# الرؤية الإستراتيجية للأمن الوطني العراقي في الفضاء السيبراني
# (( مقاربة بين المعضلة الأمنية والمكنَة الأدائية))

# Strategic Vision for Iraqi National Security in Cyberspace
# ((Approach between the security dilemma and performance machinery))

**أ.م.د.حازم حمد موسى***

**كلية العلوم السياسية/ جامعة الموصل/العراق**

**Email: hazim@uomosul.edu.iq**

**Email: hazim_aljanabi79@yahoo.com**

تاريخ الإرسال: 16-07-2020 تاريخ القبول: 14-11- 2020 تاريخ النشر: ديسمبر 2020

---

**الملخص**

ركز البحث على مكّنة بناء رؤية استراتيجية للأمن الوطني العراقي في ظل تأثير الفضاء السيبرانيالذي فاقم من حجم المعضلة الأمنية، والتعريف بها وبيان أسباب اعتمادها، وإثبات قدرتها على تحجيم المعضلات الأمنية المعلوماتية التي يتعرض لها العراق والتي أثرت عليه جيو-استراتيجياً وجيوبوليتيكياً ، بعد الارتكاز على القواعد والمسلمات العلمية-التقنية للتعامل مع معضلات الأمن السيبراني، مع الإشارة إلى حقيقة تمكين القائمين على الأمن السيبراني، لطمر فجوة الانكشاف الاستراتيجي بسبب المعضلات الأمنية، وسيجيب البحث عن التساؤل الأساسي الآتي: هل يمكن للرؤية الاستراتيجية إن تفسر المعضلات الأمنية في ظل الفضاء السيبراني الذي أوجده التغيير الدولي وتحقق طفرة في الأمن السيبراني العراقي؟

**الكلمات المفتاحية:** (الرؤية الاستراتيجية ،الأمن الوطني العراقي ، الفضاء السيبراني ، المعضلة الأمنية)

**Abstract**

The research focused on the possibility of building a strategic vision for the Iraqi national security in light of the influence of the digital actor, which exacerbated the size of the security dilemma, to identify and explain the reasons for its adoption, and to prove its ability to curtail the security dilemmas facing Iraq, which affected him geo-strategically and geopolitically, after focusing on The scientific and technical rules and axioms to deal with cybersecurity dilemmas, with reference to the fact that cybersecurity practitioners are empowered to bridge the gap of strategic exposure due to security dilemmas, will answer the basic question: Yeh explain security dilemmas in light of cyberspace created by the international change and achieve a breakthrough in cyber security?

**Keywords** (strategic vision, Iraqi national security, cyberspace, security dilemma).

***المؤلف المرسل: أ.م.د.حازم حمد موسى الجنابي / كلية العلوم السياسية/جامعة الموصل**

**المقدمة:**

إن البحث في تشكيل الأمن الوطني العراقي، وطرق تحقيقه في مرحلة ما بعد التغيير العالمي المعلوماتي المتسارع، أمراً يصعب إدراكه دون بناء رؤية استراتيجية لإدراك الحراك العالمي المعلوماتي والتعامل معه لتجنب التهديد المعلوماتي وقائياً واستباقياً ، وهذا يفضي لتوصيف مجرى ظاهرة تشكيل الاستراتيجية الأمنية، إذ يعد إدراك المعضلة الأمنية العامل الحاسم والجوهري لتمكين الأداء الاستراتيجي، عبر دورها المهم في تحديد نوع التشكيل الأمني، بالإضافة إلى دورها المهم كمحدد رئيس للتعامل مع حراك التهديد الأمني.

ومن هذا المنطلق، حاول الباحث شق طرائق خاصة توصف كيفية تشكيل الأمن العراقي في ظل الفضاء السيبراني بعد أن تزاحمت طرق البحث والدراسة فيما يخص المعضلة الأمنية وطرق تقاربها وتنافرها مع المكّنة الأدائية، لذا وجد الباحث من الضروري أن يذكر بعض المفردات المهمة قبل الولوج في تفاصيل البحث لتكون له دليلاً في البحث،ولعل أهم تلك المفردات، هي:

- **الأهمية:** تكمن الأهمية في المكانة التي احتلتها المعضلة الأمنية في المدرك الاستراتيجي العراقي بحثاً رؤية استراتيجية لبناء المكّنة الأدائية لاستدامة الأمن لا بناءه فحسب، والتي وظفت من القوى خارجية فاربك الاستقرار، وما زاد الأهمية أهمية هو "الفضاء السيبراني" (الفضاء المعلوماتي) الذي عده الكثيرون تهديد يستغله المناوئين للعب دور مؤثر سلباً على الأمن الوطني.
- **<u>الإشكالية:</u>** وتكمن في إنهناكعلاقةتقاربية-تفاعليةبينالمعضلةالأمنيةوالتمكينالأدائيفيالفضاءالسيبراني، والتي ولدت مفارقة أدائية في تفاعلات الأمنية هي: هل المعضلة الأمنية تنتج التطور الأمني أم التطور الأمني ينتج المعضلة الأمنية، وتلك هي مفارقة حقيقية.
- **<u>التساؤلات</u>:** يحاول الباحث الإجابة عن السؤال الرئيس التالي: من الأكثر شيوعاً المعضلة الأمنية أم المكّنة الأدائية في الاستراتيجية الأمنية العراقية؟

وينبثق من هذا السؤال الأسئلة الفرعية التالية:

1. ما هي الرؤية الاستراتيجية الأمنية؟
2. ما هو الأمن العراقي السيبراني؟
3. ما هي المعضلة الأمنية السيبرانية؟
4. وما هي العلاقة بين الأمن السيبراني والتهديد السيبراني ؟
5. وما هي الآلية التي يتشكل عن طريقها الأمن السيبراني العراقي؟
6. وما هو مستقبل الأمن الوطني العراقي في ظل الفضاء السيبراني العالمي والإقليمي؟

- **الأهداف:** يسعى الباحث عن طريق البحث إلى تحقيق جملة من الأهداف وعلى النحو الاتي:

1. التعرف على ماهية المعضلة الأمنية وطبيعتها.
2. الوقوف على الأسباب المفضية إلى التهديد السيبراني.
3. تحديد أعراض وآثار التهديد السيبراني والتعرف على أبعاده.

4. استعراض النماذج والمقاييس الأسس الشهيرة في الأدب الأمني حول المعضلات.
5. الوقوف على دور القائمين على الأمن في الوقاية والعلاج لظاهرة التهديد السيبراني.
6. الوصول إلى تحديد المسؤولية في مواجهة التهديد السيبراني واقتراح أفضل السبل لمواجهته.

❖ **الفرضية:** استندنا على فرضية مفادها: ((كلما اعتمد القائمين على الأمن العراقي على الرؤية الاستراتيجية، ازدادت إمكانية السيطرة على المعضلات الأمنية في الفضاء السيبراني)). وسنحاول إثباتها أو تفنيدها في نتائج البحث.

❖ **النطاق:** يتحدد بـ:

1. **موضعياً:** بظاهرة الرؤية الاستراتيجية الأمنية السيبرانية من حيث فلسفتها وطبيعتها ومسبباتها ونماذجها وأثارها، وشكلياً اقتصرت على الأمن السيراني مقابل التهديد السيراني ضمن مفهومين هما: المعضلة الأمنية، المكّنة الأدائية.
2. **الحدود المكانية:** اقتصر البحث على الساحة العراقية وبالتحديد الأمن الوطني السيبراني.
3. **الحدود الزمانية:** ركز البحث على حقبة ما بعد التغيير العراقي2003.

