

نحو فهم إشكالات الأمن السيبراني في السياسة العالمية:
مقاربة من منظور التعقّد

**"Towards Understanding the Challenges of
Cybersecurity in Global Politics:
A Complexity Perspective"**

الزهرة حروري*، جامعة باتنة
zohra.harrouri@univ-batna.dz

تاريخ القبول: 2025/05/27

تاريخ الاستلام: 2025/04/26

ملخص:

تلعب التكنولوجيا دوراً عميقاً في تشكيل مشهد المخاطر العالمية؛ حيث أدى الإهتمام المتزايد بالأمن على المستوى العالمي في ظل التحولات الناجمة عن الثورة الرقمية إلى التوسع في استخدام التقنيات الرقمية، ما انعكس على الواقع العالمي بشكل مباشر، حيث أصبحت تصنف التهديدات السيبرانية ضمن المخاطر التي تقع في مركز الإهتمام الدولي.

فقد شهد العالم في العقود الأخيرة تصاعداً في التهديدات السيبرانية، التي تجاوزت كونها مجرد اختراقات تقنية لتصبح أدوات استراتيجية في الصراعات الدولية. في هذا السياق، بات الأمن السيبراني محورياً أساسياً في تفكير صانعي القرار ومحلي العلاقات الدولية. الأمر الذي جعل النماذج التقليدية لفهم الأمن، التي تقوم على ثنائية الدولة والعدو، لم تعد كافية لفهم شبكة العلاقات المعقدة التي تتشكل في الفضاء السيبراني.

في سياق هذه التحولات، تطلب هذا الواقع مقاربة تنظر إلى الفضاء السيبراني كنظام معقّد، ديناميكي ومتداخل. من هنا، يهدف هذا المقال إلى تسليط الضوء على إمكانية توظيف التعقّد كمقاربة في فهم وتحليل الأمن السيبراني في سياق السياسة العالمية، وفحص واسع النطاق للتعقّد بهدف اختبار طبيعة العلاقة

*المؤلف المراسل

جويلية 2025

المجلة الجزائرية للأمن الإنساني

بين أنظمة التعقد والأنظمة السيبرانية، من خلال تتبع فهم للتعقد وسلوك الأنظمة المعقدة، ثم معالجة الأمن السيبراني وإشكالات الاختراق في ضوء التكنولوجيا الحديثة، ووصف للأنظمة الأمنية السيبرانية كأنظمة معقدة، وقد توصلت الدراسة إلى أن النماذج الأمنية التقليدية التي تعتمد غالباً على الكشف التوقعي والوقائي الثابت، تعجز عن التكيف مع التهديدات السيبرانية المعاصرة التي تتسم بالديناميكية والتعقيد والتمويه. وأظهرت أن الفضاء السيبراني لا يمكن تحليله أو تأمينه بمعزل عن فهم العلاقات التفاعلية بين العناصر المختلفة فيه (المستخدمون، الأنظمة المعقدة، الشبكات، البيانات، السياسات، والأدوات).

الكلمات المفتاحية: الأمن السيبراني، السياسة العالمية، التعقد، الأنظمة المعقدة، الأنظمة السيبرانية.

Abstract:

Technology plays a profound role in shaping the global risk landscape. The growing focus on security at the international level, driven by the transformations of the digital revolution, has led to an expanded use of digital technologies. This shift has had a direct impact on the global reality, where cyber threats are now classified among the top priorities in international security concerns.

In recent decades, the world has witnessed a surge in cyber threats that have evolved beyond mere technical breaches to become strategic tools in international conflicts. As a result, cybersecurity has become a central focus for policymakers and international relations analysts. This shift has revealed the inadequacy of traditional security models, which are based on the binary of state and enemy, in capturing the complex network of relationships that define cyberspace.

Given these transformations, there is a need for an approach that views cyberspace as a complex, dynamic, and interconnected system. This article aims to explore the potential of employing complexity theory as a framework for understanding and analyzing cybersecurity within the context of global politics. It conducts a broad examination of complexity to investigate the nature of the relationship between complex systems and cyber

systems. This includes tracing the concept of complexity and the behavior of complex systems, then addressing cybersecurity and breach challenges in light of modern technology and cybersecurity systems as complex entities.

The study concludes that traditional security models, which often rely on static, predictive, and preventive detection, fall short in adapting to modern cyber threats characterized by dynamism, complexity, and obfuscation. It further demonstrates that cyberspace cannot be analyzed or secured without understanding the interactive relationships between its various components—users, complex systems, networks, data, policies, and tools.

Keywords: Cybersecurity, Global Politics, Complexity, Complex Systems, Cyber Systems

مقدمة:

كشفت معالم تعقد السياسة العالمية عن هشاشة الأنظمة الأمنية، ما أدى إلى تحول في طبيعة التهديدات التقليدية إلى تهديدات أفرزتها التحولات الجيوسياسية والاقتصادية والتكنولوجية على وجه الخصوص، صدمات عالمية هزت أركان الأمن من منظوره الضيق، فضلاً عن تغير منحنى الاهتمام في ظل هيمنة الفضاء الأزرق (الإلكتروني) التي أنتجت الأنترنت حيث فرضت الديناميات العالمية الراهنة إلى بروز التهديدات السيبرانية إلى الواجهة في مقابل تراجع التهديدات ذات البعد العسكري.

