مركز البيان للدراسات والتخطيط
Al-Bayan Center for Planning and Studies

مفاهيم الجيش الإلكتروني ـ الذباب الإلكتروني وصناعة الرأي العام

وفاء فوزي

سلسلة إصدارات مركز البيان للدراسات والتخطيط

عن المركز

مركزُ البيان للدراسات والتخطيط مركز مستقلٌّ، غيرُ ربحيّ، مقرُّه الرئيس في بغداد، مهمته الرئيسة -فضلاً عن قضايا أخرى- تقديم وجهة نظر ذات مصداقية حولَ قضايا السياسات العامة والخارجية التي تخصّ العراق بنحو خاصٍ، ومنطقة الشرق الأوسط بنحو عام. ويسعى المركز إلى إجراء تحليلٍ مستقلٍّ، وإيجاد حلول عمليَّة جليَّة لقضايا معقدة تهمُّ الحقليْنِ السياسي والأكاديمي.

ملحوظة:

لا تعبِّر الآراء الواردة في المقال بالضرورة عن اتجاهات يتبناها المركز، وإنَّما تعبِّر عن رأي كتابِها.

www.bayancenter.org
info@bayancenter.org

Since 2014

مفاهيم الجيش الإلكتروني - الذباب الإلكتروني وصناعة الرأي العام

وفاء فوزي *

المقدمة:

تلعبُ التكنولوجيا دورًا مهمًا في جميعِ جوانبِ حياتنا، فقد أحدثت ثورةً في الطريقة التي نتواصلُ ونعملُ بها، وطريقة حصولنا على المعلوماتِ وتحليلها وأماكن توظيفها بالشكل المطلوب، كما أنَّها جعلت العديد من المهامِ أسهل وأكثر كفاءةً، وأثرت بشكلٍ كبيرٍ على الطريقة التي نعيشُ بها، حتى أنَّ كلّ شيء حولنا صارَ لهُ صلة بالتكنولوجيا، خاصةً بعد جائحةِ كورونا إذ جعلت استخدامن ا للإنترنيت والتكنولوجيا جزءاً أساسياً من المجتمعِ الحديثِ، ومن المرجّح أنْ تستمرَّ التكنولوجيا في تشكيل الطريقة التي نعيشُ ونعملُ بها.

أمّا الجيوش الإلكترونية فترتبطُ باستخدام التقنيات الرقمية لمهاجمة وتعطيل أنظمة وشبكات الكمبيوتر، عادةً تكون بهدفِ تحقيق ميزة استراتيجية أو عسكرية على الخصم، ويمكنُ أنْ يشملَ ذلكَ أنشطة مثل القرصنة، وخرقُ البيانات، وهجمات رفض الخدمة الموزعة (DDoS)،و من بين الأمور الأخرى أصبحت الهجمات السيبرانية بما في ذلكَ هجمات (DDoS)، وهجمات البرامج الضارة وهجمات التصيّد الاحتيالي ذاتَ أهمية متزايدة مع استمرارِ نمو استخدام التقنيات الرقمية، وأصبحت أكثر أهمية في حياتنا اليومية، وعلى هذا النحو، تتخذُ العديد من الحكومات والمنظمات خطوات لتعزيزِ دفاعاتها السيبرانية، والتي يتم تنفيذها من قبل مؤسسات الدولة أو المتسللين الذين ترعاهم دول معينة أو مجموعات وأفراد آخرين، فسيكون النتاج الطبيعي أن تقومَ الدول بتكوين خطوط دفاعية سيبرانية، وخطوط أخرى هجومية ومن هنا تأتي أهمية تشكيل الجيش الإلكتروني والذي أحيانا تتخطى مهمته تعطيل البنية التحتية الحيوية، أو سرقة البيانات الحساسة، وصولاً للتأثير على العالم، لذلكَ حرصتْ الحكوماتُ والمنظماتُ في جميع أنحاء العالم على تخصيص موارد لتكوين الجيوش الالكترونية وخطوطه الدفاعية والهجومية، لكنها لا تزال تمثل تهديدًا كبيرًا.

* باحثة.

