مجلة بحوث الإعلام الرقمي

دورية علمية محكّمة تصدر عن كلية الإعلام وتكنولوجيا الاتصال - جامعة السويس

العدد الثالث: يناير – يونيه ٢٠٢٤

مجلة بحوث الإعلام الرقمي

العدد الثالث: يناير-يونيه ٢٠٢٤

Digital Media Research Journal

Quarterly Scientific Journal issued by The Faculty of Media and Communication Technology - Suez University

The 3rd Issue
Jan-June
2024

مجلة بحوث الإعلام الرقمي

دورية علمية محكّمة

تصدر عن كلية الإعلام

وتكنولوجيا الاتصال

جامعة السويس

الهيئة الاستشارية:

أ. د. أحمد فاروق رضوان	الأستاذ بكلية الإعلام - جامعة الشارقة - الإمارات
أ .د. حمدى حسن	الأستاذ بكلية الإعلام - جامعة مصر الدولية
أ. د. سامى عبدالعزيز	العميد الأسبق لكلية الإعلام - جامعة القاهرة
أ. د. سامي الشريف	عميد كلية الإعلام - الجامعة الحديثة
أ. د. سهير صالح	عميد المعهد الدولي العالي للإعلام بأكاديمية الشروق
أ. د. السيد بهنسي	الأستاذ بكلية الإعلام - جامعة عين شمس
أ. د. عادل عبدالغفار	رئيس الأكاديمية الدولية للهندسة وعلوم الإعلام
أ. د. عادل فهمي	الأستاذ بكلية الإعلام - جامعة القاهرة
أ. د. عبد الرحمن محمد الشامي	الأستاذ بقسم الإعلام - كلية الآداب - جامعة قطر
أ.د. عبد الرحمن بن نامي المطيري	الأستاذ بجامعة الإمام محمد بن سعود الإسلامية - السعودية
أ.د. عبد الرزاق محمد الدليمي	الأستاذ بكلية الخوارزمي الجامعية التقنية - الأردن
أ. د. محمد شومان	عميد كلية الإعلام - الجامعة البريطانية بمصر
أ. د. محمد سعد	الأستاذ بقسم الإعلام - كلية الآداب - جامعة المنيا
أ. د. مني الحديدي	الأستاذ بكلية الإعلام - جامعة القاهرة
أ. د. هويدا مصطفي	عميد كلية الإعلام - جامعة مصر للعلوم والتكنولوجيا

مجلة بحوث الإعلام الرقمي
دورية علمية محكّمة تصدر عن
كلية الإعلام وتكنولوجيا الاتصال- جامعة السويس

المراسلات:

ترسل المراسلات باسم الأستاذ الدكتور رئيس مجلس الإدارة ورئيس التحرير - كلية الإعلام وتكنولوجيا الاتصال - جامعة السويس- السويس- مدينة السلام (١).

تليفون: 0623523774

البريد الإلكتروني: dmrjournal@media.suezuni.edu.eg

رقم الإيداع بدار الكتب المصرية: 24417 / 2023

الترقيم الدولي للنسخة المطبوعة: ISSN: 2812-5762

أهداف المجلة:

- الإسهام في تطوير المعرفة ونشرها، وذلك بنشر البحوث العلمية الأصيلة، والمراجعات العلمية في مجالات البحوث والدراسات في مجالات تخصص الإعلام الرقمى المختلفة.
- نشر البحوث العلمية المبتكرة، التي يعدّها أعضاء هيئة التدريس والهيئة المعاونة بالجامعات المصرية والعربية، والباحثون في المجالات العلمية لتخصص الاعلام الرقمى.
- توفير فرصة التقويم العلمى للبحوث من خلال إخضاع البحوث للرأي العلمي الذى يأخذ على عاتقة تقويم الجوانب العلمية والمنهجية في البحث العلمي.
- معالجة القضايا المعاصرة في إطار البحث العلمى، وتوظيفها في خدمة المجتمع، وخدمة القضايا الجوهرية التي تأسست من أجلها المجلة، وعلى رأسها التحول الرقمى.
- رصد ومتابعة اتجاهات البحث العلمى، من خلال الوقوف على النتائج العلمية للبحوث التي تصدرها المؤسسات الأكاديمية ومراكز البحوث المتخصصة.
- اهتمامات المجلة:
- تعنى المجلة بنشر:
- البحوث العلمية الرصينة في مجالات تخصص الإعلام الرقمى.
- البحوث والدراسات النقدية التي تتصل بالإصدارات في مجالات التخصص التي تعنى بها المجلة.
- البحوث والدراسات العلمية المعنية بمعالجة المشكلات المعاصرة والقضايا المستجدة في المجتمع، وخصوصًا التحول الرقمي.
- البحوث والتقارير والترجمات العلمية، وعرض الكتب الجديدة في مجال الإعلام الرقمي ومراجعتها.
- التقارير عن المؤتمرات والندوات العلمية في تخصص الإعلام الرقمي في مصر والعالم العربي والعالم.

قواعد النشر:

- أن تكون البحوث متخصصة في مسألة من المسائل التي تهتم بها المجلة.
- أن تكون البحوث متّسمة بالعمق والأصالة، بحيث يضيف كل بحث جديداً إلى المعرفة.
- أن تكون البحوث موثقة من الناحية العلمية بالمراجع والمصادر والوثائق.
- تنشر البحوث في المجلة باللغات العربية والإنجليزية والفرنسية.
- أن يقر صاحب البحث بأن بحثه عمل أصيل له وليس مشتقاً من رسالتي الماجستير والدكتوراه العائدتين له.
- ألاّ يكون البحث قد سبق نشره، ويقدم الباحث تعهداً بذلك.
- ألاّ يكون البحث مقدماً للنشر في مجلة أخرى.
- لا يجوز نشر البحث في مكان آخر بعد إقرار نشره في مجلة كلية الإعلام جامعة السويس إلاّ بعد الحصول على إذن كتابي بذلك من رئيس التحرير.
- موافقة المؤلف على نقل حقوق النشر كافة إلى المجلة، وإذا رغبت المجلة في إعادة نشر البحث فإن عليها أن تحصل على موافقة مكتوبة من صاحبه.
- أصول البحث التي تصل إلى المجلة لا تردّ سواء أنشرت أم لم تنشر.
- يُمنح الباحث نسخة واحدة من العدد المنشور فيه بحثه مع خمس مستلات منه.

متطلبات النص المقدم للنشر:

- يجب ألاّ يزيد عدد صفحات البحث عن (٣٠ صفحة) بما فيها الأشكال والصور والجداول والمراجع)بمقاس A4 / أو حوالي ٩٠٠٠ كلمة).
- يذكر اسم المؤلف وعنوانه الحالي بعد عنوان البحث مباشرة مع ذكر عنوانه، ومرتبته العلمية، وبريده الإلكتروني.
- تقدم البحوث مكتوبة بخط Arabic Simplified حجم (١٤) للنصوص في المتن، وبالخط نفسه بحجم (١٢) للهوامش في نهاية البحث، وتكون الهوامش (٢,٥ سم) من كل طرف.

- تُدرج الرسوم البيانية والأشكال التوضيحية في متن البحث، وتكون الرسوم والأشكال باللونين الأبيض والأسود وترُقم ترقيمًا متسلسلاً، وتُكتب أسماؤها والملاحظات التوضيحية في أسفلها.
- تُدرج الجداول في متن البحث وترُقم ترقيمًا متسلسلاً وتُكتب أسماؤها في أعلاها، أما الملاحظات التوضيحية فتُكتب أسفل الجدول.
- تُذكر الهوامش آخر البحث، وتُذكر بعدها مباشرة قائمة المصادر والمراجع مرتبة ترتيباً هجائياً.
- يجب أن يحتوى البحث على ملخص وافٍ بحدود (١٥٠-٢٠٠) كلمة باللغة المكتوب فيها البحث، وملخص وافٍ أيضًا بحدود (١٥٠-٢٠٠) كلمة باللغة الإنجليزية، ويُكتب الملخصان في صفحتين مستقلتين.
- يُذكر مرة واحدة في البحث المصطلح العلمى باللغة العربية وبجانبه المصطلح باللغة الإنجليزية أو الفرنسية عند وروده أول مرة، ويُكتفى بعد ذلك بكتابته باللغة العربية.

فهرس المحتويات

فهرس المحتويات

مقدمة العدد

"أما قبل"

إن صدور مجلة علمية متخصصة هو ميلاد أمل جديد، وخصوصًا إذا كانت هذه المجلة بعنون "مجلة بحوث الإعلام الرقمي"؛ لأنها تأخذنا مباشرة إلى ساحات علوم المستقبل، وهي علوم وبحوث العصر الرقمي الذي تعيشه الإنسانية الآن، ويأتي العدد الثالث من هذه المجلة الوليدة أيضا كخطوة من خطوات استكمال البناء العلمي لكلية الإعلام وتكنولوجيا الاتصال بجامعة السويس، وذلك بعد اعتماد وبدء برنامج الماجستير: «الإعلام الرقمي»، وهو أحد البرامج الخاصة بالدراسات العليا بالكلية، فضلا عن الدبلومات المهنية، التي تم اعتمادها أيضا، والعمل مستمر في باقي البرامج في مرحلتي الماجستير والدكتوراه للانتهاء منها قريبا إن شاء الله.

ويطالع القارئ في هذا العدد مقالين علميين، المقال الأول تحت عنوان: «الحرب الرقمية»، للأستاذ الدكتور أمين سعيد، عميد الكلية. والمقال الثاني للأستاذ الدكتور حسن علي، العميد الأسبق للكلية، وهو بعنوان: «إشكاليات بحوث الإعلام الرقمي».

كما يضم هذا العدد بين دفّتيه عشر دراسات تتناول موضوعات بحثية على قدر كبير من الأهمية، فقد جاءت الدراسة الأولى تحت عنوان: «حول الاتجاهات الحديثة في دراسات وممارسات الإعلام: الابتكار وريادة الأعمال الإعلامية»، قراءة وترجمة وتحرير الأستاذ الدكتور عبدالله بن محمد الرفاعي، الأستاذ بقسم الصحافة والإعلام الجديد، كلية الإعلام والاتصال، جامعة الإمام محمد بن سعود بالرياض.

أما الدراسة الثانية فقد أعدها كلّ من الأستاذ الدكتور مناور بيان الراجحي، الأستاذ بقسم الصحافة، كلية الآداب، جامعة الكويت، والدكتور سليمان محمد آرتي، الأستاذ المساعد بقسم النقد والأدب المسرحي وعضو مجلس إدارة المجلس الوطني للثقافة والفنون والآداب بالكويت، وهي تحت عنوان: «أثر وسائل التواصل الاجتماعي في تعزيز الهوية الوطنية لدى الشباب الكويتي: دراسة ميدانية».

وجاءت الدراسة الثالثة تحت عنوان: «أخلاقيات العلاقات العامة وممارستها: بحث تأصيلي تنظيري»، وهي من إعداد الأستاذ الدكتور عبدالرزاق محمد الدليمي، الأستاذ بقسم الإعلام بكلية الخوارزمي الجامعية التقنية الأردنية، والأستاذ وليد كاطع، بكلية الإدارة والاقتصاد، الجامعة المستنصرية، العراق.

أما الدراسة الرابعة فقد جاءت تحت عنوان: «توظيف الأسطورة في وسائل الإعلام: بحث استقرائي تحليلي في إطار القرن ٢١"، وهي أيضا من إعداد الأستاذ الدكتور عبدالرزاق محمد الدليمي، الأستاذ بقسم الإعلام بكلية الخوارزمي الجامعية التقنية الأردنية.

