

## ما وراء أفعال الكلام: الممارسة التقنية وحالة الاستثناء في الأمن السيبراني

## كقطاع سادس

*Beyond "Speech Acts": Technical Practice and the State of Exception in Cybersecurity as a Sixth Sector*عبد الرحمان فريجة<sup>\*1</sup>Abderrahmane FRIDJA<sup>1\*</sup><sup>1</sup> جامعة العربي بن مهيدي، أم البواقي، (الجزائر)، abderrahmane.fridja@univ-oeb.dz

تاريخ النشر: 2026/06/11

تاريخ القبول: 2026/05/15

تاريخ الإرسال: 2026/03/19

## ملخص:

ترصد هذه الورقة الفجوة النظرية للإطار الكلاسيكي لمدرسة كوبنهاغن، عند التطبيق على الفضاء السيبراني كقطاع سادس، حيث تنطلق في مسعاها من إشكالية التناقض البنوي بين احتكار الدولة للأمننة والبيئة اللامركزية للشبكات المتميزة بـ معضلة الإسناد والعمى التقني. وبتبني منها نقدياً لتحليل الخطاب مدعوماً بالأدلة التجريبية، تناقش الورقة أن هذا التناقض ينتج فجوة سيادية تنقل سلطة الفاعل المؤمن وفعل الكلام من النخبة السياسية إلى الخبراء والشركات التكنولوجية عبر آليات الأمننة التقنية المفرطة؛ وبوصف انتقال الكيانات المرجعية للحماية نحو البنى التحتية الحيوية والمعلوماتية، نخلص إلى أن خصخصة الأمن القومي عبر المنصات يخضع السيادة الرقمية لمنطق الكيانات التجارية العابرة للحدود.

**الكلمات المفتاحية:** القطاع السيبراني، مدرسة كوبنهاغن، فعل الكلام، الفجوة السيادية، الامننة التقنية، الفاعل المؤمن.

## Abstract:

This paper examines the theoretical gap in the Copenhagen school's framework when applied to cyberspace. It explores the structural contradiction between state-led securitization and decentralized networks defined by the attribution dilemma and technical blindness. By adopting a critical discourse analysis approach supported by empirical evidence, the paper argues that this contradiction produced a sovereignty gap that shifts authority over the speech act from political elites to technical experts and corporations via technical securitization; by tracing the shift of referent objects toward critical infrastructure, the research concludes that privatizing national security via platforms subjects digital sovereignty to the logic of transnational commercial entities.

**Keywords:** Cyber Sector, Copenhagen School, Speech Act, Sovereignty Gap, Technical Securitization, Securitizing Actor.

## 1. مقدمة

شهد حقل الدراسات الأمنية تحولات ابستمولوجية عميقة مع تنامي التوجهات التوسيعية التي قادتها مدرسة كوبنهاغن، عبر عملها التأسيسي "الامن: إطار جديد للتحليل" الذي وسع نطاق التهديدات، ليتجاوز البعد العسكري التقليدي لصالح قطاعات أمنية متعددة. فمع بروز الفضاء السيبراني كواقع شبكي لا مركزي يتجاوز الجغرافيا والحدود السيادية، انتقلت التهديدات الرقمية من نطاق السياسة المنخفضة إلى أعلى مراتب السياسة العليا؛ مؤسسة لما تصفه نازلي شوكري<sup>(1)</sup>، بمجال سياسي جديد تتأكل فيه المركزية الدولية والقوة المادية لصالح تدخل قوى بين الفواعل الحكومية والشركات الخاصة العابرة للحدود.

عن هذا التمييز الانطولوجي للقطاع السيبراني السادس، المحكوم بقواعد هانسن ونيسنباوم (Hansen and Nissenbaum)<sup>(2)</sup> للأمننة المفرطة والتقننة، أصبح الواقع يفرض ضرورة إعادة تقييم الآليات التقليدية لبناء التهديد في ظل انعدام أمن وجودي متأصل داخل النظم المعلوماتية، وهو ما يجعل من استقلال هذا القطاع ضرورة ابستمولوجية لفهم تحولات القوة في العصر الرقمي. وتكمن إشكالية هذه الورقة البحثية في رصد الفجوة النظرية التي

تواجهها مدرسة كوبنهاغن عند تطبيقها على بيئة سيربانية تتسم بـ "معضلة الإسناد" و"التعقيد الخوارزمي"؛ حيث يصطدم مفهوم الفاعل المؤمن التقليدي بما يسمى "العمى التقني" لدى النخب السياسية أيضا، مما يعجزها وفقا لمiriam دان كافلتي<sup>(3)</sup> عن صياغة فعل كلام (speech act) مقنع للجمهور دون الاعتماد البنيوي على الوسطاء التقنيين؛ لتتبلور إشكالية هذه الدراسة في التناقض البنيوي بين الإطار التحليلي الكلاسيكي لنظرية الأمانة ومقتضيات الفضاء السيرباني، والتي يمكن صياغتها كالتالي:

إلى أي مدى تعيق البنية اللامركزية والتقنية للفضاء السيرباني تطبيق الآليات الكلاسيكية لمدرسة كوبنهاغن؟ وكيف يعيد هذا الفضاء تشكيل هوية الفاعل المؤمن وآلية فعل الكلام وطبيعة الكيان المرجعي في ظل انتقال سلطة تحديد التهديدات من النخب السياسية إلى الفواعل التكنولوجية الخاصة والخوارزميات؟

وتتطلب الدراسة من فرضية أن الاستقلالية الأنطولوجية للفضاء السيرباني، تخلق فجوة سيادية بنيوية، تؤدي إلى نقل سلطة الأمانة (الفاعل المؤمن وفعل الكلام) من احتكار الدولة لصالح الخبراء التقنيين والشركات التكنولوجية الكبرى (big tech)؛ وقد ينتج عن ذلك إحلال الأمانة التقنية محل المداولات السياسية، مما يعيد تعريف الأمن القومي وفق منطق استمرارية الأعمال، ليفضي إلى إعادة تموضع الكيان المرجعي للحماية من الأفراد إلى النظم التقنية والبنى التحتية المادية للدولة والمجتمع.