يعودُ تاريخ ظهور الجيوش الإلكترونية إلى الثمانينيات، عندما استخدم مصطلح «الجيوش السيبرانية» لأول مرة لوصف استخدام شبكات الكمبيوتر للهجوم والدفاع ضد الأهداف العسكرية والحكومية، ففي التسعينيات وأوائل العقد الأول من القرن الحادي والعشرين، بدأ المتسللون بتنفيذ الهجمات الإلكترونية، وكانت تركز بشكل عام على القرصنة أو التسبب في اضطراب بدلاً من التسبب في ضرر مادي.

في عام(2010)، أصبحت الجيوش الإلكترونية مصدر قلق متزايد، وتحضى بالأهمية بالنسبة للحكومات والجيوش في جميع أنحاء العالم، حيث بدأت الدول بتطوير أسلحة وتكتيكات إلكترونية متطورة، وتم الإبلاغ عن العديد من الهجمات الإلكترونية البارزة على أهداف حكومية وعسكرية، وغالبًا ما كانت لهذه الهجمات عواقب وخيمة، تمثلت في سرقة البيانات الحساسة وتعطيل البنية التحتية الحيوية للمستهدف.

في السنوات الأخيرة، استمرَّ استخدام الجيش الإلكتروني في التطور والتوسع، كما خلقت التقنيات الجديدة مثل الذكاء الاصطناعي، وإنترنت الأشياء (IoT) ثغرات الجديدة التي يمكن استغلالها في الهجمات الإلكترونية، وأصبح الخط الفاصل بين الحرب السيبرانية وأنواع الصراعات الأخرى ضبابيًا بشكل متزايد، كالذي حدث في الحرب الاقتصادية والمعلوماتية.

ما هو الجيش الالكتروني؟

هو مصطلحٌ يستخدمُ لوصفِ مجموعة من الأفراد الذين تم تنظيمهم لتنفيذ هجمات إلكترونية، إما لدعم قضية أو لمجرد تحقيق مكاسب شخصية، وهناك أنواع مختلفة من الجيوش الإلكترونية، بما في ذلك الجيوش الإلكترونية التي ترعاها الدولة والناشطون في مجال القرصنة الجماعات والمنظمات الإجرامية والجيوش الإلكترونية التي ترعاها الشركات.

الجيوشُ الإلكترونية التي ترعاها الدولة: مجموعاتٌ من المتسللين والعاملين الإلكترونيين المدعومين من دولةٍ معينة وينفذونَ هجمات إلكترونية لدعمِ المصالح الاستراتيجية لبلدهم، عادةً يتم تمويلهم جيدًا ولديهم إمكانية الوصول إلى الأدوات والتقنيات المتقدمة، كاستخدام تقنيات التشفير، إنشاء عمليات علم كاذبة لإخفاء الهوية الحقيقية للمجموعة ونواياها، هجوم (zero day) لاكتشاف

الثغرات في الأنظمة الإلكترونية قبل أنْ تكتشفها الجهات المطورة وتصحيحها، تشمل الأمثلة على الجيوش الإلكترونية التي ترعاها الدول، الوحدة العسكرية الصينية (61398) و (APT28) ال روسية.

مجموعاتُ القرصنة: هي مجموعاتٌ من المتسللين الذين ينفذون هجمات إلكترونية للترويج لقضيةٍ اجتماعية أو سياسية، غالبًا ما يستهدفون الوكالات الحكومية والشركات والمنظمات الأخرى التي يرونها أعداء لقضيتهم، مثل المجموعات الناشطة للقرصنة (Anonymous) لمحاربة الحكومات الظالمة لشعوبها، كذلك مجموعة (LulzSec) هي مجموعة قرصنة تدعي بأنها المسؤولة عن بعض الهجمات الإلكترونية البارزة خلال الأعوام السابقة، تستخدم هذه المجاميع تكتيكات الهندسة الاجتماعية للوصول إلى الأنظمة والمعلومات، اكتساب الدعاية والتأثير والترويج عن طريق تبنيهم عمليات القرصنة البارزة والكثير من التقنيات المتقدمة لتحقيق الغاية المرجوة.

