for understanding global events.

27

المضايقات الإلكترونية

القائمة على النوع الاجتماعي: تشمل المضايقات والتحيزات المستهدفة من خلال التكنولوجيا ضد الأشخاص، وخاصة النساء، استناداً إلى جنسهم.

Online Gender-Based Harassment

involves the targeted harassment and prejudice through technology against people, disproportionately women, based on their gender.

28

المضايقات عبر الإنترنت

قد تتخذ أشكالاً مختلفة، بما في ذلك السلوك المؤذي والمتطفل المستمر، مما يشكل تهديدات كبيرة للسلامة الشخصية والراحة ويزيد عدد المسؤولين الانتخابيين، الذين أوكلت إليهم المسؤولية الحاسمة المتمثلة في ضمان نزاهة العمليات الديمقراطية، الذين أصبحوا أهدافاً لمثل هذه الهجمات.

Online Harassment

can take various forms, including persistent and intrusive behavior, posing significant threats to personal safety and well-being. More and more electoral officials, entrusted with the crucial responsibility of ensuring the integrity of democratic processes, become targets of such attacks.

29

المحتوى المخادع/ المضل

يشمل الممارسة المضللة باستخدام وانتحال شخصية المصادر الحقيقية أو الشخصيات العامة باستخدام العلامات التجارية لمؤسسة ما.

Imposter Content

involves the deceptive practice of impersonating genuine sources, or public personalities, utilizing established agency branding.

30

المعرفة الإعلامية

هي اكتساب القدرة أو المهارة على تحليل المحتوى المنشأ والمستهلك في وسائط مختلفة، بما في ذلك الراديو والتلفزيون والإنترنت ومنصات التواصل الاجتماعي، بغرض تقييم الدقة والمصداقية ووجود أدلة على التحيز. وفي عصر يتسم بانتشار سريع للمعلومات عبر الراديو والتلفزيون والإنترنت ووسائل التواصل الاجتماعي، تمنح المعرفة الإعلامية أصحابها القدرة على تمييز المعلومات الحقيقية من السرديات المضللة. وتصبح المعرفة الإعلامية ضرورية بشكل خاص خلال فترات الانتخابات، حيث يمكن أن يكون لانتشار الأخبار الكاذبة تأثيرات عميقة على المؤسسات الديمقراطية والثقة في مخرجاتها عموماً.

Imposter Content

is the ability or skills to critically analyze for accuracy, credibility, or evidence of bias the content created and consumed in various media, including radio, television, the internet, and social media platforms. In an age marked by the rapid dissemination of information through radio, television, the internet, and social media, media literacy skills empower individuals to discern factual information from misleading narratives. Media literacy becomes particularly crucial during electoral periods, where the spread of disinformation can have profound implications on democratic institutions and public trust.

31

التشهير الرقمي

هو توفير معلومات تحدد هوية الأفراد أو المنظمات علناً، التشهير عبر الإنترنت. يتضمن ذلك الكشف عن العناوين الخاصة وأرقام الهواتف وعناوين البريد الإلكتروني، مما قد يؤدي إلى التعرض للتهديد والتحرش.

Doxing

is the act of publicly providing personally identifiable information about individuals or organizations, usually over the internet. This involves the exposure of private addresses, phone numbers, and emails, potentially leading to threats and harassment.

32

العنف عبر الإنترنت

يشمل استخدام أنظمة الكمبيوتر لإحداث الضرر، بما في ذلك الضرر الجسدي والنفسي والاقتصادي. قد يشمل استغلال ظروف أو صفات أو ضعف فرد ما.

Online Violence

involves computer systems to cause harm, including physical, psychological, or economic suffering. It may include the exploitation of an individual's circumstances, characteristics, or vulnerabilities.