ولمعالجة هذه الإشكالية، تتبنى الدراسة منهجا نقديا لتحليل الخطاب يركز على تفكيك مفاهيم الأمانة والطروحات النظرية التوسيعية مدعومة بأدلة إمبيريقية وحالات دراسية واقعية لتعميق الحجج وتجسيد المفاهيم المجردة. ومن خلال هذه المنهجية تنتظم خطة البحث في أربعة محاور: يبدأ الأول بتأصيل القطاع السادس وفجوات مدرسة كوبنهاغن مستشهدا بمعضلة الإسناد، ثم نعالج في الثاني بروز الشركات التكنولوجية كفواعل أمنية بديلة؛ فيما

نفكك في الثالث آليات الأمنة التقنية وتحول الكيان المرجعي نحو البنى التحتية الحيوية؛ وأخيرا نبرز تداعيات استقلالية قطاع الأمن السيبراني على الأمن القومي.

## 2. القطاع السادس المستقل: تأصيل المفهوم وديناميات القوة

يستوجب الفهم الدقيق للتهديدات في البيئة الرقمية الإقرار بعجز القوالب الأمنية الكلاسيكية عن استيعاب تعقيدات البنية التحتية للمعلومات، حيث يهدف هذا المحور إلى تأصيل الأمن السيبراني كقطاع سادس متمايز (Distinct Sector)، تسيره ديناميات قوة شبكية وتتخلله معضلات هيكلية أبرزها معضلة الاسناد التي تعطل آليات الردع التقليدية وتكشف عن فجوة جوهرية في آلية الأمنة ذاتها.

### 1.2 الطبيعة الأنطولوجية للقطاع السيبراني السادس:

يتأسس الفهم النقدي للأمن السيبراني كقطاع أمني مستقل على تجاوزه لرفض مدرسة كوبنهاغن لتنظيره كقطاع منفرد عبر عملها التأسيسي، الأمن: إطار جديد للتحليل، (4) وخلافا للقطاعات المادية الكلاسيكية التي طورها باري بوزان وآخرون، يتميز هذا الفضاء السيبراني بوجود انعدام أمن وجودي متأصل داخل أنظمة الكمبيوتر والمعلومات، وهو ناتج عن الإخفاقات التقنية غير المتوقعة وليس الفواعل المتعمدين فحسب. ووفقا لـ هانسن ونيسنباوم، الفضاء السيبراني بفعل بنيته التحتية عالمية التصميم والتطوير، تبلور واقع شبكي لا مركزي يتجاوز الجغرافيا والحدود السيادية من خلال تدفقات عابرة للحدود وإمكانية عمل المهاجمين على مسافة تشويش هوياتهم ومواقعهم ومسارات دخولهم. (5)

ويعد فيروس ستوكسنت (STUXNET) الذي استهدف منشأة "ناتانز" النووية الإيرانية عام 2010، تجسيدا تجريبيا لمناقشة فكرة الاستقلالية الأنطولوجية، فقد صممت هذه البرمجية لتعمل باستقلالية تامة عن مشغليها داخل شبكات معزولة عن الانترنت (air-gapped)، (6) حيث دمجت كافة الوظائف اللازمة للتخريب والتحكم مباشرة ضمن ملفها

التفنيدي للدودة دون الحاجة لأي مدخلات إضافية من المهاجم. ونتيجة لذلك نجح الكيان التقني المستقل في أحداث تدمير مادي فعلي اتلف نحو 1000 طارد مركزي<sup>(7)</sup> ليبرهن هذا النموذج أن التهديد في القطاع السيبراني قادر على التبلور ككيان تقني مستقل، تنتج عنه تأثيرات تدميرية مادية تعادل في جوهرها الهجمات الحركية للجيش النظامية.

ونتيجة لهذا البناء الشبكي اللامركزي المتميز، انتقلت قضايا الفضاء السيبراني من نطاق السياسة المنخفضة إلى مراتب السياسة العليا. كما توضح نازلي شوكري في تحليلها لتأثير السيبراني على السيادة الإقليمية، نشأ مجال سياسي جديد تتداخل فيه الفواعل ما دون الدولة مع الفواعل الحكومية، فأصبح هذا الفضاء متنازعا عليه بشدة ومعاد تشكيله من قبل الحكومات والجيش والشبكات الخاصة. وبهذا التداخل الوثيق تشكل تحدي للنظرية التقليدية التي تركز بشكل أساسي على المركزية الدولية والقوة المادية المرتبطة بالإقليمية. لتسقط بذلك فكرة احتكار مفهوم للقوة المادية المهيمنة على تنظيم الأمن التقليدي؛<sup>(8)</sup>

يتقاطع هذا الطرح تقاطعا واضحا مع إطار مدرسة كوبنهاغن. الأمر الذي يفرض دراسة الأمن السيبراني بدinاميات قوته المتباينة كقطاع مستقل يمتلك قواعد أمنية -الأمننة المفرطة، ممارسات الأمن اليومية، التقنية- لا تتناسب مع قوالب الأمن التقليدي.<sup>(9)</sup>

## 2.2 معضلة الإسناد كفاصل بنيوي عن القطاعات الكلاسيكية:

إضافة إلى هذه الهندسة اللامركزية، تتجذر معضلة الاسناد كعائق بنيوي أساسي يكرس استقلالية الفضاء السيبراني ويفصله عن المنطق العسكري الكلاسيكي؛ ففي الحروب التقليدية يعرض الجنود في الجيوش النظامية هويتهم علنا، مما يجعل هوية المهاجم ومصدر التهديد مرئيين، أما في الفضاء السيبراني فتتيح بنيته استخدام خوادم وسيطة، فيبقى الهجوم مجهولا وبدون دعم سياسي. وبالتالي يصبح ربط الهجوم بفاعل سياسي أمرا محفوفا بالشكوك ومفتقرا إلى اليقين المادي، وهو ما يجعل الاسناد غير المؤكد أسهل تحقيقا من الإسناد

المحكم أو اليقيني المطلق (waterproof attribution)، حيث يكون للمهاجمين سواء بالتخريب أو التجسس مصلحة دائمة أو مؤقتة في تجنب الاسناد، فتصبح الجريمة السياسية أكثر ازدهارا من أعمال الحرب في هذا المجال.<sup>(10)</sup>

ويظهر ذلك بوضوح في هجمات إستونيا عام 2007، التي استمرت لثلاثة أسابيع وتطورت لتشمل توظيف شبكات (botnets) لشن هجمات حجب الخدمة (DDoS) عبر 85,000 حاسوب مخترق. فعلى الرغم من اتهام المسؤولين الإستونيين للكرملين، فقد عجزوا عن تقديم أدلة مادية تحدد مصدر الهجوم مما أدى على سحب التصريحات، كما فشل خبراء حلف الناتو والمفوضية الأوروبية من رصد أي بصمات روسية. وقد لخص توماس ريد كل ذلك في عبارة بقيت الإشارات مجهولة وبدون دعم سياسي، وهذا يجسد كيف أن بنية الفضاء السيبراني عبر استخدام حواسيب وسيطة تجعل عملية إسناد الهجوم لفاعل سياسي محفوفة بالشكوك وتفتقر لليقين المادي.<sup>(11)</sup>