المنظماتُ الإجرامية: هي مجموعاتٌ من مجرمي الإنترنت الذينَ ينفذونَ هجمات لتحقيقِ مكاسب مالية، غالبًا ما يستهدفون المؤسسات المالية والربحية والشركات الأخرى ببيانات أو أصول قيّمة، كتقنية التصيّد الاحتيالي (Carbanak)، ومجموعة (Lazarus) وهي مجموعة إجرامية سيبرانية تنسب لها العديد من عمليات القرصنة البارزة.

الجيوشُ الإلكترونية التي ترعاها الشركات: مجموعاتٌ من المتسللين والعاملين الذين توظفهم شركة ما لتنفيذ هجمات إلكترونية لدعم مصالح الشركة، قد يستهدفون المنافسين أو يسرقون الملكية الفكرية أو ينخرطون في أنشطة أخرى للحصول على ميزة في السوقِ من خلال عمليات التصيّد الاحتيالي وأساليب الهندسة الاجتماعية الأخرى للوصول إلى الشبكات والأنظمة المنافسة والحصول على ميزة في المفاوضات أو الصفقات التجارية.

الوحدات الشائعة للجيش الالكتروني:

1. مركز العمليات السيبرانية (COC): مركز العمليات السيبرانية مسؤول عن تخطيط وتنفيذ العمليات السيبرانية، وهذا يشمل إجراء الاستطلاع وتحديد الأهداف وتطوير استراتيجيات الهجوم والتنسيق مع الوحدات العسكرية الأخرى.

2. عمليات المعلومات (IO): قسم عمليات المعلومات مسؤول عن إدارة معلومات واتصالات الجيش، وهذا يشمل إدارة الشبكات وتطوير وتنفيذ استراتيجيات الاتصال، والرصد والدفاع ضد الهجمات السيبرانية.

3. الاستخبارات الإلكترونية (CI): قسم الاستخبارات الإلكترونية مسؤول عن جمع وتحليل المعلومات الاستخبارية بشأن التهديدات السيبرانية، يتضمن ذلك مراقبة وسائل التواصل الاجتماعي والمصادر الأخرى عبر الإنترنت، وتتبع نشاط المتسللين، وتطوير تقييمات التهديدات.

4. الدفاع السيبراني (CD): قسم الدفاع السيبراني مسؤول عن حماية شبكات وأنظمة الجيش من الهجمات الإلكترونية، وهذا يشمل تنفيذ تدابير الأمن السيبراني، وإجراء تقييمات الضعف، والاستجابة للحوادث.

5. قسم التدريب والتطوير (CST): قسم تدريب الأمن السيبراني مسؤول عن تدريب الأفراد العسكريين على أفضل ممارسات الأمن السيبراني، ويشمل ذلك تطوير برامج التدريب وإجراء تدريبات الأمن السيبراني وتقديم الدعم للوحدات العسكرية.

أهمية امتلاك الدول لجيوش إلكترونية قوية:

- ردع الخصوم: قد تتمكن الدولة التي تتمتع بجيش إلكتروني قوي عبر الإنترنت من ردع الخصوم عن تنفيذ الهجمات الإلكترونية من خلال إظهار القدرة على الرد بفعالية على مثل هذه الهجمات.

- حماية البنية التحتية الحيوية مثل شبكات الطاقة وشبكات الاتصالات، من الهجماتِ الإلكترونية.

- جمعُ المعلومات الاستخبارية: يمكنُ استخدام الجيش الإلكتروني لجمع المعلومات الاستخبارية عن الدول الأخرى، بما في ذلكَ معلومات حول قدراتها العسكرية، والتطورات السياسية، والأنشطة الاقتصادية، التوجهات المجتمعية.

- تعطيل عمليات العدو بما في ذلك عن طريق تعطيل أنظمة الاتصالات والملاحة باستخدام نظام تحديد المواقع العالمي(GPS) والتقنيات الأخرى التي تعتبر بالغة الأهمية للعمليات العسكرية.
- التأثير على الرأي العام: يمكن استخدام الجيوش الإلكترونية للتأثير على الرأي العام، عن طريق نشر معلومات مضللة أو التلاعب بمنصات التواصل الاجتماعي.

