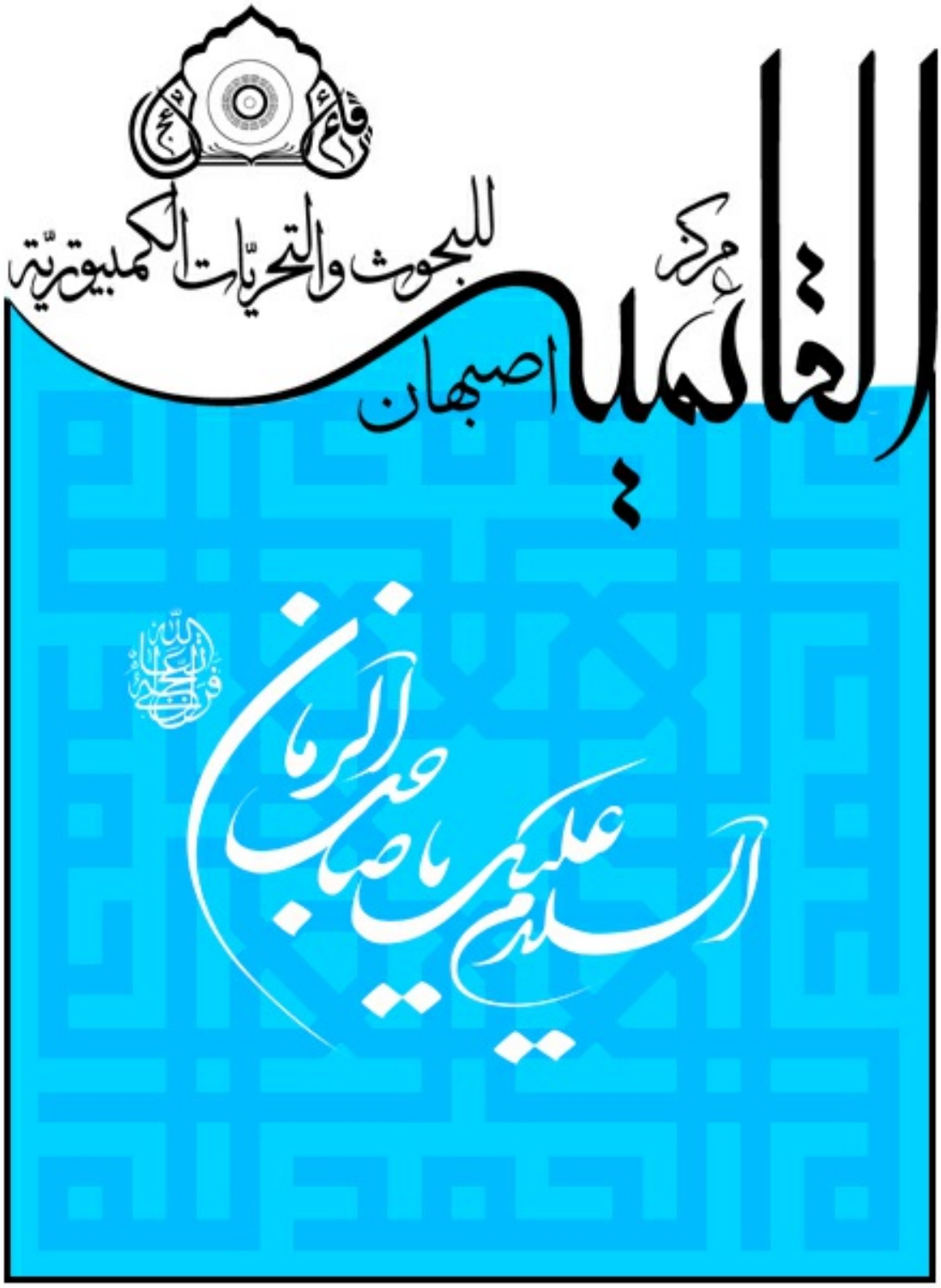

سلسلة مصطلحات معاصرة
21

السيبرنيطيقا

(الشبرانية)
علم القدرة على التواصل
والتحكم والسيطرة

محمود يزبك


بسم الله الرحمن الرحیم

سلسلة مصطلحات معاصرة

كاتب:

الشيخ مرتضى فرج

نشرت في الطباعة:

العتبة العباسية المقدسة

رقمي الناشر:

مركز القائمية باصفهان للتحريات الكمبيوترية

الفهرس

سلسلة مصطلحات معاصرة : السيبرنيطيقا المجلد 21

هويّة الكتاب

برّي، محمود مؤلف.

السيبرنيطيقا: (السبرانيّة) علم القُدرة على التواصل والتحكم والسيطرة / تأليف محمود برّي

الطبعة الأولى – بيروت، لبنان: العتبة العباسيّة المقدّسة، المركز الإسلامي للدراسات الاستراتيجية،

1440 هـ- = 2019.

190 صفحة ؛ 24-سم – سلسلة مصطلحات معاصرة؛(21)

يتضمن إرجاعات ببليوجرافية.

ردمك: 9789922604138

1- السبرانيّة. أ. العنوان.

LCC : Q310 .A45 2019

DCC: 003.5

مركز الفهرسة ونظم المعلومات التابع لمكتبة ودار مخطوطات العتبة العباسية المقدسة.

محرر الرقمي: علي حسن بياني

ص: 1

اشارة

بِسْمِ اللّٰهِ الرَّحْمَنِ الرَّحِيمِ

ص: 2

برّي، محمود مؤلف.

السيبرنيطيقا: (السبرانيّة) علم القُدرة على التواصل والتحكم والسيطرة / تأليف محمود برّي

الطبعة الأولى – بيروت، لبنان: العتبة العباسيّة المقدّسة، المركز الإسلامي للدراسات الاستراتيجية،

1440 هـ- = 2019.

190 صفحة ؛ 24-سم – سلسلة مصطلحات معاصرة؛(21)

يتضمن إرجاعات ببليوجرافية.

ردمك: 9789922604138

1- السبرانيّة. أ. العنوان.

LCC : Q310 .A45 2019

DCC: 003.5

مركز الفهرسة ونظم المعلومات التابع لمكتبة ودار مخطوطات العتبة العباسية المقدسة.

ص: 3

الفهرس

ص: 4

ص: 5

ص: 6

مقدمة المركز

تدخل هذه السلسلة التي يصدرها المركز الإسلامي للدراسات الإستراتيجية في سياق منظومة معرفية يعكف المركز على تظهيرها، وتهدف إلى درس وتأصيل ونقد مفاهيم شكلت ولما تزل مرتكزات أساسية في فضاء التفكير المعاصر.

وسعياً إلى هذا الهدف وضعت الهيئة المشرفة خارطة برامجية شاملة للعناية بالمصطلحات والمفاهيم الأكثر حضوراً وتداولاً وتأثيراً في العلوم الإنسانية، ولا سيما في حقول الفلسفة، وعلم الإجتماع والفكر السياسي، وفلسفة الدين والاقتصاد وتاريخ الحضارات.

أما الغاية من هذا المشروع المعرفي فيمكن إجمالها على النحو التالي:

أولاً: الوعي بالمفاهيم وأهميتها المركزية في تشكيل وتنمية المعارف والعلوم الإنسانية وإدراك مبانيها وغاياتها، وبالتالي التعامل معها كضرورة للتواصل مع عالم الأفكار، والتعرف على النظريات والمناهج التي تتشكل منها الأنظمة الفكرية المختلفة.

ثانياً: إزالة الغموض حول الكثير من المصطلحات والمفاهيم التي غالباً ما تستعمل في غير موضعها أويجري تفسيرها على خلاف المراد منها، لا سيّما وأن كثيراً من الإشكاليات المعرفية ناتجة من اضطراب

الفهم في تحديد المفاهيم والوقوف على مقاصدها الحقيقية.

ثالثاً: بيان حقيقة ما يؤديه توظيف المفاهيم في ميادين الاحتدام الحضاري بين الشرق والغرب، وما يترتب على هذا التوظيف من آثار سلبية بفعل العولمة الثقافية والقيمية التي تتعرض لها المجتمعات العربية والإسلامية وخصوصاً في الحقبة المعاصرة.

رابعاً: رفد المعاهد الجامعية ومراكز الأبحاث والمنتديات الفكرية بعمل موسوعي جديد يحيط بنشأة المفهوم ومعناه ودلالاته الإصطلاحية، ومجال استخداماته العلمية،فضلاً عن صلاته وارتباطه بالعلوم والمعارف الأخرى. وانطلاقاً من البعد العلمي والمنهجي والتحكيمي لهذا المشروع فقد حرص لامركز على أن يشارك في إنجازه نخبة من كبار الأكاديميين والباحثين والمفكرين من العالمين العربي والإسلامي.

* * *

هذه الدراسة التي تدخل كحلقة جديدة ضمن سلسلة مصطلحات معاصرة، تعني بمصطلح مستحدث جرى تداوله في السنين الأخيرة في حمى الثورة المعلوماتية عنينا به مصطلح "السيبرنيطقا". تحاول الدراسة مقاربة هذا المصطلح كمفهوم بما يعنيه من قدرة الانسانية على التواصل والتحكم والسيطرة، في مجمل نواحي حياتها المعاصرة.

والله ولي التوفيق.

مقدّمة

في عصـر المعلومـات الرقميـة ومـا تحمله من رموز ودلالات انتهى عهـد المسافات المضـنية التي كان على الخبر أن يقطعها ليصل إلينا، وصار ،الحـدث، أي حـدث وأينما حصل، يتردّد هنا وهناك وهنالك في الوقت ذاته، وغالبًا لحظـة حصوله أو بعـدها بثوان معدودة؛ وهذا ما أعطى تعبير القرية الكونيّة ثوبها اللائق بهذه التسمية.

صار بوسع من يرغب أن يُهاتف ابنه في أقاصـي المعمورة، فيخاطبه صوتًا وصورة، وبأقل جهد وتكلفة. كذلك باتت المعارف المختلفة التي ليس لها حـدّ من حيث الكم والنوع، متيسـرة من خلال كبسـة زرّ أمام الشاشـة؛ كـذلك غـدت سـفريات الطائرات والقطارات والبواخر تتمّ بانتظـام وأمـان دقيقين، تُشـرف عليهمـا الآلات والأجهزة من خلال النظم الحاسوبيـة التي زُوِّدت بها لتنقلها، هي الأخرى، من عهـد الآلة الصماء التي من معدن وبلاستيك وفحم، إلى عصرالآلة الذكيّة التي تُفكّر وتحسب وتتحكّم وتُنظم»... بأداء يكاد يكون

كاملا من دون خطا.

انخفض عديـد الأيـدي البشـريّة العاملـة، وراحت الآلات تحلّ محلّها، وتُرك للإنسان في الكثير من الميادين، مجرد برمجة الآلة وتزويدها بالجرعات المطلوبة من الذكاء، لتقوم بملايين المهام ضمن وقت محدود، وبلا أخطاء، مما كان بوسع الإنسان القيام به،

إنما خلال زمن غير محدود ، بل طويل جدا بالمقارنة ومن دون ضمانة عدم الوقوع في ألف خطا وخطا.

جاء هذا كله بفضل الذكاء الصناعي والتقانة المتصلين بالسيبرانيّة.

لم تعد الأجهزة الآليّة مُغرية مقابل مثيلاتها الإلكترونية، مع امتيازات شتّى لهذه الأخيرة، تشـمل دقة الأداء، وغزارة الإنتاج، وندرة الأخطاء التشغيلية أو التصنيعيّة، مع جزالة الاستيعاب.

نقطة الانطلاق الأساسية ابتدأت من السيبرانية، هذه اللفظة الأعجميّة الطاردة من كلمة أجنبية هي Cyber ومعناها: الافتراضي أو المتخيّل. ومن السايبر اشتقت لفظات شتّى بات لها دلالاتها، وفي طليعتها اللفظة الأهمّ من حيث فعّاليّة مدلولها وتأثيره: الفضاء السيبراني.

والفضاء السيبراني هو ذلك الحيّز الافتراضي الذي تتم من خلاله وفيه مُجمل الأنشطة السيبرانية. ويمكننا تخيله كأنّه حيّز مكاني يصل بينك وبين الآخرين هنا في الغرفة الثانية من بيتك، أو هناك في مقرّ عملك البعيد، وربما في طهران أو في بيونغ يانغ (عاصمة كوريا الشمالية، أو في ريو دي جانيرو البرازيلية أجمل مدن العالم، أو حتى في دمشق أو بغداد أو باريس. نعم؛ المسافات في الفضاء السيبراني (الافتراضي) ليست طريقـا طويلاً إذ يمكنـك أن تقطعها في لحظـة سـريعة من خلال كبسـة زرّ على ملامس جهازك الكومبيوتر أو هاتفك المحمول. ولعلّك انتبهت من خلال سياق

العبارة التي سبقت أنّ وسيلة تواصلك مع ذلك الفضاء السيبراني، تلك الآلات المذكورة من كومبيوتر وأشباهه؛ إلا أنّ ما ينبغي أيضًا إدراكه في هـذا السـياق، هو أنّ الجهاز المشار إليه لا يملك بذاته إمكانية وصـلك بأي طرف آخر عبر الفضاء السـيبراني، بل هو يحتاج إلى موصـل يصلك، أي إلى طريق تسلكها لتصل: هذه هي شبكة الإنترنت.

وباجتماع العناصـر الثلاثة، يصـير بوسـعك الدخول في الفضاء السيبراني: الجهاز، وهو الآلة المؤهلة لتحقيق جزء أساسي من هذه المهمة، وشبكة الإنترنت التي هي وسيلة وصل غير سلكية، والفضاء الإلكتروني ذاته.

بـدلاً من الرسائل الورقيـة وسّـعاة البريـد، باتت الشاشة هي ساعيك ووسـيلة إرسالك الرسائل وتلقيك إيّاها. وبدلاً من المكتبة الهائلة التي ستشـغل حيّزاً واسـعًا من البيت (إن جعلتها فيه) وتتطلّب منك جهودًا مُضـنية للبحث عن معلومـة ما أو سـيرة أو صورة...، باتت مُحركات الإنترنت وأشهرها (google) تحقق لك مطلبك خلال وقت هو ذاته الذي تفرضه مهاراتك في اسـتخدام الجهاز والإبحار في الإنترنت، من عدة ثوان وصعودًا.

وما بين الدهشة والتسـلية لم تنتبه إلا وكلّ بياناتك وبيانات عملك والشركة التي تعمل فيها، وكلّ بيانات الوزارات والمؤسسات ودوائر الدولة برمتها... كلّ ذلك بات مختزنا في الفضاء السيبراني (أي) على الإنترنت كما يُقال)، وبكبسة زرّ تحصل على مرادك منها،

ص: 11

سواء أكان رقم حسابك المصرفي أم كلمة المرور للدخول إليه، أم أيّ معلومة تريد في العلوم والموسيقى، والتاريخ، والأدب. بالنسبة إلى معلوماتك الشخصيّة أو كلّ المعلومات الأخرى التي تعود لمؤسسات خاصة أو للدولة وأجهزتها ... لا تكون سائبة ولا متاحة في الفضاء السيبراني لكلّ من يرغب؛ إنّها تكون على الدوام تحت حماية برنامج كومبيوتر خاص يمنع الآخرين عنها. هذا هو الوضع بالنسبة إلى حساباتك ومعلوماتك وبياناتك، وهذا أيضًا هو الوضع بالنسبة إلى بيانات الآخرين ومعلوماتهم.

ومن هنا ابتدأت حكاية قرصنة المعلومات» أي اقتحام برامج حماية المعلومات، والوصول إليها، والتحكّم بها ولأنّ عملاً كهذا هو لصوصية بكلّ معنى الكلمة، فإنّ القانون يُعاقب مرتكبه... إذا أمكن تحديد هذا المرتكب . وبالنظر إلى الأهمّيّة البالغة للبيانات، من حيث كونها الهيكل المعلوماتي للطرف الذي تخصّه فهو يبذل أقصى جهد لحمايتها. ومن جهتهم، يبذل «القراصنة» أقصى مهاراتهم لخرق حمايتها والاستحواذ عليها. يكون ذلك إما لبيعها لطرف منافس لصاحب المعلومات، أو عدوا له...، أو لاستخدامها ضد مصلحة صاحبها ، أو لطلب فدية» ماليّة لقاء إعادتها لتَصَرُّف أصحابها.

لماذا كلّ هذا السعي خلف البيانات؟

لأنّها بكل بساطة، مثابة صورة بأشعة إكس» الكاشفة لكلّ ما في داخل صاحبها؛ ففي هذه البيانات كلّ شيء عن الفرد، وعن

الدولة، وعن الشركة، وعن الجيوش، وعن الأسرار الأمنية، وعن ،الصناعات، وعن المعارف....

والخوف كلّ الخوف أن يتمكّن الإرهاب من قرصنة ... شيفرة إطلاق صواريخ نووية لهذه الدولة «العُظمى» أو تلك...

لقد سبق اختراق معلومات حسّاسة لوكالة الاستخبارات الأميركية ونشرها في الصحف؛ وبالتالي، فالاحتمال الأخطر قائم بالفعل.

وحين يحصل هذا، إن حصل تصبح الحياة على الكوكب مجرّد موضوع جدال بين الإنسان والآلة.

***

في هـذا الكتاب نسـتعرض الموضوع من جوانبه كافّـة؛ نُضـيء على السـيبرانية أولاً من حيث المعنى والمفهوم، ومن أين أتت اللفظـة وماذا تعني. بعـد ذلك نعمل على توضـيح الوسـيلة التي يجري بواسـطتها التواصل مع الفضاء السـيبراني، ومع الأشـخاص الآخرين، ومع خزائن المعلومات والمعارف، نعني بها الإنترنت هذه الشـبكة الأشبه بشباك العناكب، لتداخل خيوطها وتراكمها واستقلالية كلّ خد فيها. ومن هنا نُطلّ على مفهوم الحرب في الفضاء الافتراضي (السيبراني)، كيف تنشب ،معاركها، وما هي أسلحتها وأعتدتها،

ولماذا يمكنها أن تكون أكثر تدميراً من الحروب النووية المُهابة.

وطالما أنّ المعرفة والتواصل والتسيير والضبط، والتنظيم،

والمتابعـة، والمراقبـة، والإشـراف... كلّها تجري من الفضاء السـيبراني وفيه، حيث تختزن المعلومات والبيانات والأسـرار والشـيفرات، فمن البديهي أن يكون للأمن السيبراني أهمّيّته المطلقة، بحيث تتأمن المعلومات المخزنة وتكون جاهزة كلّما طلب أصحابها استعادتها، وتكون محمية فلا يقتحمها ،مقتحم ، ولا يُقرصـنها قرصان. فمن يستحوذ على معلوماتك، يُعرّيك من عناصر معرفتك وقوتك، ويمكنه أن يستعبدك لقاء الإفراج عن معلوماتك؛ هذا إذا كنت شخصًا ، فكيف إذا كنت إدارة أو وزارة أو جيشًا أو دولة؟

إنّ من يملك المعلومات يتسـيّد على أصحابها، ويُتاح له إعادتهم، ليس إلى العصر الحجري، بل إلى عصر القلم والورقة على الأقلّ ؛ وهذه خطوة انتحارية إلى الخلف.

لكلّ ذلك ينبغي التفكير جـديا في بناء استراتيجيـة سـيبرانيّة عامة لكلّ الدول العربيّة والإسـلامية، وسوف لن يمكننا تحقيق أي مسـتوى من الأـمن الوطني ولا القومي على الصـعيد السـيبراني، إلا من خلال تطوير البنى السـيبرانية عنـدنا وتعزيزها بالخبرات الجديـدة والمزيـد من التأهيل للكوادر. وفي المرحلة الراهنة، من الأفضل أن نسعى جاهدين إلى تحويل مجتمعاتنا المستهلكة ولا سيما الغنية منها،

إلى مجتمعات منتجـة ومثقفـة على المسـتويات السـيبرانية. فالقوّة والمنعة لن تكونا بشـراء واقتناء أحدث الأجهزة وأغلاها ثمنًا، بل في رفع الكفاءة العلمية والتقنية على المدى الوطني الأوسع.

وهذه ليست نصيحة بل مجرّد رأي.

الفصل الأول:

مفهوم السيبرانيّة والفضاء السيبرانيّ

ص: 15

الفصل الأول:مفهوم السيبرانيّة والفضاء السيبراني

عناوين فرعيّة:

اشارة

السيبرانية تعني الإلكترونية، واللفظة منحوتة من كلمةCyber ومعناها: المفترض أو المُتخَيّل.

الفضـاء السـيبرانيّ هو تلـك البيئـة الافتراضـية التي تعمـل فيهـا المعلومات الإلكترونيـة والتي تتصل عن طريق شـبكات الكمبيوتر الفضاء السيبرانيّ، مثل الفضاء التقليدي، يتألف من أربعة مكوّنات رئيسيّة هي المكان والمسافة، والحجم، والمسار.

كثر في الآونـة الأخيرة ورود تعابير ينظر إليها جمع كبير من القراء على أنّها جديـدة وربما ،غريبـة، وتحتوي على مقادير متفاوتـة من الإبهام وعـدم اليقين، بحيث يجري في الغالب تجنّب متابعـة قراءة النصّ الـذي يتضـمّن هذه التعابير والتي من أشـهرها السايبر والعالم السـيبراني والفضاء الإلكتروني...

والواقع أنّ هذه التعابير التي تبدو أحيانًا جديدة بالنسـبة للبعض» وغير مفهومة، إنما هي في الواقع من طبيعة هذا العصر، الطالع على أكتاف التقنيات التي باتت تُحلّق عاليًا في عوالم الابتكار العلمي والإبداع التقني، وقد راحت تنشـر وسائطها بين الناس على مستويات واسعة جدا، بحيث أنّ الهاتف الذكي على سبيل المثال، بات بين أيدي مليارات البشـر في أرجاء العالم، والنسـبة العالية منهم التي تستخدمه، لا تُحيط بكيفيات استخدامه والاستفادة من مزاياه.

ص: 16

هـذا مع الإشـارة إلى أنّ هـذا الجهـاز الصـغير حجمًـا، إنمـا يختزن من المعارف الإلكترونيـة والأنظمـة والبرامـج والمعلومات والتقنيات والمواصفات ما يحتاج لو جرى تجسيده على ورق، إلى خزائن هائلة الاتساع لكي يُحفظ فيها.

ومن هنا، من هذه الآلة واسـعة الانتشار والتي باتت بالنسـبة إلى مليارات حامليها ضـرورة حتمية لا يمكن التخلي أو الاسـتغناء عنها... من هـذه الآلـة «الشخصـيّة» يكون الدخول أكثر سـهولة ويُسـرًا إلى جملة المفاهيم الكامنة في التعابير المشار إلى غرابتها حينًا وعدم وضوحها تماما في أغلب الأحيان.

وبالمناسـبة، فهذا الهاتف الذي يماثل الكفّ حجما-، يتيح لحامله الاتصال بصديق على الجانب الآخر من الشارع، كما بصديق آخر على الجانب الثاني من الكرة الأرضية، سواء بسواء. ويتم اتصال كهذا عبر فضاء واسع، هو ما يُسمّى بالفضاء الإلكتروني أو السيبرانيّ.

1. معنى الكلمة:

قبل الإضاءة على مفهوم «الفضاء السـيبراني تضـطرنا كلمة السـيبرانية بداية إلى توضيح معناها والإضاءة على أصلها ومنبتها. اللفظة منحوتة من الكلمة اللاتينية cyber ومعناها القاموسي: تخيلي أو افتراضي. ودرج استخدامها لوصف الفضاء الذي يضم الشبكات المحوسبة، ومنها اشتقت صفة السيبراني والسيبرانية Cyberrnetic، وتعني علم التحكّم الأوتوماتي، أو علم الضبط.

ص: 17

ومن الزاوية التقنية العمليّة فالسـيبرانية هي ترابط حواسـيب مع أنظمة أوتوماتيكية، والنظم السيبرانية المركزية ستنسق كل الآلات والمعدات التي سـتخدم كلّ المدينـة، الأمـة، والعالم، بشـكل شامل، لتحقيق الرفاهيـة وضـمان كفاءة عمل جميع فعاليات المدينـة ويمكن للمرء أن يتخيّلها كنظام إلكتروني عصبي لا إرادي يمتد في كلّ مناطق التركيبة الاجتماعية.

لكنّ المعنى العملانـي – إذا جـاز التعـبير – يمكن تلمّسه من خلالـ عـالم أجهزة الكمـبيوتر والإـنترنت وبالتـالي تكنولوجيـا المعلومـات والاتصالاـت. فالأـمر المُتخيّـل أو المفترض هو أمر يمكن وعيه وليس لمسه؛ فهو مفهومي وليس ماديًّا متجسّدًا، أي أنّه مُتخيّل بمعنًى ما، وبالتالي افتراضي هذا العالم الافتراضي هو ما عرفناه حديثًا بفضل الإنترنت، وفيه نبني صناديق بريد شخصي (E-mail) أو مواقع إلكترونيّة، وكلّها تقوم في عالم قائم افتراضـيا وغير ملموس فعليًا. هذا هو العالم السـيبراني أو الإلكتروني الذي نبلغه بفضل آلات من عالم الكومبيوتر والإنترنت.

ولعله من المناسب كذلك لفت الانتباه إلى أنّ السـيبرانية يمكن أن تعني من زاوية محدّدة حالة ترابط الحواسـيب (الكومبيوترات) مع أنظمة أوتوماتيكيـة. هذه هي النظم السـيبرانية المركزية التي يمكن أن تعمل على تنسـيق كل الآلات والمعدات التي سـتخدم كلّ المدينة، الأمة، والعالم بشـكل شامل، لتحقيق أعلى رفاهية للبشر. وفقط، عندما تدمج السيبرانية مع جميع نواحي هذه الثقافة الجديدة والمتحركة باستمرار، ستستطيع الكومبيوترات خدمة حاجات البشر

ص: 18

كما يجب. ولن تتمكن أي حضارة تكنولوجيّة من العمل بكفاءة وبتأثير، من دون ، من دون دمج السيبرانية كجزء متكامل من حضارة العالم الجديدة هذه.

وبالعودة إلى السياق، فإنّ كلمة السايبر أو الافتراضي اغتنت بالاشتقاقات اللفظية التي راحت تتداعى للتعبير عن مفاهيم جديدة في ميادين التكنولوجيا الرقمية وعوالم الإلكترونيات، مبتكرة جملة جديدة من المركبات اللغويةالمفهومية التي تنطلق من هذا العلم وتستخدمه وتخضع لمقتضياته، فتُعبّر عن أنماط لا حصر لها من الأفعال والأنشطة التي تجري ضمن الفضاء السيبرانيّ.

2. البدايات:

تعود بدايات ظهور كلمة (سيبرانية) إلى العام 1960 حين أطلقها الباحثان «مانفريد كلاينس» و«ناثان كلاين»(1). وإليهما يعود الفضل في «نحت لفظة سايبورغ cyborg–أو الكائن السيبرانيّ(2). cybernetic" organism

" إشارةً إلى كائنات مُعالجة تمتلك أجزاء عضويّة وأخرى "بيوميكاترونيك" (تكون حصيلة دمج عناصر ميكانيكية وأخرى إلكترونية وثالثة حيوية). وبمعنى أبسط فإنّ السايبورغ هو كائن حي في الأساس، أمكن للعلم تعزيز قدراته خلال دمج بعض المكوّنات الاصطناعية أو بعض التكنولوجيا، في جسمه وأعضائه. وكان الفنّ السابع (السينما) سبّاقًا إلى تجسيد

1- http://www.anntv.tv/new/showsubject.aspx?id=101954.

2- David Held et al., Global Transformations: Politics, Economics, and Culture (California: Stanford University Press, 1999).

هـذه التخيّلات على الشاشـة باعتماد الحيل السـينمائية. ولعلّ أفضل مثال على ذلك ظهر في المسـلسل التلفزيوني الأميركي (رجل السـتة ملايين دولار بين العامين (1973 و 1978 ولاقى في حينه رواجًا عالميًا واسـعًا وكان من بطولة الممثل "لي مايجور" بدور "ستيف أوستن، وهو الرجل الخارق الـذي تعرّض لحادث خسـر فيه بعض أعضائه الأساسـيّة، فعمل العلماء على تعويضه تلك الأعضاء الحيّة بأخرى آلية جعلته بشريا يتمتع بقوى خارقة.

انطلاقا من هذه الفكرة الخيالية ينتشر في الأوساط العلمية اعتقاد يميل إلى اعتبار أنّ تكنولوجيا السايبورغ هذه سوف تُشكّل جزءا.

ثورة ما بعد البشـريّة المعروفة اليوم، والمعنى بروز بشـر جرى تعديل أجسامهم، وبالتالي تعزيز قدراتهم، بوسائل تقنية متقدمة، بما يمنحهم قدرات إضافية عالية ومميزة يتفوقون بها على "البشري غير المُعدّل".

إن أهمية المجال الإلكتروني في تشكيل قدرة الأطراف المؤثرة، تُظهر حقيقة عملية انتقال القوّة ،وانتشارها من النطاق الدولي التقليدي (البرّ والبحر والجوّ والفضاء إلى الفضاء السـيبراني، حيث للـدول المتقدّمـة الأسـبقية في الوجود والسـيطرة والتحكّم من دون إمكانيـة تحقيق أي مسـتوى فاعـل من الاحتكـار لكنّ المجتمع الـدولي يتابع اتجاهات التحوّل في قضـية التعامل مع تهديـدات الفضاء الإلكتروني، وإمكانية تحوّله نحو العسـكرة، الأمر الـذي بات واضـحا من خلال تصاعد الهجمات الإلكترونية ومخاطرها على أمن الفضاء الإلكتروني وما فيه من معلومات تتحكّم بدورات حياة

البشـر في مختلف الدول والمجتمعات. لذا، فإنّ تصاعد القدرات في سباق التسلّح السيبراني عبر الفضاء الإلكتروني وتبني سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن، وتصاعد حجم الاسـتثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة، كلّه يُنبئ بأنّ المسـتقبل لن يكون مضـمونًا أمام أطماع المقتدرين ما لم تتقدّم البشرية نحو المزيد من التكافؤ في المقدّرات السيبرانية، الأمر الذي لا يبدو متيسرا اليوم.