في ظل التزايد المتسارع للاعتماد على الفضاء السيبراني في مختلف مناحي الحياة، برز الأمن السيبراني كأحد أهم القضايا الاستراتيجية التي تواجه الدول والمؤسسات والأفراد على حدٍ سواء. غير أن التغير المستمر في طبيعة التهديدات، وتطور تقنيات الهجوم والدفاع، يكشف محدودية المقاربات التقليدية في التعامل مع الأمن السيبراني بوصفه نظاماً ثابتاً أو يمكن ضبطه بمجموعة من القواعد والإجراءات. ومن هذا المنطلق، يطرح التعقّد (Complexity) "نفسه كإطار تحليلي بديل لفهم الأمن السيبراني، حيث يُنظر إلى هذا الأخير بوصفه نظاماً ديناميكياً معقداً يتكوّن من عدد كبير من العناصر المتفاعلة بطريقة غير

خطية ، ما يجعل من التنبؤ بالسلوكيات المستقبلية مهمة بالغة الصعوبة ، بل أحياناً مستحيلة. وعليه ، وفي ظل هذه المتغيرات وفي ظل بيئة تتصاعد فيها وتيرة التهديدات السيبرانية ، يهدف هذا البحث إلى استكشاف مفاهيم التعقّد وتطبيقها في سياق الأمن السيبراني ، مع التركيز على سمات مثل الظهور (Emergence) ، التكيف (Adaptation) ، المرونة (Resilience) ، وعدم الخطية (Non-linearity) ، كعوامل جوهرية في بناء فهم شامل وعميق للتهديدات السيبرانية وآليات التعامل معها. وبناء على ما سبق جاءت إشكالية المقال كالتالي: كيف يسهم التعقّد كمقاربة في إعطاء تفسير وتحليل شامل قادر على فهم إشكالات الأمن السيبراني في السياسة العالمية ومحاولة معالجتها في ظل تطور الأنظمة التكيفية المعقدة؟ ولعالجة الإشكالية تم اعتماد فرضية أن الفضاء السيبراني يمثل نظاماً معقداً يتضمن تفاعلات غير خطية بين فاعلين متعددين ، بما يجعل السياسات الأمنية التقليدية غير كافية ، ما يتطلب تبني نهج تكيفي وشبكي لضمان الأمن السيبراني. وقد تم الاستعانة بالمنهج التحليلي ومقاربة متعددة التخصصات بين العلاقات الدولية ، دراسات الأمن ، ونظرية الأنظمة المعقدة لقراءة واقع الأمن السيبراني وسبل تحليله لفهم أكثر لبسه وغموضه ، ولعالجة الإشكالية المطروحة واختبار الفرضية ، تم تقسيم الورقة البحثية إلى ثلاث محاور ، يتناول المحور الأول فهم للتعقّد وسلوك الأنظمة المعقدة ، أما المحور الثاني يعالج الأمن السيبراني وإشكالات الاختراق في ضوء التكنولوجيا الحديثة ، في حين المحور الثالث يتضمن الأنظمة الأمنية السيبرانية كأنظمة معقدة.

أولاً: نحو فهم للتعقّد وسلوك الأنظمة المعقدة

نستعرض في هذا المحور تقديم نظرة تمهيدية للمفاهيم الأساسية التي يقوم عليها فهم التعقّد وسلوك الأنظمة المعقدة ، تمهيداً لاستيعاب طبيعة الظواهر الديناميكية والتفاعلية في العالم المعاصر.

1- المفاهيم الأساسية للتعقّد

التعقّد (Complexity) هو نموذج فكري يُستخدم لفهم الأنظمة التي تتكون من أجزاء متعددة مترابطة وتتفاعل بطرق غير خطية وغير متوقعة ، يُستخدم لفهم الأنظمة المعقدة مثل الطقس ، الاقتصاد ، الشبكات الاجتماعية ، والأنظمة

السيبرانية"، يمثل تحولاً في التفكير العلمي من المقاربات التقليدية الخطية إلى فهم أعمق للأنظمة التي تتكون من مكونات متعددة تتفاعل فيما بينها بشكل ديناميكي وغير متوقع، وقد نشأ في بدايات القرن العشرين، وتطور من خلال دراسات في مجالات الفيزياء، والبيولوجيا، والرياضيات، ثم انتقل تدريجياً إلى العلوم الاجتماعية والإدارية. (حمشي، 2021)

وتتمثل أهم مفاهيمه في:

- **التكيف المستمر: (Continuous Adaptation)** يشير إلى أن الأنظمة يجب أن تتكيف مع التهديدات الجديدة، ولا تعتمد فقط على استجابات جاهزة. حيث تقوم مكونات النظام بتعديل سلوكها استجابة للتغيرات في البيئة أو لتفاعلاتها الداخلية.

- **الظهور: (Emergence)** إن التهديدات الجديدة قد تظهر من تفاعل مكونات النظام، وليس بالضرورة من مصدر خارجي. حيث تنشأ خصائص أو أنماط سلوكية جديدة نتيجة لتفاعل المكونات، دون أن تكون موجودة في أي عنصر بمفرده.

- **عدم الخطية: (Non-linearity)** تشير إلى أن أي تغيير صغير في النظام قد يؤدي إلى نتائج كبيرة (مثل تسرب معلومة صغيرة يؤدي لاختراق واسع). حيث أن العلاقة بين السبب والنتيجة ليست مباشرة أو متناسبة، فمؤثر صغير قد ينتج عنه أثر كبير والعكس صحيح. (Neil e, 2006, p. 333)

- **المراقبة الذاتية: (Self-monitoring)** : يتطلب النظام آليات للكشف والتحليل الذاتي، وليس فقط الاستجابة بعد وقوع الحادث.

- **الحساسية للشروط الأولية: (Sensitivity to Initial Conditions)** مما يعني أن اختلافاً بسيطاً في نقطة البداية قد يؤدي إلى نتائج مختلفة تماماً (كما في "تأثير الفراشة").