ومع ذلك، من المهم ملاحظة أن استخدام الجيوش الإلكترونية يمكن أن يكون له أيضًا عواقب سلبية، بما في ذلك إلحاق الضرر بالمدنيين الأبرياء، والإضرار بالعلاقات الدولية، ويؤدي إلى تصعيد الصراعات على هذا النحو، كذلك وجوب الجاهزية اللازمة للتصدي فيما لو قامت الجهة المستهدفة بالرد، لذلك يجب على الدول أن تنظر بعناية في المخاطر والفوائد المحتملة لاستخدام الجيوش الالكترونية.

أهم الخطوات التي يجب الوقوف عندها لبناء الجيش الالكتروني:

يُعدُّ بناء الجيوش الالكترونية عملية معقدة ومتعددة الأوجه تتطلب موارد وخبرات كبيرة، تتلخص اهمها في الخطوات التالية:

• استراتيجيّة إلكترونية: يجب أن تحدد الاستراتيجيّة الإلكترونية للدولة أهدافها وغاياتها في الفضاء السيبراني والدور الذي سيلعبه الجيش السيبراني في تحقيقها..

• إنشاء وحدة مخصصة للجيوش السيبرانية: قد تختار الدولة إنشاء وحدة مخصصة للجيش السيبراني داخل وكالتها العسكرية أو الاستخباراتية لتنفيذ عمليات إلكترونية، يجب أن تكون لدى هذه الوحدة الأفراد والمعدات والتدريب اللازمين لتنفيذ الهجمات الإلكترونية أو الدفاع ضدها.

• بناء البنية التحتية للدفاع السيبراني: ستحتاج الدولة أيضًا إلى الاستثمار في بناء البنية التحتية للدفاع السيبراني للحماية من الهجمات الإلكترونية، قد يشمل ذلك إنشاء وحدات دفاع إلكتروني متخصصة، وإنشاء نظام لاكتشاف الهجمات الإلكترونية والاستجابة لها ، والاستثمار في التكنولوجيا للحماية من التهديدات السيبرانية.

• الاستثمار في البحث والتطوير: للبقاء في طليعة التهديدات السيبرانية، يجب على البلدان

الاستثمار في البحث والتطوير، لتطوير تقنيات وتكتيكات جديدة للدفاع ضدها.

• بناء الشراكات والتعاون: يمكن أن يساعد بناء الشراكات والتعاون مع البلدان الأخرى والشركات الخاصة والمؤسسات البحثية في الوصول إلى الخبرات والموارد والتكنولوجيا لدعم جهود الجيوش السيبرانية.

تصنيف الجيش الإلكتروني ضمن تصنيفات الجيش العسكري:

يُعد دمج الجيش السيبراني مع بقية تفصيلات الجيش العسكري أمرًا ضروريًا لضمان قدرة الجيش على العمل بفعالية في ساحة المعركة الحديثة، فيما يلي بعض الخطوات التي يمكن اتخاذها لدمج الجيش السيبراني مع بقية الجيش:

• تطوير استراتيجية إلكترونية شاملة: يجب تطوير استراتيجية إلكترونية شاملة تُحدد أدوار ومسؤوليات الجيش السيبراني في دعمِ العمليات العسكرية، مع ضرورة دمجها مع الاستراتيجيات العسكرية الأخرى لضمانِ أن جميع الأنشطة العسكرية تعمل نحو هدف مشترك.

• تدريب الأفراد على العمليات السيبرانية: يجب أن يتلقى جميع الأفراد داخل الجيش تدريبات على العمليات السيبرانية ودورهم في دعم الجيش السيبراني، سيساعدُ ذلك على ضمان فهم الجميع لأهمية العمليات السيبرانية ويمكنه المساهمة بفعالية في هذه الجهود.

• إنشاء قنوات اتصال: يجب إنشاء قنوات اتصال فعالة بين الجيش السيبراني والوحدات العسكرية الأخرى لضمان مشاركة المعلومات بسرعة وكفاءة، يمكن أن يشمل ذلك اجتماعات منتظمة، وتمارين مشتركة، وقواعد بيانات مشتركة.