❖ **مصطلحات الدراسة:** بداية لابد من توضيح بعض المفاهيم ومنها:

1. **الرؤية الاستراتيجية الأمنية**(Strategic Security Vision): هي الأدراك الاستراتيجي لتوظيف القدرات والإمكانات الأدائية لبناء واستدامة الوسائل الأمنية لتحقيق الأمن المستدام،فهي إدراك لما قد يحدث امنياً،إدراك لما يمكن إنلهمالأخرينبه امنياً لمواجهة المعضلات الأمنية، ليتقبلوا ذلك، فالتسويق الأمني، وسيلة جذب للأنموذج المقصود، أي هندسة الأمن استراتيجياً.
2. **الأمن الوطني** (National Security):هو توفير الحماية للمواطنين، والأفراد المتواجدين على أراضي الدولة، بمعنى، بناء الخطط واستخدام الإمكانات والوسائل الأمنية للمحافظة على سير الحياة اليومية بشكل صحيح، وبعيداً عن وقوع أية أزمات تؤدي إلى التسبب بضرر، لمكونات المجتمع البشرية والمادية.
3. **الأمن لسيبراني** (Cybersecurity، بناء الخطط واستخدام الإمكانات والوسائل التقنية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.
4. **الفضاء السيبراني** (Cyberspace): هو التعامل مع العالم عن طريق شبكة الإلكترونية لها استقلاليتها من الداخل وتقوم بنيتها الأساسية على التقنيات الحديثة وهي كذلك أنظمة التعامل مع الحاسوب .
5. **المعضلة الأمنية**(The security dilemma):هي الحالة التي تتسبب فيها الإجراءات التي تتخذها الدولة لزيادة أمنها في ردود أفعال من دول أخرى تؤدي إلى انخفاض في أمن الدولةبدلاً من زيادته.
6. **المكنّة الأدائية** :(Performance machine ) القدرةُوالاستطاعةُ، والقوَّةُ والشِّدّة.

❖ **المنهجية** :استخدم الباحث المنهج الاستشرافي الذي يركز على استشراف تأثير المعضلات الأمنية الرقمية على العراق وسبل التأهيل والتمكين الأدائي الذي يثيره موضوع البحث، والتطرق إلى اهم متطلبات بناء الرؤية الاستراتيجية للأمن المعلوماتي لضمان استدامة الاستراتيجية الأمنية.

❖ **الهيكلية:** يتكون البحث الموسوم ((الرؤية الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني: مقاربة بين المعضلة الأمنية والمكَنة الأدائية)) : من مقدمة ومبحثين رئيسين :الأول حمل عنوان : الأمن بين المعضلات والممكنات السيبرانية، وبدوره انقسم إلى مطلبين: الأول: اختص بالمعضلة الأمنية السيبرانية، أما الثاني:اختص بـالمكّنة أدائية الأمنية، وتناغماً مع ما مضى،جاء العنوان الثاني: فعنون بـ: الأمن الوطني والفضاء السيبراني، لينشطر إلى: أسسبناء الأمن السيبراني، والثاني: ركز على: المقاربة بين الأمن والتهديد في ظل الفضاء السيبراني، لنختم البحث بجملة من النتائج والتوصيات.

**المبحث الأول**

**الأمن بين المعضلات والممكنات السيبرانية**

يصعب تصور، أو أدرك، المعضلات الأمنية لسيبرانية لاكتظاظها بالمحفزات الدافعة لاختراق الأمن الوطني من الفجوات الرخوة، والذي بدا فيها التهديد في أوجه، لهذا بدت صعبة التشخيص والعلاج على الكثير من المعنين بها، لما تضمن من تداخل بين التهديد الواقعي والتهديد الافتراضي فانعكست سلباً على العراقيين ساسة وشعب، بعد أن لم يتمكن صناع الأمن السيبراني من حرف مسار التهديد السيبراني بالاتجاه المطلوب لفقدانهم الأدراك الاستراتيجي الرقمي، فاهتز هيكل الأمن وهيمن التهديد الرقمي، وشاع الصراع والنزاع والعنف الرقمي.

ولعل أفضل ما يفسر تلك الجدلية، هو البحث عن مصدر المعضلات الأمنية ومعرفة سبب استفحالها، فسجلات الأمن العراقي،أشرت ذلك المفهوم،وما أداه من دور في إعادة رسم الخارطة الجيو-سكيورتية بين حقبة وأخرى، فالواجب علينا أن نتصفح تلك السجلات ممعنين النظر بها، في محاولة منا لتقييم الوضع الأمني ووضع رؤية استراتيجية لمستقبل الأمن العراقي السيبراني،ولأجل أبانت هذا كله عمد الباحث إلى تقسيم المبحث على مطلبين وعلى النحو الاتي:

**المطلب الأول**

**المعضلة الأمنية السيبرانية**

تتمثل التهديدات الإلكترونية (السيبرانية) بتحديات غير مرئية توثر على منظومة الأمن، [1]ففي عصر التكنولوجيا أصبح لأمن المعلومات الدور الأكبر لصدّ أي هجوم الإلكتروني ومنعه من إحداث أضرار على منظومات الحماية الأمنية الذي تتعرض له أنظمة الدولة المختلفة، وحماية الأنظمة التشغيلية من أي محاولات للولوج بنحو غير مسموح به لأهداف غير سليمة، فالتطور التكنولوجي الذي شهده العراق في مجال المعلومات والاتصالات بعد عام 2003 تزامن معه ضعف الأمننة الإلكترونية وركاكة البنية التحتية أدى إلى أن يصبح العراق منكشفاً استراتيجياً لكثير من دول العالم، يسهل اختراقه والتجسس على المعلومات المؤسساتية،[2]لدرجة استخدام العراق كساحة لشنّ الهجمات الإلكترونية لضرب أمن معلومات دولأخرى واختراق منظومتها الأمنية الإلكترونية، فضلاً عن استراق أي معلومة واستخدامها لأغراض المساومة؛ أي: لتنفيذ عمليات هكرية وإسنادها، ومن الملاحظ أن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق إذ يشكل

---

[1]Richard A. Clarke and Robert K. Knake. Cyber War: The next threat to National Security and what to do about it. (New York: Ecco HarperCollins 2010), 228.

[2]A false sense of security؟ Cybersecurity in the Middle East, Global State of Information (-Journal Security, March 2016),p4.

هذا الإجراء خرقاً لأمن المعلومات العراقي[1]، ولتلافي مثل هذه الخروقات الكبيرة التي تتعرض لها حركة المعلومات في العراق يتوجب بناء منظومة متكاملة لأمن المعلومات؛ لذا يتوجب بناء منظومة للأمن الإلكتروني العراقي بهدف حماية الفضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية، وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية امن المواطنين وامن المؤسسات من مخاطر الفضاء السيبراني[2].

ويُعَدُ التهديد السيبراني حافزاً لإعادة صياغة الأمن السيبراني، فالمعضلة الأمنية تفسر التفاعلات الاستراتيجية واللوجستية الأمنية، لاسيما بين الأجهزة المعنية في بناء واستدامة الأمن وهذا يتطلب ادارك التهديد السيبراني وفقاً لنهج الأمن السيبراني، على الرغم من الجهود المبذولة في بناء الأمن الوطني العراقي سيبرانياً، الآن تلك الجهود لا تزال متواضعة بمقياس العالم الرقمي إن ادراك التهديد هو عامل مهم للغاية لأمننته، وهذا يتطلب التسويق الإعلامي والتوجيه الخطابي، ويتأثر الأمن بالتهديد السيبراني كلما زاد التفوق التقني، والقدرات الهجومية الرقمية،والهيمنة الإعلامية الرقمية [3].