وقد جاءت الدراسة الخامسة تحت عنوان: «الحرب الرقمية والأمن السيبراني: خطر التهديدات يقابله

تعزيز الدفاعات"، وأعدها الأستاذ الدكتور حبيب البدوي، الأستاذ بقسم اللغة اليابانية جامعة لبنان.

أما الدراسة السادسة فقد كانت من إعداد كلّ من الدكتورة سهير سيف الدين والدكتورة إيمان إبراهيم، وهي تحت عنوان: «الصحافة العلمية في ضوء التأهيل الإعلامي الأكاديمي بالجامعات المصرية».

في حين جاءت الدراسة السابعة تحت عنوان: «المداخل النظرية لدراسة الأداء المهني للقائم بالاتصال في الدراسات الإعلامية»، للدكتور مدحت رشدي، الكاتب الصحفي بمؤسسة أخبار اليوم.

وتحت إشراف الدكتورة سالي أسامة، أستاذة الإعلام المشارك بجامعة الملك فيصل، جاءت الدراسات الثامنة والتاسعة والعاشرة، فكانت الدراسة الثامنة تحت عنوان: «دور مواقع التواصل الاجتماعي في تنمية وعي المرأة السعودية بالأمن الغذائي»، للأستاذة آلاء عبدالمحسن الشعيبي، الباحثة بجامعة الملك فيصل. والدراسة التاسعة كانت للأستاذة منيره عبد الرحمن الماجد، الباحثة بجامعة الملك فيصل، وهي تحت عنوان: «دور منصات التواصل الاجتماعي للأندية الرياضية في الحد من التعصب الرياضي». أما الدراسة العاشرة فقد كانت من إعداد الأستاذة نوره فهيد عيد الدوسري، الباحثة بجامعة الملك فيصل، وهي تحت عنوان: «تحليل مشاعر مستخدمي منصة (X) للمرأة السعودية».

والله من وراء القصد،،،

مدير التحرير

أ.م.د. السيد عبدالرحمن

الحرب الرقمية

الأستاذ الدكتور أمين سعيد عبدالغني

عميد كلية الإعلام ــ جامعة السويس

مقدمة:

تسعى هذه الورقة البحثية للتعريف بمجال الحرب الرقمية، هذا المجال الناشئ الذي تتزايد أهميته، وله تأثير كبير على جميع جوانب السياسة المعاصرة والمجتمع والثقافة. إنه مجال عالمي بطبيعته، شديد الحساسية للتطورات المعاصرة ويهتم بالتغيرات التكنولوجية المستمرة وتأثيرها.

وتُفهم الحرب الرقمية على أنها الطرق التي تحول بها التقنيات والوسائط الرقمية كيفية خوض الحروب وتجربتها وعيشها وتمثيلها والإبلاغ عنها ومعرفتها وتصورها وتذكرها ونسيانها.

وهو مجال تتقاطع فيه بحوث الاعلام الرقمي مع بحوث ودراسات تقنية الحروب والصناعات العسكرية الرقمية. وتتداخل فيه بحوث العمليات العسكرية ودارسات الحرب مع دراسات الفن والسياسة والعلاقات العامة والدراسات الاجتماعية والثقافية. وتشارك فيه بحوث التاريخ والجغرافيا مع علوم الاثار.

وتكشف الدراسة عن تاريخ وتطور مفهوم الحرب الرقمية وتتبع مجموعة من استخدامات التكنولوجيا الرقمية في الحروب والصراعات المعاصرة التي بدأت بحرب الخليج عام ١٩٩١، التي غيرت التطورات التكنولوجية في مرحلة ما بعد فيتنام وأسست نموذجاً جديداً للإدارة العسكرية والإعلامية التي أصبحت وثيقة الصلة. وتكشف كيف تم تطبيق هذا النموذج في كوسوفو (١٩٩٩)، أفغانستان (٢٠٠١) والعراق (٢٠٠٣)، ومع ثورة الويب ٢.٠، تعطلت هذه السيطرة المعلوماتية وأتاحت التقنيات الرقمية الجديدة لأي شخص أن يكون منتجاً إعلامياً مما ادي إلى ظهور نمط جديد من "الحرب التشاركية"، كما يظهر في غزة والعراق وسوريا وغيرها من الأحداث السياسية الكبرى في الآونة الأخيرة، مثل أحداث ١١ سبتمبر والحرب على الإرهاب وما بعدها.

وتكشف الدراسة أخطر جانب من جوانب هذه الحرب وهو الحروب الاهلية الرقمية التي تستخدم الفروق الاثنية وللدينية والثقافية والاجتماعية لإثارة الجميع ضد الجميع في مناطق الصراعات المستهدفة. بتوظيف جديد لأساليب الحرب النفسية القديمة واستهداف مجتمعات كاملة وليس الجيوش فقط.

وتعرض الدراسة استراتيجيات الحروب الرقمية الجديدة وتقدم أبرز تكتيكات الدفاع في هذه الحرب، وتشير الى مفاهيم الاحتلال الرقمي والمقاومة الرقمية والاستقلال الرقمي.

١-مفهوم الحرب الرقمية:

تُفهم الحرب الرقمية على أنها الطرق التي تحول بها التقنيات والوسائط الرقمية كيفية خوض الحروب وتجربتها وعيشها وتمثيلها والإبلاغ عنها ومعرفتها وتصورها وتذكرها ونسيانها.

وهذا المجال الناشئ تتزايد أهميته وقد كان له تأثير كبير على جميع جوانب السياسة المعاصرة والمجتمع والثقافة. إنه مجال عالمي بطبيعته، شديد الحساسية للتطورات المعاصرة ويهتم بالتغيرات التكنولوجية المستمرة وتأثيرها.

في السنوات الأخيرة: جلبت لنا ويكيليكس رؤية جديدة لحروبنا المستمرة؛ الكتب الشعبية والأكاديمية على الطائرات بدون طيار والحرب الإلكترونية بدأت تظهر؛ بدأت الروبوتات الفتلكة المتمتعة بالتحكم الذاتي تظهر في النقاش العلني وانتشر الوعي المتزايد بالأثر الثوري لوسائل التواصل الاجتماعي في مناطق الصراع. ظهرت موضوعات مثل القرصنة، الاختراق، الحروب الأهلية الرقمية والمراقبة الحكومية؛ وكان نجاح تنظيم للدولة الإسلامية يعني أن الجميع كانوا يناقشون الإرهاب عبر الإنترنت؛ وتجرى الحروب في جميع أنحاء العالم الآن على منصات وسائل التواصل الاجتماعي والهواتف الذكية الشعبية بمشاركة من الجيوش والمواطنين والدول بأساليب مستحدثة بشكل متزايد، والتطورات الجديدة في مجال الذكاء الاصطناعي العسكري، والمحاكاة، والواقع المعزز، والأسلحة هي الأخبار الرائجة و سرعان ما أصبح الجميع على اطلاع على موضوع الهجمات الإلكترونية التي تشنها مجموعات الإنترنت.

الموضوعات الرئيسية المتقاطعة:

يتقاطع مفهوم الحرب الرقمية مع مجموعة واسعة من المجالات العلمية والبحثية والتطبيقية، ومن أهم هذه المجالات:

- **وسائل الإعلام والصحافة:** الإعلام عن الحرب الرقمية، التصوير الصحفي وصناعة الأفلام؛ وسائل التواصل الاجتماعي والحرب، بما في ذلك استخدامها من قبل الحكومات والجيوش والجنود والمدنيين؛ دور التقنيات مثل الهاتف للذكي والتطبيقات؛ التجربة العامة للحرب والمشاركة فيها؛ ويكيليكس وتسريب أخبار وهمية (الانتشار المتعمد وغير المتعمد)؛ الصور الرقمية والرسومات.
- **التقنيات العسكرية:** التقنيات الرقمية والأنظمة والأسلحة؛ الطائرات بدون طيار (وغيرها من النظم غير المأهولة)؛ حرب الكترونية؛ الحرب المعلوماتية، للدعاية، وحرب إلكترونية؛ الاستخبارات ومكافحة التمرد؛ الاستخدام العسكري للمحاكاة، الواقع الافتراضي والواقع المعزز؛ التقنيات القابلة للارتداء، تحسينات سايبورغ والأسلحة "الذكية"؛ الذكاء الاصطناعي (الذكاء الاصطناعي)؛ الروبوتات والأنظمة للذاتية القاتلة. وغيرها من التقنيات للناشئة مع الآثار العسكرية مثل تقنية النانو.
- **الفن:** التدخلات السياسية والجمالية والفنية والقانونية والأخلاقية والتجريبية والوسائط المتعددة في الحرب والصراع.
- **دراسات الحرب:** بما في ذلك نظرية الحرب وورقات الموقف حول الحرب المعاصرة ومستقبل الحرب وتحدياتها، بما في ذلك التدريب والاستعداد والعقيدة.
- **السياسة والعلاقات العامة:** القضايا الرئيسية حول الإرهاب والتقنيات الرقمية؛ المراقبة والتدابير الوقائية؛ الأمن السيبراني والبنية التحتية الحيوية؛ الحروب الأهلية الرقمية والاحتجاجات. دور

المتسللين ومجموعات "المتسللين" مثل مجهول؛ "التسليح"، وتحول ذلك إلى شيء ليس له غرض سياسي – عسكري مسبق، التصيد وظهور الحرب قليلة السياسية.

- **للدراسات الاجتماعية والثقافية:** التمثيل الشعبي للحرب الرقمية في ألعاب الفيديو والخيال العلمي؛ السياسة الرقمية مقابل السياسة التناظرية؛ وسائل الاتصال / الانفصال بين ممارسات الحرب الرقمية وغير الرقمية أو خارجها.
- **الجغرافيا:** القضايا الإقليمية حول الحرب. حرب عالمية الخبرة المكانية والسيطرة. مؤقتات الحرب؛ مناظرات الاستعمار/الاستعمار الرقمي.
- **القانون:** تمثيل النزاع في الأطر القانونية للقانون للدولي؛ أشكال جديدة لجمع الأدلة وتوثيق جرائم الحرب؛ حقوق الانسان؛ العمارة الجنائية.
- **للذاكرة والتاريخ:** قضايا حول الرقمنة. للتذكر والتنظيم الرقمي والتنظيمي؛ التعليم؛ المتاحف ومحفوظات الحرب؛ والوثائق الرقمية. علم الآثار ساحة المعركة؛ السجلات العسكرية والعامة؛ الاحتفال والتذكير في ألعاب الفيديو والوسائط التفاعلية، ومحركات البحث.
- **علم الآثار الإعلامي:** علم الأنساب التاريخي والمادي الرقمي في المنصات الوسيطة السابقة وأجهزة الطاقة/المعرفة.

الحرب في المجال الخامس:

في الأشهر التي سبقت انتخابات عام ٢٠١٦، تم اختراق اللجنة الوطنية للديمقراطية. تم تسريب المستندات، ونشرت أخبار وهمية عبر وسائل التواصل الاجتماعي – باختصار، شن المتسللون هجوماً منهجياً على الديمقراطية الأمريكية. سواء كانت هذه الحرب أم لا، فهي مسألة للنقاش. بمعنى أبسط، يتم تعريف فعل الحرب السيبرانية على أنه هجوم من جانب دولة على البنية التحتية الرقمية لأخرى.