• تطوير معايير وإجراءات مشتركة: يجب تطوير معايير وإجراءات مشتركة للأمن السيبراني عبر المؤسسة العسكرية لضمان عمل جميع الوحدات معًا لتحقيق هدف مشترك. يمكن أن يشمل ذلك استخدام التقنيات والأدوات الشائعة، فضلاً عن إنشاء أفضل الممارسات للأمن السيبراني.

• تعيين ذوي الاختصاص بالمجال السيبراني للوحدات العسكرية.

أبرز الهجمات الإلكترونية التي تقوم بها الجيوش الإلكترونية:

• هجمات رفض الخدمة الموزعة: (DDoS) في هذا الهجوم، يتم استخدام شبكة من أجهزة الكمبيوتر المخترقة لإغراق موقع الويب أو الخادم المستهدف بحركة المرور، مما يجعل من الصعب أو المستحيل على المستخدمين الشرعيين الوصول إليه.

• هجماتُ البرامج الضارة: البرامجُ الضارة هي نوعٌ من البرامج المصممة لإلحاق الضرر بجهاز الكمبيوتر أو الشبكة أو استغلالهما، يمكن أن تتضمن الجيوش الإلكترونية استخدام البرامج الضارة للوصول غير المصرح به إلى نظام أو لسرقة البيانات الحساسة.

• هجمات التصيد الاحتيالي: في هجوم التصيد الاحتيالي، يرسل المهاجم بريدًا إلكترونيًا أو رسالة أخرى تبدو وكأنها من مصدر شرعي، ولكنها مصممة بالفعل لخداع المستلم للكشف عن معلومات حساسة أو النقر فوق ارتباط ضار.

• اختراق الشبكة: يمكن أن تتضمن الحرب السيبرانية استخدام أدوات وتقنيات متخصصة للحصول على وصول غير مصرح به إلى شبكة أو نظام.

تجارب الدول:

من الصعبِ تحديد جميع البلدان التي لديها قدرات متطورة للجيوش الإلكترونية بشكل قاطع، حيث أن العديد من الدول لديها عمليات إلكترونية سرية لم يتم الكشف عنها علناً ومع ذلك، يُعتقد على نطاق واسع أن العديد من البلدان قد طورت قدرات كبيرة في الجيوش السيبرانية، بما في ذلك:

• الولايات المتحدة: تعتبر الولايات المتحدة على نطاق واسع واحدة من أكثر الدول في العالم التي تمتلك قدرات متقدمة تكنولوجيا في الجيوش الإلكترونية، القيادة الإلكترونية للجيش الأمريكي مسؤولة عن الدفاع ضد الهجمات الإلكترونية وتنفيذها نيابة عن الحكومة الأمريكية.

• روسيا: تتمتع روسيا بتاريخ طويل من التجسس الإلكتروني ويُعتقد أنها نفذت العديد من الهجمات الإلكترونية البارزة، بما في ذلك هجوم "Not Petya" لعام (2017) الذي تسبب

في تعطيل وأضرار واسعة النطاق.

• الصين: اتُّهمت الصين أيضًا بتنفيذ حملات تجسس إلكتروني ضد دول أخرى، بما في ذلك الولايات المتحدة وأستراليا، بالإضافة إلى ذلك، يُعتقد أن الصين قد استثمرت بكثافة في بناء قدراتها في جيشها السيبراني.

• كوريا الشمالية: تم ربط كوريا الشمالية بعدد من الهجمات الإلكترونية البارزة،) بما في ذلك هجوم(2014) على Sony Pictures( )وهجومWannaCry(-ransom ware) (2017.

• إيران: اتُّهمت إيران بتنفيذ هجمات إلكترونية ضد دول من بينها الولايات المتحدة وإسرائيل والمملكة العربية السعودية.

الدول الأخرى التي يُعتقد أن لديها قدرات كبيرة في الجيوش الالكترونية تشمل إسرائيل وفرنسا والمملكة المتحدة.