هذا الغموض المنهجي الناجم عن عدم قابلية الهجوم للتنبؤ وعدم اكتشافه، لا يعطل فقط آليات الردع فحسب، بل يحول التهديد السيبراني إلى مصدر للفوضى والاضطراب السياسي والاستراتيجي الدائم، مما يجبر على الدول اللجوء إلى معالجات أمنية تتجاوز الردع العسكري التقليدي، وتعتمد على تدابير دفاعية سلبية مثل تعزيز المرونة والتكرار لامتصاص الضربات وتعزيز الصمود التكنولوجي أمام تفوق الهجوم في هذا المجال.<sup>(12)</sup>

### 3.2 الفجوة النظرية: مأزق تطبيق الأمنة في قطاع لامركزي:

إن الاعتراف بأن الأمن السيبراني يشكل قطاعا متمائزا مرتبطا بالمشكلات اليومية والممارسات التقنية والمدنية،<sup>(13)</sup> يلقي ضوءا نقديا جديدا على المناقشات المعاصرة لنظرية الأمنة، إذ يعد حالة الأمن السيبراني درسا أبرز في إطار مدرسة كوبنهاغن؛<sup>(14)</sup> ففي حين تفترض النظرية الكلاسيكية فاعلا مؤمنا يمتلك الشرعية السياسية التقليدية، عادة الحكومة أو

القادة السياسيين للقيام بخطاب أمانة،<sup>(15)</sup> يكشف القطاع السيبراني عن دور مميز يمنح لعلماء الحاسوب والمعلوماتية من خلال أو عبر التقنية،<sup>(16)</sup> ليؤدي إلى تشكيل سلطة معرفية وسياسية خاصة وحركة مزدوجة خارج المجال السياسي من الميسر إلى المؤمن ومن السياسي إلى التقني.<sup>(17)</sup> وهذا التمايز يكشف عن فجوة عميقة في الإطار التحليلي الكلاسيكي لآلية الأمانة ذاتها.

غير أن تطبيق هذه الآلية الخطابية والسياسية يبدو مأزوما في بيئة لا مركزية كالفضاء السيبراني، حيث تصطدم سلطة النخبة السياسية بجهل منهجي وافتقار للخبرة التقنية الدقيقة اللازمة لفهم طبيعة التهديدات غير المادية، مما يجعلها عاجزة عن صياغة فعل الكلام مقنع دون الاعتماد على وسطاء تقنيين؛<sup>(18)</sup> وبالتالي ينتقل الثقل الفعلي للسلطة من الفاعل السياسي التقليدي إلى الخبراء التقنيين كفواعل أساسية في تحديد التهديدات.

وتتجسد المعضلة النظرية في تناقض جوهري، فبينما تركز مدرسة كوبنهاغن على أفعال الكلام السياسية من قبل فاعلين (الفاعل المؤمن) في موقف يسمح لهم بتحديد التهديد، يفرض منطق التقنية (technification) -المهيمن حاليا على الخطاب الأمني السيبراني- واقعا يصبح فيه الاعتماد على المعرفة التقنية هو العنصر الحاكم. بهذا يمنح الخبراء التقنيون شرعية أساسية تنتج تأثيرا مزيلا للطابع السياسي (depoliticizing)، يجعل المناقشة الديمقراطية بالغة الصعوبة. وهذا يتطلب إعادة تقييم جذرية لهوية الفاعلين الرئيسيين (الفاعل المؤمن) في بناء ومعالجة التهديدات الأمنية (طبيعة سلطة إعلان التهديد).<sup>(19)</sup>

### 3. أزمة الفاعل المؤمن وانتقال سلطة فعل الكلام

يحدث التناقض بين الطبيعة الإقليمية لسيادة الدولة والبنية العابرة للحدود للشبكات تقويزا مباشرا لاحتكار الدولة لممارسة السلطة الأمنية، وعليه نبحت في التفكك التدريجي

"للفاعل المؤمن"، لنبين كيف يؤدي العمى التقني للدولة إلى نشوء فجوة سيادية تملؤها الشركات التكنولوجية كجهات تمارس فعل الكلام نيابة عن المؤسسات السياسية المنتخبة.

### 1.3 تآكل الاحتكار السيادي للأمن وبروز الفجوة السيادية

تتجلى الأزمة العميقة في النهج التقليدي في التوتر الشديد والمستمر بين سيادة الدولة المقتصرة على الحدود الإقليمية والفضاء غير الإقليمي للتفاعل الاجتماعي الذي تخلقه الحواسيب الشبكية؛ ففي الفضاء السيبراني تصطدم هيكلية الدولة الهرمية بهيكلية الشبكة المرنة، فتتوزع المشاركة والسلطة ويجعل وحدات اتخاذ القرار غير مرتبطة بالوحدات السياسية، وينتج عن ذلك مؤسسات جديدة خارج نظام الدولة القومية، وهذا يضع ضغوطاً على الترتيبات المؤسسية المركزة حول الدولة في سياسات الاتصالات والمعلومات. (20)

ويمتد هذا التآكل السيادي والهيكلية ليطال الإطار النظري الأمني ذاته، حيث، تتجلى الأزمة العميقة لمدرسة كوبنهاغن عند تطبيقها على القطاع السيبراني السادس في التفكير التدريجي لمفهوم الفاعل المؤمن (securitizing actor)؛ فبينما تحتفظ الدولة ومؤسساتها السياسية باحتكار شبه حصري لسلطة إعلان التهديد الوجودي في القطاعات الخمسة، يتآكل هذا الاحتكار بشدة في الفضاء السيبراني، حيث يمتلك القطاع الخاص الجزء الأعظم من البنية التحتية، فيفتح ذلك لتعدد الفاعلين ويضع ضغوطاً جوهرية على النموذج التقليدي. (21)

يؤدي هذا التناقض البنوي الناجم عن قوى التغيير التكنولوجي إلى ما يعرف بـ "الفجوة السيادية" (Sovereignty Gap) في الفضاء السيبراني، حيث لم يعد بإمكان القطاع الخاص أن يأخذ على محمل الجد قدرة الحكومة على حمايته ضد جميع التهديدات ذات الصلة؛ وهذا يجعل تحدي الأمن السيبراني في جوهره مسألة دفاع مدني تقتضي تجهيز القطاع الخاص لحماية أرضيته الحاسوبية. (22)