33

القرصنة

مجموعة من الأنشطة التي تهدف إلى اختراق الأجهزة الرقمية والشبكات عبر الإنترنت. وفي إطار العمليات الانتخابية، تشكل عمليات الاختراق تهديداً مباشراً لسرية وأمن بيانات الانتخابات الحساسة، مما يعرض للخطر النتائج ويؤثر في نهاية المطاف على العملية الديمقراطية الشاملة.

Hacking

encompasses a spectrum of activities aimed at compromising digital devices and online networks. Within electoral processes,

33

hacking poses a direct threat to the confidentiality and security of sensitive election data, risking the manipulation of results and ultimately affecting the overall democratic process

34

الأخبار الزائفة

تشير إلى المعلومات الكاذبة التي يتم بثها أو نشرها بشكل متعمد، غالباً لأغراض احتيالية أو سياسية. يمكن للأخبار الزائفة أن تؤثر بشكل كبير على تصور الجمهور، وتؤثر على الاتجاهات والسلوكيات.

Fake News

refer to false information intentionally broadcast or published, often for fraudulent or politically motivated purposes. Fake news can greatly impact public perception, influencing attitudes and behaviour.

35

الإعلان المظلم الموجه

هو نوع من الإعلانات التي تظهر فقط للمعلن والجمهور المستهدف المحدد، وهي تشير تساؤلات خطيرة بشأن الشفافية. تسمح الطبيعة السرية للإعلان المظلم للحملات بتخصيص الرسائل لتناسب شرائح سكانية معينة دون مراقبة عامة أوسع. يصبح هذا النقص في الشفافية مشكلة، خاصة في سياق العمليات الديمقراطية.

Dark Advertising

is a form of advertising that is visible only to the advertiser and the specific target audience, raising serious transparency issues. The clandestine nature of dark advertising allows campaigns to tailor messages to specific demographics without broader public scrutiny. This lack of transparency becomes a problem, especially in the context of democratic processes.

36

الاستهداف الفردي/الجزئي

هي استراتيجية تسويقية تستخدم بيانات المستهلك والبيانات السكانية لتحديد اهتمامات وتفضيلات أفراد محددين أو مجموعات صغيرة لإرسال إعلانات مستهدفة تتوافق مع اهتماماتهم.

Micro-Targeting

is a marketing strategy that uses consumer data and demographics to identify the interests and preferences of specific individuals or small groups to send targeted advertisements that align with their interests.

37

تلوث المعلومات

يشمل تلويث بيئة المعلومات بالمحتوى غير المهم أو المكرر أو ذي القيمة المنخفضة التي يمكن أن تعوق نشر المعرفة الدقيقة، وتجعل من الصعب على المستخدمين الوصول إلى معلومات موثوقة.

Information Pollution

involves the contamination of the information environment with irrelevant, redundant, and low-value content that can hinder the dissemination of accurate knowledge, making it challenging for users to access reliable information

38

تسريب المعلومات

يشير إلى الإفصاح غير المقصود أو المقصود للمعلومات في بيئة غير موثوق بها. في الانتخابات، قد ينطوي تسريب المعلومات على الكشف عن تفاصيل حساسة للجمهور.

Information Leakage

refers to the unintentional or intentional release of information to an

38

untrusted environment. In elections, information leakage may involve the disclosure of sensitive details to the public.

39

تقييد الشبكة

يشير إلى إبطاء سرعة الإنترنت بواسطة موفر خدمة الإنترنت عمداً.

Network Throttling

refers to the intentional slowdown of internet speed by an internet service provider.

40

تعديل المحتوى

يشير إلى الممارسة المنظمة لفحص المحتوى الذي ينشئه المستخدمون عبر الإنترنت لتحديد ملائمته لموقع معين أو فئة معينة أو سياق معين. تتراوح إجراءات تعديل المحتوى من تقليل رؤية المحتوى إلى قمع المحتوى والمستخدم.

Content Moderation

refers to the organized practice of screening user-generated content online to determine its appropriateness for a given site, locality, or jurisdiction. Content moderation actions range from reducing content visibility to content and user suppression.