هذه التهديدات هي ما يسميه صموئيل وولي، مدير الأبحاث في مختبر الذكاء الرقمي بمعهد المستقبل، "الدعاية الحاسوبية"، والتي يعرفها على أنها انتشار المعلومات المضللة والهجمات ذات الدوافع السياسية المصممة باستخدام "الخوارزميات، والأتمتة، والعقل البشري". وبدأت عبر الإنترنت، وخاصة وسائل التواصل الاجتماعي. في بيان لصحيفة المستقبل، أضاف وولي أن هذه الهجمات "تهاجم أجزاء أساسية من الديمقراطية: الصحافة، الخطاب المدني المفتوح، الحق في الخصوصية، والانتخابات الحرة".

قد تكون الهجمات مثل تلك التي سبقت انتخابات ٢٠١٦ نذيراً لما سيحدث: نحن نعيش في فجر عصر الحرب الرقمية – أكثر خبثًا وأقل وضوحاً من المعارك التقليدية، مع مناوشات لا تتوج بمواجهات مثل بيرل الميناء أو ١١/٩.

إن تعريفاتنا للحرب – مبرراتها وتكتيكاتها – تتغير. بالفعل، هناك خط ضبابي بين التهديدات التي تهدد شبكات الدولة وتلك التي تحدث على ترابها. كما كتب أدريان لافورنس في *The Atlantic*: يجب اعتبار فعل الحرب السيبرانية عمل حرب.

حرب من s٠ و s١:

منذ ما يزيد قليلاً عن عقد من الزمان، بدأت القيادة الإلكترونية للولايات المتحدة في تطوير ما يمكن أن يصبح أول سلاح رقمي في العالم: دودة كمبيوتر ضارة تعرف باسم Stuxnet. وكان من المزمع استخدامها ضد حكومة إيران لإحباط برنامجها النووي، وصحيفة نيويورك تايمز ذكرت. وفقًا للطبيعة الحقيقية للعمليات السرية العسكرية، لم تقم حكومة الولايات المتحدة أبدًا بالاعتماد علنيًا على Stuxnet، ولا حكومة إسرائيل التي تعاونت معها الولايات المتحدة لإطلاق العنان لها.

تعتمد قوة Stuxnet على قدرتها على الاستفادة من ثغرات البرامج في شكل "استغلال يوم صفر". يصيب الفيروس النظام بصمت، دون مطالبة المستخدم بعمل أي شيء، مثل تنزيل ملف ضار، عن غير قصد، من أجل الدودة نافذة المفعول. ولم تنتشر فقط عبر النظام النووي الإيراني – فقد انتشرت الدودة عبر أنظمة Windows في جميع أنحاء العالم. حدث ذلك جزئيًا لأنه من أجل للدخول في النظام في إيران، قام المهاجمون بإصابة أجهزة الكمبيوتر خارج الشبكة (ولكن يعتقد أن ذلك مرتبط به) حتى يكونوا بمثابة "حاملين" للفيروس.

ومع ازدهارها، بدأ المحللون يدركون أن شركة Stuxnet أصبحت أول لعبة في الحرب السيبرانية. مثل الحرب التي تحدث في العالم المادي، فإن الحرب الإلكترونية تستهدف وتستغل نقاط الضعف. تستثمر الدول القومية الكثير من الموارد لجمع معلومات عن أنشطة الدول الأخرى. إنهم يحددون الأشخاص الأكثر نفوذاً في الدولة وفي المجتمع عامة، والتي قد تكون مفيدة عند محاولة التأثير على الرأي العام لصالح أو ضد عدد من القضايا الاجتماعية والسياسية.

إن جمع التفاصيل الدقيقة عن انعدام الأمن الاقتصادي في بلد آخر، والمشاكل الصحية، وحتى عاداتها الإعلامية هي غنائم كبرى في لعبة الاستخبارات؛ إن معرفة المكان الذي "ستؤذي فيه أكثر شيء" إذا كانت دولة ما ستشن هجوماً هو على الأرجح الكفاءة – بقدر ما هي الفاعلية.

تاريخياً، كان جمع المعلومات متروكًا للجواسيس الذين خاطروا بالحياة وأطرافهم للتسلل الفعلي إلى مبنى (وكالة أو سفارة) أو سرقة مستندات أو الملفات أو محركات الأقراص الصلبة والهروب. وكلما كانت هذه المهام أكثر سرية، وأقل قدرة على تنبيه أصحاب هذه الأهداف، كان ذلك أفضل. بعد ذلك، كان الأمر متروكًا للمحللين، أو في بعض الأحيان مفكّري الشفرات، لفهم المعلومات حتى يتمكن القادة العسكريون والاستراتيجيون من تحسين خطتهم الهجومية لضمان أقصى قدر من التأثير.

جعلت الإنترنت الحصول على هذا النوع من المعلومات شبه فوري. إذا كان أحد المتسللين يعرف مكان البحث عن قواعد البيانات، ويستطيع اختراق تدابير الأمان الرقمية للوصول إليها، ويمكنه فهم المعطيات التي تحتويها هذه الأنظمة، فيمكنه الحصول على جبل من المعلومات في غضون ساعات قليلة، أو حتى الدقائق. يمكن لدولة العدو البدء في لستخدام المعلومات الحساسة قبل أن يدرك أي شخص أن هناك شيئًا ما خاطئًا.

في عام ٢٠١١، وصف وزير الدفاع الأمريكي آنذاك ليون بانيتا التهديد الوشيك لـ "ميناء بيرل الإلكتروني" الذي يمكن لدولة معادية اختراقه في الأنظمة الرقمية لإغلاق شبكات الطاقة أو حتى الذهاب أبعد من ذلك و"السيطرة على المحولات الحيوية وعرقلة مسارها" في عام ٢٠١٤، أفادت *مجلة TIME* أن هناك ٦١٠٠ انتهاك للأمن السيبراني في الولايات المتحدة في ذلك العام؛ صنّف مدير الاستخبارات القومية آنذاك الجريمة الإلكترونية باعتبارها التهديد الأمني رقم واحد للولايات المتحدة في ذلك العام، وفقاً *لمجلة تايم*.

هجمات فيروسات الكمبيوتر التي تدعى الحرمان من الخدمة(DDS) ، حققت الإضرار الفعلي بشبكة الكهرباء – لا تزال استراتيجيات الحرب في المجال الخامس تتطور. وأصبحت جرائم القرصنة أمرا شائع الحدوث إلى حد ما عن البنوك، والمستشفيات، وتجار التجزئة، والجامعات. ولكن إذا كانت هذه المراكز من مجتمع فاعل تشلها حتى أكثر الجرائم الإلكترونية "الروتينية"، يمكنك أن تتخيل فقط الدمار الذي سيتبع هجوماً بموارد جيش الدولة المعادية بالكامل وراءه.

لا تزال الدول تحتفظ بأوراقها بالقرب من صدرها، لذلك لا يوجد أحد على يقين من الدول القادرة على شن هجمات بأكبر حجم. تعتبر الصين قوة عالمية للتكنولوجيا والابتكار، لذلك من الآمن افتراض أن حكومتها لديها الوسائل لشن هجوم سيبراني واسع النطاق. كوريا الشمالية، أيضاً، يمكن أن تمتلك التكنولوجيا – وبما أن علاقتها مع الدول الأخرى تصبح عدائية على نحو متزايد، فإن المزيد من الحافز لتحسينها. بعد التداعيات السياسية الأخيرة بين كوريا الشمالية والصين، ذُكر أن روسيا تدخلت لتزويد كوريا الشمالية بالإنترنت – وهي خطوة يمكن أن تشير إلى وجود تحالف قوي. روسيا هي أكبر تهديد بقدر ما تشعر الولايات المتحدة بالقلق؛ لقد أثبتت البلاد أنها مهاجم رقمي قادر وفاعل.

كان للتأثير الروسي تأثير واضح على انتخابات عام ٢٠١٦، لكن هذا النوع من الحروب لا يزال جديداً. لا توجد اتفاقية جنيف، ولا معاهدة، ترشد كيف ينبغي لأي دولة أن تفسر هذه الهجمات، أو ترد عليها. للحصول على هذا النوع من الحكم، سيحتاج القادة العالميون إلى النظر في تداعيات عامة السكان وتحديد كيفية تأثير الحرب الإلكترونية على المواطنين.

في الوقت الحالي، لا يوجد مبدأ توجيهي لتحديد متى (أو حتى كيف) التصرف بناءً على فعل متصور للحرب الإلكترونية. هناك غموض يزداد تعقيداً بسبب حقيقة أنه إذا استفاد من هم في السلطة من الهجوم نفسه، أو حتى قاموا بتنظيمه، فما الحافز الذي يجب عليهم الانتقام منه؟

إذا كانت الحرب الإلكترونية لا تزال شيئاً من الغرب المتوحش، فمن الواضح أن المواطنين هم الذين سيصبحون الضحايا. ترتبط ثقافتنا واقتصادنا والتعليم والرعاية الصحية وسبل العيش والاتصال بشبكة الإنترنت بشكل لا ينفصم. إذا أرادت دولة معادية أن يكون للهجوم "التقليدي" أكثر (تفجير إرهابي أو إطلاق سلاح كيميائي، أقصى تأثير)، فلماذا لا تهيئ لهجوم قد يعمل على تجريد الأشخاص من حساباتهم

المصرفية، وإغلاق المستشفيات وعزل المستجيبين للطوارئ، وأؤكد أن المواطنين لن يكن لديهم وسيلة للتواصل مع أفراد أسرهم في فترة من الفوضى لا مفر منها؟

كما أوضح خبير ومؤلف الأمن السيبراني ألكساندر كليمبرج لـــــVox، فإن أي هجوم سيبراني واسع النطاق سيؤدي إلى أضرار "تعادل التوهج الشمسي من حيث البنية التحتية الضارة". وباختصار، سيكون مدمراً.

٢- أمريكا مبادرة الدفاع الابتكاري لعامي ٢٠١٤ / ٢٠١٨

استراتيجية عسكرية جديدة:

في صيف عام ٢٠١٦، بدأت مجموعة تُسمى Shadow Brokers بتسريب معلومات سرية للغاية حول ترسانة الأسلحة الإلكترونية في وكالة الأمن القومي (NSA)، بما في ذلك الأسلحة السيبرانية قيد التطوير. لا تزال الوكالة لا تعرف ما إذا كان التسريب يأتي من شخص ما داخل وكالة الأمن القومي، أو إذا تسلل فصيل أجنبي إلى عمليات الوصول المصمم خصيصاً (الوحدة الخاصة لوكالة الأمن القومي لجمع المعلومات الاستخباراتية عن الحرب الإلكترونية).

على أي حال، فإن خرق وحدة كان من المفترض أن تكون من بين أكثر الحكومات غموضاً لم يسبق له مثيل في للتاريخ الأمريكي. وحتى ان رئيس مايكروســـوفت براد ســـميث، على الرغم من خطورة هذا الانتهاك، قارن الوضع " بسرقة صواريخ توماهوك من الجيش"، كما صاغ منشوراً مدويا يدعو الحكومة الأمريكية للاعتراف بفشلها في الحفاظ على أمان المعلومات.