ولعلّ هذا ما يدفع العديد من الدول إلى العمل على إدخال الفضاء الإلكتروني ضمن استراتيجية الأمن القومي لديها، والعمل على تحديث الجيوش من خلال إنشاء وحـدات متخصـصة في الحروب الإلكترونيـة، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب، وإجراء المنـاورات، لتعزيز الـدفاعات الإلكترونيّـة، والعمـل على تعزيز التعـاون الـدولي في مجالاـت تـأمين الفضـاء الإلكتروني، والقيام بمشاريع وطنية لتحقيق هذا الأمن وتحصينه ما أمكن.

إنّ القيمة الأساس للسـيبرانية ليست فيها بذاتها بقدر ما هي في توظيفها لخدمة الإنسان سواء لتنظيم ورفع كفاءة الإدارات على أنواعها كافّة، أم للقيام مقام الإنسان بعمليات الحساب والمراقبة والرصد والمتابعة بشكل يضمن السرعة والدقة والجدوى.

ص: 21

3. مفهوم الفضاء السيبراني

.(1)

تعبير الفضـاء السـيبراني (أو الفضـاء المعلوماتي) يعني الوعاء الـذي تُختزن فيه المعلومات وتتحرك فيه الرسائل الإلكترونيـة المتبادلـة بين جهـازك (أكـان هاتفًـا ذكيًا أم كومبيوتر أم لابتوب...) وأجهزة الآخرين. وحسب تعريف قاموس أوكسـفورد فقـد جاء أنّ "مصـطلح الفضاء السـيبراني هو البيئة الافتراضـية التي يتم عبرها إتمام عملية الاتصال عبر شـبكات الكمبيوتر. وهو يُشـير إلى مكان افتراضي يمكن استخدامه بالتواصل عبره والتخزين فيه. فالرسائل التقليدية الورقية كانت تصـلنا عبر الساعي والخدمات البريدية التقليدية، واليوم باتت تصـلنا نصوصًـا وصُوَرًا ومقاطع فيديو وأفلاما طويلة على شاشة، سالكة دروبها (من وإلى ضـمن الفضاء السـيبراني. ومن هنا تطوّر علم البرمجة ليُنتج آلات تعمل من تلقائها بفضل برامـج معلوماتيـة خاصـة؛ وهـذا من ثمار التكنولوجيا السـيبرانية. وعلى هـذه الخُطى سارت العلوم السـيبرانية لـ- «تسـتنبت» في حقولها برامج معلوماتية يمكن أن تقوم بكلّ ما يخطر وما لا يخطر على بال فتصنع التقدّم والرفاهية وتسرّع العمل كما تصنع احتمالات الرعب والخوف في ميادين القوّة والإنتاج، والتحكم والسيطرة.

صحيح أنّه كلّما أرسلت أو تلقيت رسالة إلكترونية (e-mail)،

تكون دخلت في عالم الفضاء السـيبراني المبني أساسًا بفضل علم المعلوماتية، إنما ينبغي أن تتذكر دائماً أنّ هذا الفضاء السـيبيراني لا يقوم بشكل مباشر وملموس، لا بين البشر ولا بين الشجر، ولا

1- https://www.politics-dz.com.

على الأـرض اليابسـة، ولاـ على صـفحات البحـار أو في أعماقها، ولا على القمم الجبليـة الوعرة، ولا في الأجواء ولا... ولا... بل هو فضاء افتراضي يقوم بين الأجهزة الإلكترونية المتواصلة مع بعضها بفضل الإنترنت. فأنت تُرسل بريدًا إلكترونيًا من جهاز تحت تصرّفك (كومبيوتر أو لابتوب أو هاتف محمول...) إلى جهاز آخر من هـذه العائلـة. والمجال الـذي يجتازه بريدك الإلكتروني (رسالتك) من جهازك المرسـل إلى الجهاز المتلقي، هـذا المجال (المفترض وجوده) هو الفضاء السـيبراني. وهو على ما ينبغي تحديده: فضاء افتراضـي ومُشاع، بمعنى أنّه بإمكـان أي كان أن يسـتخدمه (يُرسل منه ويتلقى عبره)، من عناوين يبنيها (E-mail) إلى عناوين أخرى بناها أصـحابها. والمعنى أنّ الرابط السيبراني بين الناس هو الآلة الذكيّة.

يستضـيف الفضاء السـيبراني اليوم معلومات البشـرية جمعاء، وجميع نُظم التشغيل والتسيير والإنتاج، والمراقبة والمتابعة، والأمن والسلامة والرفاهيـة ... لكلّ شأن من شؤون الحياة والعمل والتزويـد... ومجرّد توافر الطاقـة الكهربائيـة في البيت أو نقطـة الماء أو الغذاء، كلّها تكون مُرتهنـة لأنظمة توفير وتزويد وتوزيع بالغة الدقة، تعمل إلكترونيًا بمنتهى الترتيب والانتظام. ومن دون الأنظمة الكومبيوترية المنظمة والراعية لكلّ ذلك، فلن يتوافر شيء لأحد، اللّهم غير الفوضى العارمة والتوحش والصراعات الدموية من أجل أدنى الحاجات والحاجيات.

أمّا كلّ هذا التنظيم الدقيق، بل الفائق الدقة الذي تسـير عليه شتّى أمور الحياة اليوم، فهو يقوم على جملة مقوّمات تدين برمتها للسـيبرانية بما هي علم متكامل لتجميع المعطيات وتنظيمها

ص: 23

ومعالجتها وتوجيهها، بما يخدم الغاية الأساس منها، وهي صالح الجهة المعنيّة، دولةً كانت أم شركة أم مؤسسة خاصة. وبدلاً من ملايين ساعات العمل المكتبي وما يمكن أن يكتنف كلّ ذلك من أخطاء وحالات سهو وخلافها، تتكفّل العلوم السيبيرية بحلّ هذا النوع من المعضلات في أوقات قصيرة جدا وأحيانًا بمجرد كبسة زر.

وهذا ما يجعل من السيبرانية نقطة قوّة جبارة للأمة المعنية، يستطيع الراغب من خلالها استعادة أي معلومة ومعالجة أيّ مسألة خلال برهة يسيرة من الزمن. وبدلاً من إنتاج سيّارة واحدة كلّ ثلاثة أشهر في أوّل مصانع السيارات بات بالإمكان وبفضل العلوم الرقمية والإلكترونيات، وبالتالي السيبرانية التي تتضمّن كلّ ذلك، إنتاج مئات السيّارات في الساعة الواحدة.

ذلك أنه عندما تندمج السيبرانية في مختلف نواحي هذه الثقافة الجديدة والمتحركة باستمرار، ستتمكن الحواسيب من خدمة حاجات البشر كما يمكن أن نتخيّل. ولن تتمكّن أي حضارة تكنولوجية من العمل بكفاءة وبتأثير، من دون دمج السيبرانية كجزء متكامل من حضارة العالم الجديدة. كذلك فهذه السيبرانية جديرة بأن تُغيّر أشكال الحروب وميادينها وسُبُل خوضها، مما سيجري توضيحه في ما بعد.

ص: 24

ص: 25

الفصل الثاني:البيئة السياسيّة والاجتماعيّة والتكنولوجيّة

اشارة

ثمّة أبعاد شتّى مختلفة للفضاء العامّ يمكن إيرادها كالآتي: البعد المؤسسي: ويتمثل في ضعف دور الأحزاب السياسية والمجتمع المدني ومُمثّلي السّلطة التشريعية كمؤسسات وسيطة بين الحاكم والمحكوم، وعجزها في أحيان كثيرة عن حمل مطالب الرأي العام، الأمر الذي أدّى إلى انفصال تلك المؤسسات عن الواقع الاجتماعي والسياسي الذي تعيش فيه، بالإضافة إلى عدم التوافق بين التغييرات في الرأي العام وعمليّة وضع السياسات.

البعد التكنولوجي: ويتمثل في الارتباط المتزايد بتكنولوجيا الاتصال والمعلومات وتوفير فرص أمام لاعبين جدد، وبخاصة مع ما وفّره الإنترنت وكونه وسيلة سهلة ورخيصة وسريعة الانتشار، عن اندماج الخدمات مع بعضها بحيث تتيح الشبكة خدمة الاتصال وإمكانية التراسل المجاني، إضافةً إلى الحرية المتاحة وارتفاع سقفها عن وسائل الإعلام التقليديّة.

البُعد التنمويّ: تتمتع المجتمعات التي تكون في طور التحوّل بحالة مُتصاعدة من الحراك السياسي. وقد شهد العديد من المجتمعات عددًا وافراً من السياسات التي تُشكّل دورًا مهما في إيجاد حالة من الحراك السياسي بين المهتمين بالشأن العام. إلى ذلك فإنّ انفتاح المواطن على الخارج يولّد لديه طموحات وتطلعات أكبر قد تمثّل ضغطاً على صانعي القرار، وقد لا تتوافق مع الواقع الاجتماعي والاقتصادي السائد.

ص: 26

البُعد ذو الطابع الجيلي أو العُمري: تتضـمن المجتمعات العربية عمومًا فئة شـبابية تزيد على نصف تعدادها السـكاني، وهؤلاء لديهم رؤى تغييرية في الغالب، وهم على دراية كافية بتكنولوجيا الاتصال والمعلومات والتفاعل معها، خلافاً للأكبر سنًا.

1. شبكة المعلومات

عندما يصـبح للكومبيوتر شبكة مجسات استشعارية تمتد لتغطي المساحة الكاملة لكلّ المجموعات المادّيّة والاجتماعية المعقدة، نستطيع تحقيق المركزيـة في اتخاذ القرار، كما أنّ القرارات لن تتخـذ في الاقتصاد العالمي القائم على الموارد على أسـس سياسـيّة محليـة، بل على أساس منهجي شامل يرتكز على الحسابات والإحصاءات والمقارنات والمقاربات، وإيجاد المعالجات والحلول.

يتصـل هـذا النظـام المركزي بمختبرات بحوث وجامعـات، حيث تراقب البيانـات المتوافرة وترفـدها بمعلومـات جديـدة وبشـكل مسـتمر والتكنولوجيا اللازمة لإدارة بنية تحتية كهذه متوافرة حاليا. الفرق الرئيسـي بين تكنولوجيا الكومبيوتر اليوم، والنظام وتكنولوجيا الكومبيوتر في المسـتقبل، هو أنّ النظام الجديد سيكون على شكل جهاز عصبي يعمل ذاتيًا وبشكل مستقل بمجسات بيئية" وغيرها، ليغطّي جميع نواحي الحياة الاجتماعيـة المعقدة التركيب، وسـيقوم بتنسـيق التوازن بين الإنتاج والتوزيع ويعمل على المحافظة على نسق اقتصادي متوازن. هذه التكنولوجيا الصناعيّة المنسّقة إلكترونيًا يمكن تطبيقها على الاقتصاد العالمي كليًا.

ص: 27

على سبيل المثال، يتم بواسطة نشر مجسات إلكترونية عبر مناطق زراعية واسعة مراقبة هذه الأراضي عبر شاشات أجهزة كمبيوترية، ومتابعة وتنظيم منسوب المياه الحشرات القوارض أمراض النباتات الخصوبة، وغيرها من المعلومات التي تسمح لنا بالوصول إلى قرارات مناسبة وأكثر دقة، مبنية على البيانات التي نحصل عليها ميدانيًا.

وفي ظلّ الارتباط والاندماج بين المعلومات من جهة، والشبكة الدوليّة التي تستضيفها من الجهة المقابلة الإنترنت)، ينقلب الفضاء السيبراني من موئل ومضافة ومخزن، إلى ساحة مواجهات... وربما ميادين معارك وحروب من النوع الذي لا تُسمع فيه ولا حتى طَلقة رصاص.

والمشكلة المُحرجة هي أن لا غنى للعالم (في تقدّمه وتطوّره) عن السيبرانية والفضاء السيبراني. فمن هذا النطاق ينفذ العالم إلى ميادين المزيد من التقدم والتطوّر، وتعزيز الإنتاج، وتعميم الرفاهية.

ومن هذا النطاق ذاته أيضًا تهبّ ريح السّموم ومخاطر الاقتحامات والاجتياحات الإلكترونية المعيقة والمكلفة والمدمّرة، وعلى هذا الوتر تتراقص مفاهيم وإمكانات السيطرة والسيادة والتحكم.

ومع تزايد الاعتماد على الوسائل التقنية الحديثة في إدارة الأعمال المختلفة، بَرَزَت تحدّيات قانونية وطرحت تساؤلات حول إمكان اعتبار التواصل الإلكتروني الافتراضي (Virtual communication) الذي أصبح يتمّ اليوم بواسطة

الإنترنت (Internet) أو الفضاء الإلكتروني أو فض-اء السايبر أو الفضاء السيبراني (Cyberspace)، موازيًا للمرافق العامة الدولية التقليدية، وحول ضرورة عقد معاهدات جديدة تنسجم مع التطور التكنولوجي إن لم تكن الإمكانية الأولى متاحة أو كافيّة.

وهنا تظهر المشكلة الكبيرة في أوضح تجلياتها المحيرة بشكل بالغ الإحراج؛ السيبراني هو ضرورة حيوية لا غنى عنها البتة في هذا العصر ومستقبله المنظور على الأقل. ومن يختار الخروج أو تجميد تواجده ضمن هذا الفضاء، إنما يحكم على مقدّراته وكلّ ما يتصل بدورة حياته وإنتاجه بالاختناق والغرق خلال ساعات قليلة لا أكثر، من دون توافر أي سبيل نجاة أو استنقاذ. وربما تكون مقارنة من يختار الخروج من الفضاء السيبراني بمن اختار العودة من وادي السيليكون في القرن الواحد والعشرين إلى عصر الإنسان الأوّل (هوموس نياندرتاليس) حيث لا صناعة ولا زراعة ولا إنتاج ولا مجتمع، وحيث لا أسلحة ولا بيوت ولا طاقة ولا سلاح وحيث ستكون مواجهة الماموث العملاق والديناصورات المفترسة أحد أسط الأخطار المحدقة به.

من الضروري أن نتذكر دائمًا أنّ محتويات الفضاء الإلكتروني ليست بالأمر العادي أو البسيط، إذ هي عادة إجمالي الثروة الحيوية للجهة المخزنة ولنفترض أنّها الدولة في هذه الحال).

(فالإدارة العامة لأي دولة بما هي رئاسات ومجالس وإدارات وقطاعات وأجهزة، ينظمها كم هائل من الوثائق واللوائح والجداول والتوجيهات والقرارات والإلزامات والممنوعات... مما يحتاج،

لو تطلب الأمر توثيقه كتابةً على الورق إلى مليارات الأطنان من الكراريس والمجلّدات والمحفوظات وما إلى ذلك، إلا أنّ توفير ذلك الكم الهائل من العمل وتيسيره على شاشة حاسوب، وما يتطلبه من جهود متخصصة، جبّارة وكثيفة وطويلة الأمد، من أجل تخزينه في الفضاء الإلكتروني، وحمايته وتوفيره لأصحابه، مثل حالة تقدّم مُشرقة وعظيمة للذكاء البشري، ويسّر الأعمال والجهود من الرؤساء إلى المرؤوسين في جميع الأنحاء، واختصر بشكل أخاذ دورات العمل في جميع أماكن العمل، وأتاح رقابة لصيقة ودقيقة من قبل الحواسيب (والتي لا تُخطئ... مبدئيًا)، فانتظمت الأعمال وتيسرت، وباتت أكثر إنتاجية بأضعاف مضاعفة. وهذا الإنجاز الفريد والعظيم والهائل والذي لا يمكن إيفاؤه حقه من المديح، يحتاج أكثر ما يحتاج إلى أن يكون محميا ومضمونًا ومتيسرا على الدوام.

وبصرف النظر عن حسنات استخدام الفضاء الإلكتروني أو الإساءات التي يمكن أن تنتج عن سوء استخدامه، فقد أصبح لهذا الفضاء الدور الأـوّل والأبرز في ما يطلق عليه «القوّة المؤسسية» في السياسة الدولية، والتي تعني القوّة التي لها دور فاعل في تشكيل المنعة وتحقيق الأهداف في ظلّ التنافس بين الجميع، والمساهمة في تشكل الفعل الاجتماعي في ظلّ المعرفة والمحدّدات المتاحة والتي تؤثر في نظريات العلاقات الدولية وتشكيل السياسة العالمية.

2. المعلومة الإلكترونية

في سبيل توضيح شكل وماهيّة المعلومة الإلكترونية ينبغي

ص: 30

القول إنّهـا نوع من المعطيات (Data) يتم تسـجيلها، وبالتـالي تخزينهـا في مجـال خاص ومعين داخل الفضاء الإلكتروني، باعتماد اللغة الرقميـة التي هي لغـة الكومبيوتر ، والمختلفـة عن لغـة الأـحرف الأبجديـة المسـتخدمة في مختلف اللغات المعروفـة في العالم. وتَمتّد التعريفات المتعلقة بالمعلومة الإلكترونية Electronic)

(informationإلى فكرة واحدة هي جَمْع المعطيات (Data)

بطريقة إلكترونيّة أو ضوئية 1) Optical).

وهذه المعلومة الإلكترونية تكون معلومة مبتدعة، جرى تلقيها أو إرسالها أو حفظها خارج إطار الورق والمسـتندات المكتوبة أو المحفوظة، بوسائل إلكترونيـة (أو ضوئيّـة). ويحتاج الكومبيوتر إلى برامـج تطبيقيـة لاسـتقبال المعلومـة ولمعالجتها ولإرسالها أو تخزينها، وهذه تكون برامج نموذجيّة أو مُتخصصة، من أجل إمكان حفظ هذه المعطيات والعودة إليها لقراءتها والتعاطي معها.

3. أشكال المعلومة الإلكترونيّة

المعلومة الإلكترونية المتبادلة عبر الأجهزة الذكية من كومبيرترات وهواتف جيب وما شابه، تتّخذ العديد من الأشكال، وتتجسّد ماديًا، على سبيل المثال، عَبر الأمور الآتيـة: الشاشـة (Screen) ، أو الطابعـة (Printer)، أو الأسـطوانة الضوئيـة الرقميـة أو القرص المدمج، أو الناقل التّسَلْسُليّ العام أو الذاكرة الوميضيّة أو الهاتف الذكي. وأبرز

1- https://www.washington.edu/doit/what-electronic-and-information- technology.

الأشكال التي تتخذها المعلومة الإلكترونية هي:

تبادل المُعطيات الإلكترونية (Exchange of electronic data) من كومبيوتر إلى آخر أو هاتف ذكي إلى آخر، بواسطة شبكة مُعيّنة عن طريق استخدام قاعدة مُتّفق عليها لمعالجة المعلومة (كالحَوْسَبَة السحابيّة (Cloud computing)[1])

- التسجيل، أي المعطيات المسجّلة على كومبيوتر أو على الهاتف الذكي أو الحَوْسَبَة السحابية والتي لا تكون مُخصّصة للتبادل.

التبادل الحاصل من دون شبكة، مثلاً حين يتم نسخ المعلومات على الأسطوانة الضوئية الرقمية أو القرص المدمج (CD) أو الناقل التّسَلْسُليّ العام (USB) أو الذاكرة الوميضية(Flash memory) ونقلها إلى حاسوب أو هاتف ذكي آخر.

ممّا لا شكّ فيه أنّ هذا النوع من التواصل يفرض نفسه على المرء العصري على مختلف المستويات الداخلية والخارجيّة. وبالنظر إلى ما يُحققه التواصل عبر الإنترنت من اتساع فرصة الاختيار وسهولة التنقل بين المواقع الإلكترونية ومُقارنة المعلومات والمعطيات تُصبح حماية البيانات والمعلومات الشخصيّة والرسمية التي يتم تدفقها ضرورة حيوية وأمرًا لا غنى عنه، في سبيل مراعاة مقتضيات العصر الحديث، ومن أجل مواكبة التطور العلمي المتواصل لحظيًا

1- https://www.infoworld.com/article Morgane Fouché , Robert Macrae and Jon Danielsson. "Could a Cyber Attack Cause a Financial Crisis?" World Economic Forum (13 June 2016), online e-article.

كما هو واضح لأيّ مُتابع... هذا مع العلم بأنه يمكن للمتسللين، أفرادا كانوا أم دولاً، اختراق المواقع الإلكترونية الحساسة والقيام بتغيير معلوماتها أو إتلافها، ما لم تنجح إجراءات الحيطة والتحصين من ردّ هذا النوع من الهجمات وإفشاله. وللتسلل إلى داخل معلومات الطرف الآخر أساليب وطرق شتى، ربما من خلال اعتماد الخداع خداع البرنامج الإلكتروني أو باستغلال ضَعْف برامج الحماية المُعتمدة، أو بفضل اكتشاف نقاط ضعف فيها، ما يُسهل على المهاجم اختراقها. وثمة بالمقابل برامج وأساليب ينبغي أن تؤدّي إلى معرفة هوية المتسلل أو المعتدي والتأكد من اعتدائه، وبالتالي تَعقبه تعقبه. وحتى هذه البرامج والأساليب الهادفة إلى تحقيق الأمان للمعلومات المخزنة لها بالمقابل، برامج وأساليب أخرى لتعطيلها. وهذا ما يُفسّر استمرارية الحراك والتطوير والتحديث والتغيير ضمن العالم السيبراني الناشط على مدار اللحظة.

ص: 33

الفصل الثالث: لماذا التخزين في الفضاء السيبرانيّ؟

ص: 35

الفصل الثالث: لماذا التخزين في الفضاء السيبراني؟

اشارة

ردًا على التساؤل الساذج من نوع: لماذا (أو هل) ينبغي تخزين معلومات الشركات والدول والأمم ضمن الفضاء الإلكتروني؟ يأتي الجواب تلقائيا بأنّ العصر بات عصر الآلة الذكية التي يجتهد الإنسان في تسخيرها لصالحه ولحسن سير أعماله. وبدلاً من طريقة القلم والورقة والأنشطة الكتابية التي لا بدء لها ولا انتهاء والتي-أيضًا - لا مجال لعدم ارتكاب الأغلاط والأخطاء في سياقاتها المضنية، ناهيك عن الأوقات الطويلة التي يحتاجها هذا النوع (البدائي) من العمل، يضطر إنسان العصر للاتكال على أداء الآلة التي يُبرمجها لتقوم بالعمل خلال وقت استثنائي في قصره، مع إمكانيات حقيقية لتنفيذ هذا العمل من دون ارتكاب الأخطاء التي لا يمكن تجنّبها لدى اعتماد الطاقة البشريّة حسب أسلوب القلم والورقة سابق الذكر ذلك مع ملاحظة أنّ اعتماد الآلة الذكية وعلوم البرمجة وتكنولوجيا المعلومات وكلها من بنات الفضاء السيبراني) بات ضرورة حيوية مُلحة في سبيل تنفيذ الأعمال بالسرعة والكمّيّة والدفق، ممّا تتطلّبه مصلحة المجموعة البشرية الدولة) ومواطنوها أو الشركة وأسواقها). وبحكم الاعتماد الذي لا بد منه على الفضاء الإلكتروني كمُضيف للمعلومات، واعتماد كلّ طرف أو جهة أفضل وأقوى وأحدث ما يسعه من وسائل وتقنيّات لحماية ملفاته وتيسير أعماله وأنشطته كافّة، يصبح هذا الفضاء أشبه بمعسكرات معلوماتية محصنة بعضها حيال بعض. والمقدرة على اقتحام الفضاء السيبراني وولوج المعلومات المخزنة فيه لدولة ما، يمنح المقتحم سلطانًا

يسيطر بواسطته على هذه الدولة وهنا يأتي دور الأمن السيبراني بما يعتوره من مشاكل ومعضلات وكيفيات وإمكانيات، وتدخل الحرب السيبرانية من جميع الأبواب، حيث يحاول القادرون تكنولوجيا إخضاع الطرف الذي يرون مصلحتهم في إخضاعه، أو ربما في قهره وتحطيمه وذلك من خلال العبث بجدائل المعلومات العائدة له وتحويلها ضدّ ،مصلحته من خلال العمل على اقتحامها للسيطرة عليها والتصرف بها. وهذا الاقتحام يكون في غالب الحالات صعبًا وعلى حافة الاستحالة أو هكذا ينبغي له أن يكون، وهو ليس كذلك... مع الأسف).

ومن جهة أخرى فإنّ الفعّاليّات السيبرانية تتجاوز مجرد كون الفضاء السيبراني أداة تكنولوجية ومهنية، أو مخزناً هائلاً للمعلومات والعمليّات التبادلية السريعة وتطوّراتها المتلاحقة، لتغدو حقول فعاليات متعدّدة جغرافيا وديموغرافيا، واقتصاديا وماليا، وشعبياً واجتماعيا، وسلوكياً وصحياً وثقافيًا ونفسيا، وسياسيا وعلميا، وأمنيًا وعسكرياً، وداخليا وخارجيا، وعلى المستويات الرأسية والأفقية والاستراتيجيّة والتكتيكيّة، والسرّية والبينيّة، والتحتية والفوقية كافّة ومن دون استثناء. وهذا يتطلب برامج فائقة التطوّر وإمكانات تكنولوجيّة استثنائية تتيح للقوى الطموحة بناء سيادتها السيبرانية أوّلاً داخل حدودها عبر السيطرة غير المنقوصة على الإنترنت في الداخل. ويتضمّن ذلك النشاطات السياسية والاقتصادية والثقافية والتقنية وسواها. ويلي ذلك التوجه إلى التوسع بالعمل في ميادين السيطرة على المنافسين والأخصام والأعداء، والحلفاء

كـذلك، والاطلاع ما أمكن على طبيعة وميادين أنشـطتهم في الفضاء الإلكتروني، والسـعي إلى تحقيق التحكم بما ينبغي عليهم التحكم به مـن هـذه الأنشـطة، لوضـعها في خدمـة أهـدافهم ومصـالحهم اسـتطاعوا إلى ذلـك سبيلاً. وهـذا يشـكل جزءا أساسـيًا مـن «الحروب السيبرانيّة»(1). مع ضـرورة الإشارة هنا إلى أنّ الحروب التقليديـة بحـدّ ذاتها، باتت هي الأخرى، ترتهن في خوضـها للفضاء السـيبيري بما يحتويه من معلومات يمكن لأي طرف إذا اقتحمها وسيطر عليها، أن يدفع الطرف المعادي إلى الاستسلام له.

ولا بدّ من الإضاءة على حقيقة لا يبدو أنها في صالح الجنس البشـري على العموم، وهي باختصار تقدّم الآلة (المعزّزة بالذكاء الاصـطناعي بحيث تتخذ القرارات الكبيرة عن الإنسان، ودائما بطلب منه. فعندما يضطر مدير قسم في شركة، أو قائد عسكري في جيش ما، إلى اتخاذ قرار كبير ومهمّ يُلزمه بدايةً بخوض حسابات دقيقة وطويلة ومعقدة واسـتخلاص النتيجة بشـكل نظري من كلّ ذلك، قبل أن يوجه الأمر بالتنفيذ، فإنّه ، واختصارًا للجهـد والوقت، وتلافيًا للخطإ، يترك للآلـة أن تقوم بالعمل. ومن شأن هـذه الاتكاليـة» أن تُفسح للآلة مقعدًا على كرسـي «تحضير القرار على الأقل. المسافة من هذا الموقع إلى موقع «اتخاذ القرار ليست بعيدة جدًّا، وقد اجتازتها المخيّلات الهوليوودية مئات بل آلاف المرات لتقـدّم لهواة النوع أفلاما من نوع الخُرافـة العلمية، وجدت وتجد نجاحات تجارية كبيرة، بحيث تركت منفذا لخروج تساؤلات تنطلق بداية على

1- https://www.tech-wd.com.

سبيل الدعابة، وتتسلّل بهدوء إلى طاولات الأبحاث العلمية الجادة والرصينة : وماذا لو حصل ذلك فعلاً وتحققت – على سبيل المثال – توقعات الروائي والمسرحيّ التشيكوسلوفاكي «كارل تشابيك» الذي كان أوّل من أدخل لفظة روبوت» بمعنى الرجل الآلي، في العصرية. وفي مسرحيّته (إنسان روسوم الآلي – 1938 ، انتقد التقدم العلمي والنفاق الاجتماعي بمرارة وصوّر الحال عندما تسيطر الآلات (الروبوت) على البشر.

إنّه لمن الممكن والصائب إنجاز أي مشروع بواسطة معالجات كمبيوترية ضخمة تساعد في تحديد الطريقة الأمثل والأكثر إنسانية لإدارة الشؤون البشرية والبيئية. هذه بالحقيقة ستكون وظيفة للآلة على غرار الوظائف الحكومية، مع فارق أنّ الآلة لن تنال راتبًا فلكيّا) ولا نِسَبًا من الأرباح، ولن تعقد صفقات من أجل تحقيق منافع شخصيّة. كذلك فإنّه بتوفير كومبيوترات قادرة على معالجة تريليونات المعلومات في الثانية، فإنّ التكنولوجيا الحالية تتجاوز القدرات البشرية للتعامل مع المعلومات، وسيكون بالإمكان عبرها التوصل إلى قرارات منصفة ومستدامة حول تنمية وتوزيع الموارد المادّيّة. وبهذا سيكون المجتمع البشري المعني قد طوّر أساليبه إلى مرحلة ما بعد السياسة والسياسيين الذين هم مصدر الشكوى على امتداد التاريخ، وخرج بالتالي من مرحلة القرارات السياسية التي تتخذ عبر السلطة ونخبة من أصحاب الامتيازات الذين لا يتصفون عادة بالكفاءة الكافية.