والسؤال الرئيسي هو: كيف يستجيب العراق للتهديدات السيبرانية؟ والجواب: يستجيب عن طريق التحالف مع الآخرين ضد التهديد السيبراني السائد، ويمكن أن نؤكد ذلك، "بمقاربة العراق مع الدول التي تعد التهديد هو الأكثر شيوعاً من الأمن في الفضاء السيبراني، فلو تم استعرض التفاعلات الأمنية السيبرانية في الشرق الأوسط لوجدنا أنها تفاعلات محملة بالمعضلات لعدم وجود غطاء استراتيجي يؤمنها من الاختراق والعراق جزء من الشرق الأوسط ومعضلاته متقاربة، فهو متأثر بالانكشاف الاستراتيجي في الفضاء السيبراني، فالعراق دون رؤية استراتيجية أكثر عرضة للمعضلات الأمنية لسببين:الأول: عدم مواكبة الطفرات التقنية العالمية، والثاني: الاعتماد على القوى الإقليمية والدولية في مجال الدعم التقني- الأمني [4].

ولأن بناء المكّنة التقنية لجميع الدول امر غير منطقي – بلغة السياسية الدولية،فيعمل صناع التقنية على التحالف مع مستهلكي التقنية وتوريطهم بمخاطر التهديد، عندها يبحثون عن تشكيل الأحلاف ليدخلوا بوابة التفاعل الدولي لمواجهة

---

[1] Midea S Ali, A Brief Review of Cybersecurity Issues in Iraq,Technical Report ,(University Sains Malaysia, April 2018),p5.

[2] Sattar J. Aboud, Cybercrime in Iraq,(International Journal of Scientific and Engineering Research Vol. 5,No. 2,2018),p. 63-64.

[3] ويهدف هذا الأمن إلى حماية خطوط الاتصالات الرقمية على تنوعها وحماية الشبكات المحلية والعالمية من الاختراق الذي يتسبب في تدمير البنى التحتية لنظم المعلومات من أجهزة ومعدات وحتى برمجيات مختلفة في مجال المال والطاقة والإحصاء وغيرها، عن طريق الاختراق (التهكير) أو اختراق الأنظمة المالية وتحويل الأرصدة وسرقتها،لمزيد من التفاصيل ينظر :

Barbora Bukovska, Iraq: Draft Informatics Crimes Law, (London, Free Word Centre, Farringdon), October 2011,p11.

[4] اعلن مركز الإعلام الرقمي، الأحد، إن الترتيب الذي حصل عليه العراق في تقرير المؤشر العالمي للأمن السيبراني "متواضع"، وقال المركز في بيان تلقت، السومرية نيوز، نسخة منه، إن "التقرير الأخير الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة وضع العراق في المركز 107 عالميا للأمن السيبراني، والـ13 عربيا، وسبقته في هذا الترتيب عدة دول عربية لا يمكن مطلقا مقارنة موازناتها المالية بالعراق من بينها السودان وفلسطين والأردن" ، السومرية نيوز/ بغداد / 31/ 2019/3.

التهديد، فيسود اعتقاد لدى صناع القرار المعنيين بالتهديد إن الإذعان لإحدى القوى الفاعلة في النظام الدولي هو من يوفر لهم الأمن السيبراني، وهذا حال قوى الشرق الأوسط مع القوى الدولية والعراق من ضمنهم، وتلك اكبر معضلة[1].

فاذا ما تطرقنا إلى معضلات الأمن العراقي، نجد أن مصادر مختلفة من التهديد تساعد في تفسير سبب التحالف الأمني مع القوى العظمى (الولايات المتحدة الأمريكية، وروسيا، والقوى الأوربية) فضلاً التحالفات الأمنية الإقليمية في الشرق الأوسط، فالتفاعل والأمني الإقليمي والدولي ولد الكثير من المعضلات من بينها تشخيص وتسميه وتتبع الجرائم الإلكترونية مثل جرائم التسويق الإعلامي والتجنيد الإلكتروني للمنظمات والحركات الإرهابية وهي معضلة حقيقية للأمن العراقي [2].

فالتهديد السيبراني يفسر لنا لماذا العراق يتحالف مع القوى الفاعلة في الفضاء السيبراني ففي كثير من الأحيان، إذ كانت الأهداف من التحالفات مواجهة معضلة التهديد الإلكترونية، لكن التحالف يمكن قراءته بصورة أخرى في حال تحالف مع الجوار الإقليمي مع القوى الدولية الفاعلةفي المجال الإلكتروني المتناقضة مع بعضها امنياً، ليكون باني الأمن السيبراني العراقي في معضلة حقيقية هي إن الحلفاء له خصماء مع بعضهم امنياً مما يجعله قاعدة لعمليات سيبرانية تخريبية؛ كون الأمن السيبراني يعاني من معضلة الانكشاف الاستراتيجي للحلفاء وتلك معضلة كبرى، فالقوة الإقليمية مكانتها وهيبتها الإقليمية تأخذها من تكامل امنها واستدامته؛ كونه مقياس لقوة الدولة، فمن يحظى بأمن سيبراني رصين يمتلك مقومات المكانة والهيبة الدولية[3].

وهذا يوصلنا إلى نتيجة هي :إن التفاعلات الأمنية العراقية أمام خياريين لا ثالث لهما هما السير نحو امتلاك التقنية لبناء الأمن المعلوماتي، أو السير نحو التحالف السيبراني لحل المعضلات الأمنية والخيار الأول توازن امني ، والخيار الثاني : إذعان امني ، فالدولة القوية تقنياً الآمنة امنياً تسلك سلوك تفاعلي مع نظيراتها من منطلق استراتيجي امني، والقوى الضعيفة غير الآمنة تسلك سلوك الإذعان للقوى الفاعلة لمواجهة مصدر التهديد المعلوماتي؛ كون الضعفاء تقنياً اكثر حاجة للأقوياء تقنياً للضمان والحماية الأمنية[4] .

لهذا، إن العراق حالة من حال الدول المتفاعلة في الشرق والتي تواجه التهديد السيبرانيب التحالف مع القوى الأكثر امتلاك لتقنية الأمن السيبراني، فالدولة الأقوى بالقدرات التقنية صاحبة المصداقية في التهديد والحماية، تزيد من تفاعل القوى الأضعف تقنياً للاذعان لها، والقدرة التقنية للدولة القوية، تزيد ميل القوى التقليدية لتتماشى مع تلك القوى ومسايرتها، فكلما ازدادت القدرات الهجومية الإلكترونية للقوة القوية، يزيد من القوى الأخرى الأضعف للاذعان لها،وهذا يفضي إلى إن العراق يتفاعل مع القوى الإقليمية والدولية تفاعل تعاون إيجابي لصد التهديدات والهجمات الإلكترونية، فيلجأ إلى التحالفات التي تتشكل منظومته الأمنية ، فالمعضلات الأمنية صناعة القوى الدولية مالكة التقنية المتحكمة في الفضاء

---

[1] حسين باسم عبد الأمير، تحديات الأمن السيبراني، مقال منشور (قسم الدراسات السياسية/ مركز الدراسات الاستراتيجية- جامعة كربلاء)،آيار/2018،ص 1.

[2] Ali Ziad al-Ali,The Hidden Threats to Iraq's National Security,article in National security and defense, 07/10/2018,pp2-3.

[3] Colonel Jayson M. Spade, Chins Cyber Power and Americas National Security, Information as Power, (U.S. Army War College, May 2012),pp 2-3.