في المرة الأخيرة التي هز فيها هذا التســـرب وكـالـة الأمن القومي، كان ذلك في عام ٢٠١٣، عندما أصدر إدوارد سنودن معلومات سرية حول ممارسات المراقبة في الوكالة. ولكن كما أشار الخبراء، فإن المعلومات التي سرقها Shadow Brokers هي أكثر ضرراً بكثير. حتى أن *نيويورك تايمز* أعلنت في وقت ســابق من ذلك العام، بدأ هجوم برمجيات الفدية يعرف باســم "WannaCry" في عبور شــبكة الإنترنت، حيث قام بضرب المنظمات من الجامعات في الصين إلى المستشفيات في إنجلترا. وقع هجوم مماثل على شركة IDT Corporation، وهي شركة اتصالات مقرها في نيوارك بولاية نيوجيرسي، في أبريل، عندما اكتشفها رئيس عمليات الشركة العالمي، جولان بن أوني. كما قال بن أوني لصحيفة *نيويورك تايمز*، كان يعلم في الحال أن هذا النوع من هجوم الفدية كان مختلفاً عن محاولات أخرى ضد شركته – إنه لم يسرق فقط المعلومات من قواعد البيانات التي تسللها، بل سرق أوراق الاعتماد المطلوبة للوصول إلى قواعد البيانات هذه. يعني هذا النوع من الهجوم أن المتســـللين لا يمكنهم فقط أخذ تلك المعلومات دون اكتشافها، ولكن يمكنهم أيضاً مراقبة من يصل إلى هذه المعلومات بشكل مستمر.

اعتمد كل من WannaCry وهجوم IDT على الأسلحة الإلكترونية التي سُرقت وتم إطلاقها من قبل Shadow Brokers، حيث استخدمها بفعالية ضد الحكومة التي طورتها. ظهرت WannaCry على Eternal Blue، الذي استخدم خوادم Microsoft غير المتطابقة لنشر البرامج الضارة (كوريا الشمالية

استخدمتها لنشر الفدية إلى ٢٠٠٠٠٠ خادم عالمي في غضون ٢٤ ساعة فقط). استخدم الهجوم على IDT أيضاً Eternal Blue، لكنه أضاف إليه سلاحاً آخر يسمى Double Pulsar، والذي يخترق الأنظمة دون تعثر إجراءات الأمان الخاصة به. هذه الأسلحة قد صممت لتكون مضرة وصامتة. ينتشر بسرعة ودون رادع، يذهب دون الكشف عنها بواسطة برنامج مكافحة الفيروسات في جميع أنحاء العالم.

كانت الأسلحة قوية ولا هوادة فيها، مثلما أرادت وكالة الأمن القومي. بالطبع، ما لم تقصده وكالة الأمن القومي هو أن الولايات المتحدة ستختتم رحلتها. وكما أعرب بن أوني عن أسفه *لصحيفة نيويورك تايمز*، "لا يمكنك اللحاق به، وهو يحدث تحت أنوفنا". وقال "العالم ليس جاهزاً لذلك".

أفضل دفاع:

قد يشعر المواطن العالمي العادي بأنه محروم من قلة التأهب الواضح لحكومته، لكن الدفاع ضد مذبحة الحرب السيبرانية يبدأ فعلياً بنا: بدءاً بفحص واقعي تأخر طويلًا بخصوص علاقتنا بالإنترنت. حتى لو لم تكن الوكالات الفيدرالية آمنة رقمياً كما قد يرغب بعض النقاد، فلا يزال المواطن العادي يجب ان يحمي نفسه.

"إن أول وأهم نقطة هي أن تدرك أن هناك تهديد حقيقي، وهذا يمكن أن يحدث،" كما قال خبير الأمن السيبراني الدكتور إريك كول لصحيفة المستقبل. وأضاف Cole أنه بالنسبة للأشخاص العاديين، فإن أفضل دفاع هو معرفة مكان تخزين معلوماتك إلكترونياً وعمل النسخ الاحتياطية المحلية لأي شيء مهم حتى الخدمات مثل التخزين السحابي، والتي غالباً ما توصف بأنها أكثر أماناً، لن تكون محصنة ضد الهجمات المستهدفة التي تدمر البنية التحتية الداعمة – أو شبكات الطاقة التي تبقي هذا الإطار قيد التشغيل.

"نحن في الغالب نحب الذهاب وإعطاء الكثير من المعلومات والقيام بكل شيء إلكترونيا"، قال كول لـــ Futurism، "لكن يجب أن تسأل نفسك: *هل أريد حقًا تقديم هذه المعلومات؟*"

ومع ذلك، يجادل بعض الخبراء بأنه لا ينبغي اعتبار الهجوم الإلكتروني السريع على الشركات والمواطنين الأمريكيين عملاً حربياً. يأتي مصطلح "الحرب" مع بعض الزخارف – تورط الحكومات، وتحويل الموارد، والوضع برمته يتصاعد بشكل عام، كما قال توماس ريد، أستاذ وكاتب بصحيفة *بوسطن غلوب*. قد يكون لهذا النوع من الشدة، في الواقع، نتائج عكسية بالنسبة للهجمات الصغيرة، حيث قد تكون السلطات المحلية هي الأفضل تجهيزاً لتحييد التهديد.

مع تطور البشر، تتطور أيضاً الطرق التي نسعى بها لتدمير بعضنا البعض. يسمح ظهور الإنترنت بنوع جديد من الحرب ـــ أكثر هدوءاً بكثير ـــ واحدة من المعارك يتم قتالها عن بعد، في الوقت الحقيقي، والتي لا مركزية ومجهولة المصدر. وأخرى تقوم بها الروبوتات والطائرات بدون طيار، أو حيث يخبرنا الذكاء الاصطناعي عندما يحين وقت البدء في الحرب.

لا تختلف الحرب السيبرانية عن الأسلحة النووية – فالدول تطورها سرا، وإذا تم نشرها، فسيكون المواطنين هم من يعانون أكثر من قادتهم. "التدمير المؤكد المتبادل "سيكون ضماناً قريباً. عملت المعاهدات

التي تفرض الشفافية على إبقاء الأسلحة النووية في مخزوناتها وبعيداً عن الانتشار. ربما نفس الشيء يجب عمله من أجل الحرب الرقمية؟

قد نكون قادرين على التنبؤ بالتطورات العلمية والتكنولوجية في الأفق، ولكن لا يمكننا إلا أن نخمن ما ستفعله البشرية معهم. صنع البشر الطائرات. هذه سمحت لهم بالطيران فوق الغيوم... واستخدموها لإسقاط القنابل على بعضهم البعض.

أمام هذه التحديات أطلقت الولايات المتحدة الامريكية مبادرة للدفاع الابتكاري عام ٢٠١٤ وحدثت هذه المبادرة وتوسعت فيها وأولت الأمن السبراني والسيطرة السبرانية في ميادين الحروب حول العالم، وخصوصا في مناطق ثلاث هي الشرق الأوسط والمحيط الهادي وحول روسيا، وقد جاء في الديباجة المنشورة من وزارة الدفاع الامريكية عنها ما يلي:

يجب الاعتراف بتعقيد بيئة الأمن القومي من قبل التحديات المتزايدة من للدول القومية والجهات الفاعلة غير الحكومية التي تتحدى أمن الولايات المتحدة وحلفائها في مجالات الأرض والبحر والجو والفضاء والفضاء الإلكتروني. والتقاء هذه التحديات يشمل:

- زيادة وتيرة تطوير التكنولوجيا التي تتحدى قدرتنا لمواكبتها.
- نمو أهمية عوامل التمكين القتالية في الفضاء والفضاء الإلكتروني والطيف الكهرومغناطيسي.
- تخفيض الميزانيات والمشتريات.
- قوة "الشخص الواحد"، حيث يمكن لشخص واحد إحداث تعطيل كبير ومعقد لأنظمة المعرفة والأدوات المتاحة على نطاق واسع على شبكة الإنترنت.
- نظام التبعيات التي يمكن أن تتعطل عن طريق كسر "أضعف حلقة".

دول أخرى تستفيد بالفعل من الوتيرة المتزايدة لتطوير التكنولوجيا من خلال استهدافنا التمكين من القتال ومهاجمة هشاشة شبكات المعلومات لدينا التي تسمح يتسرب المعلومات المهمة.

وبعد سنوات من الحرب في العراق وأفغانستان فان المشهد الجيوسياسي الشرق الأوسط يستمر في التغيير، مع الاضطرابات في مصر، مخاوف الأسلحة الكيميائية في سوريا، والطموحات النووية المستمرة لإيران تجعل الوضع العام غير مستقر في أحسن الأحوال. بالإضافة إلى ذلك، تهديدات من استمرار انتشار الإرهاب عبر القارات، مما يؤدي إلى الاستمرار في تحدي ليس فقط أمن الأمة، ولكن أيضا الدول الشريكة والعلاقات التي نبني معها شركاؤنا، وأخيرا تطوير الدول الأخرى للقدرة العسكرية المتقدمة.

هذه التهديدات المعقدة والمتنامية تجعل الخيارات الاستراتيجية أكثر صعوبة. وتفرض ضرورة زيادة المخصصات المالية على البحوث والتطوير. وأيضا تغيير الطريقة التي نفكر بها.

وسمحت المبادرة بزيادة الإنفاق على عمليات البحث والتطوير بنسبة تصل إلى ٢.٨٪ من الناتج القومي الإجمالي، كما سمحت المبادرة للمؤسسات الخاصة بالمشاركة بتقديم الابتكارات الفاعلة في هذا المجال وعدم قصر الدراسات الأمنية السبرانية على المؤسسة الوطنية للعلوم (NSF).

٣-روسيا والستار الحديدي الرقمي:

تعمل روسيا في مجال الحرب الرقمية على محورين الأول دفاعي بإنشاء الستار الحديدي الرقمي، والآخر هجومي يسمح للروس بامتلاك ذراع رقمية طويلة لمهاجمة أهداف حول العالم، وذلك على النحو الآتي:

أ) خطة الدفاع:

يوم الجمعة الأول من نوفمبر ٢٠١٩ بدأ سريان قانون جديد مثير للجدل في روسيا: ما يسمى بقانون "الإنترنت السيادي"، والذي ينص على إنشاء شبكة إنترنت مستقلة لروسيا. في الواقع، منحت موسكو نفسها القدرة على إقامة نوع من الستائر الحديدية الرقمية حول شبكاتها. لكن هل سيتم التغيير من الإنترنت الحر إلى الإنترنت الروسي البحت؟ هذا ما ستراقبه شركات التكنولوجيا ومستخدمو الإنترنت الروس على حد سواء مع سريان القانون.

إليكم ما يستتبعه هذا الإجراء: في وقت سابق من هذا العام، وقع الرئيس الروسي فلاديمير بوتين قانوناً جديداً من شأنه أن يمكّن من إنشاء شبكة وطنية يمكنها أن تعمل بشكل مستقل عن بقية العالم. من بين أمور أخرى، يسمح القانون لوكالة الاتصالات الروسية بإغلاق البلاد من التبادل الخارجي للحركة، وإنشاء شبكة روسية بحتة.

قالت الحكومة إن اللوائح جزء من جهد لحماية روسيا من خلال خلق القدرة على الحفاظ على شبكة وطنية مسيجة، في حالة تدخل قوة أجنبية في الفضاء الإلكتروني الروسي. وقالت صحيفة روسيسكايا جازيتا الرسمية إن للقانون للذي يدخل حيز التنفيذ يجب ألا يؤثر على مستخدمي الإنترنت، لكنه "سيضمن توافر خدمات الاتصالات في روسيا في حالة وجود تهديدات."

يمكن للحكومة الآن مراقبة المحتوى مباشرة أو حتى تحويل الإنترنت في روسيا إلى نظام مغلق. هذا واضح من الناحية النظرية، ولكن كيف سيتم تطبيق التدابير الجديدة لا تزال غامضة. حذر النقاد من أن ذلك قد يسهل على الحكومة الروسية فرض الرقابة على حركة الإنترنت أو إعادة توجيهها أو إيقافها لمنع الوصول إلى محتوى حساس من الناحية السياسية.