وقد استخدم هذا المنظور في فهم عدد من الظواهر المعقدة كشبكات التواصل الاجتماعي، الأنظمة البيئية، الأسواق المالية، وإدارة الأزمات. وفي السنوات

الأخيرة، بدأ الباحثون في استكشاف إمكانيات تطبيقه على الأمن السيبراني، خاصة مع تزايد تعقيد وتداخل الفضاء السيبراني عالمياً، وتطور أنماط التهديدات والهجمات. (seven trends that will shape global security, 2023)

يشير التعقد في السياسة العالمية إلى نظام معقد تتفاعل فيه:

فاعلون متنوعون: (State & Non-State Actors) :دول، شركات تكنولوجيا، هكرز، مجموعات ناشطة (Hacktivists)، جماعات إرهابية، شركات خاصة للأمن السيبراني، إلخ. هذه الأطراف تتفاعل بطرق متغيرة وغير متوقعة.

التربط الشبكي: إن هجوم على بنية تحتية في دولة ما يمكن أن يؤثر على دول أخرى كما حدث مع فيروس NotPetya أو Stuxnet. (Rosenau, 1990)

2. سلوك الأنظمة التكيفية المعقدة

تتألف الأنظمة المعقدة من عدد كبير من العناصر أو العوامل، تتفاعل مع بعضها البعض ضمن بيئة مفتوحة، مما يؤدي إلى سلوكيات جماعية يصعب التنبؤ بها من خلال تحليل الأجزاء الفردية فقط. وتتميز هذه الأنظمة بعدد من الخصائص الرئيسية، منها: (hendrick, 2009, p. 8)

إن النظام المعقد هو أي نظام تمثل فيه أجزاء النظام وتفاعلاتها معاً سلوكاً محدداً، بحيث لا يمكن لتحليل جميع أجزائه المكونة تفسير السلوك. في مثل هذه الأنظمة، لا يمكن بالضرورة ربط السبب والنتيجة وتكون العلاقات غير خطية - يمكن أن يكون للتغيير الصغير تأثير غير متناسب. بعبارة أخرى، كما قال أرسطو: "الكل أعظم من مجموع أجزائه". من أكثر الأمثلة شيوعاً المستخدمة في هذا السياق نظام المرور الحضري وظهور الاختناقات المرورية؛ لا يمكن لتحليل السيارات الفردية وسائقي السيارات أن يساعد في تفسير أنماط وظهور الاختناقات المرورية.

كما أن النظام التكيفي المعقد يتسم بخصائص التعلم الذاتي والنشوء والتطور بين المشاركين في النظام المعقد. ويظهر المشاركون أو الوكلاء في النظام التكيفي المعقد سلوكاً غير متجانس. ويستمر سلوكهم وتفاعلاتهم مع

الوكلاء الآخرين في التطور. والخصائص الرئيسية للنظام الذي يمكن وصفه بأنه تكييفي معقد هي: (hendrick, 2009, p. 9)

- لا يمكن التنبؤ بالسلوك أو النتائج ببساطة من خلال تحليل أجزاء ومدخلات النظام.

- إن سلوك النظام ناشئ ويتغير مع الوقت. ولا تضمن نفس المدخلات والظروف البيئية دائماً نفس الناتج.

- إن المشاركين أو الوكلاء في النظام (الوكلاء البشريون في هذه الحالة) يتعلمون ذاتياً ويغيرون سلوكهم بناءً على نتيجة التجربة السابقة.

إن مقدمة التفكير في التعقد هي التحقيق في الأنظمة الديناميكية. وبعبارة بسيطة، فإن النظام عبارة عن مجموعة من المكونات أو المتغيرات التي تعتمد على بعضها البعض. يقف كل مكون في النظام في علاقة متبادلة مع كل مكون آخر في المجموعة وأيضاً في تفاعل مع بيئة النظام. بعبارة أخرى، تتفاعل المكونات مع بعضها البعض داخل حدود النظام للعمل ككل لأداء مهمة. هناك ثلاثة أنواع من الأنظمة: (Neil e, 2006, p. 336)

- الأنظمة المنظمة هي تلك التي يتم تنظيمها حول مجموعة من القواعد أو القوانين التي تحتوي على أنماط واضحة حيث يمكن تحديد النتائج الموثوقة. تتميز بالاستقرار والعلاقات السببية الواضحة.

- تتضمن الأنظمة المعقدة (التكيفية) عدداً من المتغيرات التي تلعب في نفس الوقت العديد من الأدوار المختلفة في تطور النظام واتباع العديد من قوانين السلوك المختلفة. هذه الأنظمة غير خطية ومتقلبة بشكل محتمل. لا يمكن اكتشاف سلوكها إلا من خلال دراسة كيفية تفاعل هذه العناصر وكيفية تكيف النظام وتغيره عبر الزمن.

- الأنظمة الفوضوية هي أنظمة معقدة مضطربة في مرحلة انتقالية إلى نظام مختلف. من المستحيل تحديد العلاقات بين السبب والنتيجة لأنها تتغير باستمرار ولا توجد أنماط يمكن إدارتها. لا يمكن التنبؤ على المدى المتوسط إلى الطويل على الإطلاق. (Neil e, 2006)

لقد خلقت دراسة الأنظمة الفوضوية والمعقدة مجالاً كبيراً وامتامياً لعلم التعقيد. في حين استخدمت مجموعة متنوعة من التخصصات هذا المنظور التحليلي والنظري، فقد كان شائعاً بشكل خاص في العلوم الطبيعية والاجتماعية بشكل متزايد. يشير هذا الاتجاه إلى حقيقة مفادها أن دراسات التعقيد قابلة للتطبيق على جميع أنواع الأنظمة، بغض النظر عن حجمها أو طبيعتها، مثل الأنظمة التكنولوجية (الفرعية)، أو الظواهر المجتمعية أو النظام السياسي الدولي. (hendrick, 2009, p. 9)