[4] Tallinn, Economic Aspects of National Cyber Security Strategies, Project )Report , 2015),p7

السيبراني،فالتهديدات التي تستهدف الأمن السيبراني العراقي بعد 2003 أصبحت في أو جذروتها من اختراقات لبعض المواقع الحكومية، أخر اختراق كان قد نبه له نائب رئيس الجمهورية السابق السيد أياد علاوي حينما بين، خلال مقابلة تلفزيونية، في نيسان 2018 " أن اعتماد نظام الأقمار الصناعية في عملية التصويت خلال الانتخابات المقبلة، امر مشكوك فيه لأن من المعروف إن هذه الأقمار تدار من قبل دول خارجية ولا يمكن التحكم بها من العراق، كما إن إمكانية اختراقها والتلاعب بنتائجها من قبل جهات خارجية كبيرة جداً "،متسائلاً "ما هي الآلية التي وضعت لضمان عدم حصول خروقات"[1].

**المطلب الثاني: المكنّة الأدائية الأمنية**

إنالمعضلات الأمنية الرقميةبحاجة إلى إمكانيات ووسائل احترازية (وقائية واستباقية وإجهاضيه) لتقويض المعضلة الأمنية أو على الأقل تحجيمها، وهذا يتطلب التأسيس لبنية تحتية الإلكترونية ترصن مقومات الأمن السيبراني، وتمكنه لمواجهة مصدر التهديد، فكلما ازدادت القدرات التقنية الداخلية ارتفعت القدرة لمواجهة التهديدات الإلكترونية الخارجية، كلما زاد تمكّنة القائمين على الأمن لتشكيل منظومة أمنية متكاملة لإفراغ التهديد من طاقته، وهذا يتطلب بناء رؤية استراتيجية أمنية تضع البرامج وتوظف الإمكانات وتستخدم كافة الوسائل لتحقيق هدفها وهو بناء واستدامة الأمن الوطني؛كونإن التهديد السيبراني يدفع باتجاه التفاعل الأمني الرقمي المتسارع[2].

فكلما ازداد حجم المعضلات أزادت الحاجة لبناء القدرات والإمكانات التقنية-الأدائية، وهذا يفضي إلى زيادة التفاعل الأمني برؤية استراتيجية تناظر القوى صاحبة التهديد أو تفوقها لتحقيق الأمن وكما إن البعد الجيوبوليتكي من القوى الدولية الفاعلة رقمياً، لا يقود إلى إيجاد دولة اكثر أماناً كون المعلومات حولة العالم إلى قرية ذكية؛ كون الفضاء السيبراني نسف كل نظريات القوة التقليدية، فالحرب أصبحت حرب غير مرئية، فكلما ازدادت التهديدات التقنية زيادة غير طبيعية مقارنة بحجمها، كلما أزادت الحاجة لبناء المكّنة التقنية لضمان امنها، ولردع التهديد وتحجيم قوته وإرجاعه لوزنه الطبيعي هو استباقها بالإمكانات ووسائل الحماية سيبرانياً ، ولذلك، فإن العراق لا بد له السعي ليكون مالك للتقنية الأمنية السيبرانية وان واجهته بعض المعضلات من معسكر الكبار الرقمي لابد هنا من تشكيل دفاعات أمنية الإلكترونية، فالدول التي تظهر نواياها العدوانية رقمياً تحفز القوى التي تستشعر التهديد للتوازن معها عن طريق تحالف المهُددين، بغية الوصول إلى حالة توازن القوى هي الحالة الطبيعية التي يتم التفاعل الدولي الإلكتروني عن طريقها لتحقيق التوائم الأمني فالتوازن الرقمي يخفض من مستويات العدوان ويحقق الأمن الدولي السيبراني[3] وهذا الأمر اصبح ضرورة لا اختيار بعد إن سجل العراق نسبة مرتفعة في الجرائم الإلكترونية عدد فاذا لاحظنا مؤشر الجرائم الإلكترونية لوجدنا لا يقل عن 60% وهذه نسبة كبيرة [4]

---

[1] زاهر الزبيدي، تهديدات افتراضية للأمن السيبراني العراقي، شبكة النباء، الأثنين 27 تشرين الثاني 2018.

[2]Jerry Brito & Tate Watkins, Loving The Cyber Bomb؟ The Dangers of Threat Inflation Incybersecurity Policy, (Aprile-2011), p14.

[3]Brahima Sanou, Global Cybersecurity Index (GCI),( ITU Cybersecurity Team ,2017),p42-43.

[4]Sattar J. Aboud,An Overview of Cybercrime in Iraq, The Research Bulletin of Jordan ACM , Vol.11 ,No.11,(June 2012), p31-32.

إنا لعراق بحاجة إلى امتلاك ممكنات الأمن السيبراني، إذ يميل إلى تشكيل منظومة أمنية ذات جودة ودقة عالمية، فالإمكانات بحاجة إلى معنيين- تقنيين تتقارب تلك المنظومة بفروعها لتشكل هرم امني-معرفي-تقني،وهذا يفضي بطبيعة الحال إلى إن تكون المؤسسات أكثر أمنا لحصانتها الذكية، ويزداد تأثيرها التقني على الأمن، فيظهر حوار التقنيات المتناغمة، أو صراع التقنيات المتضادة، مما يدفع القوى التقنية الصغرى التي تفتقر إلى مكّنة الأداء التقني والتي ستكون أكثر عرضة للتهديد للبحث عن التحالفات التقنية لزيادة قوتها وتأمين وجودها، فتتلون بلون التقنية الكبرى، وهنا، نستدل على إن هناك تأثير للتقنيات على اختيار الشركاء الأمنيين،فالعراق امنياً يبقى ضعيف ما لم يتحالف مع القوى التقنية العالمية، وتحالفها يكون تحالف تمكي[1].

ومن المتعارف عليه في السياسة الأمنية، كلما ازدادت المساعدات التقنية المقدمة من القوى الكبرى-تقنياً إلى الأخرى الضعيفة-تقنياً ، كلما زاد احتمال أن تشكيل تحالف امني بينهم، ويكون التحالف بهذه الصورة تحالف إذعان امني، والمساعدات التقنية هي شكل خاص من التحكم بالسلوك الأمني، لذلك، كلما زادت المساعدات التقنية الأمنية للعراق ازداد تهديد الاختراق والتحكم الإلكتروني، وكما إن زيادة تأثير المعونة التقنية يفضي إلىا لإذعان الأمني، وهذا نهج اتبعته مجموعة التقنيين الكبار لاحتكار الدعم والإقراض والمنح والمساعدات التقنية الأمنية، لزيادة إذعان المتلقيين، وهذا يوصلنا إلى نتيجة هي : كلما ازدادت حاجة العراق للتقنية الخارجية، قاد إلى زيادة اختراقه اللأمن وتلك معضلة حقيقية، لأن أمن المستلم يكون مهدد من قبل الُمَسلم، وتزداد الخطورة في حال عدم الدفع لُلمَسلم، فكلما ازداد حجم الاعتمادية التقنية على القوى الخارجية دون إنتاج تلك التقنية، كلما ازداد حجم تأثر القرار الأمني العراقي[2].

وزيادة على ذلك،إن القوى الكبرى المخترقة –المغيرة للقوى الأضعف، تخترق النظام الأمني وتدفعه باتجاه الإذعان لها، على سبيل المثال :الاختراق الخارجي للأمن السيبراني العراقي(دعم الحلفاء)، استناداً إلى مبدأ صناعة اللوبي الرقمي(الجيوش الإلكترونية)، وهذا ما استندت عليه الساحة السيبرانية العراقية في حقبة ما بعد التغيير 2003، إضافة إلى ذلك، فان الاختراق هو أكثر فعالية ضد المجتمع العراقي خاصة الفئات البدائية في استخدام التقنية ، أي إن الاختراق أكثر فعالية في حال تفاوت العلمي والمعرفي، ولذلك، فإن الأضعف علمياً يكون أكثر تطفلاً في تقنيات المعلوماتية، وكلما زاد الفارق التقني زاد الاختراق، وكلما زاد الاختراق زاد الإذعان، ولهذا الاختراق يكون أكثر فعالية في حال غياب الثقافة المعلوماتية، وهذا يعني استفحال معضلات التهديد ، وزاد هذا التهديد بعد أن ثبت تحكم القوى الخارجية بثورات التغيير العربي عن طريق المجال الإلكتروني [3].