إليك السبب: للتحكم في حركة المرور على الإنترنت، واكتشاف المحتوى، يتطلب القانون من جميع مزودي الإنترنت في روسيا تثبيت أجهزة خاصة مقدمة من وكالة الاتصالات الروسية قد يتيح ذلك استخدام تقنية Deep Packet Inspection (DPI)، والتي تتضمن معالجة البيانات التي تبحث بالتفصيل في محتويات البيانات التي يتم إرسالها. على سبيل المثال، يتم استخدام DPI في الصين من أجل Great Firewall لتصفية المحتوى الذي تعتبره مضرة للمواطنين الصينيين.

أعرب العديد من نشـــطاء الحقوق وخبراء الإنترنت عن مخاوفهم من أن القوانين الروســـية الجديدة تمهد الطريق للرقابة والمراقبة عبر الإنترنت. وقالت راشـــيل دنبر، نائبة مدير قســـم أوروبا وآســـيا الوســـطى في مجموعة هيومن رايتس ووتش: "يمكن للحكومة الآن مراقبة المحتوى مباشـــرة أو حتى تحويل الإنترنت الروســـي إلى نظام مغلق دون إخبار الجمهور بما يفعلونه أو لماذا ..". "هذا يعرض للخطر حق الناس في روسيا في حرية التعبير وحرية المعلومات عبر الإنترنت".

ليس من الواضح تماماً كيف تخطط السلطات الروسية لتنفيذ هذا التشريع. وقد وصفه المسؤولون في الدولة بأنه عمل مســتمر يتطلب اختبارات متعددة ولوائح إضــافية. لكن التجارب على الأجهزة جارية بالفعل. قال ألكســندر زهاروف، رئيس روســكومنادور، إن جميع مزودي خدمات الإنترنت الروس قد وافقوا على الامتثال للقانون وتثبيت الأجهزة، ويجري الآن اختباره محلياً في إحدى المناطق الروسية.

أحدث إضــافة إلى التشــريع – الذي يدخل حيز التنفيذ يوم الجمعة الأول من نوفمبر ٢٠١٩ تأخذ تلك الاختبارات على مستوى البلاد. وقع رئيس الوزراء الروسـي ديمتري ميدفيديف قانوناً الشـهر الماضـي يحدد "التدريبات" التي ســتســتضــيفها روســيا كل عام لاختبار ســيناريوهات التهديدات المختلفة لشــبكة الإنترنت في البلاد من أجل الحفاظ على "سيادتها".

وفقًا للوثيقة، ستجري روسيا ما لا يقل عن تمرين واحد من هذا النوع كل عام، مع تحذير من أن هذا العدد قد يزداد إذا أجريت مناورات مفاجئة. ستكون وزارة الاتصــالات الروسـية مسـؤولة عن تخطيط التدريبات، التي ســيتم تنســيقها مع FSB، جهاز الأمن الروســي، ووزارة الدفاع، من بين مؤســســات أخرى.

تتمتع روسـيا منذ فترة طويلة بثقافة الإنترنت المجانية نسـبيا، مقارنة بالصـين. لكن الحكومة انحرفت في اتجاه سيطرة أكبر على الوصول إلى الإنترنت في السنوات الأخيرة.

وقال جاســـون أوكســـمان، الرئيس والمدير التنفيذي لمجلس صـــناعة تكنولوجيا المعلومات بجمعية صـــناعة التكنولوجيا، إن مثل هذه القوانين يمكن أن يكون لهاتأثير على المجتمع الروســـي والنمو الاقتصادي للبلاد.

وقال "الوصـــول إلى الإنترنت المجاني والمفتوح هو مفتاح العديد من التقنيات التي تعزز الحياة اليومية للأفراد والاقتصـــادات في جميع أنحاء العالم" ."عبر ربط الناس، بغض النظر عن المكان الذي يعيشون فيه، أثبتت شبكة الإنترنت أنها أداة أساسية للعائلات والشركات والحكومات والتعليم والصحة. إن بناء الحواجز وتقييد تدفق المعلومات إلى أكثر من ١٠٠ مليون مســـتخدم إنترنت في روســـيا يهدد بقمع نمو التجارة وخنق الابتكار".

في وقت سابق من هذا العام، أدخلت الحكومة الروسية قوانين جديدة تسمح للسلطات بسجن أو تغريم أولئك الذين ينشـــرون أخباراً مزيفة أو "عدم احترام" المســـؤولين الحكوميين عبر الإنترنت. وفي العام الماضـي، حاولت روسيا فرض حظر على خدمة الرسـائل الشـهيرة Telegram. ومع ذلك، فإن حظر

Telegram أظهر حدود الجهود الروسية لتنظيم الفضاء الإلكتروني. حظرت محكمة في موسكو شركة Telegram بعد أن رفضت الشركة توفير مفاتيح التشفير لجهاز الأمن الفيدرالي، لكن مؤسس الشركة Pavel Durov قال إن Telegram ستستخدم "أساليب مدمجة" لتجاوز الحظر.

ب) خطة الهجوم:

أبدى الخبراء في منظمة "The Strategy Bridge" الأمريكية المتخصصة في الأمن المعلوماتي بالمجال العسكري، اهتمامهم بالصيغة الجديدة للعقيدة العسكرية الروسية. ونشر الخبراء مقالا موسعا بهذا الشأن، جاء فيه أن الجيش الروسي الجديد يراهن على التفوق المعلوماتي على العدو، والذي يقضي بالدرجة الأولى بالتفوق النفسي والتقني. ويرى المحللون الأمريكيون أن السلاح النفسي الذي يستعين به الروس من شأنه زعزعة الأصول الأيديولوجية للعدو وتحقيق التفوق المعنوي عليه، بما في ذلك في شبكات التواصل الاجتماعي، كما فعلت الولايات المتحدة في العراق ويوغوسلافيا على سبيل المثال. فيما يتعلق بالجانب التقني للعقيدة الروسية الجديدة، فإن روسيا تسعى إلى استخدام أحدث التكنولوجيا مثل الذكاء الصناعي لكسب التفوق في المجال المعلوماتي.

وحققت روسيا حسب المحللين نقلة نوعية في هذا المجال بعد حرب جورجيا عام ٢٠٠٨، حيث صارت تستخدم على نطاق واسع إمكاناتها في الاستخبارات الفضائية والحرب الإلكترونية.

واستعرضت حرب سوريا الدور الكبير الذي تلعبه منظومة "غلوناس" الروسية في جمع المعلومات عن العدو، وتوجيه الصواريخ وغيرها من الأسلحة فائقة الدقة إلى أهدافها.

وتعد الطائرات من دون طيار حسب المحللين الأمريكيين مصدرا هاما لجمع المعلومات بالنسبة للعسكريين الروس.

وفي هذا السياق، أشاروا إلى طائرة "أورلان-١٠" الروسية من دون طيار، التي استخدمت بالدرجة الأولى لدعم القوات البرية الصديقة. أما درون "فوربوست" الذي خضع للاختبار في سوريا، فاستخدم لتوجيه صواريخ "ياخونت" و"كاليبر" المجنحة المطلقة من السفن الحربية.

وقال المحللون إن الطائرات الروسية من دون طيار قامت بـــ ٢٣ ألف طلعة جوية قتالية في حرب سوريا، وبقيت في الجو لمدة ١٤٠ ألف ساعة.

ولفت المحللون إلى الدور الذي لعبته في حرب سوريا طائرة الاستطلاع والإنذار الرادارى المبكر "آ-٥٠ أو"، في التعرف على الأهداف ومرافقتها، وقالوا إن طائرة "آ-١٠٠" التي ستحل محلها مزودة بأحدث الأجهزة للتعامل مع الأهداف المعادية.

المصدر: روسيسكايا غازيتا

أعلن مدير الاستخبارات القومية الأمريكية، دان كوتس، أن روسيا ليست الدولة الوحيدة التي تعمل على التأثير على سير الانتخابات الأمريكية.وقال كوتس في مؤتمر عقده اليوم الخميس أن دوائر الاستخبارات الأمريكية لا تزال قلقة من المخاطر على انتخابات الكونغرس والانتخابات الرئاسية

المقبلة في العام ٢٠٢٠، ونشاط روسيا ضمن حملة تهدف إلى "إضعاف وتقسيم الولايات المتحدة"، بحسب وكالة "رويترز."وأشار المسؤول الأمريكي إلى ما أسماه "نشاط روسيا غير الشرعي الذي يتضمن جهودا إجرامية لقمع التصويت وتمويل الحملة بشكل غير قانوني والهجمات السيبرانية ضد البنية التحتية لعملية التصويت إلى جانب عمليات اختراق لأجهزة الكمبيوتر تستهدف مسؤولين منتخبين وغيرهم."وتابع: "نعرف أيضا أن الروس حاولوا سرقة المعلومات من المرشحين والمسؤولين الحكوميين"، مؤكدا أن روسيا ليست الدولة الوحيدة التي تعمل على تقويض الانتخابات الأمريكية.وذكر أن المخابرات الأمريكية "ستواصل مراقبة الوضع والتحذير من أي نشاط من هذا القبيل".

من جانبه، قال مدير مكتب التحقيقات الفيدرالي الأمريكي، كريستوفر راي، أن FBI فتح تحقيقا في "التدخل المزعوم". ويقود المحقق الخاص روبرت مولر تحقيقا جنائيا في "تدخل روسيا" في انتخابات الرئاسة الأمريكية عام ٢٠١٦ التي فاز فيها دونالد ترامب على المرشحة عن الحزب الديمقراطي هيلاري كلينتون، وكذلك في الشبهات بالتواطؤ بين حملة ترامب والسلطات الروسية.

ليس فقط في الولايات المتحدة ولكن في الديمقراطيات الأوروبية أيضًا. في هولندا، **عدت** السلطات الهولندية بطاقات الاقتراع في الانتخابات الأخيرة باليد لمنع الحكومات الأجنبية – وخاصة روسيا – من التلاعب بالنتائج من خلال الهجمات الإلكترونية. في الدنمارك، **اتهم** وزير الدفاع الحكومة الروسية بتنفيذ حملة لمدة عامين للتسلل إلى حسابات البريد الإلكتروني في وزارته. في المملكة المتحدة، **ذكرت** لجنة برلمانية أنها لا تستطيع "استبعاد" احتمال أن "التدخل الأجنبي" تسبب في تعطل موقع تسجيل الناخبين قبل استفتاء بريطانيا على عضوية الاتحاد الأوروبي. وفي فرنسا، **اكتشفت** شركة للأمن السيبراني للتو أن المتسللين الروس المشتبه بهم يستهدفون المرشح الرئاسي البارز. "إننا نشعر بقلق متزايد بشأن التدخل الذي يتم تمكينه عبر الإنترنت في العمليات السياسية الديمقراطية"، هذا ما **أعلنه** ممثلو مجموعة الدول السبع ـــــ كندا وفرنسا وألمانيا وإيطاليا واليابان والمملكة المتحدة والولايات المتحدة ــ بعد اجتماعهم في إيطاليا في وقت سابق من هذا الشهر. لم يتم ذكر اسم روسيا، وهي عضو في المجموعة حتى تم طردها بسبب ضم القرم.

٤- الحرب والسلام على طريق الحرير الرقمي في الصين:

حذر وزير الخارجية الأمريكي مايك بومبو في *١٥ مايو ٢٠١٩* من طموحات الصين العالمية، وأشار إلى أن مارغريت تاتشر لن تسمح لشركة هواوي بدخول شبكات الجيل الخامس البريطانية. يمكن أن يشير أيضاً إلى ماضي بريطانيا الإمبراطوري، الذي تعيد الصين تتبعه حرفياً اليوم.