يمكنُ أن يكونَ للجيش السيبراني عواقب خطيرة، مثل التسبب في انقطاع التيار الكهربائي أو تعطيل أنظمة النقل، كما يمكن أن تلحق الضرر بسمعة الدولة وعلاقاتها الدولية، لا سيما إذا نُسبت الهجمات إلى دولة معينة، ومن المؤكد بأن أيّ هجوم سيبراني غير مدروس وعبثي ستكون له عواقب وخيمة جداً على صاحب الهجوم والجهة المستهدفة، تتمثل بعدة نتائج منها: تصعيد النزاع بين الجهتين، وتوتر العلاقات الدولية، وفقدان البيانات الحساسة، وأضرار اقتصادية واجتماعية، وتعطيل البنى التحتية، لذلك لابد من ان تتوفر نقاط مهمة للحماية من التهديدات التي تشكلها الجيوش السيبرانية، ومنها الاستثمار في بناء البنية التحتية للدفاع السيبراني، بما في ذلك إنشاء وحدات دفاع إلكتروني متخصصة والاستثمار في التكنولوجيا للحماية من التهديدات الإلكترونية، يجب أن تعمل الدول أيضًا على وضع معايير دولية للسلوك في الفضاء السيبراني والتعاون مع بعضها البعض لتبادل المعلومات الاستخباراتية والاستجابة للتهديدات السيبرانية.

تجربة العراق مع الجيش الإلكتروني:

لعبت الجيوش الالكترونية دورًا مهما في النزاعات التي حدثت في العراق واستخدمتها الجهات الفاعلة الحكومية وغير الحكومية على سبيل المثال، استخدم تنظيم (داعش) الهجمات الإلكترونية كجزء من جهوده الدعائية والتجنيدية، واستهدفَ المواقع الحكومية والبنية التحتية بهجمات إلكترونية، استخدمت الحكومة العراقية أيضًا الجيوش الالكترونية كأداة لتعطيل عمليات داعش والجماعات المسلحة الأخرى، بشكل عام ساهم استخدام الجيوش الالكترونية في العراق في الطبيعة المعقدة والمتعددة الأوجه للصراعات في المنطقة آنذاك كما أثار أسئلة قانونية وأخلاقية حول الاستخدام المناسب للهجمات الإلكترونية في الحرب.

الذباب الالكتروني:

هو مصطلحٌ تم استحداثه في العالم الرقمي لوصف مجموعة من الحسابات الوهمية المبرمجة والتي تُدار آلياً من قبل مبرمجين تابعين لجهات رسمية او غير رسمية أو منظمات أو أفراد على مواقع التواصل الاجتماعي بشتى أنواعها، الهدف منه هو التأثير على الرأي العام في قضية ما أو شنّ حملة إعلامية ضد جهة معينة، يتم استخدام الذباب الإلكتروني لمشاركة المعلومات والبيانات التي يمكن أن تساعد في تشكيل الرأي العام حول قضية اجتماعية، اقتصادية أو سياسة معينة، فعلى سبيل المثال، إذا أرادت وكالة حكومية جمع تعليقات حول تغيير مقترح في السياسة، فقد تستخدم الذباب الإلكتروني لمشاركة المعلومات حول الاقتراح مع الجمهور وبذلك ستعرف الوكالة آراء الجمهور حول ذلك الاقتراح، أو أنّها ستروج له من خلال صناعة الرأي العام الوهمي لهذا الاقتراح وبثه على مواقع التواصل الاجتماعي وجعله مقبولاً أو مرفوضاً، ظهر هذا المصطلح قبل ست سنوات لكنه انتشر على نطاق أوسع عندما اقترن هذا المصطلح مع أزمة الخليج عام (2017)، ليتم تسليط الضوء عليه كأحد الوسائل لصنع وتوجيه الرأي العام.

فيما يتعلق بالتأثير على الرأي العام، فإنَّ ظهور وسائل الإعلام الإلكترونية والإنترنت قد أعطى الناس المزيد من الفرص للوصول إلى المعلومات والتعبير عن آرائهم من خلال منصات الإنترنت المختلفة. وقد أدى ذلك إلى إضفاء الطابع الديمقراطي على المعلومات وتنويع الأصوات

في الخطاب العام ومع ذلك، فقد سهّل أيضًا انتشار المعلومات الخاطئة وتعرض الناس لوسائل الإعلام التي تتوافق مع معتقداتهم الموجودة مسبقًا، مما أدى إلى إنشاء فقاعات تصفية وربّما تعزيز الأحكام المسبقة بشكل عام، يُعد تأثير الذباب الالكتروني على الرأي العام معقّداً ويعتمد على مجموعة متنوعة من العوامل الإيجابية والسلبية.