ولو افترضنا تحقيق هذا والتزام الإنسان بالمصلحة البشرية

خارج جاذبيّات الأنانيات والمصالـح الذاتيـة، وتوفير برامج ذكية جديرة بأن تكفّ يد التخريب والجشع وتحمي الحقوق من وحشـيّة الطمع والعـدوان، فهـذا سـيجعل من التقدم التكنولوجي سبيلاً لمنهج أكثر إنسانية ومنطقية لتشـكيل معالـم الحضارة الجديدة التي لا تعتمد على الآراء والرغبات الشخصية لفريق من الناس.

فالقرارات الكبيرة والأساسيّة على الأقلّ) ستتخذ عن طريق القيام بمسح شامل للموارد والطاقة وما يتوافر من تقنيّات ،وإمكانات، وما يحتمله اتخاذها نتائـج جانبية أو خسائر لا تكون ظاهرة منذ البداية. والآلة المعزّزة بما ينبغي من التقنيات والقدرات والضوابط سوف تحول دون منح امتيازات في غير محلّها لأي مسؤول أو مجموعة من الناس للقيام بالأمر.

أصـبح للفضـاء الإـلكتروني دور في صـناعة وتشـكيل الرأي العام، ليس فقط على المسـتوى المحلي بل العالمي، وساعـد على ذلك زيادة الارتباط العالمي بتكنولوجيا الاتصال والمعلومات.

ص: 40

1. مناخ عالميّ جديد

يرتفع عـدد مُسـتخدمي الإنترنت اليوم إلى 4 مليار مُستخدم(1). والرقم في تصاعـد، ولا يقلّ عـدد حاملي الهواتف الذكيـة عن هذا الرقم أيضًا. هذا الوضع العالمي» أوجد فرصا جديدة للتواصل وتبادل المعارف لم تكن متاحة من قبل على الإطلاق. منذ عشـرين سـنة فقط كان الاتصال هاتفيًا من بيروت إلى بغـداد مثلاً، من الأعمال الباهرة والمكلفـة أيضًا. اليوم، يمكنك التواصل وفتح حديث ثلاثي أو أكثر حسـب الرغبة) مع صديق يتسلق الهيمالايا نحو قمة آفرست، وآخر توقظه بعد منتصف الليل في مدراس بالهند، وثالث تاناناريف عاصمة مدغشقر، وبتكلفة رمزيّة لا تكاد تُذكر هذا ليس خُرافة ولا مُعجزة، بل هو أحد عطاءات هذا العصـر السيبراني. هذا الوضع أدّى إلى – بل ساهم في – ولادة مجتمع عالمي جديـد يتبادل التحيّات والمعارف ويتواصل أفراده بعضـهم مع بعض بكلّ يسـر وسـهولة؛ فقـد كسـرت الإنترنت فكرة المسافات والحـدود، ورفعت الحواجز والعوائق بحيث بات التواصل مع أبعد إنسان عنك على الكرة أو في أجوائها، مثل الاتصال بجارك في المبنى المجـاور. صار الخبر أي خبر ينتقل إليك بسـرعة الوميض الضوئي، وباتت صُوَر وفيـديوهات الحوادث الهائلـة (مثل حـدث 9/11 وقتل الألوف بتدمير (البرجين تمنحك فرصة متابعتها بالصورة والصوت وبلحظة حصولها تماماً.

وهكذا ظهر الإعلام الجديد، وبالتالي ما يمكن تسميته ب–

1– https://www.maghress.com/khbarbladi/2700.

المجتمع المعلوماتي العالمي(1)، وراجت عمليات إنتاج المعلومات ونشرها بين قطاع عريض من الجمهور، وبما يفتح المجال للتأثير على أولويات القضايا لدى الرأي العام. وتميزت عمليّات التواصل الإعلامية والمعلوماتية والاجتماعية والتجارية وسواها بالكثير من السهولة والانتشار وقلة التكلفة، سواء أكان ذلك بالاتصال المباشر (هاتفيًا أو عبر البريد الإلكتروني...) أو في شكل إنشاء مواقع على الإنترنت أو تبادل رسائل نصية قصيرة أو مدوّنات أو المشاركة في غرف الدردشة أو المجموعات البريدية أو استطلاعات الرأي أو التعليقات الإلكترونية على الأخبار أو الأحداث أو عن طريق نشر المقالات عبر الفضاء الإلكتروني أو ما يتعلّق بالتطوّر في تقنية استطلاعات الرأي العام . عبر الاستشمارات الإلكترونية أو الاستطلاع أو الاستطلاع عبر المواقع.

2. مجتمع المعلومات

لقد أدّت تكنولوجيا المعلومات وتيسير التواصل على المدى الأوسع، إلى تنامي ودفع ظاهرة العولمة التي تقوم على التواصل والترابط بين دول العالم، وكانت وسائل الاتصال السيبرانية أهمّ الأدوات التكنولوجيّة المعتمد عليها لتفجير هذه الثورة التعارفية على المدى العالمي الشامل. ولقد أدّت هذه الثورة إلى تحويل العالم بطابعه المادّيّ "Real World" إلى عالم رقمي وافتراضي "Virtual"، حيث انتقلت مجالات الحياة كافّة لتأخذ طابعًا رقميًا

1- https://scis.gov.iq/upload/upfile/ar/security.doc.

يـدور في فلـك الفضـاء الإـلكتروني، وظهر مجتمع المعرفـة المبني على ثورة المعلومـات والمعرفـة وشـهد العالـم اتجاها لانتشار الموجة الديمقراطية والتوجّه نحو اقتصاد السوق، كما كان لذلك من انعكاسات على القيم والمعتقدات والأفكار.

ولـم يُسـهـم انتشار تكنولوجيا الاتصالات الحديثة، مثل الإنترنت والإعلام العالمي، في تجاوز الحدود ومحاولات النظم الشـمولية السـيطرة على انسـياب المعلومات فحسب، وإنما أسـهـم كذلك في إرباك الثقافات السياسية التقليدية والقائمة على الطاعة العمياء للنظام الحاكم من قبل المواطنين في مقابل دور الإنترنت في تعزيز عملية تشكيل الشبكات الأفقية وتحرير الاتصالات ودعم ثقافة النقاش المفتوح. وهذا أدى إلى تجاوز الثقافات السياسـية التي تتسم بالتراتبية والسـلطوية، واتّسع بالتالي نطاق حرية التعبير بشكل غير مسبوق، مع ظهور أشكال متنوعة من الاتصالات تتجاوز الحدود القومية للدول ومفهوم السيادة بشكله التقليدي. كذلك فإنّ هذه الخطوات التكنولوجيّة الواسعة فرضت تغيرا وتبدُّلاً في الطرائق التي يعيش بها الناس في مختلف أنحاء العالم، وتغييرًا في أنماط السلوك عمومًا.

ص: 43

3. غرائب الفضاء الإلكتروني

مع التقارب في العلاقة بين العالم المادّيّ الواقعي والعالم الافتراضي راح تأثير قوة الكمبيوتر والشبكات يتزايد بسرعة كبيرة، ما جعل الناس يرون في الفضاء الإلكتروني عالماً موازيًا للواقع، على الرغم من كونه عبارة عن فيض رقمي من المعلومات لا يعتمد كلّيًا على البيئة المحسوبة التي توفّرها شبكات المعلومات، بل يتعامل مع مفرداته مثل سرعة تناقل البيانات وصلاحية الدخول إلى الشبكة، بالإضافة إلى المعالجات التي تتناول البيانات المتدفقة ضمن البيئة الإلكترونية.

والفضاء الإلكتروني، مثلما هو الفضاء التقليدي، يتألّف من أربعة مكوّنات رئيسيّة هي: المكان، والمسافة، والحجم،والمسار(1).

ويتميّز هذا الفضاء الإلكتروني بغياب الحدود الجغرافية والتحرّر من الحكم القاهر لعنصر الزمن إلا أنّ هذا العالم الافتراضي يتطلّب توافر هيكل مادّيّ لبنائه، وهذا ما تُشكله أجهزة الكمبيوتر ووسائط الاتصالات عبر الإنترنت. ومن ثم فإنّ ما يعمل داخل هذه الأجهزة يمثل نمطا من القوة والسيطرة، حيث تصبح القيمة الحقيقية للفضاء الإلكتروني هي القدرة على الاستفادة من كمّ المعلومات الموجودة داخله، والمساهمة والتحكم بها.

ولابدّ من الأخذ بعين الاعتبار أن الفضاء الإلكتروني هوعبارة عن تلك البيئة الافتراضية التي تعمل بها المعلومات

1- https://arabic.rt.com.

الإلكترونيـة والتي تتصـل عن طريق شـبكات الكمبيوتر ، كمـا يُعرف بـأنّه ذلـك المجـال الـذي يتميّز باسـتخدام الإلكترونيـات والمجـال الكهرومغناطيسي لتخزين البيانات وتعديلها أو تغييرها عن طريق النظم المتصلة والمرتبطة بالبنية التحتية الطبيعية.

كذلك يُشـير الفضاء الإلكتروني إلى مجموعة المعلومات المتوافرة إلكترونيًا فيه والتي يتم تبادلها وتشكيلها. وهو يعمل تحت ظروف مادّيّة غير تقليديـة، حيث يكون وسـيطاً عبر العمل من خلال أجهزة الكمبيوتر وشـبكات الاتصال ويختلف الفضاء الإلكتروني أو السـيبراني عن الفضاء الخارجي في أنّ الأوّل يعمل وفق قوانين فيزيائية مختلفة عن قوانين الفضاء الخارجي؛ فالمعلومات في الفضاء السيبراني مثلاً لا تزن شيئًا ولا تمتلك كُتلة مادّيّة وبإمكانها أن تظهر للوجود وأن تختفي حسب الرغبة، ويتم تعديلها وتبادلها من خلال نظم مُرتبطة بالبنية التحتية ويتعامل الفضاء الإلكتروني مع المعلومات والتي تتوقف فائـدتها إما من خلال تفاعلها مع غيرها من المعلومات أو بإنتاج معلومات جديدة أو أخرى متوارثـة تتفاعل داخل هـذا الفضاء وخارجه. ويشـهد الفضاء السـيبراني تـدفّقاً هائلاً وغير محدود للمعلومات، يختلط فيها ما هو صحيح بما هو غير ذلك، فيمكن الوقوع على الغثّ كما على السـمين، وعلى المعلومة الصـحيحة كما على المعلومة المضلّلة. ويبقى على المرء نفسه أن يُحسن اختيار ما يلائمه وأن يكون جديرا بالتمييز بين أنواع المعلومات الصحيحة والخاطئة .

ويحتوي الفضاء الإلكتروني على المعلومات الاستراتيجية

ص: 45

بالنسبة إلى الدول والشركات وهي تكون متوافرة لمن يُسمح له بمعرفتها فقط. والسماح هنا أو عدمه يكونان من خلال إجراءات إلكترونية، مثل جعل المعلومة تحت كلمة سرّ معيّنة ينبغي أن يكون اكتشافها مستحيلاً لضمان بقاء هذه المعلومة بتصرف أصحابها، ولا يستطيع بلوغها أي طرف آخر.

وبالإمكان تخزين هذه المعلومات داخل الفضاء الإلكتروني مهما كانت صغيرة أو كبيرة، من دون أن يكون لحجمها تأثير على تخزينها، وكذلك من دون دفع أي تكلفة. كذلك يكون بالإمكان استعادتها وتعديلها وإنقاصها وزيادتها كما يرغب صاحبها، ودائمًا من دون أي تكلفة مادّيّة. كذلك بإمكان صاحب المعلومات أن يجعلها مُباحة للعامّة، وه- حال العديد من الصحف والكتب وأنواع المعارف التي تتوافر على الشبكة، ويمكن لأي كان ولوجها والاستفادة منها. كذلك بالطبع يمكن لصاحب هذه المعلومات حجبها عن العامّة كما سبقت الإشارة. وفي حالات معينة يبذل «البعض» جهودًا كبيرة لاقتحام خصوصية معلومات تكون متوافرة فى الفضاء الإلكتروني تحت مظلة حماية لها كلمة مرور -password)، وهذا ما هو ممنوع قانونيا، فضلا عن صعوبته، باعتبار أنّ أصحاب المعلومات المهمّة أو الخطيرة التي تتصل بأمن الدول مثلاً أو باقتصادها أو بعمليّات الشركات الاستثمارية على أنواعها، يعمدون بالطبع إلى حماية معلوماتهم بحيث يتعسّر اقتحامها. وهنا يبتدئ فصل القرصنة (قرصنة المعلومات)

والقراصنة الإلكترونيّين والتجسّس الإلكتروني، مما سيجري تفصيله في فصل خاص.

يُعـد الفضاء الإلكتروني مجالاً عامًا وسوقاً مفتوحة، ويُدلل على وجود شـبكة من التواصل والعلاقات بين من يسـتخدمونه ويتفاعلون انتقال مختلف مجالات الحياة من حكوميـة معًا من خلاله، مع وخاصـة، وكلّ ما يتصل بشؤون العمل والإنتاج والاسـتهلاك والصـحة والسياسـة والدفاع والأمن والمعرفة ... كلّه بات يقوم معلوماتيًا ضمن الفضاء السيبراني الذي بات وسيطا ووسيلة في الوقت ذاته؛ وسيلة لتسيير الشؤون، ووسيطا في تنفيذ الأعمال، مثل تنفيذ صفقة أو شنّ هجوم، ما جعله وسيطا جديدًا للتعاملات والتفاعلات وللصراع والمواجهة.

ص: 47

الفصل الرابع:ممّ يتكوّن الفضاء السيبرانيّ؟

ص: 49

الفصل الرابع:ممّ يتكوّن الفضاء السيبراني؟

اشارة

يتكوّن أثاث» الفضاء الإلكتروني من المكوّن الأوّل الطبيعي أو المادّيّ والـذي يتمثل في الأسـلاك والمحولات والبنية التحتية المعلوماتية، كالكابلاـت والمكوّن الثـاني يتمثل في المحتوى المعلوماتي المخزون فيه. أمّا المكوّن الثالث فيتمثل في عمليّـة التوصـيل بين المعلومات والبشر ويرتبط بتصوّرات الناس وثقافاتهم.

ولاـ يتكوّن الفضاء الإلكتروني فقط من شـبكة من الاتصالات، بل يتكوّن كـذلك من المعلومات التي تنتقل من خلال هـذه الشـبكة أيضًا. وأهم ما يميّز مجتمع المعلومات هـذا هو أنّ المعلومات المتوافرة لها قيمـة اقتصاديـة وقيمة ميدانية بالنسـبة إلى الجهات العسـكريّة، وكلّما زادت الفاعليـة في إدارة تلك المعلومات كلّما زادت الفائـدة التي يمكن الحصول عليها، وأصـبح تفوّق المعلومات إحـدى القيم الأساسـية للقوة العسكرية، وأصبحت المعلومات مجالاً للسيطرة والتحكّم .

المعلومات الاسـتخباراتية باتت جزءًا كبيراً من المعارك السياسية الدائرة في العالم اليوم. لقد أصبحت الغَلَبة للمعلومات، والأسلحة الأكثر فعّاليّـة باتت تتمثل بالوثائق «السـرّية للغاية التي يجري تسـريبها بعد أن أثبتت مرارًا جدواها في إحداث الأزمات الدولية وتغيير السـياسات الخارجية وإحراج أصحاب النفوذ.

تخبرنا التسريبات أنّ الولايات المتحدة الأميركية أنفقت المليارات في سبيل التجسس على... حلفائها الغربيين(1). وأنّ

1- archive.aawsat.com/details.asp?section=4article=601367.

واشـنطن التي ابتكرت أخطر الفيروسات لتدمير المشروع النووي الإيراني ستوكس (نت واستخدمته في العام 2006 بالاشتراك مع إسرائيل، انتهت إلى الفشل، وأنّ هيلاري كلينتون كانت تنقصها النزاهة طيلة خوضها المناظرات الانتخابية الرئاسية الأخيرة، حيث كانت تتلقى مُسبقًا الأسـئلة التي سوف تُطرح عليها أمام الكاميرا، وأنّ الرئيس الروسـي الـذي كان ضابط اسـتخبارات خـدم في ألمانيا الشـرقية خلال المرحلة السوفياتية، يحتفظ بدلائل لا تدحض على فضائح جنسية خاصة بترامب.

1. التسريبات الاستخبارية

...إنّهـا أفيون شـعوب العـالـم وحكوماته في هـذا العصـر. والفضل الأساسـي في ذلك يعود إلى الحشـرية والفضول البشـريين أولاً ثمّ إلى منشورات موقع ويكيليكس» الذي أسّسه الصحافي الأميركي جوليان أسانج – 46 عامًا – بعد فراره من بلده، واستخدمه لنشر الوثائق السرية الأميركيـة التي يُعتبر عـدم نشـرها إهانـة لشـعب الولايـات المتحـدة حسب اعتقـاده، وذلـك في إطـار جهوده لمكافحـة الفساد الحكومي والمؤسساتي، مُستفيدًا من المادة 19 من الإعلان العالمي لحقوق الإنسان، والتي تنص على أنّ لكلّ شـخص الحق في حرية استقاء الأنباء والأفكار وتلقيها وإذاعتها بأي وسيلة كانت، دون تقيّد بالحدود الجغرافية.

لا شكّ أنّ وثائق ويكيليكس» غيرت العالم بشكل كبير(1).

1- https://www.sasapost.com/battles-of-leaks-mt.

فالتسريبات الاستخباراتية التي راج سوقها بشكل جنوني كانت سلاحًا مؤثرًا في ما سُمِّيَ «الربيع العربي» في العام 2011. ولو أخذنا الحالة التونسيّة مثلاً على اعتبار خصوصية وتأثير ما شهدته تونس في تلك الآونة، فالحقيقة التي لا بد من الإضاءة عليها هي أنّ التأثير الكبير والخاص في «الثورة التونسية» لم يكن لبائع الخضار والفاكهة وحده الذي أضرم النار في جسده اعتراضًا على ظلم الدولة للفقراء، بل إنّ دورًا رئيسًا في إشعال الاحتجاجات يعود إلى ما نقلته السفارة الأميركيّة هناك في تقاريرها المسرّبة العام 2008 عن فساد الرئيس السابق بن عليّ وأسرته.

ولقد شكّل ذلك أيضًا وسيلة ضغط على المجتمع الدولي كي لا يتدخل لمعارضة الاحتجاجات التي لم تلبث أن وصلت إلى سوريا. لقد سبق ل«أسانج» أن تحدّث عن ذلك مُعربًا عن اعتقاده أنّ موقعه الإلكتروني ساهم في تأجيج الغضب في الشوارع لكن هذه لم تكن أقوى ضرباته.

ففي العام 2010 نشر « أسانج» على موقعه حوالي 400 ألف وثيقة تتعلّق بحرب العراق، ما اعتُبر أكبر عملية تسريب التاريخ العسكري الأميركي. وكشفت المعلومات التي أعلنتها الوثائق المنشورة أنّ القوات الأميركيّة قتلت أكثر من 400 ألف نسمة معظمهم من المدنيين. كذلك أظهر فيديو مُسرّب أنّ مروحيتين أميركيتين من طراز «أباتشي» أطلقتا الرصاص الغزير على مجموعة من المدنيين كان من بينهم اثنان من صحافيي وكالة «رويترز» الأميركيّة. وعلى الرغم من أن اللقطات أظهرت بوضوح أنّ هناك صحافيين ضمن المجموعة يحملون

«كاميرات كبيرة بوضوح، إلا أنّ ذلك لم يمنع المروحيتين من الاستمرار في إطلاق النار.

وفي ما نشره ويكيليكس من يوميات الحرب الأفغانية، ظهرت وثيقة بالغة الأهمية حول الحرب التي تشنها الولايات المتحدة في تلك البلاد تضمّنت تسريبات تجاوزت 90 ألف وثيقة(1)، تكشف عن مقتل أكثر من 30 ألف مدني جرّاء الحرب الأميركية هناك، كما أظهرت أنّ القوات الأميركية كانت تطلق النيران العشوائية،

بينما كانت الغارات الجوّية قد قصفت البيوت مراراً دون تحديد. ورأى البعض أنّ تلك التسريبات العسكرية ستجعل الولايات المتحدة عاجزة عن التورط باحتلال دولة مرة أخرى. وهذا ما حدث بالفعل عندما رفضت إدارة أوباما في عام 2012 إرسال قوات برية إلى العراق لمحاربة تنظيم الدولة الإسلاميّة – داعش»، ثم عادت ونكصت على أعقابها من دون أن تضرب سوريا، بعد أن كانت قد هيأت العالم لتلك الضربة ... التي لم تحصل.

وعاد (ويكيليكس بقوّة إلى النشاط بعد أزمة اقتصادية أصابته، فعمل على تسريب 500 ألف وثيقة سرّيّة لوزارة الخارجية السعودية، ساهمت في إحراج المملكة مع دول الجوار، حيث كشفت عن دور المال السياسي في التأثير على عدد من وسائل الإعلام الإقليمية، ومنع نشر تقارير إعلامية لا تروق لسياساتها، بما في ذلك جهود المواجهة وسائل الإعلام غير الصديقة وعرقلة بنها عبر الأقمار الصناعية.

1- https://www.alghadpress.com/news/100812/Alghadpress.

ومهما قيل في شأن «أسانج» وموقعه «ويكيليكس»، فقد كشف النقاب عن وجه شديد البشاعة والقبح للسياسة الأميركية الخارجية، وساهم في توضيح الصورة الحقيقية لمواقف الأنظمة العربية القائمة، والتي لم تكن في صالح تلك الأنظمة على الإطلاق.

وبعد وثائق مستر أسانج» جاءت تسريبات وثائق «بنما» لتواصل المهمّة ،إيّاها ، كاشفة عن مقدار هائل من الثروات في حسابات بعض الزعماء العرب، إضافة إلى فضحها عمليّات فساد هائلة طالت دولاً عربيّة، من بينها السعودية والإمارات وقطر.

تعتبر وثائق «بنما» أكبر تسريبات صحافية في التاريخ قام بها مصدر مجهول لم يُكشف عنه حتى الآن. فقد اشتملت عمليّة التسريب على 11.5 وثيقة خاصة بشركة موساك فونسيكا للخدمات القانونية في بنما، طالت 72 من القادة والشخصيات العامة حول العالم، وهي شركة تمتلك منظمة مصرفية تقوم على إدارة المليارات بصورة يصعب تعقبها، ولا يمكن تحديد المستفيد النهائي منها، وذلك عن طريق تحويل الأصول إلى شركات وهميّة بأسماء غير أسماء مُلاكها الحقيقيين.

ومن ضمن الأسماء العربية التي كشفتها التسريبات يُذكر ملك السعودية سلمان بن عبد العزيز، ملك المغرب محمد السادس، رئيس دولة الإمارات الأمير خليفة بن زايد آل نهيان، أمير قطر السابق حمد بن خليفة آل ثاني، الرئيس المصري الأسبق حسني مبارك وبعض أفراد عائلته، رئيس الوزراء العراقي السابق إياد علاوي، إضافة إلى رئيس وزراء الأردن السابق علي أبو الراغب، وغيرهم كُثُر.

ص: 54

وبعـد ويكيليكس» و وثائق بنما لمع نجم الفضـيحة التي سـربها إدوارد سـنودن بشأن تجسّـس السـي آي إي»، والتي طالت عددًا أكبر من ضحايا وثائق «بنما».

فقد أعلن "إدوارد سنودن" وهو موظف سابق في وكالة الاستخبارات الأميركية آي إي"، خلال حديث مع مجلّة .آي.إي Spiegel الألمانية، أنّ مسؤوليّة مهاجمة كمبيوترات الحزب الديمقراطي الأميركي تقع على عاتق عدة مجموعات.

وأضـاف ردًّا على سؤال عن مسؤوليـة الروس المحتملـة: "لا ـ أعرف من المحتمـل طبعًا أن يكون الروس من هاجموا منظومـة الكمبيوترات لحزب هيلاري كلينتون الـديمقراطي، ولكنّ هـذا الأمر لـم يثبت (...) لا شكّ في أنّ وكالة الأمن القومي في الولايات المتحدة، تعرف بدقة من وقف خلف تلك الهجمات التي اسـتهدفت السيّدة كلينتون؛ ولكنّني أعتقد بأنّ هذه المؤسسة تمكنت من كشف مهاجمين آخرين ربما ست أو سـبع مجموعات عملت هناك. تجدر الإشارة إلى أنّ الكونغرس الأميركي يشـهد تحقيقات مسـتقلة حول تدخل روسـي مزعوم في الانتخابات الرئاسية الأميركية التي فاز بنتيجتها دونالد ترامب كما يقوم مكتب التحقيقات الفدرالي "إف.بي.آي" بإجراء تحقيق مماثل.

وعلى صـعيد مواز ذكرت وكالـة «نوفوستي» الروسـيّة للأنبـاء أنّ وكالـة الأـمن القومي الأميركيـة قامت بالتنصت على أكثر من 150 مليون مكالمة هاتفية داخل الولايات المتحدة خلا العام 2016، على الرغم من القيود

التي كان الكونغرس أعلن وضعها على هذا النوع من النشاطات.

وذكر تقرير صادر عن مكتب مدير أجهزة الاستخبارات الأميركية نفسه أنّه في العام 2016 تمّ جمع معلومات عن 151 مليون مكالمة هاتفية وذلك بتصريح من المحكمة السرّيّة الخاصّة بشؤون مراقبة الأجانب ((FISA) في الولايات المتحدة.

ومع ذلك، لم تعثر وكالة الأمن القومي الأميركية في مجال رصدها طيلة تلك الفترة، على أكثر من 42 مشتبها بهم في الإرهاب من بينهم مواطن أمريكي واحد فقط، كُشف نتيجة مراقبة لا علاقة لها بأهداف استخباراتية، بحسب التقرير الذي لم يحدّد عدد المواطنين الأميركيين الذين وقعوا في شباك التنصت بالعلاقة مع نشاط استخباراتي فعلي.

وجمعت وكالة الأمن القومي الأمريكية على نطاق واسع معلومات وصفية عن توقيت المكالمات الهاتفية وعناوينها ومدتها بعد هجمات 11 سبتمبر 2001.

وكان عميل الاستخبارات الأميركية السابق إدوارد سنودن كشف في العام 2013 النقاب عن وجود برنامج رسمي أميركي واسع النطاق للتنصت، ما دفع الكونغرس يومها إلى تبني قانون جديد يقيّد قدرة وكالة الأمن القومي في القيام بعمليات بحث في قواعد البيانات الوصفية المرتبطة بالمواطنين الأميركيين.

ص: 56

ص: 57

الفصل الخامس:المجال العام والتحوّل من المجتمع الواقعي إلى الإلكتروني

اشارة

تقوم نظريـة المجال العام من عمليـة تشـكيل الرأي العام والمؤشـرات الاجتماعيـة والثقافيـة التي تساعـد على تطوير هذا الرأي العام الذي يتوسّط مجالات السلطة العامة والحكومة والمجال الخاص المتصل بالأسرة والأفراد.

أحد أبرز آباء نظرية المجال العام هو الفيلسوف وعالم الاجتماع الألماني المعاصـر يورغن هابرماس (Habermas)(1)، وقد عرف المجال العـام بـأنّه مجتمع افتراضـي أو خيالي ليس من الضـروري يتواجـد في مكان معروف أو مُميّز، ويتكوّن من مجموعـة من الأفراد الـذين لهم سمات مُشتركة مجتمعين مع بعضهم كجمهور، يتفاعلون معًا على قدم من المساواة حول قضايا مشتركة.

يعتمـد المجـال العـام برأي هابرمـاس» على حريـة الـدخول والتحوّل إلى الطـابع العـالميّ كلّمـا أمكن، ودرجـات التحرر التي يتمتع بها المواطنون، ورفض الهرمية الاجتماعية، بحيث يُتاح لأيّ فرد المشاركة على قدم المساواة.

ولا يفترض وجود معرفة مُسبقة بالضرورة بين المشاركين في المجال العام،بل يكفي وجود نوع من إدراك وفهم متقاربين لقضيّة ما والتباحث بشأنها،أو الاهتمام بأحداث معيّنة أو التعبير عن وجهة نظر تجاه المجتمع أو العالم في الفضاء العام يمكن لأي شخص أن يُشارك بآرائه أو

1- Midan.aljazeera.n.

مُساهمـاته، بفضل وسائل الإعلام الجديـد التي تتيـح الخروج من النطاق الخاص إلى المجال العام الأوسع والأكثر اسـتقطابًا للعديـد من الأفراد. ومع هـذا الانتقال يتم التحوّل من قضايا فرديـة إلى أخرى ذات طبيعـة عامـة، وكذلك الانتقال من ردود الأفعال المادّيّة التي تتمّ من خلال المظاهرات في الشارع أو الاعتصامات أو حتّى أعمال الشـغب، إلى فضاء جديـد لديه وسائل جديدة وآليات متنوعة يتمّ اسـتخدامها للتعبير والاحتجاج تجاه المجتمع أو الدولـة، وبـذلك يكون مجال تبادل الرأي قـد اتسع ليضُـمّ فاعلين آخرين لـديهم القدرة على التأثير في الرأي العام باسـتخدام تلك الوسائل الجديـدة التي تقوم على التواصل. وهـذا ما يُتيح الفرصة لتلاقح الأفكار وتوالدها في نطاق أوسع لتنتقل إلى مجال ومدى أرحب هو المجال العام. ومن هنا تكون إمكانية التأثير متاحة سواء في المجتمع عمومًا أو في صانعي القرار.