**المبحث الثاني: الأمن الوطني العراقي والفضاء السيبراني**

---

[1]Julie E.Mehan. Cyberwar, Cyberterror, Cybercrime: a Guide to the Role of Standards in an Environment of Changeand Danger. (Ely, U.K.: IT Governance Publishing, 2008),p 52.

[2]Richard A. Clarke and Robert K. Knake. Cyber War: The next threat to National Security and what to do about it (New York: Ecco HarperCollins 2010) ,p26-27.

[3]Christopher Dickey, R. M. Schneiderman, and Babak Dehghanpisheh, "The Shadow War; Someone is Killing Iran'sNuclear Scientists,But a Computer Worm May be the Scarier Threat." Newsweek Journal ,Vol. 156, No. 25,( New York, December, 2010), p20.

تبعاً لضخامة القصد من ماهية امن الوطني العراقي، تداخلت الكثير من العلوم الاختصاصية في تفسير تلك الماهية، فاحتدم الجدل والنقاش حول ما تعنيه تلك المفردة من رؤى وأفعال وصور ناطقة، فالأنموذج المؤصل للتكتلات الأمنية وأن كان يقوم أساساً على التقارب التفاعلي بين القوى الأمنية المتعاونة تكاملاً لتحقيق الأمن،عبر نوافذ التحالف والتآلف ومسالك التناسق الأدائي، لم يعد يمثل مرجعية للتطابق والاتساق بين تلك العناصر فحسب، وانما بدا الإطار العام الذي يتم من خلاله تحديد صلاحية الأمن التكاملي ومدى اتساقه بفلسفة صناع القرار.

ولكي ننأ عن أي خلل،يمكن القول: إن هناك علاقة بين القوى الرقمية الفاعلة على المستوى الدولي، والمعضلات الأمنية العراقية، فبقدر ما يحتويه هذا الأسلوب من صعوبة قياس ودقة استحضار ونباهة ربط، فانه يمثل الأسلوب الأكثر قدرة على تفسير التوازنات الأمنية في الشرق الأوسط، وهذا يأتي من المرجعية الإدراكية للقيمين على المؤسسات الأمنية التي يفترض أن تتناغم عندهم مكّنة الإدارة مع المرجعية الأدائية، ولتوضيح الصورة الأمن الوطني العراقي والفضاء السيبراني أكثر، عرجنا لتقسيم المبحث إلى مطلبين وعلى النحو الاتي:

**المطلب الأول: أسس بناء الأمن السيبراني:**

إن عملية "الأمننة السيبرانية" والتي تعني "إضفاء الطابع الأمني المعلوماتي "على بعض المعضلات المعلوماتية التي تركز على تهويل التهديد وتضخيمه لإنتاج" الفزع والخوف"؛ فالأمن والتهديد سيبرانياً مترافقان، وفي هذا السياق هناك ثلاثة خطوات لنجاح عملية إضفاء الطابع الأمني السيبراني:

- توضيح كيف أن التهديد المزعوم يمس امن العراق الوطني .
- تحديد التدابير الاحترازية التي يمكننا عن طريقها ضبط هذه التهديدات والسيطرة عليها .
- إمكانية الخطاب الأمني الرقمي في الحصول على رضا المواطنين إزاء ما يرافق عملية إضفاء الطابع الأمني السيبراني على مسألة الإلكترونية معينة، وبالذات خرق القواعد المعمول بها التي تمس الأمن والسيادة العراقية [1].

يبدو أن عملية تحويل معضلة ما إلى حيز المعالجات الأمنية الطارئة، مثلما حصل مع قضية امننة " العنف" في العراق، يتطلب تضافر عوامل سوسيولوجية سهلت مسعى صناع "العنف والكراهية" لتحريك جيوشهم الإلكترونية ضد كتل القائمين على الإدارة الأمنية ومن تلك العوامل على سبيل المثال تأجيج ركائز الكراهية:" الانتقام ، والثأر، والمظلومية"، أو غسل أدمغتهم وتحكم بهم باختراق العقول باستثارتهم بالأعلام الحماسي، بالمقابل عمل القائمين على الأمن على امننة مسألة "حراك الكراهية والعنف" باعتباره تهديد، فكان استهداف أنظمة العنف والكراهية كفيلاً بعكس الصراع الأمني على ارض الواقع، إذ تدمير أنظمتهم الإلكترونية يفكك أنظمتهم الأدائية، لكن "هناك مسألة أخرى ليست بأقل أهمية: هل تعد العملية برمتها شيئاً إيجابياً أم سلبياً؟ يرى البعض بأنها سلبية لسبب منطقي وهو أن تحويل الملفات إلى حيز المعالجات الأمنية يؤشر على شيء غير إيجابي وهو إخفاق السياسة العادية في التعاطي مع الخلافات والاختلافات في الإدارة

[1]Jeremy Ferwerda ,at.al, Institutional Foundations for Cyber Security: Current Responses and New Challenges, Paper ,(Composite Information Systems Laboratory CISL, Massachusetts Institute of Technology, Cambridge, September 2010),p16-17

الأمنية، ولذلك فإن وجود عدد من الملفات في "الحيز الأمني" يجب أن ينظر إليه بمثابة استثناء، والحل عنده هو نزع الطابع الأمني عنها "وتحويلها لحيز السياسة الأمنية الطبيعية حيث الرقابة والتقيد بالقوانين والضوابط والتعليمات الأمنية[1].

ولنسأل: ما الذي يحدد التفاعلات الأمنية العراقية مع القوى الإقليمية والدولية لتحقيق الأمنة المعلوماتية؟ نبدأ بالإجابة، قائلين: لتقديم رؤية علمية للتفاعلات الأمنية، لا بد من التعامل مع مدركات صناع القرار في الاستراتيجية الأمنية الدولية، وماذا يعني لهم الأمن السيبراني، لكن مقدماً دعونا نتفق على: استحالة معرفة الحراكات في الفضاء السيبراني دون رؤية استراتيجية، ولا توجد سلطة دولية تحقق الأمن السيبراني الدولي، وصناع الأمن في الشرق يخشون بعضهم بعضاً، وان العراق يمكن أن يُهاجم من أي دولة أخرى الالكترونياً، ويحق لأي دولة في الشرق أن تتحالف مع أي دولة أخرى بحثاً عن الأمن في الفضاء السيبراني، والمصالح هي محفز الحراك الدولي الرقمي، وجميع الدول يجمعها هدف واحد هو تحقيق التكامل الأمني، والعالم يعيش " القرية الذكية" أي رفض الروتين والتمرد عليه؛ وبسبب انعدام الحكومة الإلكترونية العالمية، والتحالفات التقنية هي التي تخل بالتوازنات الأمنية الدولية[2].

**المطلب الثاني**

**المقاربة بين الأمن والتهديد في ظل الفضاء السيبراني**

ونحن نتحدث عن مستقبل الأمن الوطني العراقي يراودنا تساؤل: ما هو أساس اعتبار أو عدم اعتبار حدث ما معضلة حقيقية لأمن العراق؟

دعونا نتفق على إن ليست كل الأحداث تعد تهديدات حقيقية في العراق، فالحراك المجتمعي في منصات التواصل الاجتماعي وزيادة مساحة المواقع(المطالبة بالحقوق)، وتكوين المنصات الإلكترونية (البحث الدور والمكانة) هذا يفتح المجال بين "الارتياب العرضي" من جهة، لكنه ليس بتهديد، على سبيل المثال: يمكن أن ترى أخطاراً غير موجودة على ارض الواقع(التهويل) ، او تتجاهل التهديد الحقيقي (التهاون المفرط) من جهة أخرى، أي لا يعترف القائمين على الأمن بالتهديدات التي هي فعلاً حقيقية ويهتمون بالتهديدات الشكلية كما حدث في عام 2014.