على الرغم من أن Huawei تواجه مقاومة في الموجات الهوائية الغربية، إلا أنها تتسابق في قاع البحار العالمية. تحمل الكابلات الخارجية ٩٥ في المائة من جميع البيانات للدولية، وتقوم Huawei ببناء أو تحسين ما يقرب من ١٠٠ منها. أحد المشاريع الرائدة هو باكستان شرق إفريقيا كابل إكسبريس، أو السلام، والتي من المقرر أن تصبح أقصر طريق لحركة الإنترنت عالية السرعة بين آسيا وأفريقيا.

منذ قرن ونصـــف،كلنت بريطانيا تغلف العالم بكابلات التلغراف، بما في ذلك واحد عبر جوادر، وهي نفس المدينة الساحلية في باكستان حيث يبدأ كابل PEACE. وتدير الصين اليوم ميناء جوادار، وهو جزء من الممر الاقتصادي الصيني الباكستاني. يتوقع الكثيرون أن تصبح منشأة بحرية صينية في السنوات القادمة.

في البداية، كانت الدوافع البريطانية تجارية بشكل رئيسي. وضعت شركاتها أول كابلات بحرية في خمسينيات القرن التاسع عشر، وسيطرت المواد المبتكرة وتقنيات مد الكابلات على السوق. صُنعت أكبر شركة تلغراف في بريطانيا ثلثي الكابلات المستخدمة خلال القرن التاسع عشر ونصفها تقريباً. لكن المخاوف الاستراتيجية أخذت في نهاية المطاف. في نهاية القرن التاسع عشر، بدأت الحكومة البريطانية في تطوير نظام أصغر من الكابلات التي تمس بريطانيا وممتلكاتها فقط. مع توسيع شبكة طرق"All Red" ، عارضت الخزانة البريطانية بعض المشاريع لأسباب اقتصادية. ولكن تم التغلب عليها إلى حد كبير من قبل وكالات الدفاع البريطانية، كما يوضح المؤرخ بول كينيدي.

عندما لندلعت الحرب العالمية الأولى، أثبتت تلك الاستثمارات أنهاقديمة.كان البريطانيون أكثر استعداداً من أي شخص للحفاظ على الاتصالات بين قواتهم أثناء مراقبة اتصالات العدو وتعطيلها. لم يكن المفتاح هو الملكية البريطانية للكابلات فحسب،بل خبرتها الفنية التي لا تضاهى، والتي تم تسخيرها لقطع خطوط العدو في بداية الحرب. بالنسبة لبعض المسؤولين الألمان، تبعت مدافع آب (أغسطس) بصمت قاتل.

لا تتبع الصين خطى بريطانيا فحسب، ولكنها تتسلق على أكتافها. الشركة التي تمتلك كابل PEACE، Huawei Marine Networks، هي مشروع مشترك بين Huawei والشركة Global Marine Systems البريطانية، وهي الشركة التي مدت أول كابل تلغراف عبر المحيط الأطلسي في عام ١٨٦٦. من خلال شراكات كهذه، اكتسبت الصين معرفة مهمة مع التعلق بوعد الوصول إلى السوق المحلية الكبيرة.

طريق الحرير الرقمي في الصين هو المكان الذي تلتقي فيه سياسات شتى. بدأت Made in China 2025 بقوة في صناعات التكنولوجيا الفائقة في الصين بدعم حكومي وأهداف طموحة، بما في ذلك الاستحواذ على ٦٠ في المائة من سوق الاتصالات بالألياف البصرية في العالم. تعد مبادرة الحزام والطريق الصينية، التي وعدت باستثمار تريليون دولار في البنية التحتية خارج حدودها، وسيلة للشركات الصينية للتوسع في الأسواق الخارجية والوصول إلى هذه الأهداف.

سيكون دفع البنية التحتية في الصين أقل تهديداً إذا كانت حكومتها أكثر تركيزاً على زيادة التواصل من السيطرة. في الداخل، تستفيد تكنولوجيا جديدة للرقابة وتتبع مواطنيها، وتحويل المدن الذكية إلى مدن مراقبة. الديمقراطيات مروعة، لكن القادة الاستبداديون مفتونون.

ومع ذلك، يشير التاريخ إلى أن طريق الحرير الرقمي في الصين لن يستمر عند هذا الحد. لم تنقل شبكة التلغراف الواسعة في بريطانيا الأوامر الاستعمارية فحسب، بل كانت تحمل أيضًا أفكاراً قوية

للتغيير. استخدمت الحركات القومية هذه الأدوات في معاركها من أجل الاستقلال، وحتى على الرغم من الرقابة، أصبحت شبكة بريطانيا "وسيلة لتحدي وتقويض الإمبراطورية ذاتها التي خلقتها"، كما يكتب المؤرخ دانييل هيدريك.

هناك جانب أكثر استنارة من تجربة بريطانيا يحمل أيضًا درسًا. خلال سباق التلغراف العالمي، على عكس معظم للدول، منحت بريطانيا حقوقًا لكابلات الهبوط على أراضيها دون قيود. وبعيداً عن إضعاف شركاتها، فقد ساعد ذلك في تحويل لندن إلى مركز عالمي للاتصالات والمال الذي لا يزال قائماً حتى اليوم. في نهاية المطاف، فإن أفضل إجابة من الصين على الشكوك حول أنشطتها في الخارج ستكون انفتاح أكبر في الداخل.

جوناثان إي هيلمان كبير زملاء كرسي سيمون في الاقتصاد السياسي ومدير مشروع إعادة ربط آسيا *بمركز الدراسات الاستراتيجية والدولية في واشنطن العاصمة.*

طريق الحرير الرقمي في الصين: المنافسة التكنولوجية الاستراتيجية وتصدير اللامبريالية السياسية:

مع تعزيز الصين لنموذج للرأسمالية التي تقودها الدولة والليبرالية السياسية، والتكنولوجيا الرقمية تلعب دوراً مركزياً متزليداً في جميع جولنب المجتمع، يجب على الولايات المتحدة العمل مع حلفائها لتعزيز القيم الليبرالية الأساسية وتقديم نموذج إيجابي للتطور التكنولوجي والاتصال الرقمي.

عادت المنافسة على القوة العظمى كميزة مميزة للمشهد الجيوسياسي، حيث تتنافس الولايات المتحدة والصين على النفوذ الإقليمي والعالمي. سيكون التطور التكنولوجي حاسماً بالنسبة لنتائج هذه المنافسة، وقد اعتمدت الصين نموذجاً يجمع بين الرأسمالية التي تقودها الدولة وشكل من أشكال الليبرالية السياسية التي تدعمها مجموعة واسعة من التقنيات الرقمية. تستخدم بكين طريق الحرير الرقمي، وهو مجموعة فرعية من مبادرة الحزام والطرق (BRI) لتعزيز الاتصال الرقمي في الخارج، وتوسيع نفوذها، وتعزيز صعود الصين كقوة عظمى تكنولوجية.

مبادرة الحزام والطريق:

تم الإعلان عن طريق الحرير الأبيض الصادر عن الحكومة الصينية في عام ٢٠١٥، وله أهداف سياسية خارجية ومحلية تتضمن إنشاء بنية تحتية رقمية تركز على الصين، وتصدير الطاقة الإنتاجية الصناعية المفرطة، وتيسير التوسع في شركات التكنولوجيا الصينية، والوصول إلى مجموعات كبيرة من البيانات، وإبراز الأهداف الصينية بقوة وكذلك التلاعب بالمفاهيم السياسية، وبالتالي تقويض العمليات الديمقراطية في الخارج. في حين أن طريق الحرير الصيني الرقمي لديه القدرة على تعزيز التواصل الرقمي في الاقتصادات النامية، إلا أنه يتمتع في نفس الوقت بالقدرة على نشر الاستبداد، والحد من الديمقراطية، وكبح حقوق الإنسان الأساسية.

يتألف المشروع من أربعة مكونات مترابطة، مركزة تقنياً. أولاً، تستثمر الصين في البنية التحتية الرقمية في الخارج، بما في ذلك شبكات الهاتف الخلوي من الجيل التالي وكابلات الألياف البصرية

ومراكز البيانات. ثانياً، تحتوي المبادرة على تركيز محلي على تطوير التقنيات المتقدمة التي ستكون ضرورية للقوة الاقتصادية والعسكرية العالمية، بما في ذلك أنظمة الملاحة عبر الأقمار الصناعية والذكاء الاصطناعي والحوسبة الكمية. ثالثًا، نظراً لأن الصين تدرك أهمية الترابط الاقتصادي لنفوذها الدولي، فإن طريق الحرير الرقمي يشجع التجارة الإلكترونية من خلال مناطق التجارة الحرة الرقمية، مما يزيد التجارة الإلكترونية الدولية عن طريق الحد من الحواجز التجارية عبر الحدود وإنشاء مراكز لوجستية إقليمية. رابعا، تعمل الصين على إنشاء بيئة رقمية دولية مثالية من خلال الدبلوماسية الرقمية والحكم المتعدد الأطراف. وقد شمل ذلك استخدام المؤسسات المتعددة الأطراف لوضع معايير تكنولوجية متعلقة بالبنية التحتية للاتصالات وتعزيز مبدأ سيادة الإنترنت في منتديات الأمم المتحدة.

لقد سعت الولايات المتحدة إلى تقييد طريق الحرير الرقمي وصعود الصين التكنولوجي من خلال تقديم شركات التكنولوجيا الصينية كخطر غير مقبول للأمن الدولي، بما في ذلك محاولات لإقناع الحلفاء بمنع الشركات الصينية من المساهمة في بنيتها التحتية الرقمية الحيوية. حققت هذه الجهود نجاحاً محدوداً، حيث حظرت أستراليا ونيوزيلندا واليابان مشاركة الشركات الصينية في تطوير شبكات الجيل الخامس الخاصة بها، بينما كانت جهات أخرى مثل المملكة المتحدة وألمانيا أقل استعداداً لمنع المشاركة الصينية تماماً في مثل هذه البنية التحتية. بالإضافة إلى ذلك، أدرجت الولايات المتحدة التواصيل الرقمي كجانب من جوانب منطقة تطوير المحيط الهادي الحرة والمفتوحة السياسة في محاولة لمواجهة الاستثمار الصيني في البنية التحتية الرقمية في المنطقة.

من خلال مد طريق الحرير الرقمي على نطاق أوسع، تهدف الصين إلى الحفاظ على النظام الاقتصادي الليبرالي الذي سمح بنموه مع الترويج لبيئة سياسية غير ليبرالية. إن النظام السياسي غير الليبرالي من شأنه أن يعزز الأنظمة الاستبدادية، ويحد من الحقوق الفردية، ويعيق سيادة القانون في جميع أنحاء العالم. لا تقوم الصين بتصديرها فقط من أشكال الاستبداد الرقمي أو اللينينية الرقمية من خلال البنية التحتية الرقمية، بل تقدم أيضًا نموذجاً وإرشادات حول كيفية استخدام الحكومات للتكنولوجيا لقمع سكانها.

واشنطن على حق في تحدي بكين في المجالين التكنولوجي والاقتصادي؛ ومع ذلك، إذا اقتربت الولايات المتحدة من هذه المنافسة الاستراتيجية لأنها اقتربت السياسة الخارجية عموماً في ظل الإدارة الحالية، وبدون تعزيز القيم السياسية الليبرالية بما فيه الكفاية، سوف تلعب دورها في أيدي الصين. ينبغي على الولايات المتحدة أن تتبع نهجا أكثر شمولية يشمل العمل مع الحلفاء للتصدي لانتشار الاستبداد الرقمي وضمان أن تخلق التواصل الرقمي الدولي عبر بيئة إلكترونية آمنة وحرة ومنفتحة، بما في ذلك من خلال إشراك المنظمات الدولية والمجتمع المدني والقطاع الخاص. ينبغي على الولايات المتحدة والديمقراطيات المتشابهة في التفكير أن تقدم نموذجاً إيجابياً للتطور التكنولوجي والاتصال

الرقمي الذي يعزز قيمها الأساسية، وإلا فإن المنافسة على التفوق التكنولوجي العالمي يمكن أن تبشر بنظام دولي غير ليبراليًا سياسيًا.