هكـذا يجري العمل على تضـييق فجوة المعرفـة بشـكل عام، وإنتاج المعلومات ونشـرها، مع إتاحـة حرّيّة الوصول إليها وقدرة أيّ فرد على إنتاجها. وهـذا ما يفتـح مجال تفاعل مُنتـج يقوم على ثلاثـة أضـلاع هي جمع المعلومات التعليق عليها والتحاور حولها ثمّ اتخاذ خطوات فعلية بشأنها.

من هنا يكون المجال العام هو تلك السـياقات التي يمكن لأيّ شـخص أن يُشارك فيها، من دون أن يكون المشاركون على معرفـة بعضـهم ببعض ؛ لكنّهم وعلى الرّغم من ذلك – يتشاركون فهما عاما –للعالـم المحيط المحيط بهم، ويُطوّرون هويّة مُشتركة، تطوّر بدورها اهتمامًا

جمعيًا بنصوص مُشتركـة، سواء أكانت هـذه النصوص تُعبّر عن رؤيـة كونيّة أو عن قضايا مُحدّدة أو عن أفعال وأحداث بعينها. وتسود في هذا المجال تفاعلات محكومة بمنظومة قيم ضابطة للأداء في نطاق هذا المجال الخاص، وليس من حق الآخرين خارج هذه السياقات الخاصة أن يُشاركوا في تفاعلاتها أو مناقشة قضاياها.

ويرى Habermas أنّ المجال العام يتشكل ويتكوّن من خلال إتاحة ساحات ومنتديات للنقاش في القضايا السياسية التي تعمل على إعادة تنظيم وبلورة الآراء المعروضة وترشـيحها وفق جدارتها، ووفق ما تحظى به من اهتمام عام من قبل المشاركين في النقاش. وهو يُقسّم النظام المجتمعي إلى ثلاثة أنظمة فرعية : النظام السياسي، الأنظمة الوظيفية كالتعليم والصحة والخدمات، والمجتمع المدني.

ويعمل المجال العامّ المتمتع بالاسـتقلالية، على ربط حالـة التفاعل بين هذه الأنظمة، ويكون جديرا بإدارة النقاش وترشـيح الآراء المقدّمة وتنقيتهـا وبلورتها لتكون في النهايـة أكثر من مجرد آراء مطروحـة، بل آراء لها أولويـة وتقـدير وتُعبر عن حالـة النقاش العامّ التي دارت من خلاله.

ومن هنـا يمكن اعتبار المجال العام مصـدرًا لتكوين الرأي العام؛ فهو يُبرز الآراء والاتجاهات من خلال السـلوكيات والحوار، ويعمل على محاولـة فهم حـدود الـدور الـذي تقوم به وسائل الإعلام الجديـدة (مُتمثّلة في المدوّنات والمنتديات ومجموعات النقاش في إتاحة النقاش العام وتسهيل بلورة توافقات تعبر عن هذا الرأي العامّ،

ص: 60

والسـعي إلى توجيه النقـاش السياسـي والاجتمـاعي في المجتمع، من أجل تعزيز المشاركـة العامـة، وتوثيق كفاءة الفعل الـديمقراطي في المجتمعات عبر بلورة رأي عام يحظى بأولويات تحظى باتفاق جماهيري وتمنح الشرعية للعمليّات السياسيّة المُختلفة.

ويعتمد نجاح المجال العامّ وفقًا لما حدّده Habermas على عوامل عدة منها: مدى الوصول والانتشار، ودرجة الحكم الذاتي، حيث يجب أن يكون المواطنون أحرارًا ويتخلّصوا من السـيطرة والهيمنـة ،والإجبار، ورفض التراتبية الاجتماعية، بحيث أنّ كلّ فرد يُشارك الآخرين على قدم المساواة، وأن يكون دور القانون واضحًا وفعّالاً، ووجود سياق مجتمعي ملائم.

1. بروز الفاعلين الجدد في المجال العامّ

في مجتمع المعلومات يمكن التمييز بين أنواع مختلفـة من المعرفة والتي تكون أوسع من مفهوم المعلومات، حيث تتكوّن من «معرفة ما – Know what » تُشـير إلى دخول على الحقائق السياسـية التي يمكن أن تتحوّل إلى معرفة رقميّة في شـكل معلومات وبيانات تصـبح موقفًا سياسـيًا يتم ترويجه أمام الرأي العام؛ ومعرفة أخرى مشابهة للأولى تُشـير إلى المهارة والقدرة على فعل شـيء ما عن طريق تدريب الكوادر السياسـية التي تتعامل مع المعلومات السياسـية وكيفيـة إدارتها و معرفة لماذا – Know why»، تشـير إلى المعرفة العلمية لمبادئ وأسس التنمية السياسية والتي تُشكّل الدفع للتنمية في الأحزاب السياسيّة أو المنظمات الوسيطة؛ ومعرفة من

هو – know who»، وتتعلّق بمن يستطيع أن يملك القدرة والمهارة السياسيّة لحشد الرأي العام، ولديه من الخبرات التنظيمية والسياسية والإعلامية ما يؤهله للتأثير بما يُساعد على عملية الحراك السياسي داخل النظام السياسي والنخبة السياسيّة.

عمليّة التدفّق الحرّ للمعلومات أدّت إلى إزالة الحواجز بين النظم السياسيّة بشكل أدّى إلى تحوّل الإنترنت إلى سوق عالمية للأفكار الديمقراطية، فضلاً عن أنّ الشبكة ذاتها أوجدت ثقافة نابعة من حرّيّة ونمط اللامركزية في الاختيار. كذلك جرى استخدام الإنترنت في الترويج للأجندة الدولية لحقوق الإنسان، وأثمر انفتاح المجتمعات المُنغلقة على ثقافات جديدة بشكل أدى إلى مزيد من الضغط على النظم السياسية القائمة لتلبية مطالب مواطنيها وكلّ ذلك بفضل ما أتاحته الإنترنت من حرّيّة الحوار والتعبير عن الرأي من خلال منتدياتها ومدوّناتها ومواقعها.

هكذا نجح فيلس يورغن هابرماس فيلسوف النقد والتواصل الألماني في التأسيس لأخلاق تواصلية تقوم على أساس الاعتراف بالآخر والتحاور معه من دون ادّعاء أي من الطرفين بامتلاك الحقيقة، داخل فضاء عمومي مشترك. فالأمر الأساس بالنسبة إليه كان العمل الدؤوب والنزيه على تقويم الحداثة من خلال خلق صيغ تواصل مع الآخر تستهدف إتاحة المجال العام لتداول ومناقشة حرّة تصل بالمجتمع إلى بناء إجماع حرّ بلا إكراهات أو ضغوط. وهذا ما عملت الشبكة العنكبوتية على تيسير حصوله بسلاسة وتلقائية، داخل هذا الفضاء العام المفتوح على رياح الأرض جميعًا. وبفضل

الإنترنت تسنّى ل-«هابرماس» دفع الرأي العام إلى انتقاد النتائج المدمّرة التي أفضت إلى العقلنة المفرطة لكلّ أشكال الحياة المعيشة من جهة، ونشر وتعميم أفكار تنويرية ووعود تحرّريّة كان من أبرز المنادين بها والمشجعين عليها.

2. ماذا فعلت السيبرانية؟

لقد نجحت العلوم السيبرانية في رفع الإنسان من عصر الآلة وبذله الجهد لتشغيلها، إلى زمن تشغيلها والتحكم بها عن بعد، وجعلها تراقب وتتابع وتحسب... من دون خطا أو تعب.

فالماء والتيار الكهربائي يتمّ توزيعهما إلى ملايين البيوت، والوزارات والإدارات والمصانع والمصالح والإنشاءات، والأسواق والمتاجر... بدقة، ومن خلال تنظيم متكامل تجري مراقبته بفضل الآلة المُبرمجة للقيام بالمهام المنوطة بها، من خلال برامج رقميّة معيّنة.

هكذا انتظمت حاجات الحياة اليومية من باب أوّل، وتلاءمت مختلف دوائر الأعمال والإنتاج والتوزيع والتصدير والاستيراد، بحيث يمكن للمنى بأي من هذه الشؤون أن يقف على دقائق حالتها من حيث الكم والكيف، في أي لحظة يشاء.

باتت الطائرات تتحرّك إقلاعاً وهبوطاً من وإلى المطارات، عبر خطوط وممرّات جوية مستقلّة أحدها عن الآخر بفضل نظام إلكتروني دقيق وممنهج يحقق الغاية والأمان والفعالية، من دون

أخطـاء... اللّهم مـا لـم تكن أخطـاء بشـريّة. وما يُقال عن الطائرات ينطبق أيضًا على القطارات وشتّى وسائل النقل المنظمـة والمعتمـدة في الميادين المدينيّة والريفية على السواء.

تواصـل النـاس بعضـهم ببعض عـبر المـدن والقرى وعـبر الـدول والمحيطـات والقـارات، حـتى بـات التواصـل من أبرز سـمات العصـر (facebook,watsap,twitter....) وبـدلاً من الرسالـة وسـاعي البريـد، بـات بوسع من يرغب أن يتصل بقريبه أو صـديقه أو زميله في أي مكـان في العـالم من خلالـ جهـاز لا يزيـد عن حجم شـطيرة حلوى. وهكـذا قام مجتمع عالمي واسع ومترامي الأطراف، وتقارب البشـر وتناقشوا في مختلف الشؤون والشجون والمصالح، من فوق رغبات الدول وسُلطاتها .

ساعـد الفضاء الإلكتروني في زيادة فرص وعـدد الفاعلين في تشـكيل الرأي العام وكسـر حواجز الخوف، بما أدّى إلى حالـة من الانفجار أو العشوائية من جانب، وأدّى من جانب آخر إلى إتاحة الفرصة أمام فئات جديدة كالمهمشين للتعبير عن مصالحها.

وأوجـد الفضاء الإلكتروني عـددًا من الأدوات والآليات الجديدة التي تتميز بعناصـر تنافسـية وجاذبة للجمهور، ووفّر أدوات جديدة للتعبير والاتصـال تتميّز بالسـهولة والانتشـار وتجاوز الحـدود المكانيـة والزمانيـة، ووفّر الفضاء الإلكتروني – كوسـيلة إعلام دوليـة الطابع الفرصـة لتحويل القضايا المحلّيّة إلى الطبيعة الدولية، بما ساعد على دمج المجتمع المحلي في السياسة العالمية مع كسر سيطرة

ص: 64

الإعلام الغربي على حركـة الإعلام الـدولي، وأتاح الفضاء الإلكتروني الفرصة لتداخل التأثير بين ما هو محلي وما هو دولي حيث التلاحم ما بين الجمهور وقادة الرأي بشكل يُتيح فرصة تشكيل التحالفات والتكتلات التي تقف خلف مصالح معيّنة.

ومثلت التجمعات الإلكترونيـة والحملات والمجموعات البريديّة والنشـطاء على المواقع الاجتماعية منصات للرأي والتأثير وجمع وجذب أكبر عدد من المستخدمين.

وضاعف الفضاء الإلكتروني من القنوات التي من خلالها يتم تدوير المعلومات والأفكار في نطاق موسع، واستطاعت هذه الوسائل في ذات الوقت أن تضعف من قدرة السُلطات على الرقابة والقمع والتأثير في الرأي العام.

وعمل الفضاء الإلكتروني كوسـيط أو كمؤسسة للرقابة على أداء السلطات التنفيذية، من خلال ما يتمّ في شكل مُعارضة أو احتجاج قد تأتي في صورة تعليقات إلكترونيّة أو مشاركة في اسـتطلاعات الرأي أو غرف الدردشة أو بتشـكيل تحالفات وحركات معارضة،وذلك مع التجاوز النسبي للقيود على حرية الرأي والتعبير.

وأتاح الفضاء الإلكتروني الفُرصة للتعبير عن المهمشين اقتصاديًا؛ كالفقراء أو دينيًا؛ كالأقباط والشيعة والبهائيين والقرآنيين وغيرهم، بما أدّى إلى ظهور هويـات كـانت سـرية من قبـل وظهرت إلى العلن لتُعبر عن نفسـها، ومنحتهم القـدرة على مخاطبـة الرأي العام وصوغ أهـدافه، والتلاحم مع مشاكله بدرجة أكبر وأسرع من

المؤسسات التقليديّة.

وكـان لاتّسـاع الفضـاء الإـلكتروني أمام الفاعلين كافـة وأمام جاذبيـة أدواته، دور في اسـتخدامه كأداة لبثّ الكراهيـة والعنف، وشن الحرب النفسية، ومحاولة التأثير على الاستقرار السياسي والاجتماعي والاقتصادي الداخلي، وقد تقف وراء هذه الأداة جهات خارجيّة أو مُعادية.

وأدّى ظهور الفضاء الإلكتروني واسـتخداماته إلى تغيير شـكل عمل النظام السياسي وطبيعته إذ لعب دور المؤسسات الوسيطة والتواصل ما بين عملية صنع القرار والرأي العام.

وحري بنا – نحن العرب – بمختلف أديانا وأوطاننا، أن نولي هـذا القطاع ما يسـتحقه من اهتمام، بل ما نسـتحقه نحن من إمكانات وقُدرات لكي تلبي حاجاتنا، وعلى طريق إشباع حاجات أجيالنا الجديدة.

السيبرانية هي التحدّي الذي يواجهنا والذي علينا التصدّي له واستيعابه وتدجينه ليخدمنا

الفصل السادس:سحر الإنترنت... هذا العالم الافتراضيّ الذي يحكم الجميع

ص: 67

الفصل السادس:سحر الإنترنت، هذا العالم الافتراضي الذي يحكم الجميع

اشارة

الإنترنت كناية عن شبكة تواصل عبر شبكة تواصل عبر الفضاء الإلكتروني الأجهزة الإلكترونية المؤهّلة من كومبيوترات وهواتف ذكيّة وأشباهها .

نشأت بداية في العام 1969 في الولايات المتحدة الأميركية وكانت مُعدّة للجيوش ومُكرّسة لخدمة وتلبية الأغراض العسكرية. وقد اعتمدت بديلاً عن أنماط التواصل الأخرى التي كانت معروفة خدمات البريد المخصصة للجيوش والتواصل الهاتفي واللاسلكي وما إلى ذلك، ممّا كان سائدا في ذلك الحين. وقد عُرفت يومها بشبكة «أربانت – Arpanet (1)».

وفي مرحلة مُعيّنة، ولأسباب تعني السلطات الأميركية نفسها، اتخذت المُشار إليها القرار بإخراج هذه الشبكة من نطاق السرّية إلى العلن، وإطلاقها على مستوى العالم لخدمة أهدافها، وأطلقت عليها اسم الإنترنت – Internet)؛ وهنا ملاحظة توضيحية سريعة: لكي تتوافر لديك خدمة الإنترنت لا بدّ أوّلاً من أن تشترك مع إحدى الشركات المُزوّدة، وهذه تعطيك جهازاً يتيح لك تلقي الخدمة (وهو) راوتر)) أي مُوجّه للحزم الإلكترونيّة يجعل بإمكانك استقبال خدمة الإنترنت على أجهزة الاستقبال لديك من كومبيوتر وهاتف جيب ومختلف الأجهزة اللوحية.

1- ARPANET/ https://www.britannica.com/topic .

1. ثورة المعلوماتية

يعيش العالم منذ نهاية القرن العشرين ثورة في مجال المعلوماتية، وبصورة خاصة في نطاق تكنولوجيا المعلومات ووسائل التواصل. بعد انتشار الأمر والشبكة سارعت بعض الشركات المتخصصة إلى إنشاء نظام يَسّمَح بتيسير الاتصال والتواصل والتعارف بين البشر (بروتوكولات الاتصال IP (مثلاً ، وأنشأت كيانات افتراضية الفضاء الافتراضي، تُتيح لكلّ شخص أو شركة الحصول في على صندوق بريد إلكتروني (Email)، وعلى مواقع على الشبكة العنكبوتية العالميّة (World Wide Web)(1) والتي يُمكن الدخول إليها والاطلاع على المعلومات المُتوافرة من خلالها.

وقد تحوّلت هذه الشبكة اليوم إلى وسيلة لا غنى عنها، ليس للتواصل فقط، بل لتبادل المراسلات والنصوص والصور والأفلام والجداول، وكلّ أنواع المعارف والمعلومات، بطريقة مضمونة وسريعة وسهلة التنفيذ. وباتت شبكة الإنترنت بأهمية الشبكات الحيوية الأخرى التي لا غنى عنها لإنسان اليوم، مثل شبكات الماء والتيار الكهربائي. وصارت كذلك وسيلة للإبحار عبر أصناف المعارف، وفي بطون الكتب ومراكز الدراسات والأبحاث، وملاذ كل باحث في أي علم أو فنّ. ودخلت الإنترنت في مختلف مناحي الحياة، والإدارة والإنتاج، والاقتصاد والصناعة والتجارة، وكلّ شأن وباتت هي أبرز وسائل التحكّم والسيطرة الخاصة بمعظم العمليّات الحيويّة الموجودة على الأرض، وانتقلت إلى الفضاء كواحدة من

1- https://webfoundation.org/about/vision/history-of-the-web.

وسائـل التواصـل مع المحطـات الفضائيـة والأقمار الصـناعية، وصارت من دون منازع نجمـة العالـم الافتراضـي الـذي ابتكره الإنسان منذ اختراعه الكمبيوتر والذاكرات الإلكترونية وشـبكات المعلومات، مؤسسا بذلك جغرافية افتراضية جديدة، زاخرة بالإنجازات الباهرة، والوعود الهائلة، والمفاجآت التي لم يفكر فيها كبار كتاب الخيال العلمي.

هـذا التطوّر أتاح إمكانيـة التعامل الـدولي بأسـلوب جديـد لـم يَكُن ملحوظاً أو مُتوقعًا عنـد وضع النظم القانونية التقليدية؛ فبعد أن كان هذا التعامل خلال المنازعات المسـلحة يتم على الأرض أو البحر أو الجوّ أو الفضاء الخارجيّ، أصـبح، بفعل هذه التقنية، يتمّ بطريقة إلكترونية ضمن نظـام معلومـاتي يختلف كليا عن الحرب البريّـة والبحريّـة ،والجوّيّـة إن لجهـة اختراق منظومـة العـدوّ ، الإلكترونيـة أو لجهـة جمع المعلومات الإلكترونية الحسّاسة أو نقلها أو تبادُلها(1). ومع تزايد الاعتماد على الوسائل التقنية الحديثة في إدارة الأعمال المختلفة، برزت تحـدّيات قانونيـة وطرحت تساؤلاـت حول إمكان اعتبار التواصل الإلكتروني الافتراضـي (Virtual communication) الذي أصـبح يتم اليوم بواسطة الإنترنت (Internet) أو الفضاء الإلكتروني أو فضاء السايبر أو الفضاء السيبراني (Cyberspace موازيا للمرافق العامة الدولية التقليدية(2)،

ص: 70

1- الحرب الإلكترونية أو حرب الإنترنت أو حرب الفضاء Battle space))، هي حرب رقميّة أسلحتها افتراضية (Virtual) وهمية بمعنى أنّها لا تتجسّـد ماديًا) تهدف إلى الإضـرار بالبنية الرقمية للخصم (أو العدوّ) أو إتلافها. كما تشـمل هذه الحرب أيضًا التجسّـس على العدوّ ودسّ معلومات مغلوطة بين معلوماته.

2- لمزيـد من المعلومات عن موضوع النطاق الـدولي، راجع د. محمـد المجـذوب، «القانون: الـدولي العام، الطبعـة السادسة منشورات الحلبي الحقوقية، بيروت، 2007، ص 403-559.

وحول ضرورة عقد معاهدات جديدة تنسجم مع التطور التكنولوجي إن لم تكن الإمكانيّة الأولى مُتاحة أو كافية.

.2 المبادئ التقنية للإنترنت توجد ثلاثة مبادئ تقنيّة تأسست عليها شبكة الإنترنت وما زالت تخضع لها حتى وقتنا الراهن، وهي:

نظام اسم النطاق (Domain Name System) وهو النظام الذي يقوم بترجمة اسم النطاق من حرف إلى رمز ليتعرّف عليه جهاز الكومبيوتر أو الهاتف الذكي.

بروتوكول الإنترنت (Internet Protocol) وبروتوكول التحكم فى نقل البيانات (Transmission Control Protocol) اللذان يُعرفان بالاختصار TCP/IP ويُعتبران العصب المحرك للإنترنت ويمنحان الكومبيوترات القدرة على التواصل مع شبكة الإنترنت.

أنظمة السرفيرات أو الخوادم الرئيسية (Root Servers) ويوجد منها ثلاثة عشر خادمًا، تتحكم بها بعض المؤسسات الخاصة والحكومية، مثل الإدارة الوطنيّة الأميركية للملاحة الجوية والفضاء ناسا، المؤسسة الهولندية غير الربحية بعض الجامعات الجيش الأميركي، وبعض الشركات الخاصة. وتتواجد عشرة خوادم عملاقة من أصل ثلاثة عشر في الولايات المتحدة، بينما يتواجد واحد في كلّ من أمستردام واستكهولم وطوكيو.

مع تزايد أهمية الإنترنت وانتشارها استطاعت الحكومة الأميركية التوصل إلى اتفاق بين عدة هيئات خاصة والحكومة

الفيدرالية لإنشاء هيئة تقوم بالإشراف على شبكة الإنترنت سمّيت (هيئة الإنترنت للأسماء والأرقام المتخصصة هيئة أيكان .(Internet (Corporation For Assigned Names and Numbers – ICANN

إلا أنّ الهيئة حافظت على طابعها المدني والأهلي منذ نشأتها، حيث لم تخضع بشكل مباشر للسيطرة الحكومية أو العسكرية، غير أنّها كانت خاضعة من تحت الستار للنفوذ الأميركي، حيث رفضت الولايات المتحدة التنازل عن هيمنتها على الهيئة، على الرغم من التوصية الصادرة عن لجنة مختصة شكلتها الأمم المتحدة في عهد أمينها العام الأسبق كوفي عنان، والتي دعت إلى ضرورة انتقال صلاحيات هيئة آيكان إلى الولاية المباشرة للأمم المتحدة.

ومن باب الهيمنة اعتبرت واشنطن أنّ المحافظة على سيطرتها على الإنترنت لأجل غير مسمّى سوف يتم التعامل معه أميركيا وفق مبدأ مونرو لهذا العصر، بمعنى أنّ أيّ تحدٍّ لشكل وبنية نظام الإنترنت في وضعها الحالي يعتبر تحدّيا لواحدة من المصالح الحيوية الأميركية. والمعنى الصريح لهذا من دون أي لبس أو إبهام، هو أنّ الإنترنت هي مصلحة أميركية أولاً وأخيراً، وأن إقدام واشنطن على حرمان) جيوشها وسيلة التواصل هذه، لم يكن عمل خير من أجل البشرية ورفاهية الإنسان، بل كان تلبية لمصالح خاصة... إن لم تكن واضحة تمامًا للجميع فهذا لا يعني أنها غير قائمة ولا موجودة.

ص: 72

3. بين «الفأرة» و «الناقل»

في بدايات ظهور الكمبيوتر وانتشاره في ثمانينات القرن الماضي ثم خروج شبكة الإنترنت من ظلمات الجيوش الأميركية إلى العالم، كان لكلّ قطعة جديدة يتم انتاجها في إطار الاستخدامات، كابل متناسب معها، ومخرج خاص بها في جهاز الكمبيوتر. وقبل ذلك كانت قد انتشرت تسميات جديدة تُشير إلى أدوات لم تكن معروفة من قبل. وأشهر هذه الأدوات والتسميات كانت ال- فأرة - Mouse) (وهي إحدى وحدات إدخال المعلومات في الكومبيوتر، يتمّ وصلها به واستعمالها يدويًا للتأشير والنقر لتظهر التأثيرات على الشاشة). فعلى سبيل المثال إذا كان الجهاز موصول به ((ماوس) (فأرة) وكي بورد لوحة مفاتيح الحروف) وسماعة وطابعة وشاشة، يكون لزامًا توافر خمسة مخارج مختلفة ،فيه تتحكّم في كلّ منها دائرة إلكترونية معيّنة وهذا يعني أنه مع إنتاج الآلاف من الملحقات التي يتم تركيبها مع الكومبيوتر المعد للاستخدام، سيكون على المستخدم شراء جهاز كمبيوتر آخر ليستطيع توصيل تلك الأدوات وتشغيلها. ويمثل عدم توافق الملحقات الجديدة مع منافذ أجهزة الكمبيوتر مشكلة كبيرة تتجلى في عدم الاستفادة من الأجهزة المنتجة إلا لشرائح معيّنة أو لشركات معينة فقط.

ومن أجل حلّ هذه المشكلة المعيقة كان لا بد من اختراع الجهاز الذي نعرفه اليوم باسم يو إس بي USB.

ص: 73

4. كيف يفهم الكومبيوتر عليك؟

ربما كان الواحد منا يستخدم الكومبيوتر بشكل يومي، لكنّه لم يتساءل كيف يفهم الكومبيوتر عليه ويُنفّذ أوامره؟

وإذًا إذا كان كلّ ما يعتمل في تلك الأجهزة ليس سوى التيار الكهربائي فقط، فكيف تنتج لنا تلك المعلومات التي نفهمها، كالعمليات الحسابية أو الموسيقى أو ملفات النصوص أو الصُّوَر أو الفيديو؟ وكيف يستطيع ذلك العملاق الصغير تنفيذ ملايين العمليات الحسابية في ثوان معدودة، والاحتفاظ بمعلومات مختلفة في شتى المجالات من دون أخطاء تذكر؟

ما نعرفه عن لغة الكومبيوتر أنّها تقوم على رقمي الصفر (0) والواحد (1) فقط. هكذا قالوا لنا مراراً وتكرارًا، لكنّنا لم نفهم... ربما لأنّهم لم ينجحوا في الشرح.

لمعرفة كيف يفهم الكمبيوتر البشر علينا أن نعرف أوّلاً ماذا تعني الكهرباء لنا. فالكهرباء على ما ينبغي أننا نعلم هي عبارة عن طاقة محرّرة تتكوّن من سيل من الإلكترونات يسمّى الشحنة. وهذه تمر عبر مادّة موصلة كالنحاس أو الحديد أو غيرهما من المعادن.

ونستخدم هذا السيل من الإلكترونات في تحويل طاقتها إلى أشياء يحتاجها البشر كتشغيل مصباح ؛ بتحويل الطاقة إلى ضوء أو مروحة ؛ بتحويل الطاقة إلى حركة. وبهذه الطريقة تتسلّم أجهزة الكومبيوتر ما نودعه إيّاها من إشارات كهربائية (عن طريق ملامس الجهاز)، وتُلبّيها كرموز تشغيل لبرامج تعمل على تنفيذ مطلوبنا.

ص: 74

الفصل السابع: التجسّس والقرصنة

اشارة

حين نـذكر الإنترنت، يتبادر إلى الـذهن مجموعـة متشابكة من الإمكانات والإيجابيات والمخاطر التي تتصل بالشـبكة وطرق اسـتخدامها. ولعلّ البداية تكون مع خطر القرصنة... قرصنة المعلومات؛ بمعنى الاعتداء على خصوصيتها وتجاوز برامج حمايتها وقوانين الحق الحصري ثمّ وضع يد «غريبة» هيمنتها على هذه المعلومات والتصـرّف بها. والطرف الذي يقوم بهذا الفعل هو من يُلقب ب-: (القرصان – Hacker ، والجمع قراصـنة . يشـمل مصـطلح "القراصـنة" الأشـخاص المنخرطين في أنشطة غير قانونية تقوم على العدوان والسلب والنهب والابتزاز والتخريب. كـلّ ذلـك يقوم به القرصـان، حين يسـتطيع تجـاوز الحمايـة التي يضـعها كـلّ صاحب حساب على الإنترنت للمحافظـة على معلومـاته المخزنـة في الفضـاء الإـلكتروني. وعمليّـة القرصـنة تكون بالتـالي عمليـة إلكترونيـة تجري في عـالم الإنترنت الـذي هو العالم الافتراضـي القائم في الفضاء الإلكتروني. ولا تتصل معظم العمليّات الإلكترونية بنزاع مسلّح، ومن ثم فإنّ القانون الدولي الإنساني كان في الأساس لا يطبّق عليها. وحتى في النزاع المسـلّح كان القراصـنة يعتبرون مـدنيين يسـتمرون في التمتّع بحماية القانون الدولي الإنساني من الهجوم المباشـر عليهم، على الرغم من أنّهم يظلّون خاضـعين لعمليـات إنفاذ القانون، وقـد يتعرّضون للمقاضاة الجنائيـة تبعًا لما إذا كانت أنشطتهم تنتهك مجموعة أخرى من القوانين.

ويوما بعد يوم تثبت موجات هجمات القراصنة الإلكترونيّة

ص: 76

الخطيرة (التي امتـدت ذات مرة لثلاثـة أسابيع بلا انقطاع أن مجتمعات الدول المتقدّمة الأعضاء في حلف الناتو على سبيل المثال) وسواها أيضًا، تعتمد بشكل أساسي على الاتصالات الإلكترونيّة، وهي معرّضة بشكل كبير للمخاطر على الجبهة الإلكترونيّة.

ومعلوم أنّه أثناء أزمـة كوسوفو، واجه حلف الناتو أوّل حادث خطير من الهجمات الإلكترونيّة. وقد أدّى ذلك، من بين أمور كثيرة، إلى إغلاق حساب البريـد الإلكتروني للحلف لعدة أيام أمام الزوار الخارجيّين مع التعطيل المتكرّر للموقع الإلكتروني للحلف والحوادث التي جرت في السنوات التالية زادت من الوعي المتنامي تجاه خطورة التهديد الإلكتروني.