41

تنقية المحتوى

هو إجراء مصمم لتنظيم ومراقبة الوصول إلى رسائل أو صفحات الويب عبر الإنترنت بهدف منع الوصول إلى المحتوى الضار.

Content Filtering

is a procedure designed to regulate and monitor access to online messages or webpages with the aim of preventing access to harmful content.

42

حماية البيانات

تشمل حماية المعلومات الحساسة من احتمالات الضرر أو فقدان أو التلف. تزداد أهمية حماية البيانات بشكل كبير بسبب الارتفاع غير المسبوق في إنشاء وتخزين البيانات.

Data Protection

involves the safeguarding of sensitive information from potential damage, loss, or corruption. The importance of data protection has grown significantly due to the unprecedented surge in the creation and storage of data.

43

حق الوصول إلى الإنترنت

ويشار إليه أيضاً بحق الوصول إلى الشبكة أو حرية الاتصال، يؤكد أن كل فرد يجب أن يكون لديه القدرة على استخدام الإنترنت لممارسة والاستمتاع بحقوقهم الأساسية كبشر، بما في ذلك حرية التعبير والرأي. وبالتالي، يتعين على الحكومات ضمان توافر الوصول إلى الإنترنت على نطاق واسع.

Right to internet access

also referred as the right to broadband or the freedom to connect, asserts that every individual should have the capability to use the internet to exercise and enjoy their fundamental human rights, including freedom of expression and opinion. As such, governments are obliged to ensure widespread availability of internet access and are prohibited from unreasonably limiting an individual's ability to connect to the internet.

44

خطاب الكراهية عبر الإنترنت

يشير إلى الخطاب المسيء الذي يستهدف مجموعة أو فرداً بناءً على خصائص متأصلة (مثل العرق أو الدين أو الجنس) والذي قد يهدد السلام الاجتماعي. خلال الانتخابات، يمكن أن يخلق خطاب الكراهية عبر الإنترنت بيئة سياسية سامة، مما يقسم الناخبين ويعوق الحوار البناء.

44

Online Hate Speech

refers to offensive discourse targeting a group or an individual based on inherent characteristics (such as race, religion or gender) and that may threaten social peace.. During elections, online hate speech can create a toxic political environment, polarizing voters and hindering constructive discourse.

45

روبوتات الانترنت (البوت)

تشير كلمة "البوت"، المشتقة من مصطلح "الروبوت"، إلى برامج الحاسوب التي تعمل كوكلاء تؤدي مهام للمستخدمين أو البرامج الأخرى وتحاكي النشاط البشري. تلعب الروبوتات دوراً أساسياً في تنفيذ المهام والتفاعلات في المشهد الرقمي. إذا تم استخدامها لأغراض خبيثة، يمكن استخدام الروبوتات لتضخيم الروايات الكاذبة وخطاب الكراهية والدعاية من خلال ما يُعرف باسم "تأثير مكبر الصوت". وينطوي ذلك على النشر السريع للمحتوى على جمهور واسع، والذي يمكن أن يؤثر على السلوك الاجتماعي والمواقف الاجتماعية للمستهدفين. إن قدرة الروبوتات على العمل في شكل مضخمات للروايات الضارة تسلط الضوء على الحاجة إلى المراقبة اليقظة والتدابير المضادة للتخفيف من تأثيرها السلبي على الخطاب الرقمي.

Bots

derived from the term robots, refer to computer programs that function as agents, performing tasks for users or other programs and simulating human activity. Bots play a pivotal role in executing tasks and interactions within the digital landscape. If used for malign purposes, bots can be employed to amplify fake narratives, hate speech, and propaganda through the so-called "megaphone effect." The phenomenon involves the rapid dissemination of content to a wide audience, potentially influencing social behavior and attitudes among those targeted. The ability of bots to serve as amplifiers of harmful narratives underscores the need for vigilant monitoring and countermeasures to mitigate their negative impact on the digital discourse.