خريطة طريق الحرير الرقمي

٥- الاحتلال الإسرائيلي الرقمي للمنطقة العربية:

ـقال بنيامين نتنياهو، رئيس الوزراء الإسـرائيلي، في جامعةـتل ابيب إن جهدنا في مجال الأمن السبرانى عمل رائع، أنه في تطور هندسي مستمر؛ لأنه لن تكون هناك حل دائم، وهو عمل لا ينتهي أبدا، وذلك في مؤتمر الأمن السـيبراني السـنوي. في السـابع من أكتوبر ٢٠١٩. كما أعلن توماس بوسـرت، مسـاعد الرئيس الأمريكي للأمن للداخلي ومكافحة الإرهاب، في هذا الحدث عن إنشاء مجموعة عمل إلكترونية ثنائية أمريكية – إسرائيلية تعمل على تطوير "دفاعات إلكترونية مبتكرة يمكننا اختبارها هنا ثم العودة إلى أمريكا".

أصبحت إسرائيل قوة للأمن السيبراني في مركز صناعة تبلغ قيمتها ٨٢ مليار دولار. بالإضافة إلى التعاون مع القوتين العظميين، إسرائيل هي مساعدة الدول الصغيرة، على سبيل المثال، سنغافورة، وصدرت إسرائيل في العام الماضي بقيمة ٦.٥ مليار $ من منتجات الأمن السيبراني، تم إقناع أكثر من ٣٠ شركة متعددة الجنسيات لفتح مراكز البحث والتطوير المحلية وجذب المستثمرين الأجانب. وقال نتنياهو: "في عام ٢٠١٦، حصلنا على حوالي ٢٠٪ من استثمارات الأمن السيبراني العالمية الخاصة".

وشاركت في المؤتمر في سلسلة من المؤسسات الإعلامية بوفود من الصحفيين الأجانب استضافتهم وزارة الخارجية الإسرائيلية. شمل ذلك القاء نظرة عامة على نظام الأمن السيبراني الإسرائيلي الذي قـدمه اللواء (المتقاعد) البروفيسور إسحاق بن إسرائيل، رئيس مركز أبحاث الإنترنت المتعدد التخصصات (Blavatnik) في جامعة تل أبيب والرئيس السابق للبحث والتطوير لقوات الدفاع الإسرائيلية (IDF) وزارة الدفاع؛ الدكتور إيفياتار ماتانيا، المدير العام لمديرية الإنترنت الوطنية الإسرائيلية (INCD)؛ ومسؤول كبير في جيش الدفاع الإسرائيلي. وفيما يلي ٦ عوامل أساسية ساهمت في جعل إسرائيل مركزاً عالمياً لأبحاث وممارسات الأمن السيبراني:

١- *الحكومة كمنسق:*

عندما طلب رئيس الوزراء نتنياهو من البروفيسور بن إسرائيل في عام ٢٠١٠ وضع خطة مدتها ٥ سنوات حول كيفية الاستجابة، على المستوى الوطني، لتهديدات الإنترنت المتزايدة، أجاب الأخير أن ٥ سنوات في الأمن السيبراني حوالي ٣ أو ٤ أجيال تكنولوجية، مما يجعلها من المستحيل التنبؤ والتخطيط. بدلاً من ذلك، أوصى بن إسرائيل وفريق العمل التابع للمبادرة الوطنية سايبر بتطوير "نظام إيكولوجي سيعرف ماذا يفعل عندما تأتي هذه التهديدات غير المتوقعة. "إن النظام البيئي هو إطار متطور باستمرار للتعاون بين الحكومة (بما في ذلك الجيش) والشركات والجامعات، حيث تلعب الحكومة في الغالب دوراً توجيهياً واستشارياً. يقول الدكتور ماتانيا، نظراً لأن الفضاء الإلكتروني عالمي وليس له حدود وطنية، "لقد أدركنا أن المؤسسات تشكل أساساً الحدود الرقمية لأمتنا". لكن الشركات – في إسرائيل وفي كل مكان آخر – تحجم عن رؤيتها تعمل جنباً إلى جنب مع حكوماتها؛ لأنها تعمل على الصعيد العالمي. بالإضافة إلى ذلك، تشكل الحريات الفردية مشكلة في إسرائيل كما هي الحال في جميع الديمقراطيات الليبرالية الأخرى. لقد مرت إسرائيل بمحاولات متعددة لإنشاء هيكل تشغيلي يعمل على حل هذه التوترات، كان آخرها إنشاء الهيئة الوطنية للأمن السيبراني في عام ٢٠١٥. وهو يجسد مهمة الحكومة المزدوجة المتمثلة في تعزيز تنسيق الأمن السيبراني مع إزالة الحكومة بشكل أكبر من قواعد البيانات وقرارات الشركات الفردية.

٢-*الحكومة كمحفز للأعمال:*

تملماً كما لعبت الحكومة الإسرائيلية دوراً مهماً في إطلاق ودعم قطاع التكنولوجيا المزدهر في إسرائيل، فقد كانت بمثابة حافز لصناعة الأمن السيبراني سريعة النمو في إسرائيل. في عام ٢٠١١، عندما أُنشئ المكتب الإلكتروني السيبراني كنتيجة لتوصيات فرقة عمل بن إسرائيل، شملت ولايته، بالإضافة إلى تنسيق الأمن السيبراني وتطوير السياسات، "رؤية لوضع إسرائيل بين الدول الخمس الأولى الرائدة في هذا المجال ضمن عدد قليل نسبيا من السنوات. "

نظراً للأمن السيبراني على أنه "محرك النمو الاقتصادي"، حددته الحكومة كقطاع تتمتع فيه إسرائيل بميزة تنافسية تعتمد على أحدث الأبحاث والخبرة العملية الفريدة. وقد تم تصور هذه الميزة أيضاً والعمل عليها كمساهم مهم في التعاون الدولي وزيادة حسن النية تجاه إسرائيل، مما يوفر فائدة إضافية للبلاد.

٣-*جعل الجيش حاضنة بدء التشغيل ومسرع:*

أجبرت الظروف الجغرافية السياسية المعاكسة التي وجدت إسرائيل نفسها فيها منذ تأسيسها عام ١٩٤٨ الدولة الصغيرة على استثمار مواردها الضئيلة في تطوير قدرات عسكرية متفوقة والحفاظ عليها. نظراً لأن أجهزة الكمبيوتر وجدت طريقها إلى كل مناحي الحياة والحرب، أصبح الدفاع الإلكتروني نشاطاً مهماً للجيش الإسرائيلي.

مع سنوات من جمع المعلومات الاستخباراتية والأمن السيبراني، تطورت وحدة جيش الدفاع الإسرائيلي رقم ٨٢٠٠ لتصبح حاضنة ومسرعاً للشركات الناشئة في إسرائيل، في مجال الأمن السيبراني ومجالات أخرى. يقول نداف ظافر، القائد السابق لـ ٨٢٠٠ واليوم، الرئيس التنفيذي لفريق: Team 8 "لقد نجحنا في تحويل وضع غير مؤات إلى ميزة". ظافر: "في الماضي، كان يُنظر إلى الخدمة العسكرية على أنها مضيعة للوقت، بينما الأمر مختلف الآن. لم نخطط لها بهذه الطريقة. لم يفكر أحد في كيفية تحويل جيش الدفاع الإسرائيلي إلى حافز للاقتصاد الإسرائيلي، ولكن هذا ما حدث".

يواجه الشباب الذين يخدمون في عام ٨٢٠٠ ووحدات جيش الدفاع الإسرائيلي المماثلة تحديات وحلول الأمن السيبراني المتطورة والحقيقية. ولكن نظراً لأن هذه الوحدات تعمل مثل الشركات الناشئة، فإنها تتعرف أيضاً على تجربة العمل الجماعي، وقيادة الآخرين، وتحمل مسؤولية اتخاذ القرارات المهمة، وفشل البقاء على قيد الحياة، وكل ذلك يعد استعداداً رائعاً لحياة رواد الأعمال. لمنعهم – على الأقل لفترة من الوقت – من بدء مشاريعهم الخاصة، فإن جيش الدفاع الإسرائيلي يحثهم على مد خدمتهم بتمويل دراسات الدكتوراه أو تقديم حوافز أخرى مثل التحديات التي لن يجدوها في الحياة المدنية.

٤- الاستثمار في رأس المال البشري:

يعد الأشخاص – مهاراتهم وخبراتهم وطموحاتهم – العنصر الأكثر أهمية في الدفاع الإلكتروني. تشتهر إسرائيل بثقافتها الديناميكية، بسمات الارتجال والابتكار والمبادرة. يتم توجيه طاقات وأفراد شعبها إلى مساعي أكاديمية محددة من خلال الاستثمارات والبرامج الحكومية والخاصة. يبدأ التعليم في مجال الأمن السيبراني في المرحلة المتوسطة وإسرائيل هي الدولة الوحيدة في العالم التي يعتبر فيها الأمن السيبراني مادة اختيارية في امتحانات شهادة الثانوية العامة. يقدم عدد من الجامعات الإسرائيلية تخصصاً جامعيا في مجال الأمن السيبراني، وكانت إسرائيل أول دولة تحصل فيها على درجة الدكتوراه في الأمن السيبراني (كنظام مستقل، وليس كموضوع في علوم الكمبيوتر). يوجد اليوم ستة مراكز أبحاث جامعية مخصصة للأمن السيبراني.

بالإضافة إلى العديد من البرامج التي ترعاها الحكومة والتي تهدف إلى إيجاد الشباب الواعد وتزويدهم بالتدريب المتخصص قبل وأثناء خدمتهم العسكرية، يشارك القطاع الخاص، بما في ذلك المؤسسات غير الربحية، في تنمية تعليم العلوم والتكنولوجيا. على سبيل المثال، يقوم مركز Cyber Education Center بتجنيد المهندسين والمبرمجين للتدريس في المدارس، وتنظيم جولات لشركات التكنولوجيا لأطفال المدارس، ويساعد المعلمين المتطوعين في الحصول على وظائف في شركات التكنولوجيا.

٥- اعتناق التخصصات والتنوع:

في كلمته، أوضح البروفيسور بن إسرائيل أنه بينما يتطلب الأمن السيبراني حلولًا تكنولوجية، فإن مشكلات وقضايا الأمن السيبراني ليست تكنولوجية بطبيعتها. نتيجة لذلك، من المهم تطبيق نهج متعدد

التخصصات على الأمن السيبراني وفهم المجالات القانونية والنفسية والاجتماعية والاقتصادية وغيرها من المجالات التي تؤثر عليه. سلط بن- إسرائيل الضوء على حقيقة أن الطلاب في جامعة تل أبيب، بغض النظر عن الانضباط الذين يدرسون (باستثناء الفنون)، يمكنهم التخصص في الأمن السيبراني (أعتقد أن هذا هو السبب في أنه، من أجل الإدماج التام، حصل على أعضاء في تقوم كلية الآداب بإنشاء "حصان طروادة" الفعلي، وهو نوع من البرامج الضارة في العالم الافتراضي).