هذا يعطينا طريقتين للنظر إلى موضوع الأمن في العراق لدينا المفهوم التقليدي لمفهوم التهديدات التي يمكن أن تكون "تهديدات قيمية" ،وكذلك تكون التهديدات الإلكترونية مؤسساتية( القرصنة وتهكير وسرقة وحرق المعلومات)، أما درجة التهديد المعلوماتي يعتمد على تحديد صناع القرار الأمنيين لما يعدوه تهديداً خطراً أو ما هي دون ذلك، وهذا ما نجده في العديد من التفاعلات الأمنية[3].

ثم يأتي بعدها الشق الامننة الإلكترونية، لنتساءل ما هي العملية التي تتشكل وفقها التهديدات الإلكترونية؟ من يُحددها؟ من يسوقها؟ كيف يمكن لجزيئات حدث ما إن تجتمع ونتقبلها كتهديد؟

---

[1]Ben Buchanan. The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations,( New York: Oxford University Press, 2017),p23.

[2] George Fujii. ISSF Roundtable 10-6 on The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations وH-Diplo, (01-19-2018),p7.

[3]Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyperspace, " International Security, Vol. 41, No3 (Winter 2016/17): 44-71;

ومن هنا يمكن، أن نرى مثالاً على هذه العملية مثلاً: الأمن مهدد من قبل "الإرهاب الإلكتروني"،وكذلك الحال مع التجارة الإلكترونية غير المشروعة، فان التهديد انعكس داخلياً لظهرت مصطلحات الدولة العاجزة، والمشلولة، والفاشلة، والرخوة، والركيكة سيبرانياً[1].

لا شك، إن زوال التهديد يفضي إلى "استدامة الأمن"، وهذه العملية تعني انعدام الشعور بالخطر من عدو لم يعد موجوداً على الساحة، فالامننة السيبرانية توصف بانها استجابة للشعور بالتهديد اتجاه معضلة عبر شبكات التواصل الاجتماعي، وان ليس كل العمليات الاستخبارية الرقمية في العراق عمليات امنيه سيبرانية، بل البعض منها جزء من السياسة الرقمية[2].

وهنا، نجد معادلة صعبة هي:"كلما فُعلت الامننة السيبرانية في العراق فُعل التهديد السيبراني فيه كذلك لاستدامة التهديد"، وهذا يعني إنللرؤية الاستراتيجية العراقية السيبرانية دور فاعل في جعل الظاهرة الخاضعة للامننة مقبولة في الراي العام العراقي، لهذا نجد من هم سعداء جداً "الراغبين" على ما يسمى بالحرب على "الإرهاب الإلكتروني"، لأنه سبب مقنع للتدخل وشن الحروب المعلوماتية؛ كونه سبب يمكن التعويل عليه، بينما هناك شق أخر: يرى أن هذا مجرد الهاء عن التهديدات الحقيقية الواقعية، أي التهديد لا يعني إلا الوجود الواقعي الفعلي وليس الافتراضي[3].

لهذا يختلف المفهوم باختلاف الوضع واختلاف الأولويات، ففي الأمن السيبراني لا توجد معرفة مطلقة بالتهديد وعواقبه، مالم تكن هناك إمكانات تقنية عالية، والا كان من الصعب اتخاذ قرار الأمني مع معرفة معلوماتية غير كاملة[4].

علينا أن ندرس عملية تشخيص معضلة الإلكترونية ما على إنها معضلة امنية الإلكترونية، لكن التساؤل هو من سيقرر هذه المعضلة الرقمية هي تهديد فعلي؟ من له صلاحية تقرير هذا؟ الجواب حسب ما تصفه الحياة الأمنية، إنالقائمين على الأمن هم المخولون بتقرير المواضيع الأمنية، لكن لا يمكن أن تكون اعتباراتهم دائماً مقبولة، إذا فكرنا مثلاً بالحرب الإلكترونية بين القوات الأمنية والجماعات المتطرفة المسلحة، وأجرينا مقارنة بينهما وهما من أبرز الأمثلة على الامننة الرقمية، فالحرب على تلك الجماعات نجحت فيها الامننة الإلكترونية ونجحت، حتى برزتها كتهديدات حقيقية[5].

أما المقاربة فنقول: لابد من التمييز بين أن تكون جزء من عملية بناء الأمن والحفاظ عليه وضمان استدامته، أو تكون خارج دائرة المنظومة الأمنية وتساهم بالتنظير والتحليل لرسم السياسية الأمنية[6]، فالموضوع يبدأ بتحول لشيء أكبر

---

(1)Marco Marsili, The War on Cyberterrorism, Democracy and Security Journal , Vol.15,No.2, (July 2018),p175.

(2)Sara Hower, Kathleen Uradnik, Cyberterrorism, 1st ed. (Santa Barbara, CA: Greenwood, 2011), pp142–146.

(3)Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", Vanderbilt Journal of Transnational Law ,Vol.43, no. 1 ,2010,p33.

(4)Murat Dogrul & et.al, Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism, CCD COE Publications, 2011,pp.31-34

(5)Ministry of Culture & Information of Saudi Arabia (ed.), The Kingdom Versus Terrorism: Stances and Achievements, 1st ed. (Riyadh: Al-Quiman Multimedia, 2010), p.20.

(6)Jonalan Brickey, "Capturing a Broad Range of Activities in Cyberspace", CTC Sentinel, Vol.5, No. 8 (2012), pp.4-6.

مما كان عليه لامننته رقمياً، فالعراق أمام إستراتيجية أمنية كاملة طويلة الأمد، الموضوع الأهم في الأجندة الأمنية هو كسب المكّنة الأدائية الرقمية، هذا رهن أن يكون القائمين على الأمن من ذوي المعرفة التقنية[1] .

واذا ما طبقنا هذه المقاربة والمقارنة على الأمن العراقي"نكتشف أن المعضلات الأمنية الرقمية لا تكون أكثر شيوعاً من المكّنة الأدائية اذا ما اعتمد الرؤية الاستراتيجية، فوفرة البرامج التخطيطية وجاهزية الإمكانات وموائمتها للوسائل التقنية تفضي إلى بناء الأمن السيبراني العراقي وهو الهدف المستقبلي المنشود[2].

وهذا يفسر لنا لماذا شهد العراق ظاهرة الامننة لكثير من المعضلات الامنية؟ إذ كانت مصدر أو محصلة للنزاع بين المجموعات المجتمعية، والتي تعمل في كل حالة على تغذية هذه الوضعية، ففي غضون ذلك يختفي تحكم الدولة بإقليمها وتنتفي مظاهر سيطرة الحكومة واحتكارها لاستخدام القوة ووسائل القهر، والأهم من ذلك هو أن المجموعات المتناحرة تتبنى استراتيجية إشاعة التهديد لتحقيق أهدافها، وهدفها بالتالي ليس الاستيلاء على السلطة لأن ذلك ليس في حدود إمكاناتها، إلا أن اعتمادها على استراتيجية إشاعة التهديد جعلها تلجأ إلى أسلوب جديد للمواجهة باستخدام حرب المعلومات، الجرائم الإلكترونية، التحريض والحشد على منصات التواصل الاجتماعي، إذ وجدوا سهولة تعبئة هذه الفئات والتحكم بها وحتى توريطها في أعمال إجرامية محظورة دولياً ،ولذلك، فإن الخاصية المميزة لصراعات ونزاعات في" الفضاء السيبراني" تتمثل في اعتماد أسلوب الصراع الرقمي بين المجموعات أو الأطراف المتصارعة وذلك عن طريق استهداف المواقع الإلكترونية الجماعية، التأثير على المراهقين وتجنيدهم، اختراق العقول وبرمجتها، التضليل، وغيرها ويتم ذلك بالاعتماد على أسلحة الإعلام الإلكتروني وهذا تمتعت به "الجماعات المتطرفة" لا تراعى فيها القوانين والأعراف الدولية الخاصة باستخدام التقنيات الإلكترونية للأغراض السلمية، وفي هذه الصورة ، تبدو صعوبة استشفاف المقاربة للأمن والتهديد بالمنظور الرقمي، ما لم يكن القائمين على الأمن من ذوي المعرفة الإلكترونية[3].