هجوم الحرمان من الخدمة الموزعة

هجوم الحرمان من الخدمة هذه محاولة خبيثة لتعطيل التدفق المنتظم أو حركة المرور إلى موزع أو خدمة أو شبكة معينة عن طريق إغراق الهدف أو البنية التحتية المحيطة به بكمية مفرطة من حركة المرور على الإنترنت.

Distributed Denial-of-Service (DDoS)

Attack is a malicious effort to disrupt the regular flow of traffic to a specific server, service, or network by inundating the target or its surrounding infrastructure with an excessive volume of internet traffic.

منهجية تجميع المصطلحات

تم جمع التعريفات من مصادر أكاديمية وتقارير دولية، مع مراعاة الدقة والوضوح، كما تم الاستعانة بمحرركات البحث الأكاديمية مثل Google Scholar و JSTOR للوصول إلى التعريفات المتخصصة. تم تنظيم المصطلحات وتدقيقها لضمان التوافق مع الاستخدامات الحديثة في مجال الإعلام الرقمي والأمن السيبراني.

قاموس مصطلحات البيئة الرقمية

Digital Environment lexicon

الإصدار الأول
ديسمبر 2024

المصادر:

منظمات دولية ومؤسسات بحثية:

- الاتحاد الأوروبي (European Commission): تقارير حول التضليل الإعلامي وحماية الانتخابات (خطة العمل للديمقراطية الأوروبية).
- اليونسكو (UNESCO): أوراق عمل حول أخلاقيات الذكاء الاصطناعي ومكافحة التضليل.
- معهد ستانفورد للذكاء الاصطناعي (Stanford Institute for Human-Centered AI): أبحاث حول تأثير الخوارزميات على المحتوى الرقمي.
- مركز برينان للعدالة (Brennan Center for Justice): دراسات حول التهديدات الإلكترونية للانتخابات.

مصادر متخصصة في الأمن السيبراني:

- وكالة الأمن السيبراني الأوروبية (ENISA): تقارير حول الهجمات الإلكترونية وحماية البيانات.
- شركات الأمن السيبراني مثل سيمانتيك (Symantec) وكاسبرسكي (Kaspersky): تحليلات حول البرمجيات الخبيثة وانتهاكات البيانات.

أدبيات التضليل الإعلامي:

- مشروع التضليل الإعلامي (Disinformation Project): دراسات حول "الروبوتات" و"الحشود الاصطناعية" (Astroturfing).
- مختبر التضليل الأوروبي (EU DisinfoLab): تحقيقات حول الحملات المتضامنة عبر المنصات.

قواميس وقواعد بيانات مصطلحات:

- قاموس أوكسفورد للإنترنت (Oxford Internet Institute): تعريفات مصطلحات مثل "الخوارزميات" و"التنمر الإلكتروني".
- موسوعة قانون البيانات (The Data Governance Legal Encyclopedia): مفاهيم متعلقة بحماية البيانات والخصوصية.

أبحاث أكاديمية:

تم الرجوع إلى دراسات منشورة في مجلات علمية :

- Journal of Cybersecurity
- Harvard Kennedy School Misinformation Review
- Proceedings of the ACM on Human-Computer Interaction
- <https://iris.paho.org/handle/10665.2/26494/search-filter?field=subject&filterorder=COUNT&locale-attribute=pt>
- https://www.hunton.com/images/content/3/2/v2/3209/Editorial_Privacy_Data_Protection_Vol9_Issue6.pdf

ملاحظة هامة :

تم تجميع هذه التعريفات من مصادر متعددة تشمل تقارير رسمية، أبحاث أكاديمية، ومؤسسات متخصصة في الأمن السيبراني والإعلام الرقمي، لضمان الدقة والشمولية. تم الرجوع إلى عدة جهات دولية ومؤسسات بحثية متخصصة، وتم تغيير بعض الصياغة في معظم المصطلحات بما يوافق بيئة تقنية المعلومات في ليبيا ..