تعني التخصصات المتعددة رؤية الأشياء من زوايا مختلفة واختراق الحدود المصطنعة. في إسرائيل، يتم الاهتمام بهذا من خلال التجربة الفريدة لمحترفي الإنترنت. أثناء الخدمة العسكرية الإلزامية (وفي وقت لاحق، عند التقديم في الاحتياطيات)، تُستكمل المقدمة الأكاديمية الأولية للأمن السيبراني وتعززها بخبرة عملية. ثم ينضم هؤلاء المحترفون عبر الإنترنت إلى الجامعات ومراكز الفكر والشركات من كل الأحجام والهيئات الحكومية. إن الخبرة المشتركة لهؤلاء المحترفين تثير التلقيح القوي والدائم بين هذه القطاعات – وجهات نظر متعددة – وتضمن أن كل أنواع حلول وسياسات وأنشطة الأمن السيبراني يتم غمرها من خلال النظرية والتطبيق والتفكير الاستراتيجي والتكتيكي الخبرة والخبرة المحددة.

علاوة على ذلك، فإن تنوع الخبرات والمناهج ووجهات النظر يعززها الخلفيات المتنوعة للمشاركين. في عام ٢٠١٤، كان ٢٥٪ من السكان اليهود الإسرائيليين من المهاجرين و٣٥٪ من أطفال المهاجرين، وهو نسيج بشري يضمن نسيجاً من حلول الأمن السيبراني المبتكرة.

٦- إعادة التفكير في مربع (السيبرانية):

كان النهج المعتاد تجاه الأمن السيبراني، في معظمه، رد فعل وركز على المهاجمين المحتملين. عندما تتدخل الحكومات (بما في ذلك الحكومة الإسرائيلية لسنوات عديدة)، فإنها تسند مسؤولية التعامل مع أنواع مختلفة من المهاجمين إلى كيانات مختلفة، مما يجعل السياسات الوطنية مجزأة وغير منسقة على النحو الأمثل.

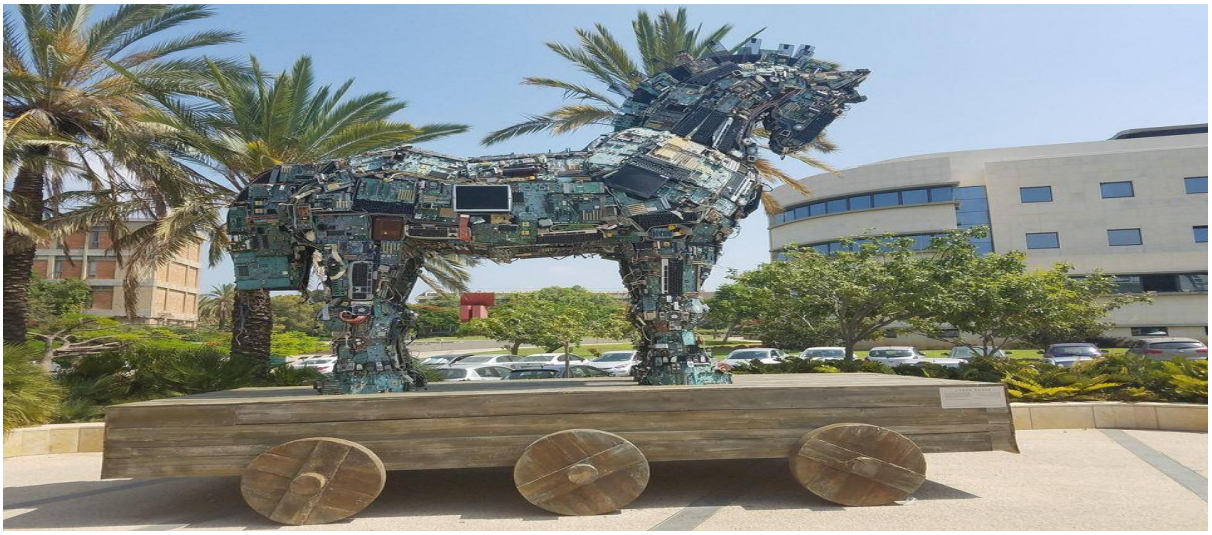
بعد سنوات من التجربة والخطأ، تعكس سياسة الأمن السيبراني الوطنية لإسرائيل اليوم مقاربة مختلفة للأمن السيبراني. لقد تطورت لتصبح استراتيجية للأمن السيبراني استباقية وشاملة وطويلة الأجل، لا تركز على المهاجمين المحتملين بل على التهديدات المحتملة (والأصول التي تتطلب الحماية) وعلى المنظمات كخط الدفاع الأول.

يحتوي هذا النوع الجديد من إستراتيجية الأمن السيبراني على ٣ مستويات: المتانة والمرونة والدفاع. يقول ماتانيا: "إذا قمت ببناء أول طبقتين بالطريقة الصحيحة، فسوف تخفف ٩٥٪ من التهديدات". المستوى الأول، المتانة، يشبه التحصين في القطاع الصحي. قد تقدم الحكومة المشورة والتوجيه، ولكن تقع على عاتق المنظمات الفردية مسؤولية التحصين. الحكومة أكثر نشاطًا قليلاً في المستوى الثاني، المرونة، المساعدة في تبادل المعلومات، تحليل وتخفيف الهجمات الإلكترونية المحددة. تستجيب الطبقة الثالثة لحدث ضخم — حصريا مسؤولية الحكومة، بما في ذلك الإسناد ومتابعة المهاجم.

يعد متنزه التقنيات المتقدمة، المتاخم لجامعة بن غوريون في مـــــدينة بئر السبع بجنوب إسرائيل، عرضـــا لفلســفة الأمن الســيبراني في إســرائيل، ومزيجها الفريد من الناحية العملية والنظرية، بين التخصصات والتلاقح، من المصالح العامة والخاصة..

من خلال مهمتها المتمثلة في جعل المنطقة مصـدراً رئيسـياً للمواهب والخبرات، لا سـيما في مجال الأمن السيبراني، اجتذبت الحديقة الشركات الكبرى متعددة الجنسيات ومراكز البحث والتطوير الخاصة بها (مثل دويتشــه تليكوم و Dell EMC و IBM و Oracle) وشـركات رأس المال الاسـتثماري، مختبرات الأبحاث المتقدمة، والمعهد القومي لبحوث الإنترنت، وفرق الاسـتجابة للطوارئ الإلكترونية. علاوة على ذلك، فإن جيش الدفاع الإسـرائيلي بصـدد نقل وحدات التكنولوجيا الاسـتراتيجية إلى الحرم الجامعي ذاته.

في نهاية المطاف، سـتتولى وحدات جيش الـــــدفاع الإسـرائيلي حوالي ثلث الحديقة، كما صـرح البروفيســور ريفكا كارمي، رئيس جامعة بن غوريون، للوفد الصــحفي. ولكن لن يكون هناك ســور بينهما وبين الباحثين المدنيين ورجال الأعمال وغيرهم من خبراء الأمن الســيبراني العاملين هناك. إن محور فلســفة الأمن الســيبراني الإســرائيلي هم الأشــخاص – تفاعلاتهم وتبادل الأفكار والمناقشــات والتعاون والمسابقات – هم الحلول للتهديدات الإلكترونية وأساس تحويل المخاطر إلى فرص.



حصان طروادة في جامعة تل أبيب

٦- الحرب بالإرهاب ساحة تقاطع الحروب الرقمية:

بعد عرض ســياســات القوى الكبرى من مبادرة الدفاع الابتكاري الامريكية بنســختيها الأولى عام ٢٠١٤ والمعدلة عام ٢٠١٨, والستار الحديدي الرقمي والزراع الروسية الرقمية الطويلة واستراتيجية طريق الحرير الرقمي الصــينية وجهود ســايبر الإســرائيلية في الاحتلال الرقمي للمنطقة العربية من

خلال بيع مستلزمات الامن السبرانى لأغلب الدول العربية من خلال شركاتها وشركات دولية وسيطة. نستطيع بسهولة أكبر فهم الحرب بالإرهاب التي تجرى في منطقتنا العربية وهي حرب أفكار في الأساس لتفجير الشعوب العربية من خلال الحرب الاهلية الرقمية بين مكونات هذه المجتمعات العرقية والدينية وخلق أعداء من الخارج. وان العمليات الإرهابية والمنظمات الإرهابية المستخدمة هي فقط مجرد أدوات لرفع اعلام ولافتات ارشادية على مناطق العمليات وساحات المعارك على أرضنا. والأسلحة الأكثر فتكا هي أسلحة الحرب النفسية القديمة والتي يلخصا أمر القيادة الامريكية في مجال الحرب النفسية على النحو التالي "الاستخدام المخطط للدعاية وغيرها من الإجراءات النفسية التي لها هدف أساسي هو التأثير على آراء وعواطف ومواقف وسلوك الجماعات الأجنبية المستهدفة بطريقة تحقق الأهداف الوطنية وتوظيفها بتقنيات جديدة أكثر قدرة على الوصول إلى كافة الأفراد والجماعات المستهدفة. وهو ما يجعلنا نسأل ماذا أعددنا من قوة ومن رباط الخيل الرقمي لمواجهة كل ذلك.

نبذة مختصرة

الخلاصة

تتحدى الخصائص الفريدة للفضاء الإلكتروني الهياكل الوطنية الحالية، التي بنيت في الأصل لمواجهة التهديدات التقليدية. يؤدي هذا الإدراك إلى قيام الدول بالبحث عن الهياكل والعمليات المناسبة التي يمكنها معالجة الخطر السيبراني الجديد على النحو الأمثل مع حماية الحقوق المدنية الأساسية. تصف هذه الورقة عملية التطور على ثلاث مراحل التي مرت بها معظم البلدان بالفعل وهي:

أولا: تنظيم أنشطة الأمن السيبراني، ويتم ذلك من خلال القيام بتحليل حدود المرحلة الحالية وتحديد الحاجة في المرحلة القادمة.

ثانيا: تطوير الهياكل الحكومية، بإصدار التشريعات وتهيئة البيئة الاقتصادية والسياسية والاجتماعية والثقافية للتعامل مع التحديات الرقمية.

ثالثا: تشكيل هيئة وطنية مركزية للفضاء الإلكتروني، وهي كيان مدني واحد يتمتع بقدرات تشغيلية ملموسة، ومسؤول عن الدفاع عن الفضاء الإلكتروني الوطني وقيادة جهود الأمن السيبراني الوطنية.

المصادر والمراجع

1- ABBY NORMANDigital Warfare As humans evolve, so too do the methods with which we seek to destroy each other. DECEMBER 8TH 2017

2- Human–Cyber–Physical Systems (HCPSs) in the Context of New-Generation Intelligent Manufacturing

Zhou et al., Engineering, 2019

3- Cyber security meets artificial intelligence: a survey

Jian-hua Li, Frontiers of Information Technology & Electronic Engineering, 2019

4- Cyber security meets artificial intelligence: a survey

Jian-hua LI et al., Frontiers of Information Technology & Electronic Engineering, 2019

5-ماري إليوشينا ، ناثان هودج وهداس جولد ، سي إن إن بزنس
تم تحديثه الساعة ١٦٢١ بتوقيت جرينتش (٠٠٢١ بتوقيت هونغ كونغ) في ١ نوفمبر ٢٠١٩

6-جوناثان إي هيلمان الحرب والسلام على طريق الحرير الرقمي في الصين

16مايو ٢٠١٩ *نُشرت نسخة من هذا التعليق في الأصل في* الفاينانشيال تايمز *في ١٥ مايو ٢٠١٩ .*

7-ديميتري (ديما) أدامسكي، "الأوديسة الإسرائيلية نحو إستراتيجيتها الوطنية للأمن السيبراني " ، واشنطن كوارترلي ، يونيو ٢٠١٧