لكن ما هي القيم التي تتعرض للتهديد بحيث تجعل استقرار المكونات المجتمعية محوراً جوهرياً للمنظومة الأمنية، أن المعضلة الأمنية تتمحور حول الهوية، حول ما يمكّن المجموعة من الإشارة إلى نفسها باسم وكنية افتراضية(حركية)، لكن مكمن التحدي هنا هو جانبها التطوري،فهي عملية تفاعلية مستمرة للتحكم في المطالب الملحة وإشباع حاجات معينة، حيث يلعب مفهوم "الاسم والكنية" دوراً مهماً في التأثير الإعلامي الرقمي، غير أن هذا المسار التفاعلي يقود إلى معضلة أمنية مجتمعية إذا أصبحت "الهوية" جوهراً للصراع على المصالح وسنداً للسعي من أجل الوصول إلى السلطة، ويتضح ذلك في تغليب مظاهر "المجموعة" على المظاهر المجتمع، وهذا بالالتجاء إلى المكونات فئوية، بدل مؤسسات الدولة، كإطار للصراع من أجل البقاء، وكذريعة وحيدة لهمللحصول على مكون افتراضي في مناخ يسوده التهديد الحقيقي،ولكن سلسلة الأفعال وردود الفعل في التفاعل بين المجموعات المختلفة قد يؤدي إلى رفع سقف الوعود لدى قياداتها بالمطالبة (بالإفناء) ولدى المجموعات الأخرى بتقديم وعود (بالإقصاء)، وبتداول خطابات الخطر، وزيادة مستويات الاستقطاب، فإن

---

[1]Gabriel Weimann, Terrorism in Cyberspace: The Next Generation (New York, NY: Columbia University Press, 2015),p23.

[2]Imran Awan and Brian Blakemore, Policing Cyber Hate, Cyber Threats, and Cyber Terrorism (Farnham: Ashgate Publishing, 2012),p.43

[3]Thomas J. Holt, George W. Burruss, Adam M. Bossler, Policing Cybercrime and Cyberterrorism (Durham, NC: Carolina Academic Press, 2015),p31.

ذلك يفتح المجال أمام تفجر العنف الحقيقي والذي يتم تغذيته بوجود دعم من صناع التهديد، هنا تظهر ملامح العنف المسلح ، وهكذا، وعندما يمتزج العنف بالعجز الاقتصادي، والفوضى الاجتماعية وتكون الدولة أمام استفحال وهيمنة التهديد[1].

والإشكالية، هي ربط الأمن أساساً بالفضاء السيبراني(رقمّنة الأمن)، "الأمن وكل ما هو أمني إنما يعود على القضايا التواصل الإلكتروني التي يتم التعامل معها بشكل متميز عن باقي القضايا الواقعية الأخرى، ويتم ذلك عبر تحويل بعض القضايا في منصات التواصل الاجتماعي من الحيز العادي إلى الحيز الحساس التي تقتضي معالجة خاصة، وأكثر من ذلك، يتم المداولة بشأنها في إطار غير الأطر السياسية الاعتيادية، "إذ يقومون بعدها بالربط بين الأمننة والتسيس، "يمكن القول أن الأمننة بمثابة الصورة الأكثر تشدداً لعملية التسيس، بالنسبة لتصور التسيس، فهو يتعلق بإضفاء الطابع السياسي على قضايا الإلكترونية بعينها، إذ أن القضايا التي يتم تسيسها تعد جزء من السياسة الرقمية، ما يعني أن الحكومة تصور للراي العام إنها مجبرة على التعاطي معها عبر اتخاذ قرارات وتخصيص موارد لتنفيذ هذه القرارات، يشكل ذلك في مجمله وضع هذه القضايا ضمن الإطار "الانتقائية"، فإن ذلك يعني عدها خارج إطار الضبط الإلكتروني الذي يمارسه القائمين على الأمن، والتي تستوجب اتخاذ تدابير عاجلة بما يبرر تبعاً لذلك كل التدابير الإجرائية والاحترازية والاستثنائية والطارئة لمحاسبة الفئات الاجتماعية الضد الذين يتخذون من منصات التواصل الاجتماعي وسيلة لتهديد الأمن[2].

ولغرض الحفاظ على الأمن السيبراني الوطني من الهجمات الخطيرة ؛ على الحكومة إن تعقد العزم على ذلك وفق رؤية واضحة ومهمة هدفها تكوين جيش دفاع وطني إلكتروني بعدة حديثة وبعدد مناسب لتؤسس "الهيئة الوطنية للأمن السيبراني العراقي" ، كما في بعض الدول التي وعت قبل حين أهميته، وتشكيل هيئة عالية المعرفة تشرف على هذا الأمن الخطير وتكون النواة الحقيقية للحوكمة الإلكترونية التي طال انتظارها، وتكون هناك مديرية في كل المؤسسات بذات الاسم تتابع البرمجيات والمعدات التي يتم شرائها من الأسواق المحلية والكشف عليها قبل دخولها الخدمة ومتابعة وسائل الحماية من برمجات مختلفة، يقودها المختصون في هذا المجال وتلك مهمة كبيرة وجسيمة تلقى على عاتق الشرفاء من حملة العلم والتجربة والوطنية ليكونوا حصناً لوطنهم فالألاف من مهندسي الحاسوب والمبرمجين ساعدهم الوضع بعد عام 2003 والتوسع في إدخال المعدات الحديثة ليمتلكوا الأهلية لقيادة تلك الهيئة مع بعض التدريب في الدول التي تمتلك القابليات في هذا المجال،سيكونون أهل لتلك المهمة فشبابنا كفوء وعلى درجة كبيرة من المهنية في هذا المجال، ندرب ونطور ونهيأ الموازنة الكافية لتغطية نفقات تلك الهيئة التي ستكون وزارة الدفاع والأمن السيبراني العراقي.

**الخاتمة**

خلاصة لكل ما عرض آنفاً، يمكن القول: أن هناك علاقة طردية بين المعضلة الأمنية والمكّنة الأدائية فعلما ازدادت المعضلة الأمنية ازداد والتهديد، وكلما ازداد التهديد أزادت الحاجة لرفع الإمكانات الأدائية المعرفية والتقنية للحفاظ على

---

[1]Lee Jarvis, Stuart MacDoland, Thomas M. Chen (eds.), Terrorism Online: Politics, Law and Technology (London and New York: Routledge, 2016).

[2]Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare (New York: Cambridge University Press, 2017),p33.

الأمن وضمان استدامته، وهذا الأمر يعتمد كثيراً على امتلاك القائمين على الأمن أجهزة الحماية الإلكترونية التي تقوى كلما تطور التهديد لحصره وتحجيمه،وهذا إن دل على شيء، فانه يدل على أهمية الرؤية الاستراتيجية الأمنية للتعامل مع المعضلات المستقبلية.