وتتمظهر الفجوة السيادية في عملية مايكروسوفت في أكتوبر 2020 لتفكيك شبكة (TRICKBOT)؛ حيث استبقت الانتخابات الأمريكية بأمر قضائي مدني ( Preliminary Injunction) أتاح تعطيل عناوين خوادم القيادة والسيطرة (IP).<sup>(23)</sup> وبموجب ذلك مارست مايكروسوفت دورا يشبه صاحب السيادة في حماية الفضاء الوطني بمعزل عن التنسيق المباشر مع القيادة السيبرانية الأمريكية. ويرى لوبين ومارينوتي أن الواقعة تكرر تفوق القطاع الخاص في توظيف الإغاثة القضائية، بامتلاك الشركات ترسانة قانونية تتجاوز الصلاحيات المتاحة للإدعاء العام الفيدرالي بموجب القانون الحالي.<sup>(24)</sup>

### 2.3 العمى التقني واعتماد الدولة البنيوي على القطاع الخاص:

يمكن ارجاع هذا التآكل إلى عملية التقنية التي تميز قطاع الأمن السيبراني، حيث يصبح فهم طبيعة التهديد وصياغة الخطاب الأمني مرهونا بمعرفة تقنية معقدة لا تتوافر لدى الجمهور العام أو النخبة السياسية؛ فبينما يستلزم فعل الكلام وفق إطار مدرسة كوبنهاغن إبراز التهديد بصورة وجودية قابلة للفهم حتى يصبح مقنعا للجمهور، تحول الطبيعة الفورية للتهديدات السيبرانية دون قدرة المؤسسات السياسية التقليدية على امتلاك الإدراك المباشر ما نسميه بالعمى التقني. ويؤدي هذا التفاوت المعرفي إلى فرض اعتماد بنيوي على القطاع الخاص الذي يعد الأكثر جاهزية وهيكله للاستجابة. ونتيجة لذلك تفقد النخبة السياسية تدريجيا قدرتها على المبادرة في عملية الأمانة، فتصبح القضية معتمدة على الخبرة التقنية التي تقدم نفسها كمجال محايد سياسيا وغير قابل للنقاش السياسي.<sup>(25)</sup>

ويتكرس مفهوم الفجوة السيادية في حالة الدولة التي تعاني من عمى تقني وتجد في نفس الوقت نفسها في حالة المشاهد لعملية أمانة تدار بكارر بشري من خارج أجهزتها الرسمية من طرف القطاع الخاص، عند فحص هجوم (WannaCry) عام 2017 هشاشة مؤسساتية عميقة إزاء التهديدات السيبرانية، حيث بينت هيئة الصحة الوطنية البريطانية

(NHS) عجز الخطط النظرية في ظل غياب الرقابة الفعلية. وهو ما أكدته تقرير مكتب التدقيق الوطني بشأن افتقار الجهات المعنية لأدوات قياس الامتثال للتحذيرات الأمنية المسبقة، والمفارقة الجوهرية أن هذا الفيروس تسبب في اضطراب حوالي (34%) من هيئات الرعاية الصحية (NHS Trusts) والغاء آلاف المواعيد الطبية. ورغم اعلان حالة الطوارئ، لم تفلح خطط الاستجابة المؤسسية المركزية في إيقاف انتشاره.<sup>(26)</sup> ولكن تحقق الاحتواء الفعلي بتدخل فردي من باحث تقني مستقل اكتشف وفعل آلية مفتاح الإيقاف (Kill-Switch).<sup>(27)</sup> ولولا هذا التدخل لتضاعف الشلل الرقمي، ومن ثم يطرح هذا المشهد تساؤلات جوهرية حول خطورة ارتهان أمن البنى التحتية الحيوية لجهود تقنية خارج اسوار المؤسسات السيادية.

### 2.3 الشركات التكنولوجية الكبرى (big tech) كفاعل مؤمن بديل؟

في سياق الفجوات السيادية، تبرز الجهات الفاعلة التكنولوجية الكبرى مثل مايكروسوفت بفريق (MSTIC) سابقا، وغوغل (مانديانت وفريق threat analysis group)، وبالو ألتو نتوركس (بفريق 24 unit)، وميتا بفريق (Adversarial Threat Division)؛ كحامي سلطة خاصة بديلة تمارس اشكالا مؤسسية من السلطة المعرفية والتقنية،<sup>(28)</sup> حيث لا تقتصر هذه الشركات على توفير البنية التحتية بل تمارس وظائف شبه سيادية من خلال استغلال حضورها العالمي في البرمجيات والأجهزة لتصبح مصادر موثوقة ضد الأنشطة الخبيثة والثغرات التي ترصدها عبر شبكاتها.<sup>(29)</sup> فقد أصبحت تقارير هذه الشركات مصدرا رئيسية للمعلومات الأمنية، مما يمثل خصخصة للأمن ونقله تنزع سلطة تحديد التهديدات الأمنية الوطنية من المؤسسات الحكومية إلى فرق التحليل الرقمي الخاصة العابرة للحدود.<sup>(30)</sup> لتبرز الشركات التكنولوجية كفاعل بديلة لأمنه القضايا الأمنية السيبرانية من خلال قدراتها على رؤية التهديدات ضمن الشبكات المعلوماتية العالمية.

تشكل الممارسات العملية لهذه الشركات تطبيقا تقنيا مباشرا لـ فعل الكلام. ويتجلى ذلك بوضوح في الاسناد العلني (Public Attribution) للهجمات السيبرانية؛ حيث تنشر شركات الأمن السيبراني تقارير علنية مفصلة تفكك شفرات الهجوم وتسندها تقنيا إلى مجموعات تهديد متقدمة ومستمرة (APTs) قبل الإعلانات الرسمية، مثل مجموعتي (APT28) و (APT29).<sup>(31)</sup> كما يوضح توماس ريد وبوشانان (Rid and Buchanan) فإن الإسناد العلني يعد فعل أمنة مكتمل الأركان؛ يسمى التهديد بوضوح ويحدد مصدره ويقنع الجمهور بخطورته، مما يجعله تدخلا مؤثرا ومباشرا في السياسة الأمنية العليا.<sup>(32)</sup>