وفي نظرية التعقد، يتم تفسير ظهور النظام الجديد من خلال مفهوم التنظيم الذاتي، الذي يشير إلى تكوين تلقائي لنمط مستقر ولكنه معقد من كيانات تبدو عشوائية. ويحدث التنظيم الذاتي من خلال عمليات التباين الداخلي، والتي تسمى "التقلبات". وبمرور الوقت، تصبح الأنظمة المعقدة أكثر حساسية للتقلبات الداخلية والخارجية - وكلما كان النظام أكثر تعقيداً، كلما أصبح أكثر حساسية وعرضة للتقلبات. وعند نقطة معينة، تتجاوز هذه التقلبات عتبة حرجية، تسمى أيضاً نقطة التفرع، ثم بعد مرحلة انتقالية من التقلبات الفوضوية، تعيد تنظيم النظام بالكامل. (Kavalski، 2015)

كما أن الأنظمة الكبيرة ذات المكونات العديدة تميل إلى التطور إلى حالة "حرجية" متوازنة وغير متوازنة للغاية حيث قد تؤدي الاضطرابات البسيطة إلى أحداث تسمى الانهيارات الجليدية. وهذا يعني أن الأنظمة المعقدة تميل إلى التكيف مع الفوضى، أو تكون هي نفسها على حافة الفوضى، وأن أغلب التغيرات تحدث من خلال أحداث كارثية بدلاً من اتباع مسار تدريجي سلس. ولا يمكن التنبؤ بالمسار الجديد الذي سيسلكه النظام أو التحكم فيه قبل أن يسلكه. وبسبب هذا السلوك الناشئ، لا يمكن فهم النظام المعقد عن طريق تقليصه إلى أجزائه؛ فضلاً عن ذلك فإن السلوك الذي نهتم به يتغير عندما نحاول تقليص النظام إلى نظام أبسط وأسهل فهماً. (johan eriksson, giampiero giacomello, 2007, p. 3)

ثانياً: الأمن السيبراني واشكالات الاختراق في ضوء التكنولوجيا الحديثة

لقد أصبحت أجهزة الكمبيوتر والأنترنت من الأشياء التي لا غنى عنها للمنازل والمؤسسات على حد سواء. ويزداد الاعتماد عليها يوماً بعد يوم، سواء بالنسبة لمستخدمي المنازل، أو في التحكم في الفضاءات المهمة، أو إدارة شبكات الطاقة، أو التطبيقات الطبية، أو أنظمة التمويل للشركات. ولكن هناك أيضاً تحديات متوازية تتعلق بالتوصيل المستمر والموثوق للخدمة، وهو ما أصبح مصدر قلق أكبر للمنظمات. ويأتي الأمن السيبراني في طليعة جميع التهديدات التي تواجهها المنظمات حتى أعلى من تهديد الإرهاب أو الكوارث الطبيعية. (johan eriksson, giampiero giacomello, 2007, p. 3)

1- جدلية الأمن في العصر الرقمي

إن فهم الأمن في العصر الرقمي أو عصر المعلومات مهمة صعبة في عالم واسع النطاق وحدود غير واضحة والتي تطرح إشكالات عديدة: ما هو الأمن في عصر المعلومات وكيف يمكن تعريفه بطريقة هادفة؟ هل هناك حقاً أي شيء جديد حول أمن عصر المعلومات يميزه بوضوح عن مسائل الأمن التقليدية؟ هل هناك حاجة إلى نظرية أمنية في عصر المعلومات؟ من الواضح أن نطاق وطبيعة نظرية محتملة لعصر المعلومات يعتمد على كيفية إدراكنا وتفسيرنا لحجم وعمق التحولات الحالية من خلال الإجابة على ما تقدمه نظرية التعقد من تفسيرات للأمن في عصر المعلومات، فإن الأمن المعلوماتي يُنظر إليه تلقائياً على أنه ظاهرة محددة تحدد سياقاً محدداً له تأثير محدد وبالتالي يخلق الحاجة إلى نهج جديدة، تظهر أن الدول تركز اهتمامها بشكل أساسي على حماية البنى التحتية المعلوماتية الحيوية بسبب صورة تهديد عصر المعلومات. (johan eriksson, giampiero giacomello, 2007)

في هذا السياق برزت المخاوف بشأن الاحتيال على البيانات والهجمات الإلكترونية في استطلاع تصوّر المخاطر العالمية، حيث توقع 82٪ من المشاركين حدوث هجمات إلكترونية على شكل سرقة بيانات أو أموال، وتوقع 80٪ زيادة في شكل اضطرابات في العمليات أو البنية التحتية في عام 2019. وبالمثل، احتلت مسألة "احتيال البيانات أو سرقتها" و "الهجمات الإلكترونية" المرتبة الرابعة

والخامسة على التوالي من حيث احتمالية حدوثها، في الواقع، كان هناك المزيد من خروقات البيانات في عام 2018، وتم الكشف عن نقاط ضعف جديدة في الأجهزة، وأشارت الأبحاث إلى الاستخدامات المحتملة للذكاء الاصطناعي لهندسة هجمات إلكترونية أكثر فاعلية. كما قدمت العام الماضي أدلة إضافية على أن الهجمات الإلكترونية تشكل مخاطر على البنية التحتية الحيوية، مما دفع البلدان إلى تعزيز فحص الشراكات عبر الحدود لأسباب تتعلق بالأمن القومي. (luis, 2010, p. 30)

وعلى الرغم من كل التركيز الذي حظي به الأمن السيبراني، إلا أنه كان رحلة صعبة حتى الآن. ومن المتوقع أن يصل الإنفاق العالمي على أمن تكنولوجيا المعلومات إلى 120 مليار دولار بحلول عام 2040، وهذه هي إحدى المجالات التي ظلت فيها ميزانية تكنولوجيا المعلومات لمعظم الشركات ثابتة أو زادت قليلاً حتى في الأزمات المالية الأخيرة. ولكن هذا لم يقلل بشكل كبير من عدد نقاط الضعف في البرامج أو الهجمات التي تشنها الجماعات الإجرامية. (seven trends that will shape global security, 2023)

2. الأمن السيبراني كمخرج من مخرجات الذكاء الاصطناعي:

تأتي تقنيات الذكاء الاصطناعي كأداة مساندة لخبراء الأمن السيبراني لتحقيق مستوى أعلى من الأمن، يستخدم الذكاء الاصطناعي لتحقيق ثلاث (03) أهداف رئيسية: الاكتشاف (Detection)، التنبؤ (Prediction)، الاستجابة (Response) يتم اكتشاف التهديدات السيبرانية باستخدام أنظمة ذكية للتحليل السلوكي بمعنى يقوم نموذج الذكاء الاصطناعي بمراقبة سلوك النظام ثم يعطي إشارات وتنبؤاتها في حالة وجود أي مخاطر « Risk Assessment »، يمكن التنبؤ بالتهديدات السيبرانية من خلال نماذج ذكاء اصطناعي باستخدام كميات هائلة من البيانات والذي يوفر فرصة للقيام بإجراءات استباقية للتنبؤ بالهجمات وتطوير آليات حماية جديدة بتقنيات متطورة، بناء على تقرير « The New Frontier In Digital Security » التابع إلى « Reinventing Cybersecurity With Artificial Intelligence » هدفها اكتشاف التهديدات المنظمات التي تستخدم الذكاء الاصطناعي في مجال الأمن السيبراني. (n.rosenau, 1994, p. 259)

وتعزز القدرة التخريبية للذكاء الاصطناعي (AI) قوتها، ولكن أيضاً إمكاناتها الإجرامية، على سبيل المثال تقنية التزييف العميق (Deep Fack) كما هو الحال في الحوسبة الكمية أو الحقائق المختلطة أو إنترنت الأشياء. يُنظر إلى ازدواجية الفرص والمخاطر هذه على أنها تتطوي على إمكانية المساعدة في اتخاذ قرارات الأعمال من خلال إنترنت السلوكيات، ولكنها أيضاً تمثل خطر الهجمات الإلكترونية الفعالة وعمليات الابتزاز في بعض المناطق، يمكن أيضاً استخدام الذكاء الاصطناعي في تهديد واضعاف الامن السيبراني لأن تقنياته من خصائصها انها تفوق القدرات البشرية، في بعض الأحيان يؤدي الى القيام بهجمات التي لن تكون ممكنة التنفيذ بواسطة الانسان نفسه. (alexander mcleod, 2008, p. 1)

لا جدال في أن المشكلات المعقدة آخذة في الارتفاع في عصر المعلومات مما يعني أن قوة الحوسبة ترتفع بشكل كبير بمرور الوقت. في وقت ترتفع فيه قيمة نظام الاتصالات وتنمو مع زيادة عدد مستخدمي النظام، مما يعني زيادة التعقيد في أنظمة البنية التحتية للمعلومات، حيث يؤدي التطور التكنولوجي إلى التغيير ويبرز عدداً متزايداً من الشبكات والعقد والروابط لتزايد الاعتماد المتبادل. بالإضافة إلى ذلك، يزداد تعقيد هذه الأنظمة مع امتداد النطاق الجغرافي وتوسيع الخدمات المقدمة، وإدخال مكونات جديدة بوظائف أكثر ثراءً باستخدام تقنيات متنوعة، وطبقات الأنظمة فوق الأنظمة ترقى التفاعلات الديناميكية للأنظمة المعقدة واللامركزية والمفتوحة وغير المحدودة (التقنية) إلى إرهاب القدرات على تحديد المشكلة وتقييمها، مما يخلق تحدياً عملياً لأولئك المشاركين في صياغة تدابير التأمين. (gandhi, 2014, pp. 2-3)

إن سلوك البرنامج ووظائفه تحت الهجوم يأتي ضمن موضوع أمن البرمجيات، وهو جزء من هندسة البرمجيات. خبراء أمنيون لديهم ثلاثة عوامل يمكن تحميلها مسؤولية تدمير التفرد المنطقي للنتائج المتوقعة. تؤثر هذه العوامل الثلاثة بشكل كبير على عملية النمو والتقييم لعمليات تطوير البرمجيات. ومع ظهور هذه المكونات في أثناء عملية تطوير التطبيق، سيتم التعرف بسهولة على وجود تعليمات برمجية ضارة. العوامل الثلاثة هي التعقيد والاتصال والتوسع. ومع تزايد

نمو نظام المعلومات بسرعة، يمكن العثور على السبب الرئيسي للعيوب الأمنية في شكل التعقد.

من منظور التعقد، فإن إدارة التعقيد المتعدد المستويات تفرض تحديات كبيرة. وبشكل عام، أدت هذه الفترة إلى تشتيت السلطة، وخاصة بعيداً عن الدول القومية. وفي عالم مليء بالترابطات المتبادلة والظواهر العابرة للحدود الوطنية والتعقيد المتسارع، تضاعفت قدرة الدول القومية على تعبئة الحدود المادية (والافتراضية) والتحكم فيها، وأنظمة الاتصالات والمالية، وحركة السلع والأشخاص. باختصار، فإن النماذج الحكومية الثابتة التي تركز على الدولة غير مجهزة بشكل جيد للتعامل مع هذه البيئة لأنها غير مرنة إلى حد كبير - تعوقها التسلسل الهرمي والهيكل البيروقراطية التي تحد من تدفق المعلومات، ومشاركة الجهات الفاعلة المتعددة، والقدرة على التغيير والتكيف بسرعة. (gandhi, 2014)

بالإضافة إلى ذلك، فإن سلوك النظام هو الأكثر إزعاجاً لمجال الأمن إذا تم الجمع بين التأثيرات المتتالية والمفاجأة. التأثيرات المتتالية هي تلك التي تنتج سلسلة من الأحداث التي تعبر الجغرافيا والوقت والأنظمة. مثل هذه التأثيرات شائعة في الأنظمة الأكثر ترابطاً وترابطاً (يشار إليها باسم الاقتران الوثيق). التأثيرات المفاجئة هي أحداث غير متوقعة، ولكنها أيضاً أحداث غير قابلة للمعرفة حقاً تنشأ عن التفاعلات بين الوكلاء وحلقات التغذية الراجعة السلبية والإيجابية الناتجة عن هذا التفاعل. (myriam dunn cavelty, 2011)