1. ستوكس نت... البرنامج الخبيث

لا يزال فيروس "ستوكس نت" Stuxnet يشـكل الرمز الأشهر لإحدى أكثر العمليات الهجومية تعقيدًا وغموضًا التي تمّ إطلاقها حتى يومنا هذا. الفيروس المذكور جرى تصميمه خصيصًا لمهاجمة المفاعلات النووية في إيران.

الخبير الألماني في مجال الكومبيوتر "رالف لانجر" وصف سـتوكس نت" بأنه "الأكثر تعقيدًا وعدوانية في التاريخ". وأضاف لانجر" الذي هو واحـد من أوائل الخبراء الـذين حلّلوا شـفرة سـتوكس نت، أنّه تسـبّب في إعادة البرنامج النووي الإيراني عامين إلى الوراء، وأنّ فاعليته كانت بنفس مقدار فاعلية الهجوم

العسـكري وربما أفضل لعدم وجود خسائر بشـرية ولا حرب حتّى يسود الاعتقاد بأنّ هذا الفيروس الذي اكتشف في العام 2010 كان ثمرة تعاون عميق بين الولايات المتحـدة الأميركيـة وإسـرائيل، على الرغم من أنّ المصادر الأميركية تنفيه من أساسه، الأمر الذي لم يرفع التهمة ولا الشـكوك التي تكتفت بفعل النفي الأميركي ذاته. وعلى الرغم من أنه لم يتم الاعتراف رسـميًا بأصول سـتوكس نت" ومصـدره، فلا يزال مدى الانغماس الأميركي ومعه الإسرائيلي في البرمجيات الخبيثة غير معروف(1).

تعتبر الوسائل الإعلاميّة أنّ "سـتوكس نت كان عمليّة اسـتخباراتية أجرتها سـلطات الاسـتخبارات بمعزل عن سـلطات قيادة الإنترنت؛ لذا، فالمعلومات حول طبيعة هذه العملية غير متوافرة كان قد قام بتنفيذها، فقد أعلن عن أمر جديد كان حقا، وأيا من يحدث ف ستوكس نت غير قواعد اللعبة، وأصـبحت الإنترنت بعده مكانًا أكثر خطورة؛ لأنّ الجميع بدأوا يستعدون للحرب. وبينما راحت إدارة الرئيس الأميركي السابق أوباما تُفصح ببطء عن مزيد من المعلومات حول سـياسة الهجوم الإلكتروني للولايات المتحدة الأميركيّة، يعمل عدد كبير من الخبراء على خوض نقاش علني أوسع نطاقا بشأن كيف أنّ الولايات المتحـدة تعتزم اسـتخدام قـدراتها تلك؛ فالفرق العسـكرية الواحـدة والأربعين التي انتهت عملية إنشائها بحلول نهاية العام 2016 هي جزء من مجهود كبير قامت به

1- https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

وزارة الدفاع الأميركيّة لتوسيع وتنظيم الجهود العسكرية الإلكترونية، حيث كشفت الوزارة في العام 2013 أنّها أنشأت 133 فرقة مهمتها شنّ عمليّات هجومية ودفاعية، من بينها 27 فرقة تركز على بناء قدرة لشنّ هجوم على عدوّ في الخارج. وقد جرت إدارة العمليات من مقرّ القيادة الإلكترونية الأميركية في «فورت ميد» في ولاية ماريلاند التي أسسها الجنرال كيث ألكسندر في العام 2010، حيث تولى رئاسة قيادتها، وكان في نفس الوقت مديرًا لوكالة الأمن القوميّ في تلك الفترة.

2. حروب المستقبل... إلكترونيّة

المجال الإلكترونيّ أو السيبرانيّ هو أحد أكثر الحقول حداثة وغموضًا وسرّيّة، وهو أيضًا من أكثرها خطورة. لا جدوى ولا فائدة من النكران. وليس من المفاجئ القول إنّ الجيش الأميركي الذي أقوى الجيوش في العالم وأفضلها تجهيزا، لديه استراتيجية إلكترونية متكاملة، يحرص على إبقائها طي الكتمان بحيث أنّه لا يزال يلفّ قدراتها وبرامج حمايتها بالغموض والإبهام، ليحول دون استهداف مخزوناته في الفضاء السيبراني بالهجوم والقرصنة. ففي الحرب التقليديّة تكون الأسلحة والاستراتيجيات مفهومة بشكل جيّد إلى حدّ بعيد ما يجعل شنّ الحرب عملاً «صائتا» وليس صامتًا، إذ يستحيل خلال الحرب طمس دوي انفجاراتها. لذا، فقد وضع المجتمع الدوليّ قواعد طريق للصراعات المسلّحة بهدف الحفاظ ما أمكن على المدنيين والمؤسسات المدنية إلى أبعد قدر ممكن.

لكنّ هـذا جميعه لا ينطبق في عالم الإنترنت. فالهجمة الإلكترونية تنطلق من على شاشة المهاجم ربما بشـكل إرسال رسالة»، من دون أيّ إطلاق نار ولا إحداث ضجة ولا ضوضاء. لكنّ الخسائر التي يمكن أن تتسبّب بها الهجمة السيبرانية قد تصل إلى درجة تفوق بالويلات التي تسـبّبها، كلّ ما عرفته البشـريّة من حروب وويلات حتّى اليوم. فقد تُفجِّر المخزونات النووية في أماكن تخزينها وإخفائها تحت الأرض وفي بطون الأوديـة وأعماق البحار. وهـذه ليست سوى إمكانيـة واحـدة من مروحـة إمكانيات لا بـدء لها ولا انتهاء. كـذلك يمكن تعطيل التيار الكهربائي في قطاع عمليات العـدو، أو وقف تزويده بالماء أو بالوقود... أو حتى التشويش على اتصالاته لإعمائها. ولسوء الحظ فقد بات من المُسلّم به على نطاق واسع أنّ الضربات الهجومية الإلكترونية التي يجري تطوير أسلحتها على قدم وعدة سيقان، ستكون عنصرًا ضروريًا في أي حملة عسكرية في المستقبل.

ومثل هذه الهجمات تتراوح بين إقفال حساب للعدوّ أو تنشـيطه بطريقة عكسـية ليلحق الضـرر بصاحبه، بل أفظع ما يمكن أن تُصوّره مُخيّلة وحشيّة. وكلّ ذلك من دون إطلاق رصاصة واحدة.

الواقع أنّ تاريخ 11 أيلول/سبتمبر من العام 2011 كان هو اليوم الـذي غير كلّ شـيء، واعتبره البعض» بداية عهد جديد. فمع انهيار برجي التجارة انهارت المفاهيم التقليديـة التي كانت سائـدة عن التهديـدات الأمنيّـة، وتغير معها سـيناريو الحرب الباردة الذي هيمن على العالم على مدار أكثر من نصف قرن.

لم يتحدّث أحد علنًا عن أن حدث تدمير البرجين في نيويورك كان

ثمرة لإرهاب إلكتروني، بل إنّ المسؤوليّة وضعت على كاهل فلان وعلتان من سعوديين وغير سعوديين، وقيل إنّ التخطيط والإشراف على التنفيذ كانا من عمل تنظيم «القاعدة» الإرهابي وزعيمها في حينه «أسامة بن لادن». إلا أنّ الأهم من هذه التهمة «السلسة» بحدّ ذاتها هو الافتراض، مجرّد الافتراض باحتمال أن تكون الطائرات التي اصطدمت بالبرجين وبمبنى وزارة الدفاع الأميركية (البنتاغون)، لم تكن تخضع لربابنة في مقصورات قيادتها، إنما كان يجري تسييرها إلكترونيًا باتجاه أهدافها التي جرى تحديدها لها، وبعكس إرادة الربابنة، بمعنى أن يكون الفاعل قد تمكن من السيطرة على الطائرات إلكترونيًّا وعمد ربما إلى إكراه الطيارين والطاقم أو قتلهم سلفًا، وترك الطائرة لأوامر توجيهها إلكترونيًا حسب إرادة المعني بالتنفيذ والذي كان ربما في فندق فخم بعيد عن «حلبة المنازلة».. وعلى الرّغم من أنّ هذا الرأي لم يطفُ على السطح ولم يتحدّث به من كان ينبغي عليهم استدراكه لأسباب غير واضحة)، إلا أنّ الحدث ذاته جاء ليعلن بصراحة دموية جامحة أنّ استخدام الطائرات المدنيّة كأدوات للهجمات... وسرعان ما تبين أنّ الفيروسات الإلكترونيّة المتنقلة (وهي برامج تدميرية) تحوّلت من مجرد مصدر إزعاج إلى تحدّيات أمنية خطيرة، وأدوات مثالية لشنّ الهجمات وتخريب الشبكات، وأيضًا لممارسة التجسّس الإلكترونيّ.

وتابع: هناك سلسلة من علامات الاستفهام التي لا نهاية لها. يجب القول إنّ الإنترنت عالم خطير يسود فيه عدم الأمان، ما يعني وجود الخطر المتربص باستمرار (...). ومثل هذا الكلام لا يصحّ

التغاضـي عنه واعتبار أنّه لم يكن بل لعلّ الأصوب الإشارة إلى أنّه غيض من فيض في هذا الاتجاه. ومن جهة ثانية يقول «سكوت بورغ مدير وحـدة عواقب الشـبكة العنكبوتية الأميركية، (وهي مركز أبحاث لا يبغي الربح يركز أبحاثه على الآثار التي تنتج عن الهجمات الإلكترونية)، وفي السـياق ذاته: «إنّ الهجوم الإلكتروني الشامل قـد يُحـدث أضـرارًا ضـخمة لا يتجاوز حجمها إلا الحرب النووية الشاملة "؛ إنّه أكثر من جرس إنذار.

وإن شـئنا الحقيقـة بلا مداورة، لا بدّ من الاعتراف بأنّ الأسـلحة السـيبرانية تتواجد في عالم لا تختلف ظروف المعرفة البشـرية فيه كثيرا عما كانت عليه في الأيام الأولى لعصـر البرنامج النووي. فالأسـلحة السيبرانية محاطة بالسرّيّة وتبعث على الفضول من خلال المعلومات العامة المسـرّبة حولها والشائعات الهائلة التي ترافقها، وتولّد المخاوف المبهمة من نتائجها. وليس من السـهل تجنّب ذلك؛ فالمحافظة على سرّيّة القـدرات السـيبرانية لـدى كلّ دولـة تعتبر ضـرورة حيوية قصوى، ولا سـيما بالنسـبة إلى دولة بحجم الولايات المتحدة الأميركيّة. لذا، فإنّ واشـنطن لا تتورع عن العمل صراحة وجهارًا في سبيل السيطرة على العالم برمته من خلال الفضاء السيبراني، وهو بالطبع هدف يسعى إلى تحقيقه العديـد من القوى الجبّارة أو الطموحـة الأخرى في عالم اليوم. وهذا ما يوافق عليه المساعد الخاص للرئيس الأميركي ومنسق الأمن الإلكتروني في مجلس الأمن القومي الأميركي مايكل دانييل بقوله من دون توريـة:» إن كنت تعرف الكثير عن قـدرات الشـبكة العنكبوتيّـة، فمن

السهل جدا مواجهتها. ولهذا السبب نحرص على إبقاء الكثير من قدراتنا السيبرانية تحت حراسة مشدّدة».

3. صفر يوم – Zero-day

إنّ أقوى قـدرات الإنترنت هي ما أُطلق عليه اسم "zero-day" وهذه القدرة الهجومية تسـتغلّ نقاط ضعف البرمجيات غير المعروفة حتى من صاحب البرنامـج نفسه. وعلى سبيل المثال، كانت هناك ثغرة أمنيّة في نظام تشـغيل Windows Microsoft لم يكن مخترع البرنامج انتبه لوجودهـا. ومن خلال هـذه الثغرة جرى اقتحام نظام مايكروسوفت العملاق والتسـبّب فيه ببعض الأضـرار إلى أن تمكّن المعنيّون من معالجـة الخرق وإقفال الثغرة. ما جرى هنا هو ما ما أطلقَ عليه zero-day ، والسـبب أنه بمجرد اكتشاف نقطة الضعف فى البرنامج، يكون قـد فـات الأوان للنجاة من الضـرر، بمعنى انّه لـدى اكتشاف الثغرة في أي برنامـج ما يكون أمام صاحب البرناج «صـفر يوم – zero-day» لإصلاح الأمر.

والعبرة من هذا أنّ القدرات الإلكترونية كأسـلحة تختلف بأشكال رئيسيّة عن الأسلحة التقليدية كالصواريخ والقنابل. فهي أوّلاً تسبّب ضررًا أقلّ علنيّـة ولكن أكثر انتشارًا من الهجوم المادّي، إذ يمكن للسـلاح الإلكتروني أن يشلّ الاقتصاد المحلي عبر مهاجمة الأنظمة الاقتصادية أو الاتصالات في بلـد معين. وثانيًا، يمكن شنّ هجوم فوري ومباغت تقريبًا ضـد أي هدف في العالم، ومن أي جهاز كومبيوتر في... مقهى عام. فالإنترنت تلغي المسافة المادّيّة بين

المتحاربين، الأمر الذي يفتح لهؤلاء الطريق لشن الهجمات التي يصعب رصدها . ثالثًا، غالبًا ما تستخدم القدرة السيبرانية مرة واحدة: إذا كانت الحكومة تمتلك رمزاً خبيثًا وتستخدمه لاستغلال خلل في التعليمات البرمجية للعدوّ عندها يصبح استخدام هذه القدرة غير فعّال في المستقبل، اذ يكون بإمكان العدوّ اكتشاف نقطة الضعف

في برنامجه وإصلاحها.

4. «فاضح أسرار أميركا»

في السنوات القليلة الماضية حدث تطوّر جديد داخل المؤسسة العسكرية الأميركيّة، حين جرى نقل الشبكة العنكبوتية من فكرة نظريّة إلى جزء معتمد – وإن كان سرّيًا – من السياسة الأميركية. وظهرت الإشارة الأولى على ذلك في كانون الثاني من العام 2013، عندما ذكرت صحيفة واشنطن بوست» أنّ البنتاغون يوسّع بشكل لافت قواته الأمنية على الإنترنت في جميع فروع الخدمة لديه. كما أطلق الجيش الأميركي في تشرين الأوّل من العام نفسه فريقين من الخبراء التقنيين ينحصر تخصصهما فقط في عالم الإنترنت. ولم يكد يمضي عام واحد حتى وصل عدد الفرق المتخصّصة المشابهة إلى عشر، وهي في ازدياد.

تحدّد الاستراتيجية الإلكترونية الجديدة لوزارة الدفاع الأهداف والغايات الاستراتيجية للوزارة؛ لكنّها لا توفّر إلا تفاصيل قليلة في ما يختص بطريقة تطبيق الجيش لهذه الاستراتيجية، إذ ينبغي على وزارة الدفاع أن تتمكّن من توفير القدرات الإلكترونية المتكاملة لدعم العمليات العسكريّة وخطط الطوارئ. فعلى سبيل المثال،

قـد يسـتخدم الجيش الأميركي العمليات الإلكترونية لإنهاء نزاع دائر بحسب شـروط الولايات المتحدة، أو لتعطيل أنظمة العدوّ العسـكرية لمنع استخدام القوة ضد المصالح الأميركية.

لكن عنـدما يتعلّق الأـمر بالتفاصـيل، يرى مراقبو الإـنترنت من الخبراء المتـابعين أن الوثـائق التي سـرّبها موقع «ويكيليكس» الـذي يـديره الأسترالي الأصل «جوليان أسانج» منذ العام 2006، وهو هارب من السلطات الأميركية التي تجد في أثره، وقد نشر على الموقع الذي يديره ملايين الوثائق التي تفضـح الولايات المتحـدة والعديـد من الـدول الأخرى والحُكّام والسياسـيين في مختلف أنحاء العالـم ... ما قصة تلك الوثائق ؟؟؟

وابتداءً من العام 2013 انضـمّ «مُسـرّب» معلومات سـرية آخر إلى أسانج»، وهو التقني السيبراني الأميركي المتعاقد كمحلل معلومات مع وكالة الاسـتخبارات الأميركية إدوارد سـنودن، صاحب لقب «فاضح أسرار أميركا والمطلوب الأوّل لواشنطن. وعلى الرغم من أنّ الزمن كان قد تخطّى معظم المعلومات التي فضـحها، إلا أنّها تضمّنت معلومات مفصلة عن كيفية بناء الحكومة الأميركية الترسانة قدراتها الإلكترونية وطريقـة اسـتخدامها لها في تلك الفترة، وتضـمنت كـذلك برنامـج التجسّس السـيبراني الأميركي المعروف باسم بريسم)، والذي كان بالغ السِّرِّيّة قبل كشفه وفي العام 2013 نقلت صحيفة واشنطن بوست من تسريبات «سنودن» أنّ الحكومة الأميركيّة نفّذت 231 عمليّة إلكترونيّة هجومية في العام 2011، لم تصل أي منها إلى مستوى هجوم فيروس «ستوكس نت».

ص: 85

ونشـر سنودن» أيضًا «تعليمات السياسة الرئاسية – 20»، وهي وثيقة سـرّيّة للغاية وضعت مبادئ الإدارة الإلكترونية في الولايات المتحدة، لكنّها، كما الاستراتيجيـة الإلكترونيـة لوزارة الـدفاع الأميركية، لا تتضـمن أجوبة على أسـئلة كثيرة، إنما تقدم مبادئ توجيهيّة عامّة لأهداف العمليات الإلكترونيّـة الهجوميـة للبلاد. وقد أدّى هذا الغموض إلى إصابة بعض الخبراء بالإحباط فاستراتيجية وزارة الدفاع «الغامضة» هي بالضـرورة غير مأمونـة بالنسـبة إلى كثيرين، ومع ذلك فقـد دافع خبراء آخرون عن وثيقـة وزارة الـدفاع، بقولهم إنّه لا يُقصـد بها وضع قواعد محدّدة للاستخدام العسكري للأسلحة الهجومية الإلكترونية، إنما تشكل الخطوة الأولى في عمليّة تؤدّي إلى وضع قواعد التزام

محدّدة أكثر للفضاء السيبرانيّ.

5. أولويّة الحرب السيبرانيّة

الحقيقة أنّ العمليّات السـيبرانيّة برزت كأولوية على المستويين الأميركي والعالمي، بعد أن أسس الجنرال كيث ألكسندر ما بات يُعرف ب– «القيـادة الإلكترونيـة»، وأصـبح من الواضـح أنّ الجيش الأـميركي سـيحتاج إلى الـدفاع عن البلاد على نطاق أوسع، بـدلاً من عن شـبكاته الخاصة، ويتطلب ذلك قدرات إلكترونيّة هجوميّة الدفاعيّة عاليّة.

أمّا الجزء الثاني من تلك الاستراتيجية فيتعلّق بكيفية بناء قوّة يمكنها تنفيذ هذه المهمة. وجاءت التفاصيل

على التوالي: تعمـل وزارة الـدفاع على إنشاء 133 فرقـة إلكترونيـة وأربعـة مقرّات جديـدة للقوّة الإلكترونية المشتركة، بما فيها المقرّ التابع للجيش في ولاية جورجيا. ويتضـمن الفرع الإلكتروني التابع للجيش الآن أكثر من ألف شخص، لكنّ القواعد المحدّدة لا تزال قيد الإنجاز وفي مراحلها الأولى».

إنّ التوافق على إجابـات مقنعـة على مختلف الأسـئلة التي تطرحها معضـلة الأمن السـيبراني، هو أمر عسـير ولم يتحقق بعـد، غير أنّه ليس مسـتحيلاً. فقد بدأ المجتمع الدولي يتلاقى مثلاً حول اتفاق ينص على منع التجسّس الإلكتروني لأغراض تجاريّة، ومع أنّه ليس من الواضح أن كل البلـدان قد تلتزم به . ثمّ إنّ وضع قاعدة مفصـلة للردّ على أي حادث أو نشاط هو أمر مسـتحيل عمليا. ومن جهة أخرى فهناك العديد من كبـار المسؤولين في الحكومـة، ولا سـيّما القادمين من المعترك السياسـي، لا يتمتعون بمعرفـة كافيـة في التكنولوجيا، وبالتالي فهم لن يُحسـنوا تقدير الأمور ولا العواقب وما يزيد الأمر حساسـية أيضًا أنّ أيا كان يسـتطيع إطلاق حرب إلكترونية بسـرعة كبيرة، ويكفي أن يكون ملماً بالموضوع. وليس من الصـعب تخيّل سـيناريو محـدّد حيث يحرّض بلد ما على إطلاق حرب إلكترونية بطريقة يقع فيها اللوم على بلد آخر، مما يتسبب في تصعيد إعلامي يمكن أن يؤدّي إلى تصعيد حركي يكون مُرشّحا للوصول، ولو بطرق الخطإ إلى المستوى النووي... إنّه سيناريو

غير مرجّح لكنّه ليس بعيد الاحتمال والمعنيّون يعلمون جيّدًا أنّ العالم حاليًا يعيش مرحلة هشة من السلام الإلكتروني. إنما، وعلى الرغم من عمليّات السرقة والقرصنة المتواصلة، فليس في أحد شن اعتداءات سافرة على البنى التحتيّة والأصول لأي طرف دولي آخر، وبخاصة أنّ الإنتائج ومستوى ردّات الفعل لن تكون من الأمور المضمونة. والأرجح أنّ هذا الاستقرار النسبي السائد اليوم ليس سوى قناعًا لتهديدات كامنة في عالم الإنترنت. فالعالم في حالة حرب باردة لم تعد خفيّة على أحد، وليس هناك حال سلام موثوق بل نمطًا هشًا من توازن المخاوف.

ص: 88

الفصل الثامن: عملة الإنترنت

ص: 89

الفصل الثامن: عملة الإنترنت

اشارة

نعم؛ للإنترنت عُملة (بل) عُمُلات) يجري التداول بها على الشبكة العنكبوتية. صحيح أنّها، كما العالم السيبراني، إفتراضية، إلا أنّ لها قيمتها المحفوظة، ويمكن بواسطتها شراء ما يريد الشاري، كما بالإمكان استبدال أي عملة من هذا النوع، بعملات حقيقية من المتداولة. تعتبر بيتكوين عُملة الإنترنت الأولى والأكثر شهرة وانتشاراً، وهي عملة معماة (cryptocurrency) بمعنى أنها تعتمد بشكل آساسيّ على مبادئ التشفير في جميع جوانبها.

وال- «بيتكوين» ليست العملة الرقمية الوحيدة من نوعها التي تعتمد على مبادئ التشفير في جميع جوانبها، وإن كانت الأولى والأكثر شهرة على شبكة الإنترنت. فثمة ما يزيد عن ستين عملة تشفيرية مماثلة، ستة منها فقط هي الرئيسيّة والأكثر اعتمادًا. ولقد وصفت ال- بتكوين بأنّها عملة رقمية، ذات مجهوليّة، بمعنى أنها لا تمتلك رقماً متسلسلاً ولا أي وسيلة أخرى من أي نوع، تتيح تتبع ما أنفق للوصول إلى البائع أو المشتري. وهذا ما يجعل منها فكرة رائجة لدى كلّ من المدافعين عن الخصوصية، أو من قبل بائعي البضائع غير المشروعة (مثل المخدّرات عبر الإنترنت على حد سواء. وجميع العُملات التشفيرية الحالية مبنية على مبدإ عمل عُملة بيتكوين نفسها. وبحكم أنّها عملة مفتوحة المصدر ، فمن الممكن استنساخها وإدخال بعض التعديلات عليها ومن ثمّ إطلاق عُملة جديدة.

ص: 90

يقول القـائمون على بيتكوين إنّ الهـدف من هـذه العملة(1). هو تغيير الاقتصـاد العـالمي بالطريقـة نفسـها التي غيرت بها الويب أساليب البشر. وفي العام 2016 أعلن رجل الأعمال الأسترالي «كريغ ستيفن رايت أنّه هو «ساتوشي ناكاموتو مقدّمًا دليلاً تقنيا على ذلك، ولكن تم كشف زيف أدلّته بسهولة.

تتشـارك جميع العُقـد المتواجـدة على شـبكة بيتكوين هـذا السـجلّ عـبر نظـام يعتمـد على بروتوكول تحتوي سلسـلة الكتـل على جميع الإجراءات التي تمت باسـتخدام...، وهو ما يمكن من معرفـة الرصـيد الـذي يملكه كلّ عنوان على هـذه الشـبكة. يُطلق على هذا المفهوم وصف «السلسـلة» للترابـط المتواجـد مـا بين الكتل، حيث تحتوي كلّ كُتلـة على «هاش» الكتلـة التي تسـبقها ، ويتواصل الأمر إلى غاية الوصول إلى الكتلـة الأولى التي يُطلق عليها اسم «كتلة التكوين (genesis (block) وتكوين السلسلة بهذه الطريقة يجعل من مهمة تغيير أيّ كُتلة بعد مرور مُدّة مُعيّنة على إنشائها، في غاية الصـعوبة، حيث أنّ تغييرها يتطلب تغيير كل الكتل التي تليها، بسـبب إلى إعادة حساب (هاش كلّ كُتلة لتحديث قيمة «هاش» الكتلة السابقة فيها. هذه الخاصـية هي ما يجعل من مُشكل الإنفاق المتكرّر للعملات ذاتها في غاية الصعوبة على... بل ويمكن اعتبار سلسلة الكتل العمود الفقري الذي لا يمكن لعملة الوقوف من دونه.

1- Block chain – Bitcoin Wiki.

1. متى ولماذا؟

ظهرت عملة «بيتكوين» التشفيرية للمرة الأولى في العام 2008 حين ابتكرها شخص مجهول أطلق على نفسه لقب «ساتوشي ناكاموتو»(1).

ثم جرى طرحها للتداول في العام التالي. وصفها مبتكرها بأنها نظام نقدي إلكتروني يعتمد في التعاملات المالية على مبدأ الند للند (Peer-to-Peer)

(2). وهو مصطلح تقني يعني التعامل المباشر بين مستخدم وآخر دون وجود وسيط. وقد وصفها مبتكرها بأنها نظام نقدي إلكتروني يجري اعتماده. وزعم المتعاملون بهذه العملة أن الهدف منها هو تغيير الاقتصاد العالمي بالطريقة ذاتها التي غيرت بها الويب أساليب النشر(3).

ما لفت الانتباه بشدّة حينها، أنّ هذا الفعل قد يتيح نسّقاً للإرهابيين يمكنهم من خلاله الحصول على ملايين الدولارات، كتمويل لعمليّاتهم الإرهابية حول العالم.

ولضمان السير الحسن لعمليات التحويل، يقوم بالاحتفاظ بسجل حسابات تُسجل فيه جميع الإجراءات التي تتم على الشبكة يُطلق عليه اسم سلسلة الكتل (بالإنجليزية(block chain).

(4).

1- Me4onkof. "ArabChain". arabchain.com.

2- http://www.aljazeera.net/news/scienceandtechnology/2016/5/ 3.

3- http://www.aljazeera.net/news scienceandtechnology /2016/5/ 3/

4- https://bitcoin.org/bitcoin.pdf

وعلى الرغم من السـرّيّة العاليـة التي تتمتع بها عملـة «بيتكوين»، حيث كلّ ما تحتاجه لإرسال بعض البيتكوينات لشـخص آخر هو عنوانه فقط، من المتعارف عليه بأنّ عُملـة بيتكوين تتمتع بقـدر عال من السـرّيّة، حيث أنّ كلّ لإرسال بعض البيتكوينات لشـخص آخر هو عنوانه فقـط، لكن بحكم أنّه يتم تسـجيل كلّ عمليـة تحويل في سـجلّ بيتكوين، فإنّه على الرغم من عـدم معرفتك لهويّـة مالك أيّ عُنوان، إلا أنّه بمقدورك أن تعرف كم عدد البيتكوينات التي في حوزته وما هي العناوين التي أرسلت بيتكوينات إليه.

2. عملات رقمية بديلة

بيتكوين ليست العملة الافتراضية الوحيدة المتواجدة حاليًا في الاسو الأسواق الافتراضيّة؛ فقد برزت بفضل نجاحات ال- بيتكوين مجموعة متنوعة ممّا يسمّى ب (altcoins) أو العملات الافتراضـية البديلـة ذات القيمة الجيّدة في الأسواق... ومن أكثرها انتشارًا نذكر: لايتكوين، دوجيكوين وبيركوين وغيرها.

الخلاصة أنّ شـبكة الإنترنت حملت البشـرية إلى الغد الذي لم يكن مفهومًا تمامًا في البدايات، وهو ذاته الغد الذي ما انفك يحتفظ بالكثير من إبهاماته على الرّغم من التقدّم الهائل الذي تحقق في الميدان العملي على امتداد العقدين الأخيرين بشكل خاص.

إنّ على الـدول العربيـة والإسـلامية أمـام هـذه الوقائع أن تسارع المواجهـة متطلبات هـذا النوع من المعارف، من دون الاكتفاء بالتحركات الاستعراضية في الغالب والتي تمارسها أكثر من دولة

غنيّة في هذا العصر. فالقفزات الاستعراضية يمكن أن تستقطب جمهورًا ينذهل ويصفّق لكنّها لا تصنع رأيًا عامًا جديرًا بالردّ على ، تحدّيات العصر السيبراني الذي بات يلفّنا من كل جانب.