المثال الأبرز لهذا التحول لتمثيل آليات التنازع حول الاسناد ضمن بيئة معلوماتية شديدة التسييس، توضح في حادثة اختراق شبكات اللجنة الوطنية الديمقراطية الامريكية (DNC) عام 2016؛ ووفقا لـ فلوريان إيغلوف توجه الحكومة ووكالات الاستخبارات لم تبدأ بالاستجابة، ولكنها استدعت شركة (Crowdstrike) الخاصة في أبريل من العام ذاته لاحتواء الاختراق وتكشف تغلغل مجموعتين، وإسناد هذه الاختراقات السيبرانية لمجموعتي التجسس الروسية (APT28/APT29) والمعروفة بـ (cozy bear) و (fancy bear). وهي استنتاجات أكدتها كيانات أمنية أخرى (من بينها Fidelis-ThreatConnect-SecureWorks-Mandiant). وأتاح التأخر الحكومي لمخاوف سياسية ظهور (Guccifer 2.0) المشكك في الإسناد، فاضطرت الحكومة لاحقا إلى بذل جهود لاستعادة مصداقية روايتها الرسمية بما في ذلك تعيين مستشار خاص وإصدار لوائح اتهام مفصلة ضد النشاط الروسي.<sup>(33)</sup>

من المثال السابق، يبرز أن سلطة هذه الشركات تتجاوز مجرد إعلان التهديد إلى ممارسة نوع خاص من "فعل كلام تقني" يعلن حالة الطوارئ تقنية، ويشرعن تنفيذ إجراءات استثنائية بعيدا عن النقاش الديمقراطي أو تفويض سياسي كلاسيكي، لتؤكد "ميريام دان كافلتي وفلوريان إيغلوف" أن سلطة فعل الكلام في القطاع السيبراني السادس، قد خضعت

لعملية خصخصة فعلية من خلال الجهات الفاعلة خارج الحكومة مما يستدعي مراجعة نقدية صارمة لأدوات مدرسة كوبنهاغن التقليدية التي تركز على الفاعل الواحد القوي.<sup>(34)</sup>

#### 4. الأمنة الخوارزمية والكيان المرجعي اللامركزي

تتجاوز تحولات الفضاء السيبراني مسألة الفواعل لتشمل الأدوات ومواضيع الحماية؛ وهذا أساس هذا المحور الذي يسلط الضوء على التحول العميق من الخطاب السياسي اللغوي إلى الخطاب التقني المؤتمت (الأمنة الخوارزمية أو التقنية)، لنوضح من خلالها كيف انتقل الكيان المرجعي المراد حمايته من الفرد والدولة الإقليمية إلى البنى التحتية للمعلومات وأنظمة الامداد الحيوية للدولة والمجتمع.

##### 1.4 من الخطاب السياسي إلى الخطاب التقني والأمنة الخوارزمية:

يبرز ميهاي أولتيانو، أن انتقال سلطة تحديد التهديدات للفواعل التكنولوجية الخاصة آثار تحولا جوهريا في فعل الكلام والكيان المرجعي؛ ففي القطاعات الكلاسيكية يظل فعل الكلام خطابا سياسيا علنيا؛ أما في القطاع السيبراني تصبح الكيانات المرجعية أصولا تقنية (أنظمة SCADA)، ويصبح فعل الكلام مرتبطا بالطبيعة التقنية للثغرات. ويتجسد ذلك في تقارير شركات مثل (MICROSOFT)، القائمة على تحليل الضعف التقني، لتجعل عملية الأمنة أقل اعتمادا على الخطاب العام التقليدي وأكثر ارتباطا بالخبراء التقنيين.<sup>(35)</sup>

وينجم عن هذا التحول الجذري بروز ظاهرة يمكن قراءتها نقديا من منظور الأمنة الخوارزمية،<sup>(36)</sup> كمفهوم - برز في جهود جون بورتون إلى أمنة الذكاء الاصطناعي نفسه نظرا لدوره البارز تغذية الاستقطاب والتطرف -<sup>(37)</sup> تبلور في سياسات الزمن المتسارعة، التي تتجاوز حدود الإدراك البشري، وتفرض استجابات لحظية لا تترك مجالا يذكر للمداولات السياسية أو المسارات التشريعية البطيئة، التي اشترطتها مدرسة كوبنهاغن لضمان قبول الجمهور وتبرير الخروج عن القواعد السياسية المعتادة.<sup>(38)</sup>

وفي هذا السياق يجادل "تيم ستيفنز" بأن ضراوة الهجمات الخبيثة وسرعتها تدفع نحو تفويض قرارات الأمن القومي إلى منظومات دفاعية آلية.<sup>(39)</sup> حيث لم يعد دور الخوارزميات يقتصر على رصد التهديدات، بل امتد ليشمل اتخاذ تدابير استثنائية فورية كعزل الخوادم أو حجب البيانات بمعزل تام عن التدخل البشري؛<sup>(40)</sup> وهذه الممارسات تقضي إلى إقصاء ممنهج للجمهور كفاعل مانح للشرعية عبر ما يعرف بـ "التقننة"، ويؤدي في جوهره إلى تآكل البنية الديمقراطية لفعل الأمننة محولا حالة الطوارئ من استثناء سياسي مؤقت إلى واقع تقني مستمر.<sup>(41)</sup>

وقد تجلّى هذا التحول الاستيمولوجي في هجمات (NOTPETYA) التي طالت شركة (MEARSK) عام 2017 بوصفها عملية تخريب واسعة النطاق، لتعكس توظيف القدرات السيبرانية الهجومية للدول.<sup>(42)</sup> وبتحليل هذه الحادثة من منظور تنظيمي، يرى "نيبيل وآخرون" أنها واقعة جسدت حالة استثناء (state of exception) وفق رؤية أغامبين (Agamben's Theory)؛ حيث لم يكن هناك متسع من الوقت للمداولات السياسية، فقد استدعت الأزمة قرارا سياديا تقنيا من رئيس قسم تكنولوجيا المعلومات الذي قضى بإيقاف البنية التحتية للاتصالات.<sup>(43)</sup> ولم يكن تعليق الإجراءات التنظيمية نهاية المؤسسة، بل تدخلا لحالة استثناء دائمة، وفي مواجهة هذا الانتشار الخوارزمي، دمجت خلالها المنظمة نمط الهجوم لتطوير نظام مناعة رقمي يحاكي النظم البيولوجية في التعلم من الفيروس الأول وتخزين خصائصه لضمان مرونة الاستجابة في مواجهة التهديدات المستقبلية.<sup>(44)</sup>