كيفية استخدام الذباب الإلكتروني لتوجيه الرأي العام:

• مشاركة المعلومات: يمكنُ استخدام الذباب الالكتروني لمشاركة المعلومات حول مشكلة او ظاهرة ما مع الجمهور، يمكن أن يشمل ذلك البيانات والأبحاث والمعلومات الأخرى ذات الصلة بالمشكلة او الظاهرة. يمكن أن تساعد مشاركة هذه المعلومات في تشكيل الرأي العام حول هذه القضية ويمكن أن تساعد أيضًا في إثراء عملية صنع السياسة.

• التماس التعليقات: يمكن القيام بذلك من خلال الاستطلاعات عبر الإنترنت أو حملات البريد الإلكتروني أو طرق أخرى، يمكن أن يساعد جمع التعليقات من الجمهور صانعي السياسات على فهم وجهات نظر عامة السكان ويمكن أن يساعد في تشكيل السياسة النهائية.

• التعامل مع أصحاب المصلحة: يمكن استخدام الذباب الالكتروني للتفاعل مع أصحاب المصلحة، مثل قادة الأعمال، ومجموعات المناصرة، والأطراف المهتمة الأخرى، لجمع المدخلات والتعليقات حول قضية ما، مما سينتج عنه فهم وجهات نظر المجموعات المختلفة وبالتالي بناء وضع خارطة الطريق.

• التأثير على التغطية الإعلامية

الفرق بين الجيش الإلكتروني والذباب الإلكتروني:

يتمثلُ الاختلاف الرئيسي بين الجيوش الإكترونية والذباب الإلكتروني في أن الجيوش الإلكترونية تنطوي على استخدام الكمبيوتر والهجمات القائمة على الإنترنت لإحداث ضرر، بينما يركز الذباب الالكتروني بشكل أكبر على مشاركة المعلومات ونشرها، يمكن أن يكون الاستخدام السيّئ للجيش الإلكتروني عواقب وخيمة، بما في ذلك إلحاق الضرر بالمدنيين،

والإضرار بالعلاقات الدولية، والتي بدورها تؤدي إلى تصعيد الصراع، بينما ينطوي استخدام الذباب الإلكتروني للتأثير على السياسة وعملية صنع القرار، بدون أذى جسدي أو عنف.

أمّا فيما يخص الاعتبارات القانونية، يمكن أن يثير استخدام الجيوش الإلكترونية أسئلة قانونية وأخلاقية، لأنها قد تنطوي على انتهاك للقوانين والمعايير الدولية في المقابل، يعتبر استخدام الذباب الإلكتروني لتشكيل السياسة بشكل عام عملية شرعية وديمقراطية.

الاستنتاج :

في العصر الرقمي اليوم، أصبحت التهديدات السيبرانية مصدر قلق كبير للدول في جميع أنحاء العالم والتي يمكن أن تتسبب في إلحاق أضرار جسيمة بالبنية التحتية للدولة واقتصادها وأمنها القومي لذلك ، فإن الغرض الأساسي من امتلاك جيش إلكتروني هو تعزيز مكانة الدولة من خلال إعطائها أداة قوية للدفاع ضد التهديدات الإلكترونية وشن هجمات إلكترونية ضد دول أخرى أو جهات فاعلة غير حكومية وحماية مواطنيها والبنية التحتية الحيوية من التهديدات الإلكترونية، استخدامه كأداة هجومية لتحقيق الأهداف الاستراتيجيّة، اكتسابه يُحسب كميزة تكتيكية لتعزيز موقع الدولة في الساحة الدولية ضمن العالم الحديث، في الوقت الذي أصبحت في هـ الحرب السيبرانية جزءاً لا يتجزأ من الحرب الحديثة، وتستثمر الدول في جميع أنحاء العالم بكثافة في قدراتها الإلكترونية لحماية أمنها ومصالحها الوطنية.