3. الأمن السيبراني

العصر الحالي هو عصر الفضاء الإلكتروني بامتياز. أصبح هذا الفضاء الافتراضي بمثابة العمود الفقري لمعظم التفاعلات اليومية، واتجهت معظم الدول لتبنّي مبدأ «الحكومة الذكيّة أي الإلكترونية التي تُسيّر مختلف أمورها على الشاشات وعبر الأنظمة الرقمية. وتعدّى الأمر ذلك إلى حدّ بناء مدن ذكيّة. ومع سهولة الاستخدام ورخص التكلفة وعظم العائد، زاد عدد مستخدمي الإنترنت، حيث من المتوقع أن يصل هذا العدد إلى حدود 5 مليارات مستخدم بحلول عام 2018، أي أكثر من نصف سكان العالم. ومع تزايد الاعتماد على الإنترنت في مجالات الحياة كافة، سواء أكانت سياسية أم اقتصاديّة أم عسكرية أم قانونية أوغيرها، ومع تحوّل مواقع التواصل الاجتماعي لتكون فاعلاً غير تقليدي في العلاقات الإنسانية على مختلف المستويات المحلية وحتى العالمية، يتأكد أنّ شبكة الإنترنت باتت سلاحًا ذا حدّين؛ فكما أنّها وسيلة لتحقيق الرخاء والتقدّم البشري، هناك جانب آخر مظلم لها يتمثل في تزايد التهديدات والمخاطر الناجمة عن الاعتماد المتزايد عليها، من دون توافر حمايات منيعة لشتّى أصناف البيانات المخزنة في الفضاء السيبراني، وذلك في ظلّ عالم مفتوح تحكمه تفاعلات غير مرئية، وغياب سلطة قانونية عليا تسيطر عليه.

ص: 94

هـذا التطوّر الكبير في مجـال الإـنترنت، كمـا من حيث عـدد المسـتخدمين والخـدمات التي يمكن الحصول عليها، وكيفا من حيث تطوّر خصـائص شـبكة الويب بالإضافـة إلى تزايـد الاعتمـاد على تطبيقـات الهـاتف المحمول في الحصول على الخـدمات التي توفّرهـا شـبكة الإنترنت، كلّ ذلك أوجب على الدول والحكومات أن تُغيّر من مفاهيمها التقليدية، وأن تتبنّى مفاهيم تتلاءم مع عصـر جديد يمكن تسميته ب- العصـر الإلكتروني، وأن تضع سياسات تمكنها من تعظيم الاستفادة من هذه الشبكة وتفادي مخاطرها، فتضخّم المحتوى المعلوماتي على مختلف الأصـعدة المدنيـة والعسـكرية والأمنيّـة والإنتاجيـة والفكريـة والسياسـية والاجتماعية والاقتصادية والخدمية والبحثية، إلى ما هنالك، وتوجـد علاقـة بين الإنترنت والأمن القومي، فضـلاً عن ارتباط معظم الخـدمات وقواعـد البيانات والبنى التحتيـة والأنظمـة المالية والمصرفية بشبكة الإنترنت.

وكنتيجة لهذا التوسع في اسـتخدام الإنترنت ودخوله إلى العديد من المجالات كان من الطبيعي دخول المجال الإلكتروني ميادين الحروب واسـتخدامه في بثّ الرعب والفزع، حيث من المتوقع أن تكون الحروب الإلكترونيّة السّـمة الغالبة للمسـتقبل، إن لـم تكن السـبب الرئيسي للحروب المستقبلية الشاملة.

4. الأقوى هو الأعلم بالخصم

تتضاعف الأخطار المحدقة بالأمن السيبراني مع تزايد الاعتماد على ربط البنى التحتيّة

لمختلف الإدارات في القطاعين العامّ

والخاص، فترتفع أهمية وخطورة الفضاء السيبراني، وضرورة الحفاظ على أمنه، الأمر الذي دفع ويدفع القوى العالمية إلى البحث عن كيفية تحقيق وتأمين مصالحها من خلاله.

هكذا ظهرت أجيال جديدة من البنى التحتية، أبرزها تلك البنى المعلوماتية التي ترتبط بها مختلف القطاعات الإنتاجية والتزويدية على مختلف مستوياتها، وما يتصل بها من خدمات حكومية ومالية وعسكرية وأمنيّة. وبات واضحًا أنّ أي تهديد أو هجوم على إحدى تلك المصالح أو عليها جميعها، يمكن أن يؤثر على حراك الدائرة التي استهدفها الهجوم أو يوقفها عن العمل. وأصبح هذا النوع من المخاطر أحد أبرز أنماط التهديدات التي تصيب الأمن الحيوي للمؤسسة أو الأمن القومي العام للدولة، في حال كانت الدولة بكليتها هي المستهدفة(1).

إنّ القاعدة المنطقية في تعامل القوى الفاعلة في العالم ما برحت على حالها منذ القدم كلّما ازددت معرفة بالآخر ونقاط قوته وضعفه، كلّما صرت أكثر استعدادًا لتأمين مكانك وملكيّتك والتفوّق عليه. وعلى مرّ الأزمان ارتبط المفهوم التقليدي للأمن والسيادة الوطنيّة بعوامل القوّة التقليدية التي لها صلة وثيقة بالوفرة والجغرافيا والعديد البشري والكفاءات القتالية. وفي مرحلة متقدمة بات قصب السبق للجيوش المجهزة والمعدات الحديثة والأعتدة المتطورة، حتى وصل الأمر إلى السلاح غير التقليدي من نووي وأشباهه. هكذا دخل مصطلح «الدول العُظمى في قاموس التداول، وصار

1- https://www.scribd.com.

الهمّ الأبرز لدى هذه الدول «النووية» يكاد يقتصر على... منع الآخرين من امتلاك هذا السلاح الذي هو سبب عظمتها، باستخدام الشعار ذي المظهر الإنساني الفضفاض «الحدّ من انتشار السلاح «النووي الذي قصدوا منه «الحدّ من انتشار السلاح النووي لدول غير دولهم».

اليوم جرى طيّ هذه الصفحة. فالعصر بات عصر المعلومات وأمن الفرد والمجتمع والدولة بات يقوم على أمن معلوماته وعلى مقدار حمايتها، وقدراته على استخدامها على أوسع نطاق لخدمته ولتحقيق مصالحه وغاياته وأغراضه في هذا العصر، كلّ شيء صار يعتمد على التقنيات الرقمية، وحتّى الأمن الشخصي والوطني والدولي العام، صار مرتهنا للتقنيات السيبرانية، من خلال كون كلّ المصالح والدوائر والمؤسسات باتت منضبطة تحت لواء البرمجات الإلكترونية. كذلك فإنّ النموّ المطّرد على الصعيد الدولي لقطاع تقنية المعلومات والشبكات واستخدام أكثر من نصف سكان العالم تقريبًا للإنترنت وخدماتها التي لا تُحصى، جعل أمن الوطن والمواطن يعتمد على تطوير هذه التقنيات وحمايتها. وهذا ليس مفاجئًا؛ فقطاع الأعمال مثلاً، وبمختلف مكوناته، بات يعتمد بشكل أساسي في تعاملاته على الأنظمة الرقمية الحديثة وشبكات الإنترنت، كذلك شهد حجم التجارة الإلكترونية نموا كبيرا خلال السنوات القليلة الماضية مع ارتفاع عدد مستخدمي الإنترنت وهذا كله يتطلب المزيد من الاهتمام والبحث والإنفاق والتطوير بهدف توفير حماية مضاعفة لهذه العمليّات التجاريّة وللشبكات والأنظمة

ص: 97

داخل الشركات والمؤسسات والإدارات جميعها، حفاظا على مصالح الأفراد والمجموعات والدول.

5. المفهوم الأمني

إثر انتشار الهجمات الإلكترونيّة والقرصنة والبرمجيات الخبيثة في السنوات الأخيرة، وشيوع حوادث اختراق صفحات المؤسسات والشركات أصبحت الحرب السيبرانية جزءًا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول واتخذ الأمن السيبراني أهميته العالية بعد أن أصبح عمادًا أساسيًا للحياة اليومية وسبيلاً معتمدًا لحماية مختلف الأنشطة التي يشهدها المجتمع البشري على جميع الأصعدة.

فالمعلومات جاءت بتغيرات هائلة في مفاهيم القوة وكيفيات تحقيق السيطرة والتحكم؛ فقد انتقلت نقاط القوة والمنعة من العديد البشري والكفاءات العسكرية غير التقليدية والخصوصيات الاقتصادية والجغرافيّة للبلد، لتتحوّل إلى ما يتصل بالفضاء السيبراني والإمكانات المتاحة فيه لهذا الطرف أو سواه، ولا سيّما ما يتعلّق بعولمة الاتصالات وتبادل المعلومات وسهولة انتقالها بشكل عابر للجغرافيا. وبالنظر إلى الأهمية القصوى لهذه المعلومات، سواء بالنسبة إلى أصحابها، وهي ثروتهم الحيوية وسواعد حياتهم وقواهم وإنتاجهم وصيرورتهم ، أم بالنسبة إلى الآخرين من منافسين ومضاربين وشركاء وأخصام وأعداء... فرض الأمن السيبراني كونه واحدة من أوّل وأهم وأبرز الحاجات الملحة للإنسان الحديث.

ص: 98

فطالما أنّ تجريـد أي جهة كانت من معلوماتها المخزنة في الفضاء الإلكتروني، هو مثابة تجريد لها من م حياتها الأول والأساسـي الذي لا غنى لها عنه ولا بـديل فكيف بالحري سـيكون حال تلك الجهة في ما لو اسـتخدمت جدائل معلوماتها ضدّها... ولصالح الآخر الذي ربما يكون عدواً أو منافسًا أو قرصانا...؟

والواقع أن مفهوم الأمن السـيبراني (Cyber security) (1).يعني مجموع الوسائل التقنيـة والتنظيميـة والادارية التي يجري اعتمادها لمنع الاسـتخدام غير المصـرح به للمعلومات المخزنة، والحيلولة دون إساءة اسـتغلال الفضاء السيبراني أو العبث بالمعلومات الإلكترونية ونظم الاتصالاـت والمعلومات التي يحتويها، وذلك بهـدف ضـمان توافر واسـتمرارية عمل نظم المعلومات، وتعزيز حمايـة البيانات الشخصـية وسـرّيّتها وخصوصـيتها، واتخاذ التدابير اللازمة لحماية المواطنين والمسـتهلكين من المخاطر في الفضاء السيبراني. ويتضمّن ذلك تحقيق وضمان ومتابعة هذه المعلومات ومنع بلوغها أو استخدامها من قبل غير أصحابها المصرّح لهم، والحيلولة دون سوء استغلالها أو العبث بها أو تعديلها أو حبسـها تقييدها أو إلغائها، مع توفير وتأمين سُبُل وصول أصـحابها إليها مع نظم الاتصالات التي تحتويها، ورعاية اسـتمرارية عمل نُظم هذه المعلومات لتحقيق مصالح أصحابها، مع وضع المعايير والإجراءات الكفيلة بضمان أصالة وصحة هذه المعلومات ولا شكّ أنّ فكرة اختراق شبكات المعلومات، والسطو على

1- www.tra.gov.lb/Cybersecurity-AR.

البيانـات و ضـرب القطاعـات الخدميـة والعمـل على شلّ حركـة الاقتصادات من خلال هجمات إلكترونيـة، ليست بالفكرة الجديـدة التي يتداولها خبراء المعلوماتية في العالم، إلا أن وتيرتها ارتفعت بشـكل واضح ومُحرج خلال العقدين الأخيرين، وتركزت الجهود المتخصصة على رفع طاقات الحماية الإلكترونية داخل الفضاء السـيبراني، من دون أن يكون بالإمكان تحقيق الحماية المُطلقة للبيانات أو الحفاظ على سرّيّـة ما يجري تداوله على الشـبكة العنكبوتية بشـكل تام وكامل، الأمر الذي جعل عملية السـعي إلى تحقيق الأمن المثالي للإنترنت مثل لهاث الانسان وراء ظلّه.

ص: 100

الفصل التاسع:"بريسم" برنامج أميركي للتجسّس

ص: 101

الفصل التاسع: "بريسم" برنامج أميركي للتجسّس

اشارة

لابـدّ من اسـتذكار برنامج التجسـس السـيبراني الأميركي «بريسم»(1) الـذي سـربه إدوارد سـنودن عميل الاسـتخبارات الأميركية السابق (المرتـد)، وهو البرنامـج الـذي يُعتبر نوعـا من الفضـيحة المُركّبـة التي تلفّ في ردائها الوسـخ ما هو أكثر وأوسع من وكالـة الاسـتخبارات الأميركية من شركات سيبرانية ضخمة ذات سمعة عالميّة.

بدايـة، إنّ لفظـة بريسم» هي اختصـار العبارة «أداة التخطيط لتكامل الموارد والتزامن والإدارة وتعني عمليا «أداة معلومات مصـمّمة لجمع ومعالجـة بيانات غير الأميركيين أي «الأجانب الـذين تمرّ بياناتهم من خلال خوادم الإنترنت الأميركية». وهذا النوع من التجسّس السـرّيّ على الناس هو من متطلبات الديمقراطيّة الأميركيّة

على طريقة الرئيس السابق باراك أوباما» على ما يبدو، أنّه هو الذي قدّم بنفسه التوصية بهذا المعنى، وحرص على قبولها والعمل بمقتضاها.

أما عن كون البرنامج «فضـيحة مُركّبة» فيعود إلى أنّه كبرنامج تجسّسـى قام أساسًا على التشـكيك بالآخرين لمجرد أنهم غير أميركيين، وهذا يُعتبر قمّـة في العنصـرية. هـذا من دون تجاهـل ذكر الشـركات التي منحت ثقـة عملائها بها للشـيطان»، أي التي أباحت بيانات عملائها أو زبائنها للاستخبارات الأميركية، من دون معرفة أصحاب المعلومات، ومن دون طلب الإذن منهم، ولا إخطارهم.

1- https://www.theguardian.com/us-news/prism.

وهذه الشـركات هي مايكروسوفت ياهو ، AOL، فيسـبوك، غوغل، آبل، وبالتوك، يوتيوب، وسكايب. أما دروب بوكس فيزعم أنه كان طريقه للانضـمام للبرنامـج. ومن الجدير ذكره في هذا الصدد أنّ 98% من بيانـات بريسم)) كان يجري أخـذها من غوغل وياهو ومايكروسوفت وحدها فقط.

وبالنسـبة إلى الجـانب المضـحك، فهو أنّ كـلّ الشـركات التسع أنكرت أنّها أباحت للحكومـة الـدخول المباشـر لخوادمها. أما تويتر فزعم القائمون عليه أنّهم رفضوا المشاركـة في التعاون مع وكالـة الاسـتخبارات القومية الأميركية في هذا الشأن، مع أن جهات عديدة كذّبت هذا الادعاء.

والحقيقة القاسـية هي أنّه لم يكن أحد يعلم أنّ الاسـتخبارات الأميركيّة تقوم بالتجسـس على ملايين البشر (1) حول العالم بطريقة ما، قبل قصّة الصدام الشـهيرة بين شـركة «آبل» ومحكمة العدل الأميركية؛ إذ رفضت الشـركة أمرًا فيدراليا أميركياً يقضي باختراق جهاز هاتف آيفون الخاص بأحـد المشـتبهين بالتورط في تفجيرات كاليفورنيا. وعلّقت الشـركة أنّ هذا الاختراق سـيقوّض حق المسـتخدمين في الحفاظ على سرّيّة بياناتهم، وسيقوض تشفير هواتفها برمته ويوفّر الفرصة للحكومات لاختراق هواتف أخرى مستقبلاً، كما أنّه يُشكك في مصداقيّة الشركة مع عملائها في جميع أنحاء العالم.

أمّا الحقيقة الأقسى من قاسية فقد كشفتها تسعة آلاف وثيقة

1- www.mc-doualiya.com/.../2015/ 7/ 17.

سرّبتها ويكيليكس من داخل ال- سي آي إي»، تفيد بما لا يقبل الشكّ أنّ وكالة الاستخبارات المركزية تعاونت مع مثيلتها البريطانية في هندسة طريقة لاختراق أجهزة التلفزيون الذكية وتحويلها إلى أجهزة مراقبة لمالكيها وللمحيط الذي يكون كل منهم فيه.

وهذا كله يعني باختصار أنّ الأمن السيبراني أصبح هما كبيراً اليوم، سواء لأصحاب البيانات من أشخاص ومؤسسات ودول تؤرقهم الخشية على بياناتهم وسلامتها، وأيضًا للعاملين على قرصنتها، من جهات رسميّة ومن قراصنة ومن إرهابيّين.

1. وجوه وقِوى

الواقع أنّ الأمر لم يقتصر على الاهتمام بالأمن الإلكتروني في بُعدِه التقني وحسب، بل تجاوزه إلى أبعاد أخرى كثيرة؛ منها الثقافية والاجتماعية والاقتصادية والعسكرية وغيرها، مع التركيز على أنّ الاستخدام غير السلمي للفضاء الإلكتروني يؤثر بالضرورة على الأمن العالمي، وعلى سلامة البشرية ورخائها الاقتصادي واستقرارها الاجتماعي في جميع الدول التي أصبحت تعتمد على البنية التحتية الكونية للمعلومات في سبيل تسيير جميع أمورها الحياتية المختلفة وعلى الصعد كافة، في حين أنّ أيّ إضرار أو تجاوز للحقوق في ميادين الفضاء السيبراني يمكن أن يشكل تهديدًا مخيفا لكلّ من يتأثر به، وربما للبشرية برمّتها.

وينبغي الإشارة هنا إلى أنّ تصاعد دور المؤثرين والفاعلين من غير الدول في مجالات العلاقات الدولية، قد أثر بدوره على سيادة

الـدول، وبخاصـة مع بروز دور الشـركات التكنولوجيـة العابرة للحـدود الوطنيّـة. وتضاعف هذا النوع من الأخطار مع بروز ظاهرة القرصـنة والجريمـة الإلكترونيّـة والجماعات الإرهابيـة. كلّ هـذه التحـدّيات جعلت من المحافظة على أمن البنى المعلوماتية في الفضاء السـيبراني ضرورة حيويـة لا يمكن إغفالها ولا التساهل فيها من قبل جميع المعنيين وأصـحاب المصـلحة من حكومات، ومجتمع مدني، وشـركات، وقطاعات أكاديمية وتقنية وتصنيعية وعسكرية، ومختلف مؤسسات ومصالح القطاع الخاص.

كذلك يتطلب توفير الحماية الفضـلى لشـبكات المعلومات ومنع احتمالات اختراقها في البلاد عامة، ولا سيما تلك التي تحتوي معلومات سرية تخص أصـحابها في مختلف القطاعات العامة والخاصة، وتحصـينها أمام عمليات التعطيل والهجمات الإلكترونية واعتداءات قراصنة المعلومات (الهاكرز – Hackers)، والحمايـة من الجريمة الإلكترونيّة، ومن تهديدات الفيروسات التي تهدّد سـلامة الأجهزة الإلكترونية ال– سوفت وير وسياقات عملها.

فقد ثبت بشكل لا عودة فيه أنّ الأمن السيبراني هو جزء حيويّ بالغ الأهميّة من الأمن الجماعي للمجتمع البشريّ.

ص: 105

2. ثورة الاتّصالات

الملاحظ أنّه غالبًا ما يمرّ تطور المجتمعات البشـرية وتاريخها بمنعطفات تاريخيّـة تحـدّدها الثورات في العلوم والتكنولوجيا وتطور وسائل الإنتاج المتاحـة، وانعكاساتها على البنى الفوقيـة للمجتمع، منذ الثورات التي شـكلت الدول الأولى في التاريخ في مصـر والعراق والصـين واليونان إلى الثورة الصناعية وانعكاساتها على مختلف الأصعدة الاجتماعية والثقافية والأخلاقية والفلسفية وحتّى شكل السلطة وطبيعتها.

وكامتـداد لهـذه المنعطفات الحادّة في التاريـخ، فإنّنا الآن نعيش ثورة جديـدة في تطوير وسائل الإنتاج والاتصال. فالكومبيوتر أصـبح يمثل الآن لعقولنا ما مثلته الآلة البخارية لعضلات أسلافنا فمنذ صنع أوّل جهاز كومبيوتر كان الهدف منه تحقيق سرعة أكبر من عقولنا البشرية في إجراء العمليات الحسابيـة المعقدة، وبدقة أكبر، من دون انحيازات أو تشـتت، وهو ما تحقق وتجاوزه العلماء في العقود الأخيرة، بما سـمح للمسـتخدم العادي أن يمتلك قدرات هائلة عبر حاسوبه الشخصي. وقد تضاعفت إمكانيات التواصل ملايين المرات بفضل شبكة الإنترنت التي بدورها تطورت من اسـتخدامات عسـكرية وأكاديمية إلى اسـتخدامات اجتماعية شاملة، فربطت معظم سـكان الأرض بعضهم ببعض بشـكل لم يشـهده التاريخ من قبل وزادت قدرات الشـبكة على تخزين المعلومات واسترجاعها وتحليلها وإيصالها بسرعة تصل إلى سرعة الضوء، وفي الوقت ذاته تطوّرت الأدوات المستخدمة سواء في الأعمال أم في الاستخدامات

الشخصيّة بشكل متسارع، وتوفّرت الأدوات الكافية لمستخدم واحد ليصبح بوسعه شنّ هجمات معقدة على أكبر الشبكات، باستخدام برمجيات ذات واجهات سهلة الاستخدام.

في بدايات القرن العشرين شهد العالم سباقا محمومًا للتسلّح بين العديد من القوى الدولية التقليدية والصاعدة والذي أدّى – من بين أسباب أخرى – إلى اندلاع الحرب العالمية الأولى واستخدام آليات وتكتيكات جديدة فى مجالات الحروب، وما أدّت إليه من تغير في الخريطة السياسية (والجغرافية) العالميّة، الأمر المشابه كثيراً لما يشهده العالم حاليًا من سباق تسلّح من نوع آخر في مجال جديد هو مجال الحروب السيبرانية، بما يشوبه من غموض وإبهام، ممّا شبهه اللواء كيث ألكسندر المدير السابق لوكالة الأمن القومى الأميركيّة بمحاولة الجيوش في الفترة بين الحربين العالميتين فهم دور سلاح الطيران في الحروب.

3. أخطار معلوماتيّة

كثيرة هي الأنشطة السيبرانية. ولعلّ في طليعتها الحيلولة دون تمكن الجهة (فردا) أو شركة أو جهازاً رسميًا من استخدام مواردها وبرمجياتها والتجهيزات المعلوماتية التي تتمتّع بها، ما يؤدي ويؤدّي إلى انهيار النظام الذي تعمل عليه، ومنعها من الاستفادة منه.

الاحتمالات غير الإيجابية التي يمكن أن تشهدها يلي ذلك خطر التسلسل والاختراق Intrusion Attack وهو

(1)

1- https://www.rsaconference.com/blogs/network-intrusion-methods- of-attack.

دخول طرف غير مصرّح له إلى الأنظمة والموارد المعلوماتية، والتحكّم بها أو استغلالها للهجوم على موارد وأنظمة أخرى. وفي حالات غير قليلة يعمد الدخيل إلى سرقة المعلومات للتصرف بها، مُستفيدًا من ثغرات في برامج الحماية. كذلك بإمكان القرصان استخدام وسائل برمجيّة متنوّعة بما فيها فيروسات مُعدّة خصيصًا لاختراق الحسابات المحمية.

وهذا كله يتطلّب رفع عتبة برامج الحماية لتحقيق أكبر قدر من الأمن للمعلومات والحيلولة دون قرصنتها.

وبموجب ذلك غدا مفهوم الأمن السيبراني Cyber security أحد أهمّ مفاهيم الحقبة الراهنة، وما سوف يلي، لا سيّما أنّ الغد ربما يشهد "حروبًا إلكترونية" تحلّ محلّ الحروب التقليدية، لتصل إلى ذات مداها في الخسائر المادية، وربما تتعدّاه. وهذا ما حدا بالخبراء المعنيين للعمل ما أمكن على تحديد أبرز تحدّيات الأمن السيبراني وتأثيرات الحروب السيبرانية، بما في ذلك استغلال الجماعات الإرهابية لتكنولوجيا المعلومات الجديدة، وتطويعها لصالح أنشطتهم المدمرة.

أنّه في طليعة المفاهيم الأساسية التي يقوم عليها الواقع الأمن السيبراني، لابدّ أن يكون سيادة الدولة" على فضاء البلد الإلكتروني، وهذه السيادة، كما هو معروف، تواجه تحديات كثيرة ومتجدّدة تنبع من جزالة وتنوّع الأنشطة عبر الإنترنت، التي يمكن ممارستها وتوجيهها عبر جميع أنحاء العالم بشكل غير منضبط، من دون وجود إطار واضح لمساءلة الأفراد القائمين على هذه الأنشطة.

ص: 108

كذلك يصعب في الفضاء الإلكتروني تمييز مبدأ الحرب العادلة"، كما في الأنشطة المدنيّة والسياسية والعسكرية.

إلى ذلك فإنه بإمكان الإرهابي وقرصان الكومبيوتر والمجرم، وكذلك الحكومة على حدّ سواء، الاستفادة من نقاط الضعف البشرية والتقنية للوصول إلى المعلومات في أجهزة الكمبيوتر الأخرى، التي تعتبر معادية أو منافسة، والقيام بهجمات سيبرانية عليها. وينبغي الاعتراف بأن الخطأ البشري هو جزء رئيسي من اختراق أنظمة الأمن السيبراني، كما أنّ الخطأ الفردي يمكن أن يكون كافيًا لمنح فرص الوصول إلى شبكات بأكملها، بما في ذلك الحكومية والصناعية، والعسكرية، وكلّ شبكة أخرى. هذا في حين يصعب تتبع آثار وأصول مطور البرمجيات الخبيثة أو الذي قام بالهجوم الإلكتروني والكشف عن هويّته.

4. الجريمة الافتراضيّة

من الضروري جعل الأمن السيبراني سدا منيعا في وجه التحديات والقرصنة الإلكترونية التي تواجهها دول العالم. ولابدّ أن تضمن جميع القطاعات سواء الحكومية أو الخاصة، حماية عالية للبيانات والمقدّرات المهمة في البنية التحتية لتكنولوجيا المعلومات، واستقطاب الكفاءات العلمية الوطنية والأجنبيّة المميّزة للاستفادة من مؤهلاتها وخبراتها، فضلاً عن مواصلة تأهيلها، بتحديث معلوماتها، وتشديد تمكينها في ميدان الأمن السيبرانيّ، وإيجاد وتفعيل الشراكات مع الجهات البحثية والأكاديمية والصناعية العامة والخاصة، والتشجيع على الابتكار والاستثمار في مجال الأمن السيبرانيّ، سعيًا للوصول إلى نهضة تقنية تخدم الاقتصاد الوطنيّ.

فالجريمة لم تعد اليوم مختصة بوقوعها على الأرض في العالم الواقعي الملموس، وإنما هناك جرائم يمكن اقترافها في الفضاء الافتراضي الذي يجري الاتصال به من خلال شبكة الإنترنت. ومن خلال ذلك يمكن اقتحام المعلومات المحمية من خلال كسر حمايتها وسحب المعلومات منها والسيطرة عليها والتصرّف بها. والفضاء المفتوح أنتج صعوبة في اكتشاف مرتكبي الجرائم، مما يتطلب وجود مختصين إلكترونيّين لمتابعة هذه الجرائم والعمل على تحديد مرتكبيها. وبينت الأبحاث الخاصة أنّ الضحايا لا يعلمون أنّهم تعرّضوا الخروقات أمنيّة لمدّة ثلاثة أشهر تقريبًا من بداية الهجوم الأولي، لذلك ينبغي على الحكومات أن تضطلع بدورها كمسؤول رئيسي عن الأمن السيبراني، وأن تضع المعايير والسياسات والحوافز والمبادرات، الهادفة إلى تبادل المعلومات الخاصة بالتهديدات. فالخطر السيبراني يهدّد الجميع، والكل مستهدف من العامل الذي ينتظر حوالة راتبه، إلى القائد الذي يدير حروبًا طاحنة للدفاع عن بلده. وتُقدّر دراسات تناقلتها الصحافة عن مجلة أميركية(1) أنّ تكلفة الهجمات السيبرانية على الشركات سوف تتجاوز ال- 2 تريليون دولار في العام 2019. وأعلنت المجلة إيّاها كذلك أن سوق الأمن السيبراني العالمي سيصل إلى 170 مليار دولار(2) بحلول العام 2020.

1- https://www.forbesmiddleeast.com.

2- المصدر السابق.

5. معايير الأمن

يحدّد المؤشر العالمي للأمن السيبراني، حالة الأمن السيبراني لكلّ بلد بالاعتماد على خمسة معايير؛ هي: الإمكانات التقنية، والتنظيمية، والقانونية والتعاون وإمكانات النمو. وأظهرت نتائج بحث جرى في هذا الصدد أنّ سنغافورة جاءت في المرتبة الأولى قائمة أفضل عشر دول في ما يتعلّق بمستويات الالتزام بالأمن السيبراني، واحتلت الولايات المتحدة المركز الثاني، بينما جاءت ماليزيا في المركز الثالث.

وأشار تقرير صادر عن الأمم المتحدة إلى أنّ الأمن السيبراني بات جزءا متزايد الأهمّيّة في حياتنا اليوم، وأن درجة الترابط بين الشبكات تعني أن أي شيء وكلّ شيء يمكن أن يتعرض للهجمات السيبرانية، ما يرفع من أهمّيّة وخطورة الأمن السيبراني، وضرورة الاهتمام بتطويره باستمرار.

فالعالم السيبراني هو نطاق افتراضي باتت تقوم عليه حضارة الإنسان اليوم وفي المستقبل المنظور على الأقلّ، بكلّ تفاصيلها وجُزئيّاتها وعموم فصولها. والمشكلة المحرجة هي أن لا غنى للعالم (في تقدّمه وتطوّره عن السيبرانية والفضاء السيبراني. فمن هذا النطاق ينفذ العالم إلى ميادين المزيد من التقدم والتطوّر وتعزيز الإنتاج وتعميم الرفاهية. ومن هذا النطاق ذاته أيضًا تهب ريح السموم ومخاطر الاقتحامات والاجتياحات الإلكترونية المعيقة والمكلفة والمدمّرة. لذلك، حري بنا من باب أولى أن نتذكر أن هذه

الخُرافة الحقيقية التي أسـميناها العالم السـيبراني، هي في آن واحد معًا، خشـبة الإنقاذ واللّغم المدمّر . والعبرة، هي في مدى إمكانية الذكاء البشري والسليقة الإنسانية النجاح في حفظ أمن المجال السيبراني والمحافظة عليه أمينًا وسليمًا بكلّ ما فيه.