ثالثاً: الأنظمة السيبرانية كأنظمة معقدة

تعد الأنظمة السيبرانية عبارة عن ترابطات بين وحدات البرامج، وأسلاك الدوائر المنطقية، والرقائق الدقيقة، والأنترنت وعدد من المستخدمين (مستخدمي النظام أو المستخدمين النهائيين). يمكن تنفيذ هذه التفاعلات والجهات الفاعلة في نموذج محاكاة من أجل إجراء تحليل ماذا لو، والتنبؤ بتأثير تغيير المعلومات والتفاعلات بين الجهات الفاعلة في النموذج. (gunitsky, 2013, p. 39)

وقد تم استخدام نماذج التعقد لتحليل خصائص الأداء بناءً على خصائص التطبيق وسلوك المستخدم لفترة طويلة الآن - تستخدم بعض أدوات إدارة القدرة والأداء الشائعة هذه التقنية. يمكن تطبيق تقنيات مماثلة لتحليل استجابة الأنظمة السيبرانية للتهديدات، وتصميم بنية متسامحة مع الأخطاء وتحليل مدى المتانة الناشئة بسبب تنوع التنفيذ. (Armstrong, 2008)

وتعد أحد مجالات التركيز الرئيسية في النمذجة القائمة على الوكيل هي عملية "التعلم الذاتي" للوكلاء. في العالم الحقيقي، يتطور سلوك المهاجم مع الخبرة. يتم تنفيذ هذا الجانب من سلوك العميل من خلال عملية تعلم للعمالء، حيث تعد الخوارزميات الجينية واحدة من أكثر التقنيات شيوعاً لذلك.

في حين تعتمد عملية التعلم الذاتي للعمالء على "الطفرات" و"التقاطعات" - عاملان أساسيان في تنفيذ الخوارزمية الجينية -، تحاكي التقاطع بين الحمض النووي والطفرات في التطور البيولوجي لأشكال الحياة من خلال التقاطعات والطفرات، يتعلم العمالء من تجاربهم وأخطائهم الخاصة. يمكن استخدام هذه النماذج لمحاكاة سلوك التعلم لدى المهاجمين المحتملين، دون الحاجة إلى تخيل جميع حالات الاستخدام ورحلات المستخدم التي قد يحاول المهاجم من خلالها اختراق نظام سيبراني. (H. Holland, 1975)

يزعم البعض أن الأنظمة السيبرانية عبارة عن أنظمة تكيفية معقدة. وينبغي استكشاف المبادئ المستمدة من علم التعقد - المستوحاة من التفكير في النظم والعلوم الطبيعية (وهو منظور تم توظيفه على نطاق واسع من قبل العلوم الاجتماعية والمالية والاقتصاد وعلم الأوبئة) - لاستخدامها في الأمن السيبراني لتكملة الأساليب الأكثر تقليدية. مع وضع هذا في الاعتبار، يقدم "جارجان غاندي"، المهندس المعماري الرئيسي في Cognit Solutions، بعض الأساليب رفيعة المستوى، على الرغم من عدم تقديم تفاصيل التنفيذ. (H. Holland, 1975)

يُقدر التأثير الاقتصادي السنوي للجرائم الإلكترونية بأنه أعلى من تأثير تجارة المخدرات وبحسب بعض التقديرات، فهو ضعف التأثير الاقتصادي لهجوم 11 سبتمبر. وبينما ركزت المنظمات على أمن تكنولوجيا المعلومات لفترة طويلة

وأنفقت مبالغ ضخمة من المال، فإن الهجمات السيبرانية والأخبار عن اختراق الأنظمة بعيدة كل البعد عن أن تكون من الماضي. تم إنشاء حوالي 6.5 مليون برنامج ضار جديد عبر الإنترنت في الربع الأول من عام 2013.

إن الترابط بين الأنظمة، المتشابك مع عنصر بشري، يجعل أنظمة تكنولوجيا المعلومات غير قابلة للعزل عن العنصر البشري. واليوم أصبحت الأنظمة السيبرانية المعقدة لها حياة خاصة بها تقريباً؛ فالأنظمة السيبرانية عبارة عن أنظمة تكيفية معقدة. (H. Holland, 1975)

في أواخر عام 2020، تعرضت شركة SolarWinds لهجوم سيبراني ضخم يُعد من أكثر الاختراقات تعقيداً في التاريخ السيبراني الحديث. نجح المهاجمون في التسلل إلى سلسلة التوريد (Supply Chain) عبر تحديث برمجي ضار تم تثبيته على آلاف الأنظمة حول العالم. يُعد هذا الهجوم مثالاً على:

- الظهور (Emergence): فنتائج الهجوم لم تكن نتيجة فعل مباشر واحد، بل نتجت عن تفاعل عدد كبير من العوامل التقنية والتنظيمية.
- الاعتماد المتبادل (Interdependence): الاختراق أثر على مؤسسات حكومية وخاصة لأن الأنظمة كانت مترابطة بشدة.
- اللامركزية في التهديد: لم يكن هناك مركز واحد للهجوم بل امتدت آثاره عبر شبكة ضخمة من الضحايا.
- في العديد من الأنظمة الحديثة، تم اعتماد تقنيات الذكاء الاصطناعي للكشف المبكر عن التهديدات. ومن أبرز الأمثلة؛

- أنظمة SIEM (Security Information and Event Management) التي تدمج التحليل السلوكي في الوقت الحقيقي.

- خوارزميات تعلم غير مراقب (Unsupervised Learning) التي تكتشف الهجمات بدون الحاجة إلى بيانات مسبقة عنها (Mesjasz, 2006).