## 2.4 إعادة تموضع الكيان المرجعي (Referent Object):

في سياق التحولات المعاصرة لمفهوم التهديد، يبرز تباين حاسم بين الأمن القومي والأمن السيبراني في نطاق الشيء المراد حمايته (الكيان المرجعي).<sup>(45)</sup> ومع اختفاء الحدود الجغرافية وتزايد الاعتمادية الوجودية على تكنولوجيا المعلومات، لم يعد موضوع الحماية

يقتصر على الشبكات الحكومية المحدودة، بل أصبح يشمل المجتمع بأسره. ووفقا لهذا التصور، انتقل التركيز الأمني نحو ضمان التشغيل السلس والموثوق والمستمر لأنظمة التحكم المترابطة التي تشكل البنية التحتية المعلوماتية الحيوية (CII)، واعتبار الحفاظ على استمرارية الأعمال (Business Continuity) غاية موازية لجهود للأمن القومي. لذا فإن التهديد السيبراني لا يمثل غزوا إقليميا تقليديا، بل ينظر إليه بوصفه تهديدا لـ القيم الأساسية للمجتمع، والرفاه الاقتصادي والاجتماعي بأكمله، يجعل استقرار الدولة رهنا بحماية البيانات من التعطيل أو التدمير أو الاستغلال لضمان استدامة تدفق الوظائف الحيوية. (46)

فقد أضحت البنى التحتية بما تشمله من قطاعات بمثابة القواعد الأساسية (Critical Foundations)، التي تنهض عليها المجتمعات المعاصرة، والضامن الوظيفي لاستمراريتها وبقائها. ويمثل هذا التحول منعطفا نظريا وإشكاليا بامتياز؛ فبدلا من حماية المواطنين، حصرا، باتت الأشياء وترابطاتها المادية والسيبرانية هي الأدوات الجوهرية في تحقيق الأمن ضد المخاطر الناشئة. وهذا التكريس للأجسام المادية كموضوع مرجعي للأمن (Referent Object)، يؤصل لعقلانية أمنية تزيح الكيانات البشرية لصالح النظم التقنية وشبكات الإمداد. (47) وبهذا توَّصل "كلوديا أراڊو" لعملية الأمانة بوصفها عملية تمتين مادي تعطي أولوية بارزة للأشياء التقنية وشبكات الإمداد المادية في سلم الأولويات الأمنية.

وما يزيد من تعقيد هذا المشهد هو أن غالبية البنى التحتية التي تشكل الكيان المرجعي مملوكة ومدارة من قبل القطاع الخاص، الذي أصبح فاعلا وظيفيا رئيسيا (functional actor) في بيئة فضاء سيبراني قروسطي جديد وفقا لـ "ريتشارد ديفيد هالوز" تتسم بسلطات متداخلة متعددة (Overlapping Authority) بين مالك موضوع الحماية ومن يشارك في تقديمها، وتظهر فجوة أمنية واضحة بين ما تطلبه الدولة كفاعل مؤمن (securitising actor) وبين الاستجابة الفعلية للفاعلين الخواص. (48)

وأقوى دليل تجريبي على هذا التحول النظري، نستعين بهجوم فيروس الفدية (ransomware) على شركة (colonial pipeline) سنة 2021، كمثال نموذجي لتحول التهديدات السيبرانية؛ فعلى الرغم من أن الهجوم السيبراني المشفر استهدف حاسوب مخصص لنظام الفوترة، فإن الشركة اتخذت قرارا احترازيا بإغلاق أنظمة التكنولوجيا التشغيلية (OT) لتجنب المزيد من العدوى وانتقالها.<sup>(49)</sup> وقد تسبب هذا الشلل التقني في اعلان حالة الطوارئ نتيجة اكبر هجوم ضد البنية التحتية للطاقة الحيوية للولايات المتحدة الأمريكية على طول الساحل الشرقي، ورافق النقص الحاد في امدادات الطاقة اضطراب اجتماعي، شكل ما يشبه لحظة بيرل هاربر سيبرانية،<sup>(50)</sup> استدعت مراجعة التنظيمات الأمنية واستمرارية الخدمات، مكرسة استقرار النظم جوهرًا لأمن الطاقة. لارتباط الكيان المرجعي بقطاع حيوي للدولة والمجتمع.

## 5. تداعيات استقلالية قطاع الأمن السيبراني على الأمن القومي

تؤكد الأدلة الميدانية أن تداعيات استقلالية الامن السيبراني كقطاع سادس، لا تقف عند حدود التنظير لإطار مدرسة كوبنهاغن الذي يواجه تحديات وجودية، بل تفرز تداعيات عملية تمس صميم العقد الاجتماعي. ومن هذا المنطلق، يظهر التركيز على الاستحقاقات النقدية لهذه التحولات، أن هذا الواقع الذي تتآكل فيه السيادة الوطنية يؤدي إلى تحدي تفرغها لصالح ما يعرف بالأمن القومي عبر المنصات (national security by platform).

وبناء على ما تقدم من تداعيات تمس صميم العقد الاجتماعي وتآكل السيادة، فإن تفكيك ديناميات القوة في القطاع السيبراني باعتباره قطاعا متميزا في إطار نظرية الأمنة،<sup>(51)</sup> يكشف عن استحقاقات نقدية جوهرية لا يمكن تجاهلها. ويتصدر هذه الاستحقاقات تصاعد العجز الديمقراطي الناتج عن الخصخصة المتسارعة للأمن القومي؛ فعندما تنتقل سلطة الأمانة وفعل الكلام وتحديد الكيان المرجعي،<sup>(52)</sup> من المجال التداولي

العام إلى خوادم الشركات التكنولوجية العابرة للحدود، يتعرض مفهوم الأمن الوطني ذاته لتفريغ سياسي عميق يكرس لنمط الأمن القومي عبر المنصات.<sup>(53)</sup>