عموماً الأمن هو أكثر شيوعاً من التهديد في العراق، فالأمنيين يميلون إلى لامتلاكهم مقومات القوة وقدرات الردع ومصداقية المعالجة في الفضاء السيبراني، ويميلون إلى بناء منظومة أمنية ذكية لها القدرة على تتفكك التهديد.

ففلسفة الامننة الرقمية تعني إضفاء الطابع الأمني على معضلة رقمية ما وعدها تهديد حقيقي وجوهري، والعلاقة بين الأمن والتهديد علاقة عكسية تضادية متلازمة، فاذا كان الأمن أكثر شمولاً ضعف التهديد، وإذا كان التهديد أكثر شمولاً ضعف الأمن.

وتبعاً لهذا الفهم، اتضح الأمن السيبراني العراقي، وبات من السهل واليسر استقراء التهديد الأمني الرقمي وتحليل الأداء الاستراتيجي في الساحة العراقية ما بعد 2016، بعد إن تم استقراء الرؤية الاستراتيجية العراقية في تشكيل الأمنة السيبرانية، لنخرج من هذه المقارنة والمقاربة بجملة من النتائج منها:

1. الأمن السيبراني من اهم فروع الأمن الوطني العراقي .
2. الأمن السيبرانية يتطلب بناء منظومة استراتيجية أمنية سيبرانية متكاملة .
3. العراق حاله حال دول الشرق الأوسط فهو يعاني من الانكشاف الاستراتيجي السيبراني .
4. العراق تعرض للعديد من الهجمات في الفضاء السيبراني بسبب المكّنة المتواضعة في المجال التقني .
5. هناك علاقة عكسية بين التهديد والأمن في الفضاء السيبراني تتقارب طردياً.

**كما خلصت هذه الدراسة إلى التوصيات الآتية:**

1- إنشاء مراكز لبحثية للأمن السيبراني.

2- بناء منابر خَطابية على منصات التواصل الاجتماعي لإشاعة لغة الامن والسلام العراقي.

3- إدانة صناع النزاع والصراع الرقمي "ومحاكمتهم.

4- بناء منظومة أمنية رقمية متكاملة.

5- تقنين الامننة وعدم اعتماد الانتقاء والتسيس لمعضلات مجتمعية القصد منها كسر أواصر النسق الأمني.

6- تطبيق الأمن السيبراني وفقاً لمبادئ الأمن السيبراني العالمي.

7- عدم الاعتماد على القوى الخارجية في حماية الامن الوطني السيبراني العراقي.

8- اعتماد "الاستراتيجية الأمنية السيبرانية العراقية "مادة تدرس في الأكاديميات العسكرية والأمنية والجامعات العراقية.

9- بناء قاعدة بيانات ذكية لجميع سكان العراق .

10- تحويل المؤسسات العراقية إلى مؤسسات ذكية عالية التقنية .

11- تفعيل الحكومة الإلكترونية العراقية بكافة تشكيلاتها .

**<u>قائمة المصادر والمراجع :</u>**

❖ **المصادر العربية:**

**أولاً : المقالات:**

1.حسين باسم عبد الأمير،تحديات الأمن السيبراني،مقال منشور (قسم الدراسات السياسية/ مركز الدراسات الاستراتيجية-جامعة كربلاء)،آيار/2018.

2. زاهر الزبيدي، تهديدات افتراضية للأمن السيبراني العراقي، شبكة النباء، الأثنين 27 تشرين الثاني 2018.

**ثانياً: التقارير:**

1.تقرير المؤشر العالمي للأمن السيبراني "مركز الإعلام الرقمي "، السومرية نيوز، بغداد،2019/3/31.

❖ **المصادر الأجنبية:**

**1.Books:**

. Barbora Bukovska, Iraq: Draft Informatics Crimes Law, (London, Free Word Centre, Farringdon), October 2011).

. Ben Buchanan. The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations, (New York: Oxford University Press, 2017).

. Brahima Sanou, Global Cybersecurity Index (GCI),( ITU Cybersecurity Team ,2017).

. Gabriel Weimann, Terrorism in Cyberspace: The Next Generation (New York, NY: Columbia University Press,2015).

. Imran Awan & Brian Blakemore, Policing Cyber Hate, Cyber Threats, and Cyber Terrorism (Farnham: Ashgate Publishing, 2012).

. Julie E.Mehan. Cyberwar, Cyberterror, Cybercrime: a Guide to the Role of Standards in an Environment of Change and Danger, (Ely, U.K.: IT Governance Publishing, 2008).

. Lee Jarvis, Stuart MacDoland, Thomas M. Chen (eds.), Terrorism Online: Politics, Law and Technology (London and New York: Routledge, 2016)

. Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, (New York: Cambridge University Press, 2017)

. Ministry of Culture & Information of Saudi Arabia (ed.), The Kingdom Versus Terrorism: Stances and Achievements, (Riyadh: Al-Quiman Multimedia, 2010).

0.Murat Dogrul & et.al, Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism, (CCD COE Publications, 2011).

1.Richard A. Clarke & Robert K. Knake, Cyber War: The next threat to National Security and what to do about it. (New York: Ecco HarperCollins 2010).

2.Richard A. Clarke and Robert K. Knake. Cyber War: The next threat to National Security and what to do about it (New York: Ecco HarperCollins 2010).

3.Sara Hower, Kathleen Uradnik, Cyberterrorism, (Santa Barbara, CA: Greenwood, 2011).

4. Thomas J. Holt, George W. Burruss, Adam M. Bossler, Policing Cybercrime and Cyberterrorism (Durham, NC: Carolina Academic Press, 2015).

**2.Magazines and periodicals:**

. Christopher Dickey, R. M. Schneiderman, and Babak Dehghanpisheh, "The Shadow War; Someone is Killing Iran's Nuclear Scientists,But a Computer Worm May be the Scarier Threat," Newsweek Journal ,Vol. 156, No. 25, ( New York, December, 2010).

. Jonalan Brickey, "Capturing a Broad Range of Activities in Cyberspace", CTC Sentinel, Vol.5, No. 8, (2012).

. Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyperspace, " International Security, Vol. 41, No,3 (Winter 2016)

. Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", Vanderbilt Journal of Transnational Law ,Vol.43, No. 1 ,(2010).

. Marco Marsili, The War on Cyberterrorism, Democracy and Security Journal , Vol.15,No.2, (July 2018)

. Sattar J. Aboud, An Overview of Cybercrime in Iraq, The Research Bulletin of Jordan ACM , Vol.11 ,No.11,(June 2012).

. Sattar J. Aboud, Cybercrime in Iraq,(International Journal of Scientific and Engineering Research Vol. 5,No. 2,(2018).

**3.Research and Studies:**

. Herry Brito & Tate Watkins, Loving The Cyber Bomb? The Dangers of Threat Inflation Incybersecurity Policy, (Aprile-2011).

. Jeremy Ferwerda ,at.al, Institutional Foundations for Cyber Security: Current Responses and New Challenges, Paper ,(Composite Information Systems Laboratory CISL, Massachusetts Institute of Technology, Cambridge, (September 2010).

**4.Reports:**

. A false sense of security? Cybersecurity in the Middle East, Global State of Information ,Journal Security, (March 2016).

. George Fujii. ISSF Roundtable 10-6 on The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations و H-Diplo, (01-19-2018).

. Jayson M. Spade, Chins Cyber Power and Americas National Security, Information as Power, U.S. Army War College, (May 2012).

. Midea S Ali, A Brief Review of Cybersecurity Issues in Iraq,Technical Report ,)University Sains Malaysia, (April 2018).

. Tallinn, Economic Aspects of National Cyber Security Strategies, Project ) ,Report , (2015).

**5.Articles**

. Ali Ziad al-Ali,The Hidden Threats to Iraq's National Security, article in National security and defense, 07/10/2018.