هذا النوع من الأنظمة يطبق فعلياً مبدأ التكيف الديناميكي ويعزز قدرة الأنظمة على التعلم من الأنماط المتغيرة.

الشبكات الاجتماعية كمساحات سيبرانية معقدة: أظهرت دراسات متعددة كيف يمكن استغلال الشبكات الاجتماعية لنشر المعلومات الكاذبة، التجسس، والهندسة الاجتماعية (Social Engineering) التهديد هنا لا يأتي من جهة واحدة بل من آلاف التفاعلات بين المستخدمين والمحتوى. من منظور التعقّد يصعب السيطرة على التفاعلات.

- تظهر اتجاهات سلوكية جديدة دون تدخل مركزي.
- يكون النظام حساساً لتغيرات صغيرة (مثلاً منشور فيروسي واحد يؤدي لانفجار معلوماتي).

• الشبكات الدفاعية الذكية: تعتمد على الذكاء الاصطناعي لتحليل الأنماط واكتشاف السلوكيات غير المعتادة.

• الأنظمة التكيفية: تُعدل استراتيجيات الحماية تلقائياً بناءً على التهديدات الجديدة.

• تحليل الشبكات: (Network Analysis) لفهم كيفية انتقال العدوى السيبرانية أو كيفية تشكّل الهجمات الجماعية.

إن أنظمة تكنولوجيا المعلومات اليوم مصممة ومبنية كما في حال المجتمع البشري من العاملين في تكنولوجيا المعلومات في منظمة بالإضافة إلى الموردين ولكن في المقابل يوجد ارتفاع لهجمات جديدة على أنظمة تكنولوجيا المعلومات كل يوم غير متوقعة؛ أحد الأسباب هو حقيقة أن أي نظام تكنولوجيا معلومات تم تصميمه من قبل آلاف الأفراد عبر مجموعة التكنولوجيا بأكملها من تطبيق الأعمال إلى مكونات الشبكة الأساسية والأجهزة التي يجلس عليها. وهذا يقدم عنصراً بشرياً قوياً في تصميم الأنظمة السيبرانية وتصبح الفرص متاحة في كل مكان لإدخال الثغرات التي يمكن أن تصبح نقاط ضعف. (Mesjasz, 2006)

تمتلك معظم المنظمات طبقات متعددة من الدفاع لأنظمتها الحرجة (طبقات من جدران الحماية، ونظام اكتشاف التسلل، ونظام التشغيل المعزز، والمصادقة القوية وما إلى ذلك)، ولكن الهجمات لا تزال تحدث. في أغلب الأحيان، تكون عمليات اقتحام الكمبيوتر نتيجة تصادم الظروف وليس ثغرة قائمة بذاتها يتم استغلالها لنجاح هجوم سيبراني. بعبارة أخرى، فإن "الكل" من الظروف وأفعال المهاجمين هو الذي يسبب الضرر.

ولكن هذا هو المدى الذي يمكن أن تساعد فيه وجهة النظر الاختزالية في تفسير سلوك النظام. عندما يتعلق الأمر بالأنظمة الناشئة مثل السلوك البشري، والأنظمة الاجتماعية والاقتصادية، والأنظمة البيولوجية أو الأنظمة الاجتماعية السيبرانية، فإن النهج الاختزالي له حدوده. لا يمكن التنبؤ بأمثلة بسيطة مثل جسم الإنسان، أو استجابة الغوغاء لحافز سياسي، أو رد فعل السوق المالية على أخبار الاندماج، أو حتى الاختناقات المرورية - حتى عند دراستها بالتفصيل. . (Mesjasz, 2006)

تقليدياً، كان هناك نهجان مختلفان ومتكاملان للتخفيف من التهديدات الأمنية للأنظمة السيبرانية والتي تُستخدم اليوم في معظم الأنظمة العملية، يعتمد هذا النهج بشكل أساسي على فريق الاختبار لأي نظام تكنولوجيا معلومات لاكتشاف أي أخطاء في النظام يمكن أن تكشف عن ثغرة يمكن للمهاجمين استغلالها. يمكن أن يكون هذا اختباراً وظيفياً للتحقق من أن النظام يعطي الإجابة الصحيحة كما هو متوقع، واختبار الاختراق للتحقق من مرونته في مواجهة هجمات محددة، واختبار التوافر / المرونة. نطاق هذا الاختبار هو عمومًا النظام نفسه، وليس الدفاعات الأمامية التي يتم نشرها حوله.

إن هذا النهج مفيد للأنظمة المستقلة البسيطة إلى حد ما حيث تكون رحلات المستخدم المحتملة واضحة إلى حد ما. وبالنسبة لمعظم الأنظمة المترابطة الأخرى، فإن التحقق الرسمي وحده ليس كافياً لأنه من غير الممكن أبداً اختبار كل شيء". (gandhi, 2014, pp. 5-6)

إن أتمته الاختبار هي نهج شائع لتقليل الاعتماد البشري على عمليات التحقق، ولكن كما أثبتت "مشكلة التوقف وعدم القدرة على اتخاذ القرار" لآلان تورينج - فمن المستحيل بناء آلة تختبر آلة أخرى في جميع الحالات. الاختبار ليس سوى دليل قصصي على أن النظام يعمل في السيناريوهات التي تم اختباره من أجلها، وتساعد الأتمته في الحصول على هذا الدليل القصصي بشكل أسرع.