وفي سياق متصل مع تحول الأمن القومي إلى نمط تديره المنصات الرقمية، تبرز إشكالية عميقة تتعلق بطبيعة الجهات الفاعلة الجديدة؛ فعلى الرغم من فاعليتها التقنية العالية أو مدى موثوقيتها للحكومات، تظل هذه الفواعل في جوهرها كيانات تجارية متعددة الجنسيات تحركها الدوافع الربحية ومنطق السوق وضغوط المساهمين، بعيدا عن مبادئ الصالح العام المتأصلة في العقد الاجتماعي.<sup>(54)</sup> وبالتالي تميل القرارات الاستثنائية لمعالجة التهديدات السيبرانية إلى خدمة مصالحها المؤسسية الخاصة ليس فقط على حساب الحقوق المدنية والحريات الأساسية لمواطني الدول المتأثرة،<sup>(55)</sup> بل بأنشطتها المرتبطة بالبيانات الحساسة أو سياسات هذه الشركات التي تعرقل تحديد التهديدات التي تواجهها الدولة وأمنها القومي بطريقة مباشرة أو غير مباشرة. كما في حالة (Apple vs Fbi) لعام 2016 التي تمثل لحظة التقنية المفرطة؛ بمحاولة أعلى سلطة أمنية وقانونية أمريكية إجبار آبل على كسر تشفير هواتف متهم بالإرهاب، إلا أن الشركة رفضت الطلب مستندة إلى مبدأ أمن الكود.<sup>(56)</sup>

وتحذر الدراسات النقدية من أن تطبيع العلاقات الدولية السيبرانية يعيد تشكيل مفهوم السيادة بطرق تقلل من استقلالية الدولة، فالخصائص التقنية و البنيوية للفضاء السيبراني تتحدى بعض المفاهيم الأساسية في العلاقات الدولية مثل السلطة والسيادة الإقليمية؛ ومع تجزؤ السيادة والسلطة والمساءلة التي تشكل التحدي الرئيسي في حوكمة هذا الفضاء، أصبحت شركات الأمن السيبراني جهات فاعلة رئيسية في هندسة الممارسات الأمنية الفعلية، بما في ذلك الكشف عن الحوادث والاستجابة لها والاسناد العلني للعمليات من خلال شبكات مترابطة تتجاوز السيطرة الحكومية المركزية.<sup>(57)</sup>

ويفضي هذا التحول إلى أمانة مخصصة قد تجعل الدول عرضة لتبعية تقنية بنوية حيث تشارك سيادتها الرقمية فعليا مع القطاع الخاص، لأن فوائد العمل ضمن شروط خدمة شركات التكنولوجيا الكبرى تفوق التكاليف، فتصبح قراراتها مرهونة بهذه الشروط بدلا من الأطر الدستورية.<sup>(58)</sup> وتجسدت هذه التبعية بشكل صريح في جانفي 2021 بقرار شركة امازون (AWS) المنفرد بفصل خوادم (Parler) لانتهاك شروط الخدمة (TOS)، لتمارس فعل كلام اقصائي سيادي أعدم بنية منصة كاملة بضغطة زر؛<sup>(59)</sup> كما برزت بوضوح في مثال الحرب الأوكرانية، حيث أصبحت أقمار ستارلينك (Starlink) والخدمات السحابية لـ (Microsoft) العمود الفقري للدفاع الأوكراني<sup>(60)</sup>، ليثبت أن الفاعل المؤمن المتحكم بزر الإيقاف/التشغيل هو رائد الأعمال التكنولوجي، وليس هيئة الأركان العسكرية حصرا.

## 6. خاتمة

تأسيسا على ما سبق، تثبت هذه الورقة البحثية أن تأصيل الأمن السيبراني كقطاع سادس مستقل، يعد ضرورة ابستمولوجية لقصور مدرسة كوبنهاغن التأسيسية عن استيعاب تعقيداته اللامركزية وآلياته كالتقنة، الأمانة المفردة ومعضلة الاسناد. وتبرز الدراسة انتقالا ثلاثي الأبعاد في بنية الأمانة: أولا، تحول الفاعل المؤمن من احتكار النخبة السياسية الحكومية إلى سلطة الخبراء والشركات التكنولوجية الكبرى نتيجة للفجوة السيادية والعمى التقني للدولة؛ ثانيا، انتقال فعل الكلام من الخطاب السياسي الجماهيري إلى الممارسة التقنية المباشرة والمؤتمتة عبر ما يسمى بالأمانة التقنية، التي تفرض طوارئ تلغي المساءلة؛ وثالثا، إعادة تشكيل الكيان المرجعي لينتقل من حماية الافراد والدولة، نحو البنى التحتية الحيوية والمعلوماتية كركيزة لبقاء المجتمع. وختاماً، تحذر هذه الدراسة من الاستسلام لمنطق الأمن القومي للمنصات الذي يفرز عجزا ديمقراطيا، ويخضع السيادة الرقمية للدول لمنطق الربح

وشروط خدمة الكيانات التجارية العابرة للحدود؛ مؤكدة حتمية تعديل المفاهيم الأمنية لاستيعاب احتكار الفاعل التكنولوجي والخبراء التقنيين لسلطة إعلان الاستثناء.

## 7. الهوامش والمراجع

- (1) Choucrist Nazli. 2012. Cyberpolitics in International Relations. The MIT Press, pp. 1-221.
- (2) Hansen Lene and Helen Nissenbaum. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, pp 1156-1161.
- (3) Cavelti Myriam Dunn. 2008. Cyber-Security and Threat Politics: US efforts to secure the information age. Routledge, pp 1-145.
- (4) Buzan Barry and et.al. 1998. Security: A New Framework for Analysis. Lynne Rienner Publishers. pp. 1-8.
- (5) Lene Hansen and Helen Nissenbaum, Op.Cit., pp. 1156-1161.
- (6) Stroppa Marta. 2023. Autonomous Cyber Capabilities And Unilateral Measures Of Self-Help Against Malicious Cyber Operations. NATO Cooperative Cyber Defence Centre Of Excellence, p.7.
- (7) Liivoja Rain and et.al, 2019. Autonomous cyber capabilities under international law. NATO Cooperative Cyber Defence Centre of Excellence, P.12.
- (8) Choucrist Nazli, Op.Cit., pp. 4-13.
- (9) Lene Hansen and Helen Nissenbaum, Op.Cit., p. 1157.
- (10) Rid Thomas. 2012. Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), pp. 12-16.
- (11) Ibid. pp.11-12.
- (12) Kello Lucas. 2013. The Meaning of the Cyber Revolution Perils to Theory and Statecraft. International Security, 38 (2), pp. 28-33.
- (13) Thumfart Johannes. 2022. The (Il)legitimacy of Cybersecurity. An Application of Just Securitization Theory to Cybersecurity based on the Principle of Subsidiarity. Applied Cybersecurity and Internet Governance, 1(1), p. 2; Hansen and Nissenbaum. Op.Cit., pp. 1157-1171.
- (14) Ibid. pp. 1157-1172.
- (15) Thumfart Johannes, Op.Cit., p.5