والعلوم السـيبرانية بما فيها من أنظمة وما تتيحه من إمكانات، يستحيل حصرها أو الإحاطة بها، لأنّها تشمل جملة الحياة برمتها. هذه العلوم تشـكّل القوة الحقيقية والأساسية للإنسان اليوم، بما هو مجموعة صغيرة أو كبيرة... وبالطبع، فإنّ توافر معلومات الجهة المعنيّة ضمن الفضاء الإلكتروني هو ما يسـمح لهذه الجهة بتنفيذ ما ينبغي عليها تنفيذه من أعمال ومهام وخدمات، وبالكميات المطلوبة، وبالسرعات المناسبة، ويتيح لها مقومات القوة والسـيطرة بالتالي إلى حد ما، على مصـيرها. وهذا هو التجلي الأعلى لمفهوم القوّة. فطالما تسير الأمور على هدي هـذه المعلومات المحفوظـة والمحمية والتي هي لصالح الجهة صاحبتها، يكون العمل منتظما ومنتجًا وناجحًا كما يريد له المبرمجون. أما إذا استطاع طرف آخر اقتحامها والاستحواذ عليها وتسخيرها لمصلحته على حساب الجهة المالكة لها)، فعندها يحصل ما هو أسوأ من أسوأ الكوابيس. وهذا ما سوف يلي استعراضه في باب القوة والسيادة والسيطرة».

وهنا تظهر المشـكلة الكبيرة في أوضح تجلياتها المحيرة بشـكل بالغ الإحراج. فالتواجد في الفضاء السيبراني هو ضرورة حيوية لا غنى عنها البتة) هذا العصر ومستقبله المنظور على الأقل. ومن يختار الخروج أو تجميد تواجده ضمن هذا الفضاء، إنما يحكم على

مقـدّراته وكلّ ما يتصل بـدورة حياته وإنتاجه بالاختناق والغرق خلال ساعات قليلة لا أكثر، من دون توافر أي سبيل نجاة أو اسـتنقاذ. وربما تكون مقارنة من يختار الخروج من الفضاء السـيبراني بمن اختار العودة من وادي السيليكون في القرن الواحد والعشرين، إلى عصر الإنسان الأوّل (هوموس نيانـدرتاليس)، حيث لا صـناعة ولا زراعـة ولا إنتاج ولا مجتمع وحيث لا أسـلحة ولا بيوت ولا طاقـة ولا سـلاح، وحيث ستكون مواجهة الماموث العملاق والديناصورات المفترسة أحد أبسط الأخطار المحدقةبه.

ينبغي أن نتـذكر دائمًا أنّ محتويات الفضاء الإلكتروني ليست بالأمر العادي أو البسـيط، إذ هي عادة إجمالي الثروة الحيوية للجهة المخزنة (ولنفترض أنّها الدولـة في هـذه الحال. فالإدارة العامة لأي دولة، بما هي رئاسات ومجالس وإدارات وقطاعات وأجهزة، ينظمها كم هائل من الوثـائق واللوائـح والجـداول والتوجيهـات والقرارات والإلزامـات والممنوعـات... ممـا يحتاج لو تطلب الأمر توثيقه كتابـةً على الورق، إلى مليـارات الأطنـان من الكراريس والمجلـدات والمحفوظـات ومـا إلى ذلك، إلا أنّ توفير ذلك الكمّ الهائل من العمل وتيسـيره على شاشـة حاسوب، وما يتطلبه من جهود، متخصـصة جبّارة وكثيفة وطويلة الأمد، من أجل تخزينه فى الفضاء الإلكتروني، وحمايته وتوفيره لأصحابه، مثل حالة تقدّم مُشـرقة وعظيمة للذكاء البشـري، ويسـر الأعمال والجهود من الرؤساء إلى المرؤوسـين في جميع الأنحاء، واختصـر بشكل أخاذ دورات العمل في جميع أماكن العمل، وأتاح رقابة لصيقة ودقيقة

ص: 113

من قِبل الحواسيب (والتي لا تُخطئ... مبدئيًا)، فانتظمت الأعمال وتيسرت، وباتت أكثر إنتاجيّة بأضعاف مضاعفة. وهذا الإنجاز الفريد والعظيم والهائل والذي لا يمكن إيفاؤه حقه من المديح، يحتاج أكثر ما يحتاج إلى أن يكون محميا ومضمونا ومتيسرًا على الدوام.

من هنا يبدو واضحًا أنّ مصدر القوة الاستثنائية هذا هو ذاته ما يمكن أن يكون نقطة الضعف الخطيرة لصاحبها، وربما مقتله أيضًا. يحصل ذلك إذا تمكن عدوّ أو خصم أو منافس أو حتى شريك من اقتحام معلومات طرف آخر (شخص أو شركة أو دولة مخزنة في الفضاء الإلكتروني، والاطلاع عليها (أي على خصوصيات صاحبها وأسراره ونقاط قوته وضعفه ...) ، وخطورة إباحة المعلومات تكمن في أن يستفيد منها غير صاحبها وعلى حساب هذا الأخير؛ فالأخطار اللاحقة يمكنها أن تكون أدهى وأشدّ. وقد يقوم المتسلّل إلى المعلومات التي اخترق برامج حمايتها، بحبس هذه المعلومات بحيث يستحيل على صاحبها بلوغها، وقد يقوم باستغلالها ضدّ مصالح ،صاحبها، وقد يبتزه على أساسها، وقد.. وقد.... وكلّ ذلك يؤدّي إلى نقل مقوّمات القوة والسيطرة إلى الطرف الذي حصل على المعلومات وحبسها عن الطرف الذي يمتلكها. إنّ استحواذ طرف «غريب على معلومات طرف آخر هو بمثابة تجريد لهذا الطرف الآخر من مقوّمات معرفته وتنظيمه وقواه فكيف بالحري سيكون وضعه إذا ما استخدمت هذه المعلومات ضده؟

من الطبيعي أن تتضـمّن كيفيّات العمل على تحقيق الأمن السـيبراني، أصولاً ومبادئ كثيرة وصارمـة في معظمها، يصـعب (والمفروض أن يُقال يستحيل) تهديد أمنها وسلامتها.

ذلك أنّ مفهوم الأمن السـيبراني هو أحـد أهم مفاهيم الحقبـة الحالية والقادمة أيضًا، التي ربما تشـهد حروبًا إلكترونية" تحلّ محلّ الحروب التقليديـة، لتصـل إلى مـداها في ميادين إنزال الخسائر المادّيّة كما الحروب بالقنابل والصواريـخ، وربما تتعـدّى ذلك بكثير بل إن هـذا هو الأرجح.

هـذا الهـمّ شـغل رؤوس كثيرين من المتخصصـين كمـا من المسؤولين في الغرب والشـرق، وجرى نشـر العديـد من الـدراسات والأبحاث والكتب بهذا الخصوص، حيث جرت الإحاطة بكل ما يمكن من أسس وتفاصيل هذا الموضوع. وبفضل هذا الحماس الاستثنائي للإضاءة على أهمية الأمن السـيبراني وضـرورة الحفاظ ،عليه جرى استعراض أبرز التحدّيات الماثلة، وتصاعد وتائر وتأثيرات الحروب السيبرانية، مع إضاءات مباشـرة على أنشـطة الجماعات الإرهابيـة في هـذا النطاق، وكيفيّات اسـتغلالها له، وتطويع ما أمكن من ميزاته في سبيل الأنشـطة الإرهابية المدمرة.

6.سيادة الدولة أوّلًا

انطلاقا من إطار الأمن الدولي التقليدي، تتمثل بداية التحديات بتحقيق السيادة الرسميّة للدولة، أي دولة وكل دولة، لتحقيق الأمن السيبراني ضمن نطاقها الوطني ومواجهة التحدّيات التي

تظهر أمامها في سياق الأنشطة التي تجري عبر الإنترنت. فمن الضروري إلزام كلّ مستخدمي النطاق السيبراني بحدود الانضباط التي تشرعها القوانين الضابطة للأنشطة الإلكترونية، مع وجود إطار واضح ومؤكد لمساءلة المتجاوزين أفراداً كانوا أم هيئات جماعية. والواقع أنّ بإمكان الجميع الاستفادة من نقاط القوة ونقاط الضعف التقنية والبشرية) الماثلة في الأطماع التي يزينها البعض" لأنفسهم، كما في عالم أجهزة الكومبيوتر بحدّ والتي هي أدوات التواصل مع الفضاء الإلكتروني ومندرجاته. ولا بد أن نأخذ بنظر الاعتبار أنّ الخطأ البشريّ هو جزء رئيسي من ميدان اختراق أنظمة الأمن السيبراني؛ فقد يمكن توريط أي تقني ما، بفتح مجال للاختراق إلى داخل النظام، من خلال إغرائه بالمال أو ما يعادله. كذلك يمكن للنظام بحدّ ذاته أن يحتوي على نقاط ضعف لا تبدو واضحة لأصحابه ومُشغليه بينما يتمكّن الأخصام من اكتشافها واستغلالها. ومن هنا يمكن اعتبار الأمن السيبراني كناية عن مجموعة من الأدوات التنظيمية والتقنية والإجرائية، والممارسات الهادفة إلى حماية الحواسيب والشبكات وما بداخلها من بيانات من الاختراقات أو التلف أو التغيير أو تعطل الوصول لما تختزنه من معلومات أو خدمات، ويُعدّ توجّها عالميًا سواء على مستوى الدول أم المنظمات الحكومية أم الشركات، وصولاً إلى الأشخاص العاملين على الشبكة.

ولسوء الحظ فإنّ التطوّر التقني الهائل الذي تحقق حتى الآن (وهو في تطوّر متواصل ، لم يكن لصالح الأمن السيبيري،

بـل جاء متوازيًا على الـدوام مع تطوّر مماثل في ميادين الجريمـة الإلكترونيـة. وبالتالي فقـد تصاعـد التهديـد الأمني السـيبراني من خلال اسـتغلال محتويات الفضاء السـيبراني جراء كسـر حمايتها واقتحامها واسـتغلالها. وهذا يتطلّب يقظة ومتابعة ملاحقة مستمرة على الصعد التقنية والبشرية والقانونية والإجرائية والتخطيطية والتعليمية والتدريبية كافّة. فما يحدث ليس سوى صراع عقول لا بد أن يتواصل مستقبلاً؛ لذا فإنّ التقـديرات تشـير إلى أنّ الإنفاق على أمن الشـبكات الإلكترونية في دول مجلس التعاون الخليجي وحدها على سبيل المثال، يمكن أن يصل إلى أكثر من مليار دولار في العام (2018).

وبكلمات أخرى، فالأمن السيبراني يشكل مجموع الأطر القانونية ،والتنظيميّة، والهياكل التنظيمية ذاتها وإجراءات سير العمل، بالإضافة إلى الوسائل التقنيـة والتكنولوجيـة والتي تمثل الجهود المشتركـة للقطاعين الخاص والعام على المسـتوى المحلي الشامل كما على المسـتوى العالمي الواسع، والتي تهـدف إلى حمايـة الفضاء السـيبراني الوطني، مع التركيز على ضـمان توافر أنظمة المعلومات، وتمتين الخصوصـية وحمايـة سـرّية المعلومات الشخصـية، واتخاذ جميع الإجراءات الضـرورية لحمايـة المواطنين والمسـتهلكين من المخاطر التي يمكن أن يحملها الفضاء السيبراني.

ولا بدّ من الملاحظة أنّ صلاحيّة الأمن السيبراني الوطني تعتمد على ركائز أساسيّة عديدة ومتنوّعة يمكن إجمالها كما يلي:

تدبير وتطوير استراتيجية وطنيّة لتحقيق الأمن السيبراني وحماية البنية التحتيّة للمعلومات عمومًا ، ولا سيما الحساسة منها.

إقامة ورعاية تعاون وطني متكامل بين الحكومة ومجتمع صناعة الاتصالات والمعلومات، بما في ذلك استقطاب الخبراء المميزين والضالعين في مجالات الاختراق والصدّ. وهذا ما شمل العمل على استقبال القراصنة المرتدّين والتائبين المستعدين لوضع خبراتهم فى الأمكنة المناسبة مقابل بدل مادّيّ.

العمل بكل الوسائل والسُّبُل على ردع الجريمة السيبرانية ومطاردة المرتكبين بأساليبهم ذاتها لتشخيص هوياتهم والسعي بالتالي إلى محاسبتهم أمام القانون.

إيجاد قدرات وطنيّة عالية والعمل على تواصل تجديدها وتطويرها لإدارة حوادث الحاسب الآلي على اختلافها والعمل على معالجتها.

تشجيع تنافس حقيقي واسع على المستوى الوطني في ميادين تحقيق الأمن السيبراني وإدامته وتطويره.

7. فكرة قديمة ... جديدة

ليس جديدا طرح مفهوم الأمن السيبراني في النقاشات البحثية، ولكنّه يُبرز في بعض الأحيان ارتباطا بأحداث ووقائع ذات صلة بهذا المجال. وقد عاد هذا المستوى من الأمن إلى الواجهة الإعلامية فى الآونة الأخيرة على خلفية انتشار «فيروس الفدية والذي اشتهر

عالميًا بسرعة قياسيّة، وتسبّب في خسائر مادية قدرت بمليارات الدولارات. وبحسب تقديرات شركة ميكروسوفت» فإنّ الهجوم الإلكتروني لفيروس الفدية) قد ضرب نحو 150 دولة حول العالم حيث سيطر هذا على ملفّات المستخدمين وحجبها، وطالبهم بدفع فدية لاستعادة المقدرة على الدخول إليها مجدّدًا.

ولا شكّ أنّ فكرة اختراق شبكات المعلومات، والسطو على البيانات، و ضرب القطاعات الخدماتية، والعمل على شلّ حركة الاقتصادات من خلال هجمات إلكترونيّة، هي فكرة قديمة يتداولها خبراء المعلوماتية في العالم خلال العقدين الأخيرين بكثافة. ولكنّ التطور الحاصل في هذا القطاع يجعل البحث عن فكرة الأمن الكامل للإنترنت مثل لهاث الانسان وراء ظلّه.

وحسب وكالة الاستخبارات الأميركية «سي. آي. إي.»، فإنّ الولايات المتحدة، على سبيل المثال، هي الدولة الأكثر تعرّضًا لخطر التهديد السيبراني في العالم، وبالتالي فإنّ التهديد الأكثر تحدّيًا الذي تواجهه الولايات المتحدة يأتي من الفضاء الإلكتروني قبل أي جهة أخرى. وهذا التطوّر في مصادر الخطر والتهديد يفسّر الزيادات الهائلة في حجم سوق الأمن السيبراني، الذي يبلغ بحسب إحصاءات العام ، 2017، أكثر من 120 مليار دولار، محققا زيادات بلغت نحو 13 ضعفًا على مدى السنوات ال- 13 الماضية. وتشير الأرقام التي جرى إعلانها إلى أنّ كلفة الهجمات الإلكترونية على مستوى العالم في مطلع العام 2017 بلغت حوالي 300 مليار دولار، مع التأكيد على أنّه رقم على ارتفاع. ومن أبرز

أسباب ذلك تصنيع نحو 315 مليون فيروس خبيث وبرامج مدمّرة (كما بينت إحصاءات العام الماضي (2016) . ولا شكّ أنّ مؤشرات هذا التهديد تنطبق أكثر ما تنطبق على دول عربيّة غنيّة بذاتها، بعد أن حققت تقدّمًا ملموسًا على الصعيد التقني.

وقال القائم بأعمال مساعد وزير الدفاع للعمليات الخاصة مارك ميتشل ، إنّه مع فقدان التنظيم الإرهابي «داعش»، للأراضي، فسيزيد اعتماده على وسائل الاتّصال الافتراضيّ.

وقال «رون جونسون رئيس لجنة الأمن الداخلي والشؤون الحكوميّة بمجلس الشيوخ: هذه هي الخلافة الجديدة – في الفضاء الإلكتروني.

وهنا لابدّ من بعض الملاحظات السريعة؛ منها :

بات واضحًا أنّ العمل على إنتاج برامج الحواسيب أو شرائها ليس مرتفع الكلفة (1)؛ ففي الوقت الذي يُكلف إصلاح الأضرار الماديّة الناشئة عن اختراق الحواسيب عشرات الملايين من الدولارات (أو) حتى آلاف ملايين الدولارات، فإنّ الكثير من الدول النامية لا تنفق إلا القليل في سبيل إنتاج هذه البرامج محليا، بل تستسهل شراءها من الأسواق، أي من حيث تكون عُرضة لكلّ أصناف التجسّس الإلكتروني، ما يُسهل عمل القراصنة وجواسيس المعلومات.

إنّ إبقاء برامج المعلوماتية الخبيثة أو المضرة (الفيروسات) ساكنة نائمة لفترة طويلة نسبيًا يُشكل تحديًا أكيدًا للحرب التقليدية (أي لحق اللجوء إلى الحرب بعد توجيه إنذار إلى العدوّ)، فهي لا تقوى عليه.

1- https://www.tech-wd.com.

بـالنظر إلى الأهميـة القصوى للمعلومـات، سواء بالنسـبة إلى أصـحابها- وهي ثروتهم ووسائـل حياتهم وقواهم وإنتاجهم، أو بالنسـبة إلى الآخرين من منافسـين ومضاربين وشـركاء وأخصام وأعداء... فإنّ فرض الأمن السـيبراني يُعتبر واحدة من أول وأهم وأبرز الحاجات الملحة لإنسان العصر.

ولاـ بـدّ من الإشـارة تكرارًا إلى أنْ لا قيمـة إيجابيـة للفضاء السـيبراني ولا فائـدة منه ولا جـدوى خارج إطار ضـمان شـروط ومقوّمات أمن المعلومات المختزنـة فيه، وإمكانيـة الوصول إليها من قبل أصـحابها دون الآخرين، وحمايتها من التلف أو السـرقة (القرصـنة) أو التبديل أو التعـديل أو التغيير أو الإنقـاص أو الزيادة، خلافًا لرغبـة أصـحابها الشـرعيين الـذين لهم وحـدهم الحق في بلوغها ومعالجتها بالطرق التي يختارونها. كـذلك، والمعنى أنّه لا بد من تحقيق ورعاية متطلبات الأمن في الفضاء السـيبراني، لتواصل أهميته وجدواه. فقد ثبت بشـكل لا عودة فيه أنّ الأمن السيبراني هو القوة الأساسية في عصر المعلومات، وأن تهديده أو استباحته تشكلان مطرقة الهدم الأكثر فعالية وتدميراً.

ص: 121

ص: 123

الفصل العاشر: الحرب السيبرانيّة

اشارة

أغرب ما في الحروب السيبرانية أنّها حروب وهميّة، بمعنى أنّها تتم في العالم الافتراضي، إلا أن خسائرها تكون حقيقيّة.

1. الماهية

يجري تعريف الحروب السيبرانية بأنّها أشكال المواجهات والصراع في سبيل الأهداف السياسية أو الاقتصادية أو العسكرية، ممّا ينشب أو يجري شنّه داخل البيئة الافتراضية التي هي الفضاء السيبرانيّ، حيث يجري اختزان أهم وأخطر ثروات الدولة؛ وهي معلوماتها التفصيلية في جميع المناحي والشؤون هذا المستوى من الحروب أصبح جزءًا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول وتدخل هذه الحرب من جميع الأبواب، حيث يحاول القادرون تكنولوجيا إخضاع الطرف الذي يرون مصلحتهم في إخضاعه، أو ربما في قهره وتحطيمه، وذلك من خلال العبث بجدائل المعلومات العائدة له.

ومجال الحرب الإلكترونيّة يقدّم ميّزات عديدة: فهي حرب غير تقليدية وغير مكلفة وجميع المزايا تصبّ منذ البداية في الجانب الهجومي.

علاوة على ذلك، ليس هناك رادع فاعل في الحرب الإلكترونية، لأنّ تحديد المهاجم عمليّة صعبة جدا، وفيها يكون الالتزام بالقانون الدولي مستحيلاً تقريبًا. وفي ظلّ هذه الظروف، قد يكون أي شكل

أشكال الردّ العسكري مشكلة كبيرة جدًا، من الناحية القانونية والسياسية.

لكن بـدلاً من الحـديث عن الحرب الإلكترونيـة كحرب في حـدّ ذاتها – يتم وصف الهجمات الإلكترونية الأولى باعتبارها «عملية تسـلّل رقمي أو هجمات 9/11 في العالم الإلكتروني – وهو وصف مناسب إلى حـدّ كبير للحديث عن الهجمات الإلكترونية كوسـيلة من وسائل الحرب. إنّ مخاطر الهجمات الإلكترونيـة حقيقيـة وتتطوّر أكثر فأكثر. في نفس الوقت ليس هناك من داع للخوف، لأنّ هـذه التهديدات في المستقبل القريب لن يكون من السهل التنبؤ

بها أو السيطرة عليها تمامًا وتحويلها ضد مصلحته .؟

مسـرح هذه الحرب يكون إذا ضـمن مخازن المعلومات في الفضاء الإلكتروني، حيث يسـعى المتحاربون إلى تعطيل الانتظام المعلوماتي لمختلف البرامج التي تضـبط حركة الإدارة، إدارة الجهة المُسـتهدفة، بمختلف مسـتوياتها وتفاصـيلها، والسـعي إلى التحكم بها والسـيطرة عليها، بما يُؤدّي إلى التسلّط على مقدّرات الخصم وإخضاعه وتحقيق السيادة عليه. ومن زاوية أخرى مختلفة، فإنّ جيوش الحرب السيبرانية وآلياتهـا وأعتـدتها هي وسائـل وأسـاليب القتال في الفضاء الإلكتروني والتي ترقى بالمنازلات والمواجهات إلى مسـتوى النزاع المسـلّح أو تُجرى في سـياقه. فالعمليات السـيبرانية سواء أكانت دفاعية أم هجومية، يمكن أن تسـبب خسائر هائلة وأضـرارًا فادحة كما يمكن أن تتسبّب بسقوط إصابات أو وفيات بشرية،فضلاً عن إلحاق الأضرار بالأدوات والآلات والأجهزة، وصولاً

إلى تعطيل عملها أو تدميرها، ما يُفضي إلى إلحاق أضرار منهجيّة يمكن أن تكون فادحة لمختلف نُظم التشغيل والتغذية والتزويد، ما يمكنه أن يعطّل دورة حياة شعب بأكمله، ويعرّضه ومصالحه الحيوية والأساسيّة لضربات قاصمة. فعندما تتعرّض الحواسيب أو الشبكات المعلوماتية التابعة لدولة ما لهجوم أو اختراق أو إعاقة، فهذا يضع الناس عمومًا في هذه الدولة (وليس الجيوش والقوى العسكرية وحدها) في حالات عمى معلوماتي» يتسبّب في تعطل ما يمكن تسميته آلة «المدينة»، أي كلّ الأنظمة والأجهزة التي تعمل فيها، الأمر الذي يتسبّب في حالات عوز في متطلبات الحياة اليومية البسيطة، من ماء وغذاء وطاقة ورعاية طبّيّة، وما يتجاوز ذلك من حالات تعطيل وإعاقة مختلف المرافق والمؤسّسات والإدارات، مع تعريض العامة لمخاطر حرمانهم الحاجات الأساسية للحياة ، إلى ما هنالك من إشكاليات بالغة الإضرار والخطورة.

2. أشكال الاشتباك السيبراني

على الرغم من اتساع آفاق هذا التعريف إلا أنّ بعض الخبراء يعتبرونه غير كاف للدلالة على أشكال الاشتباك السيبراني وصراعاته كافّة؛ فهو برأي كثيرين يُغفل العامل الأهمّ في أمن المعلومات،وهو العامل البشري والنفسي.

ومن هذه الخصوصية المتعدّدة والمركبة، تصاعدت الأهمية الخطيرة للحرب السيبرانية لبلوغ إمكانات التغلغل والتلاعب وبثّ الفوضى والتسلّل والتصيّد والاختراق، والإخفاء والمراقبة

والتجسس، والتشويه والتضليل والخداع، والحرمان والاستباق، والتجاوز الجغرافي والمادي، وصولاً إلى التملك والاستحواذ أو السيطرة والتحكّم وفرض السيادة. هذه الفعاليات هي ما يشكل حقيقةً ديناميات الحرب السيبرانية، اعتمادًا على السيطرة والتحكّم واسع النطاق في الفضاء السيبراني، والاستئثار بكل تطوّرات التقنية المستمرة، وبما يحقق للطرف الذي ينتصر في الحروب السيبرانية، الهيمنة على أخصامه وأعدائه وحتى منافسيه، ومختلف مقدراتهم.

إنّ ماهيّة وطبيعة الحرب السيبرانية وتطوّراتها وتطبيقاتها، ونفوذ هذه الحرب وتهديداتها اللامتناهية لا تقتصر على استهداف البنى المادّيّة وحماية الأرض والوطن، بل تسدّد مباشرة نحو البنية العقلية والمعرفية للطرف الآخر وهويته الوطنية، في سبيل طمس هذه الهوية وتفريغها من محتواها الإنساني وإمكاناتها الفاعلة. ويكون الهدف النهائي من كلّ ذلك، بعد تحقيق السيطرة والسيادة، تسخير الآخر وكلّ إمكاناته، حتى إذا نضب عصبه الحي، جرى العمل على تفكيك كيانه القومي الخاص وشطبه من دائرة الفعل.

ولقد تعرّضت ظاهرة الصراع إلى تغيرات مع بروز الفضاء الإلكتروني، كمجال تنشأ فيه نزاعات بين الفاعلين المختلفين، بخاصة مع الاعتماد الكثيف على تكنولوجيا الاتصال والمعلومات. وهنا، برز الصراع السيبراني كحالة من التعارض في المصالح والقيم بين الفاعلين، سواء أكانوا دولاً أم غير دول في الفضاء الإلكتروني.

وعلى الرغم من الآثار المدمرة لهذا النمط من الصراعات، فلا

يرافقه دماء، وقد يتضمن التجسّس والتسلّل إلى مواقع الخصوم الإلكترونية وقرصنتها، دون أنقاض أو غبار. كما أنّ أطرافه يتسمون بعدم الوضوح وتنطوي كذلك تداعياته على مخاطر عدّة على أمن الدول، سواء عن طريق التخريب، أو استخدام أسلحة الفضاء الإلكتروني المتعدّدة(1).

ومع انتشار الفضاء الإلكتروني، وسهولة الدخول إليه، اتسعت دائرة الصراعات السيبرانية، وزاد عدد المهاجمين، وباتت هناك حالة من الكرّ والفرّ في الهجمات الإلكترونية(2). ولذا، صار الصراع بين، الفاعلين المختلفين حول امتلاك أدوات الحماية والدفاع، وتطوير القدرات الهجومية الإلكترونية يستهدف حيازة القوّة، والتفوّق والهيمنة، وتعزيز التنافس حول السيطرة، والابتكار، والتحكّم في المعلومات، وتعظيم القدرات القادرة على زيادة النفوذ والتأثير في المستويين المحلي والدولي.

وبما أنّ المتنازعين يلجأون في الصراعات التقليدية إلى استخدام شتى أنواع أسلحة التدمير الممكنة، فقد انتقلت جبهات القتال بشكل مواز إلى ساحة الفضاء الإلكتروني(3). وكان لهذا التغيير دور

1- (تصفّح بتاريخ 2014/04/92 http:// wwwmiddle-east-online.com/id - 1?=131832.

2- الحرب الإلكترونيّة هي حرب رقميّة أسلحتها افتراضية (Virtual)، تهدف إلى الإضرار ببنية الخصم (أو العدوّ) الرقميّة أو إتلافها، كما تشمل هذه الحرب أيضًا التجسس على العدو.

3- راجع: د. محمد المجذوب، القانون الدولي العام ، الطبعة السادسة، منشورات الحلبي الحقوقية، بيروت، 2007، ص 403-559 وكذلك راجع ما كتبته صحيفة السفير اللبنانية حول لو كان الإنترنت دولة لكان أكبر خامس اقتصاد في العالم»، في 2012/03/21.

في إعادة التفكير في حركيّة وديناميكية الصـراع، بل وبروز ما يعرف ب– عصر «القوّة النسبيّة». وعنت هذه الأخيرة أنّ «القوّة العسكرية قد لا تكفي وحدها لتأمين البنية التحتية للدول، الأمر الذي يخلّف آثاراً استراتيجيّة هائلة على مستوى تركيبة وتوازنات النظام الدولي.

وأسهم عاملان رئيسيان في انتشار رقعة الصراع في الفضاء الإلكتروني،وبالتالي الإفساح في المجال لنشوء الحروب السيبرانية، وهما:

1 – تغير منظور الحرب جذريّا؛ حيث انتقلت من نسق الحروب بين الدول» إلى وسط الشـعوب، فكان الغرض من الحرب قديما هو تدمير الخصم ، إما باحتلال أرضه، أو الاستيلاء على موارده؛ أما الحروب الجديدة، فتستهدف بالأساس التحكّم في إرادة وخيارات المجتمعات.

مع هـذا التغير، أصـبحت أهـداف الحرب أقل ماديـة، وتركزت أكثر على العامل النفسـي والـدعائي، لا سـيّما مع تنامي التغطيـة الإخبارية والسـمعية والبصـرية المباشـرة للأحـداث لحظـة وقوعهـا عبر مواقع الإـنترنت والفضائيات، وضـعف سـيطرة أنظمـة الحكم على توجهات مواطنيها.