قد تثبت الأساليب التي تستخدم علوم التعقد أنها مكتملة تماماً للطرق الأكثر تقليدية. إن تعدد استخدامات أنظمة الكمبيوتر يجعلها غير متوقعة أو قادرة على السلوك الناشئ الذي لا يمكن التنبؤ به دون تشغيلها. كما أن تشغيلها بمعزل في بيئة اختبار ليس مثل تشغيل نظام في البيئة الحقيقية التي من المفترض أن يكون فيها، حيث أن تصادم الأحداث المتعددة هو الذي يسبب السلوك الناشئ الواضح (تذكرنا بالكلانية "holism"). (gandhi, 2014, p. 6)

طالما أن بيانات الإدخال والوظيفة التجارية للتنفيذ متماثلتان، فإن أي انحرافات في استجابة التنفيذ هي علامة على هجوم محتمل. إذا تم تنفيذ بنية قائمة على الخدمة الحقيقية، فقد يكون لكل "خدمة" تنفيذات متعددة (ولكن عدداً صغيراً) غير متجانسة ويمكن للوظيفة التجارية الإجمالية اختيار تنفيذ الخدمة التي تستخدمها بشكل عشوائي لكل طلب مستخدم جديد. يمكن تحقيق عدد كبير إلى حد ما من مسارات التنفيذ المختلفة باستخدام هذا النهج، مما يزيد من مرونة النظام. (gandhi, 2014, p. 7)

تم تطوير بيئات تنفيذ متعددة المتغيرات (MVEE)، حيث يتم تنفيذ التطبيقات ذات الاختلافات الطفيفة في التنفيذ في خطوة واحدة ويتم مراقبة استجابتها للطلب. وقد أثبتت هذه البيئات فائدتها في اكتشاف التطفل في محاولة لتغيير سلوك الكود، أو حتى تحديد العيوب الموجودة حيث تستجيب المتغيرات بشكل مختلف لطلب ما.

وعلى نفس المنوال، وباستخدام مفهوم البرمجة بإصدار N14، تم تطوير برنامج مكافحة فيروسات بإصدار N في جامعة ميشيغان، والذي كان له تطبيقات غير متجانسة تبحث في أي ملفات جديدة عن توقيعات فيروسية مقابلة. وكانت

النتيجة نظاماً أكثر مرونة لمكافحة الفيروسات، وأقل عرضة للهجمات على نفسه، مع تغطية اكتشاف أفضل بنسبة 35 في المائة في جميع أنحاء العقار. (gandhi, 2014)

خاتمة:

في ضوء ما تقدم، يمكن استخلاص مجموعة من النتائج:

- تستلهم نظرية التعقد إلى حد كبير من الأنظمة البيولوجية وقد تم استخدامها في العلوم الاجتماعية وعلم الأوبئة في دراسة والأنظمة الاقتصادية والأسواق الحرة على حد سواء واكتسبت قبولاً لتحليل المخاطر المالية أيضاً. وفي المقابل هناك قبول متزايد للتفكير المعقد في العلوم التطبيقية والحوسبة في مجال الأمن السيبراني.

- الأمن السيبراني لا يمكن التعامل معه كمسألة تقنية فقط، بل هو منظومة متكاملة من الأبعاد التقنية، الاجتماعية، التنظيمية، والاقتصادية.

- يُبرز تبني التعقد في الأمن السيبراني تحولاً جذرياً في كيفية فهم التهديدات الرقمية والتعامل معها، حيث يصبح الأمن ليس فقط جداراً منيعاً، بل شبكة ذكية متكيفة، تتعلم من داخلها وتعيد تشكيل نفسها باستمرار. ويُمثل هذا المنظور فرصة استراتيجية لبناء منظومات أكثر مرونة واستجابة، في عالم أصبحت فيه التفاعلات الرقمية أكثر كثافة وتعقيداً من أي وقت مضى.

- طبيعة التهديدات السيبرانية معقدة ومتغيرة باستمرار، مما يجعل النماذج التقليدية غير كافية وحدها لمواجهتها.

- الفضاء السيبراني هو نظام تفاعلي معقد، تتولد فيه الظواهر الأمنية نتيجة لتفاعلات متعددة المستويات: بشر، دول، أدوات، بيانات، شبكات.

قائمة المراجع:

- alexander mcleod, r. c. (2008). modeling security vulnerabilities using chaos theory: discovering order, structure and patterns . *chaotic behavior in complex systems*. lasvegas.
- Armstrong. (2008). *Motivation for the Study and Simulation of Cybersecurity as a Complex System*.
- gandhi, g. (2014, may). complexity theory in cyber security. *university of warwick*, 195(14).
- gunitsky, s. (2013). complexity and theories of change in international politics. *international theory*, 5(1).
- H. Holland. (1975). *Adaptation in natural and artificial systems: An introductory analysis with applications to biology, control, and artificial intelligence*. Michigan: University of Michigan Press.
- hendrick, d. (2009). *complexity theory and conflict transformation: an exploration of potential and implications*. oxford: centre for, conflict resolution departement of peace studies.
- johan eriksson, giampiero giacomello. (2007). london: centre for security studies routledge.
- Kavalski, E. (2015). *World politics at the edge of chaos: Reflections on complexity and global life*. New York : University of New York Press Albany: State .
- luis, t. (2010). security and security complex: operational concepts. *journal of international relations*, 1(1).
- Mesjasz, C. (2006). *Complex systems studies and the concepts of security* . Poland: Cracow University of Economics, Cracow.
- myriam dunn cavelty, j. g. (2011). *complexity or the governance of the inherently unperdiactable*. ISN.
- n.rosenau, j. (1994). new dimensions of security: the interaction of globalizing and localizing dynamics. *security dialogue*, 25(3).
- Neil e, h. (2006). *complexity in world politics: concepts and methods of a new paradigm*. new york: state university of new york.

Rosenau, J. N. (1990). *Turbulence in World Politics; A Theory of Change and Continuity*. Princeton: Princeton University Press.

seven trends that will shape global security. (2023). Récupéré sur <http://www.prosgur.com/en/innovation/security/seven-trends-that-willshape-global-security>.

الدوحة: (ط1.éd.)مدخل إلى نظرية التعقد في العلاقات الدولية. (2021). حمشي, م
المركز العربي للأبحاث ودراسة السياسات