- (16) Hansen and Nissenbaum, Op.Cit., p.1167 ; Thumfart, Op.Cit., p. 4.
- (17) Hansen and Nissenbaum, Op.Cit., p.1171-1172 ;Thumfart, Op.Cit, p4.
- (18) Cavelty Myriam Dunn, Op.Cit., pp 3-19, 57.
- (19) Myriam Dunn Cavelty and Florian Egloff. 2021. Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland. Swiss Political Science Review, 27(1), pp. 141-146.
- (20) Mueller Milton. 2010. Networks and states: The global politics of Internet governance. MIT Press. pp. 1-4.
- (21) Hansen and Nissenbaum, Op.Cit., pp. 1155–1161.
- (22) Lucas Kello. 2017. The virtual weapon and international order. Yale University Press, p.195.
- (23) Burt Tom. (2020, October 12). New action to combat ransomware ahead of U.S. elections. Microsoft On the Issues. <https://shorturl.at/X9izi>
- (24) Lubin Asaf , João Marinotti. (2021). Why current botnet takedown jurisprudence should not be replicated. Lawfare. <https://shorturl.at/EnYhW>
- (25) Hansen and Nissenbaum, Op.Cit., pp. 1161–1167.
- (26) National Audit Office. 2018. Investigation: WannaCry cyber attack and the NHS (HC 414). pp. 5-9.
- (27) Smart William. 2018. Lessons learned review of the WannaCry ransomware cyber attack. Department of Health and Social Care.pp10-11.
- (28) Hurel Louise Marie. 2024. Private authority and the political economy of private companies in cybersecurity crises and conflicts. In Stevens & Devanny(eds), Research handbook on cyberwarfare. Edward Elgar,pp.2, 9.
- (29) Ibid. pp. 24-25.
- (30) Korovamode, K. 2025. The rise of corporate sovereignty: How Big Tech is reshaping global power and governance. PhilArchiv. pp. 8-12.<https://shorturl.at/1la7w>
- (31) Egloff Florian. 2020. Public attribution of cyber intrusions. Journal of Cybersecurity, Volume 6, Issue 1, pp. 2-8.
- (32) Rid Thomas and Ben Buchanan. 2015. Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), pp. 25-30

- (33) Egloff Florian. 2019. Contested public attributions of cyber incidents and the role of academia. Contemporary Security Policy, Volume 41 Special issue (1), pp 12-14. <https://shorturl.at/uemcR>
- (34) Cavelty Myriam Dunn and Egloff Florian, Op.Cit., pp. 141, 145–147.
- (35) Olteanu Mihai. 2024. The Copenhagen School's widening security theory in relation to cybersecurity. Applicability and implications', Security and Defence Quarterly, 48(4), pp. 46-49.
- (36) Cristiano Fabio. 2019. Deterritorializing Cyber Security and Warfare in Palestine: Hackers, Sovereignty, and the National Cyberspace as Normative. Cyber Orient, Vo l . 13 (1), pp . 34, 36. 28–42
- (37) Burton Joe. 2023. Algorithmic extremism? The securitization of artificial intelligence (AI) and its impact on radicalism, polarization and political violence. Technology in Society, 75, Article 102262. pp.1-2.
- (38) Buzan Barry and et.al, 1998. Security: A new framework for analysis. Lynne Rienner Publishers. Pp 23-26.
- (39) Stevens Tim. 2016. Cyber security and the politics of time. Cambridge University Press. pp.73–78, 85.
- (40) Kuchtová Jana Zachar. 2025. Threats and opportunities of using artificial intelligence from a cybersecurity perspective. Auspica, (2), p.13.
- (41) Hansen and Nissenbaum, Op.Cit., pp 1165, 1167
- (42) Egloff Florian and Shires James. 2022. Offensive Cyber Capabilities and State Violence: Three Logics of Integration. Global Security Studies, 7(3), P.133.
- ( 43 ) Knebel Sebastian and et.al., 2022. Cyberattacks as state of exception Reconceptualizing cybersecurity from prevention to surviving and accommodating. Journal of Information, Communication and Ethics in Society, 20 (1), p.106.
- (44) ibid.pp.100-107.
- (45) Cavelty Myriam Dunn. 2010. Cyber-security. In J. Peter Burgess (Ed), The Routledge Handbook of New Security Studies Routledge, p. 155.
- (46) ibid. pp. 154-158.
- (47) Aradau Claudia. 2010. Security That Matters: Critical Infrastructure and Objects of Protection. Security Dialogue Vol. 41(5). pp. 491-502.

- (48) Hallows Richard David, 2020. Securitisation and the role of the state in delivering UK cyber security in a New-Medieval cyberspace, Doctoral dissertation of Philosophy, University of Buckingham. pp. 129-140, 161-163.
- (49) Kilovaty Ido. 2023. Cybersecuring the pipeline. *Houston Law Review*, 60 (3), pp 605-28.
- (50) Reeder Joe R. and Hall Tommy. 2021. Cybersecurity's Pearl Harbor moment: Lessons learned from the Colonial Pipeline ransomware attack. *The Cyber Defense Review*, 6(3), pp.15-16.
- (51) Hansen and Nissenbaum, *Op.Cit.*, pp. 1156–1157.
- (52) *ibid.* pp. 1158; Buzan, and et.al, *Op.Cit.*, pp 25–31.
- (53) Chachko Elena. 2021. National security by platform. *Stanford Technology Law Review*, 25(1), pp. 56- 61, 107–126.
- (54) Hansen and Nissenbaum, *Op.Cit.*, pp. 1160–1161; Chachko Elena, *Op.Cit.*, pp. 64, 127–129.
- (55) *ibid.* pp. 63, 135.
- (56) Schulze, Matthias. 2017. Clipper Meets Apple vs. FBI—A Comparison of the Cryptography. *Media and Communication*, 5(1), pp. 54, 58.
- (57) Cavelty Myriam Dunn and Wenger Andreas. 2020. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), pp. 20-22.
- (58) Roberts Huw.2024. Digital sovereignty and artificial intelligence: a normative approach. *Ethics and Information Technology*, 26(70). pp. 1-8.
- (59) Van Dijck José and et.al. 2023. Deplatformization and the governance of the platform ecosystem. *New Media & Society*, 25(12), pp. 3445, 3450.
- (60) Abels Joscha. 2024. Private infrastructure in geopolitical conflicts: The case of Starlink and the war in Ukraine. *European Journal of International Relations*, 30(4), pp. 843–856.