2– بروز الصـراعات ذات الأبعاد المحليّـة – الدوليـة؛ حيث ساعد اشـتعال الصـراعات الداخلية في مرحلة ما بعد الحرب الباردة، وكذلك طبيعة السـباق الدولي للفضاء الإلكتروني، في توفير بيئة مناسـبة لدمج الفئات والقوى المهمّشة في السـياسة الدولية، وخلق شبكة تحالفات مؤيّدة أو معارضة ذات نطاق دولي عريض، إمّا على أساس قيم حقوقية، أو انتماءات عرقية أو دينية.

ولقد أسهم الفضاء الإلكتروني في دعم الهياكل التنظيمية

والاتصالية للحركات والجماعات المحليّة، والمنظمات المدنية، بما ساعد الفاعلين من غير الدول على ممارسة قوّة التجنيد، ،والحشد ،والتعبئة واستجلاب التمويل.

3. من التكنولوجيا إلى الحرب

إنّ تطوّر المجتمعات البشرية وتاريخها غالبًا ما يمر بمنعطفات تاريخيّة تحدّدها القفزات العلمية والتكنولوجيّة وتطور وسائل الإنتاج الجديدة، وانعكاسات ذلك على البنى الاجتماعية والسياسية، على مختلف الأصعدة الاجتماعية والثقافية والأخلاقية والفلسفية، وحتى شكل السلطة وطبيعتها. ونحن اليوم نعيش ثورة جديدة في تطوير وسائل الإنتاج والاتصال، تقوم على العلوم السيبرانية وإنجازاتها الكبيرة والتي دخلت جميع مناحي الحياة من دون استثناء. ولعلّ الكومبيوتر أصبح يشكل الآن ما مثلته الآلة البخارية في مجال الثورة الصناعية الكبرى؛ فقد غير حياة الإنسان وقدراته ومتطلباته بشكل لم يكن ليتوقعه أحد، ونجح في تحقيق سرعة أكبر من سرعة عقولنا البشريّة في إجراء العمليّات الحسابية المعقدة، بدقة أكبر، ومن دون انحيازات أو تشتّت. ومع تطوّر الكومبيوتر واتساع إنتاجه، وبالتالي اتساع نطاق الاعتماد عليه من قبل الأفراد والجماعات والدول، فقد أتاح للمستخدم امتلاك قدرات هائلة. وهذا ما تضاعف بشكل نوعي وكمّيّ كذلك من خلال اتصال هذه الآلة عبر الفضاء الإلكتروني، بفضل شبكة الإنترنت والتي ربطت سكان الأرض في ما بينهم بشكل لم يشهده التاريخ من قبل. وما لبثت التطوّرات أن تواصلت فجعلت من الشبكة العنكبوتية وسيلة لتخزين المعلومات

في الفضاء الإلكتروني ومعالجتها وتحليلها، مع إمكانية استقبالها أو إرسالها بسرعة تصل إلى سرعة الضوء من نقطة على الكوكب إلى أيّ نقطة أخرى فيه تكون متصلة بالشبكة. وفي الوقت ذاته تطوّرت الأدوات المستخدمة سواء فى الأعمال أو الاستخدامات الشخصية والجماعيّة، فباتت كلّ حركات وسكنات المجتمع البشري مرتكزة على هذا الإنجاز الحضاري الكبير الذي لم تعد الحياة ممكنة من دونه. ومن هنا تحركت الأطماع البشرية لاستغلال هذا التقدّم التقني البارز، لخدمة أغراض أنانية تتصل بالشخص نفسه أو بالشركة أو بالدولة وكانت النتيجة دخول التقنيات السيبرانية في نصاب الحروب، حيث الآلات والأسلحة تعمل بإدارة وإشراف العلوم الإلكترونية، توخيا للدقة الفائقة والتأثير البليغ

4. المعرفة والقوّة

لابدّ من توضيح وتبسيط مفهوم الحرب الإلكترونيّة من خلال المقارنة مع مفهوم الحرب التقليدية المعروفة. فالحرب كلمة تُعبر عن مجموعة متنوّعة وهائلة من الظروف والسلوكيات التي تفضي إلى عمليات نزاع مسلّح بين القوى العسكرية لطرفين متقابلين أو أكثر. ومن الطبيعي أن تُحشد لهذه الحروب الجيوش والأسلحة والأعتدة والميزانيات. هكذا كان الأمر منذ القديم وحتى الأمس القريب، ولم تحدث تطوّرات أساسيّة إلا على مستوى السلاح والعتاد بشكل أوّلي.

لابدّ من لفت الاهتمام إلى أنه تحت تسمية الحرب السيبيرية، من المواجهات والمعارك: الأوّل هدفه اقتحام ثلاثة أنماط تندرج المعلومات ومحاولة التصرف بها في غير صالح أصحابها، بما في ذلك استخدامها ضدّ أصحابها، أو حبسها لقاء فدية أو تعديلها أو إلغائها نهائيا، لإلحاق أفدح الأضرار الممكنة بأصحابها. وهذا ما يدفع–عادة– أصحاب الحسابات المهمة في الفضاء الإلكتروني إلى الاحتفاظ بنُسخ إضافيّة عنها على حافظات إلكترونية – يو إس بي، USB.

أما الحرب السيبرانية الثانية فهي الحرب البديلة عن الحرب التقليدية، أو الملحقة بها.

وهذا ليس بالأمر المُعقد كما يبدو. فبدلاً فبدلاً من قصف العدوّ بأصناف الأسلحة النارية من صاروخية وسواها، يجري الدخول إلى البرامج التي تتحكّم بأسلحته إن أمكن)، وتعطيلها، فتتعطل فاعلية أسلحته المتصلة بها ، أو يمكن جعلها تركز قصفها على أهداف تابعة للجهة التي تمتلكها وأنواع التشويش على أنظمة الأسلحة باتت رائجة، وكان أحدث ما ذكر عنها التشويش الإلكتروني الذي اتهمت القوى السيبرانية الأميركية بتنفيذه ضدّ القوات السورية التي كانت احتلت البوكمال في المعركة الأولى، بحيث اضطرّ الجيش السوريّ وحلفاؤه إلى الانسحاب من المدينة التي عادت لسيطرة الطرف الآخر ... إلى أن أعيد فتحها من جديد.

أمّا الحرب الثالثة في هذا الإطار فهي المنازلة بين برامج

المعلومـات للمتخاصـمين، فيحـاول كـلّ طرف تعطيـل معلومـات الطرف الآـخر أو تزويرها أو منع الخصم من بلوغها، بحيث تتعطل مع حبسها، كلّ الأنشطة الحيوية للخصم.

والواقع أن الحرب السيبرانية، مثلها مثل الحرب التقليدية، يمكن تعريفها من خلال ثلاثة معالم رئيسيّة:

1- إنّها تمتلك فضاءً مستضيفًا لها هو الفضاء الإلكتروني، مثلما أنّ الحرب المادّيّة فضاؤها البرّ أو البحر أو الجوّ (وعادة الثلاثة معا).

2- إنّها تهدف إلى تحقيق مآرب سياسيّة محدّدة.

3 - الحرب السيبرانية دائمًا ما تمتلك وحدة عنف» أساسية.

والمعروف اليوم أنّ الولايات المتحـدة الأميركيـة تحاول الوصول بالحروب السـيبرانيّة إلى مسـتوى الحروب المادّيّة، من حيث طبيعة التأثير والنتائـج وبالتالي، فقد أصـبح هدف هذه الحرب من وجهة النظر الأميركية هو أن تحقق الهجمات السـيبرانية قدرا كبيرا من الدمار والضـرر المـادّيّ، أو على الأقل القـدر الكافي من التعطيل. وهنا لا غنى عن تسـليط الضوء على المفهوم الأميركي للتأثير أو الجـدوى المتوقعـة من الحرب الإلكترونيّـة. ولن نجـد أفضل من فيروس سـتوكس نت ليكون هو المثال المقصود، حيث أنّ هذا الفيروس تمكن عمليا من تحقيق الهدف (الإسرائيلي الأميركي) في تعطيل المفاعلات النووية الإيرانية التي جرى استهدافها، ما أدّى إلى تعطّلها وإخراجها من العمل.

ص: 133

ولو راجعنا الهجمات السيبرانية الأكثر شهرة على مستوى العالم والتي استهدفت مؤسسات عسكرية أو حكومية، يتضح أنها كانت تهدف بالأساس إلى الحصول على معلومات سرية، أو منع الحكومة من الولوج إلى مواقعها الإلكترونية، أو السيطرة عليها.

من خلال كلّ ذلك تصبح الحروب السيبرانية الحديثة من أخطر ما يهدّد سيادة الدول والأفراد ودورات حياة المجتمعات، حيث تستطيع أي دولة أو حتى خبير محترف أو «محتال إلكتروني قرصان» استغلال ثغرات ونقاط ضعف تقنيّة وتوجيه ضربات وهجمات إلكترونية إلى أيّ مكان في العالم، واستغلال المعلومات الحسّاسة والمهمة بأشكال مختلفة ضارّة وخطيرة، وذات تكلفة هائلة للطرف الذي يجري استهدافه بنجاح.

لذلك يُعتبر تأمين المعلومات والشبكات أكثر الطرق فعالية للحماية من الهجمات الإلكترونيّة. وثمة ضرورة متواصلة لتطبيق التحديثات الأمنية على الأنظمة المعتمدة كافة، بما فيها تلك التي لا تعتبر حسّاسة، وذلك لأنّ أيّ ثغرة في النظام يمكن استغلالها لشن هجمات والدخول إلى خزان المعلومات.

ص: 134

5. تهديد البُنى كافّة

ينبغي الأخـذ بنظر الاعتبار أنّ نفوذ هـذه الحرب وتهديـداتها اللامتناهيـة، لا تقتصـر على البنى المادية وحماية الأرض والوطن، بل تتمدد لتبلغ البنى المعرفيـة وحتى العقليـة، وكذلك الهوية الوطنية والأمن الوطني والقومي، وتضـعف العمل على مواجهة التهديدات والمؤامرات التي تستهدف تفكيك وتفتيت الوطن وتضييع المواطن.

ومثلما حصل في بـدايات القرن العشـرين، حين شـهد العالم سـباق تسـلّح محموم بين العديـد من القوى الدوليـة التقليديـة والصاعدة في العالم، وأدّى من بين ما أدّى إليه، إلى انـدلاع الحرب العالميـة الأولى، ثمّة اليوم نوعًا من سـباق التسـلح المجنون، ليس في مجال التسـلّح التقليـدي أو النووي وما فوقه، بل هو سـباق من نوع آخر وفي مجال جديـد هو المجال السـيبراني، بكلّ ما يشوب هذا المجال من الغموض وعدم اليقين. وهنا تلفتني ملاحظة للجنرال الأميركي كيث ألكساندر المدير السابق لوكالة الأمن القومي الأميركي بأنّ ما يجري يشبه محاولة الجيوش في الفترة بين الحربين العالميتين لفهم دور سلاح الطيران في الحروب.

وستشـمل حروب المسـتقبل مجموعـة عالميـة من أصـحاب الأطماع أو الطموحات، ممّن سـيقاتلون في البحر وعلى اليابسـة وفي الهواء، وكـذلك في موقعين جديدين للصـراع هما : الفضاء الإلكتروني والفضاء الخارجي وسـيواجه قباطنة السـفن الحربية معارك مسـتقبلية تشـبه معركة بيرل هاربور وسيتبارز طيارو المقاتلات مع الطائرات

الشبح بدون طيّار، وسيخوضون معارك ضد قراصنة معلومات (هاكرز)، في سن المراهقة في ملاعب رقميّة. كذلك فإنّ أثرياء وادي السيليكون وسواه من أودية المال وجبالها، قد باشروا بالفعل الاستعداد والتعبئة للحرب السيبرانية، ومثلهم العصابات المنظمة والقتلة وأصحاب الجرائم المتسلسلة... الجميع يستعدون لتنفيذ عمليّاتهم القرصنيّة أو الانتقامية في مجالات الفضاء السيبراني وعلى الإنترنت. وفي النهاية، سيكون النصر حليف من يستطيع أن يجمع بين دروس الماضي وأسلحة المستقبل.

وبالفعل، فقد شهد العالم الرقمي ظهور مجموعات جديدة من التقنيات التي انتقلت للواقع اليومي في الآونة الأخيرة بعدما كانت تقتصر على مجال الخيال العلمي فحسب. ومن المرجح أن تكون أسلحة جديدة قد ظهرت، مما سوف يُستخدم في الحروب المستقبلية التي لن تشبه أي حرب عرفتها البشرية حتى اليوم. وبالطبع، فسوف يكون للإرهاب على ألوانه الوحشية جميعها، نصيب بارز من هذا المشهد المخيف والمستقبل المرعب الذي...

ربما كان ينتظر البشريّة، من دون آمال واسعة في ردّه أو تغييره ولا بدّ أن يشمل البرنامج كلاً من الحرب السيبرانية والحرب الفضائية، إلى أجيال حديثة من النظم والبرامج السيبرانية التي يمكن أن تعطّل القدرات القتالية لأحدث الجيوش وأفضلها تجهيزا. فالقاعدة ستكون هي ذاتها على الدوام: العلوم والتقنيات السيبرانية في تطوّر مستدام الدول تُصبح أقوى والإرهابيون كذلك. فالتطوّرات السيبرانية لن تكون في صالح طرف واحد دون الآخر.

منـذ مـدّة غير بعيدة شاع عبر الإعلام الغربي أن عددًا من خبراء السـيبرانية الصـينيّين نجحوا في اختراق معلومات مكتب الولايات المتحدة الأميركية لإدارة شؤون الموظفين. وسارع بعض الخبراء الغربيين إلى اعتبار الخرق الصـيني أمرًا جَللا، ومنهم من شـبّهه بهزيمة معركة بيرل هاربور»، إنما على المستوى الإلكتروني للولايات المتحدة.

ولكن لا يمكن مقارنة هذا الخرق بأي حال، مع ما يمكن أن يتسـبّب به هجوم إلكتروني عسكري حقيقي. وعلى سبيل المثال فقط : لنتصوّر جيشًا حديثًا لدولة عُظمى يدخل في حرب فيجد كلّ أسـلحته وأجهزته وأعتدته ومقوّمات قواه الضاربة، كلّها مُعطّلة بسـبب هجمة سـيبرانية عـدوّة عطّلت برامـج تشـغيلها بـل وأكثر من الممكن أيضًـا أن تجـد قيـادات هـذا الجيش القويّ أنّ أسـلحتها وصواريخها وكلّ قواها البرّيّة والبحرية والجوية والفضائية... كلّها باتت تتوجه نحوها ونحو مدنها ومراكزها ، وليس نحو العدوّ ...!

نعم الهجوم السـيبراني يمكن أن يتسـبّب بذلك، ليس فقط بالنسـبة لدولة صـغيرة وجيش ضعيف بل أيضًا وكما جرى ذكره بدايةً حتى لدولة عُظمى وجيش جرّار. فالجبهة السـيبرانية، وعلى الرغم من أنّها لا تشـهد إطلاق رصاصة واحدة، إلا أنّها قد تُعجز القوّة العُظمى عن استخدام كلّ ترساناتها الهائلة.

وفي هذا السياق أيضًا اعترف الجيش الروسي منذ أشهر قليلة، بحجم الجهود التي بذلها على مستوى الحرب المعلوماتيّة، معلنًا

التوسّع في تلك الجهود. وهـذا ما ثبتَ عمليّاً خلال هجوم جمهوريّة جورجيا على حلفاء روسـيا في أوستيا، حيث تـدخلت قوات روسـية للدفاع عن حلفائها، واسـتخدمت الفضاء السـيبراني بشكل واسع ممّا ألحق هزيمة سريعة بالقوّات الجورجية المهاجمة، مع أدنى مقدار من الخسائر البشرية . وهذا ما أعطى التأكيد الإضافي على أنه يمكن الانتصار في حرب المعلومات بشكل تام ومن دون سفك دماء، كما تكون الحال في الصراع العسكري الكلاسيكيّ.

ص: 138

ص: 139

الفصل الحادي عشر: الدولة إلى الانكفاء

اشارة

لطالما كانت الدولـة المدافع الأساس والأوحد غالبًا عن حياض الوطن وعن القيم والقوانين والأنظمة وهذا بدأ يتغير أواخر تسـعينات القرن الماضي بفعل تطور الفضاء السيبراني. حدث ذلك خلال مجموعة من الخطوات الصغيرة التي نتجت عن التقدُّم التقني المتصاعد في مجال الفضاء السـيبراني، والإنجازات التي راحت تحتلّ الشاشات وتجتذب المزيد من المتابعين والمهتمين، ما دفع بالدولة وأجهزتها إلى الصف الثاني، ليتقدّم عليها... أيّ شخص، أمام جهاز كومبيوتر أو هاتف ذكي.

أوّل التحديات كان اقتصادياً وسياسـياً في آن؛ فظهور تكنولوجيا المعلومات عَمّم أسـلوب الاعتماد المتبادل بين الدول وشـركات تكنولوجيا المعلومـات مُتعـدّدة الجنسـية الـذي يعني أنّه لم يعـد في مقـدور أيّ دولـة الاعتمـاد على الـذات فقـط، والاكتفـاء بما تنتـج من منتجات المعلوماتية . وهذا الوضع حتّم على الدولة الاسـتعانة بغيرها من شـركات تكنولوجيا المعلومات لسدّ حاجاتها على مختلف الأصـعدة ولا سيّما العسـكرية. فتقدم صـناعة برامج المعلوماتية فَرَض على الدولة توسيع دائرة اتصالاتها الخارجية والدخول في أنماط جديدة من الشراكة مع القطاع الخاص. في الماضـي القريب، كانت الدولـة تتحكّم وحدها في آلية صـنع القرار السياسـي. لكنّ الأمور تغيرت كثيرا بعد ظهور تكنولوجيا المعلومات. لذا بات يصعب اليوم على أجهزة الدولة وهيئاتها

إدراك مُختلف أبعاد صناعة برامج المعلوماتية، واستيعاب جميع ظروفها وتطوراتها ، بقدر ما يصعب عليها مراقبة كلّ ذلك والسيطرة عليه. وبات من الطبيعي أن يتراجع دور الدولة التقليدي «الأبوي) و المسيطر ، وأن يتصاعد في المقابل دور الشركات المختصة بالصناعات السيبرانية ولا سيّما منها الحربيّة(1). وعلى الأثر صار من الصعوبة بمكان على الدولة وأجهزتها المتخصصة في الميدان، أن تمنع أنشطة القراصنة أو أن تحول دون مواصلة العديد من الأطراف التجسّس أو استراق السمع أو انتهاك سرّيّة المراسلات والاتصالات، أو اعتراض أو اختراق ما تبثّه البرامج الخبيثة من معلومات ومشاهد. وكأنّ كلّ هذه التحديات لا تكفي، حتى حلّ التحدي الأمني بكل أثقاله ومخاطره فالتطور التكنولوجي قلب مفهوم الأمن الوطني التقليدي رأسًا على عقب(2)، لأنّ وجود الفضاء السيبراني غيّر أنماط العلاقات الدولية وقواعد الحرب.

1. تقييد مبدأ سيادة الدولة

أصبحت المجالات الأساس للسيادة الإقليمية مفتوحة ومستباحة بفضل التقدم التكنولوجي، وأصبح الأقوى تكنولوجيا يتمتّع بقدرة فائقة على اكتشاف ما يجري عند الآخرين، ومعرفة أدقّ أسرارهم من دون استئذانهم ونذكر على سبيل المثال عمليات التنصّت أو استراق السمع والتجسّس، والتقاط الصور بواسطة

ما كتبه

1- راجع ما كتبه: Linant de Bellefonds et A. Hollander.

2- Droit de l'informatique et de la té lé matique, J. Delmas et cie, 2è me é dition, p. 141.

الأقمار الصـناعيّة والخطورة في مثل هذه التصرفات لا تكمن في إفراغ السيادة من مضمونها أو فاعليّتها فقط، بل تكمن أيضًا وأساسًا في أنّها لا تُعَدُّ خرقًا لقواعد القانون الدولي العام.

وتمتد الحرب إلى إقليم كلّ دولة محاربة. ويمكن أن تمتد إلى أي إقليم آخر يُسـهم في النشاط الحربي أو تسـتخدمه الدولة المحاربة كنقطة تجمع واسـتعداد لاسـتخدام الفضاء السيبراني. فنطاق الحرب يشمل ، بشكل أساس، مجال الفضاء السيبراني، الذي يستوعب كلّ ما يمكن أنْ يَصل إليه الإنسان أو يُدركه.

فالتطورات العلميّة التي تسـمح باسـتخدام الفضاء السـيبراني، وبعبور شـبكة الاتصالات الوطنيّة أحيانًا، تجعل من الصـعب عمليّا مُمارسة السـيادة الوطنيّـة على هـذا المجال السـيبراني، وإخضاعه أو إخضاع أي جزء منه للتشـريعات أو المراقبـة المحلية. ونظرا لصـعوبة الرقابة أو اسـتحالة تحديد أماكن إنتاج برامج المعلوماتية التي تسـير فى الفضاء السـيبراني وتنتقل من دولة إلى أخرى بسرعة هائلة، فإنّ الدول لم تُبدِ، منذ أنْ غَزَت البرامج المعلوماتية المجال السيبراني، أيّ اعتراض أو احتجاج على تَغَلْغُل هذه البرامج في إقليمها. ولهذا تخلّت مُعظم الدول عن التشبُّث بفكرة السيادة.

الحرب السـيبرانية، مثلها مثل أي حرب، لديها أسـبابها وأهدافها. الأسباب تماثل تلك التي تقف خلف كلّ حرب، من الأطماع، إلى تحييد الخطر. أما الأهداف فهي تختلف عن تلك التي للحروب التقليديّة، وذلك وفقًا لعوامل شتّى أساسيّة يمكن إجمالها كما يلي:

1- صـراع سـيبراني ذو طبيعة سياسية ويتحرك بدوافع سياسية، لكنّه يأخذ غالبًا شكلاً عسكريًا يجري فيه استخدام قدرات إلكترونية هجومية ودفاعية عبر الفضاء السـيبراني، بهدف إفساد النظم المعلوماتية والشبكات والبنى التحتية لدى الطرف الآخر. هنا لا تنفع الدبّابات والطائرات والعمارات البحريـة، بل يجري العمل على توظيف أسـلحة إلكترونيـة لتحقيق غايات الحرب، والتي تكون موجّهة إلى أنظمة التشـغيل عند العدوّ وأنظمة حماية المعلومات. هذه الحرب جنود ،وآليّات بل مجموعات من الخبراء

ولاـ يشن السـيبرانيين داخل المجتمع المعلوماتي، ممّن يمكن الاعتماد عليهم، سواء في محاولات اختراق معلومات العـدوّ وقرصـنتها إن أمكن أو تعطيل إمكانيّـة العـدوّ في الوصول إلى معلوماته أو اسـتخدامها ضـد العدو ذاته أو تخريبها ومحوها. وفي هذا المجال، التعاون مع قوى أخرى لتحقيق أهداف سياسية(1).

2 – صـراع سيبراني ذو طبيعة مسالمة، وهو حول الحصول على المعلومات، والتأثير في المشاعر والأفكار، وشنّ حرب نفسيّة وإعلاميّة. يتم ذلك من خلال تسريب معلومات تخدم الطرف

1- http://www.alquds.co.uk/?p=52786

الذي يعمل على تسريبها، واستخدامها عبر منصات إعلامية ناشطة بما يؤثر في معنويات الخصم كما في طبيعة العلاقات الدولية. أفضل مثال على ذلك هو الدور الذي لعبه موقع «ويكيليكس» في الديبلوماسية الدولية.

3 – صراع سيبراني على التقدّم التكنولوجي. هذا النمط من الصراعات السيبرانية يأخذ طابعًا تنافسيًا هدفه السيطرة على سباق التقدم التكنولوجيّ، وسرقة الأسرار الاقتصادية والعلمية وسواها. وقد يمتد إلى محاولة للسيطرة على الإنترنت عند الخصم، وكشف أسماء النطاقات، وعناوين المواقع، ومن خلال ذلك التحكم بالمعلومات والعمل على اختراق الأمن القومي للدول، من دون استخدام طائرات، أو متفجرات، أو حتى انتهاك حدود تلك الدول. ويتم ذلك من خلال هجمات قرصنة لمعلومات الخصم وتدمير مواقعه السيبرانية أو إعاقتها. وربما يكون لصراع كهذا تأثيرات مدمّرة على الاقتصاد وعلى البنى التحتيّة تفوق ممّا يمكن للقنابل أن تحققه(1).

4 – صراع سيبراني على المعلومات والشؤون الاستخبارية.

والواقع أنّه على الرغم من صعوبة الفصل بين أنشطة الاستخبارات وجمع المعلومات، وحروب الفضاء الإلكتروني، وإمكانيات التمييز بين الاستخدام السياسي والإجرامي، يبدو الفضاء السيبراني بيئة مناسبة تمامًا للصراعات المعلوماتية. فهو أساسًا موئل المعلومات ومخزنها، ويمكن أن يُسهم في دعم قدرة الأجهزة الأمنيّة للدول، وكذلك للجماعات الإجرامية والإرهابية على أنواعها في الطرف

1– المرجع ذاته.

الآخر، (أو (و) تشكيل شبكة تجسّسية من العملاء من دون تورّط مباشر، وذلك من خلال قرصنة معلومات.

2. دليل» «تالين» والحرب السيبرانية

من خلال دورها كحارس للقانون الدولي الإنساني، وهو القانون المنطبق في حالات النزاع المسلّح، عملت اللجنة الدولية للصليب الأحمر على رعاية مجموعة من الخبراء العسكريين الذين تمكنوا بعد دراسات ونقاشات هادفة من وضع مجموعة أصول وقواعد قانونية تعمل على كبح الأخطار والمضارّ التي يمكن أن تنجم عن الحروب السيبرانية، وترعى بالتالي كيفيات استخدام العالم السيبراني في السلم والحرب لضمان إنقاذ البشرية ، ولا سيّما شعوب القوى المتحاربة من انعكاسات التدخلات السيبرانيّة على دورات حياتها .

وبعد تدبّر المطلوب عمدت اللجنة الدولية إلى نشر ثمار ذلك تحت عنوان دليل» «تالين الذي أشار أوّل ما أشار إلى أنّ القانون الدولي الإنساني ينطبق على الحرب السيبرانية كما على أشكال الحروب الأخرى كافّة، ويحدّد الدور الذي ستشرعه قواعد القانون الدولي الإنساني في هذا المجال حماية للمدنيين وحفاظا على أمن الشعوب، بكل الإمكانات المتاحة.

الواقع أنّ «دليل تالين» الذي هو « وثيقة غير ملزمة»، نجح بامتياز تقديم رؤى مثيرة للاهتمام، فقدّم تعريفا للهجوم السيبراني» بموجب القانون الدولي الإنساني بوصفه «عملية إلكترونية، سواء

أكانت هجوميّة أم دفاعيّة، يُتوقع لها أن تتسبّب في إصابة أو قتل أشخاص أو الإضرار بأعيان من أبنية وآلات وأملاك خاصة أو عامة أو مشاع أو تـدميرها». وتمسّك الـدليل بالثنائيـة التقليديـة للنزاعات المسـلّحة الدوليـة والنزاعات المسـلّحة غير الدولية، وأقرّ بأنّ العمليات الإلكترونية وحدها قد تشـكّل نزاعات مسـلحة تبعًا للظروف – لا سيّما الآثار المدمرة لتلك العمليات. ويكمن صلب الموضوع مع ذلك في التفاصيل؛ أي ما ينبغي أن يُفهم على أنّه «ضرر» في العالم الإلكتروني. ولقد اتفق الخبراء على أنّه، علاوة على الضرر المادّيّ، فإنّ توقيف أحد الأعيان عن العمل قد يشـكل ضررًا أيضًا. وتتمثل وجهة نظر اللجنة الدولية في أنّه إذا تعطّل أحد الأعيان فليس من المهم كيفية حدوث ذلك، سواء بوسائل حركيّـة أم بعمليّـة إلكترونيـة. هذه القضـيّة بالغة الأهمية في الممارسة العملية، –ث أنّ أي نشاط إلكتروني يسـتهدف تعطيل شـبكة مدنية خلاف ذلك، لن يشمله الحظر الذي يفرضه القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية.

فمن الواضـح اليوم أنّ الأضـرار التي يمكن أن تتسـبب بهـا الحرب السـيبيرية، تصل إلى درجـة تهديـد حياة الملايين من المـدنيين الـذين يحميهم القانون الـدولي الإنساني ومختلف الشـرائع الدولية في كلّ أنواع الحروب. فمن الممكن أن يتعرّض كلّ ما يعتمد في تشـغيله على الكومبيوترات والعلوم الرقمية (السدود والمحطات النووية وأنظمة التحكّم في الطائرات ...) لهجمات سـيبرانية تتسـبب بكوارث. فالشبكات الإلكترونية تكون مترابطة إلى حدّ يجعل من الصعب

الحدّ من آثار أيّ هجوم سيبراني، وحتى لو استهدف الهجوم جزءًا من المنظومة، فالأضرار ستنتقل إلى المنظومات الأخرى بحكم التواصل الوثيق ضمن الشبكة. وقد يتضرّر صالح مئات الآلاف من الناس، وصحتهم وحتى حياتهم.

لذلك حرصت اللجنة الدولية على حثّ جميع أطراف النزاعات بتوخي الحرص بشكل مستمر في سبيل حقن دماء المدنيين، بسلامتهم وسلامة مصادر حياتهم، كما تقتضي ذلك مختلف الشرائع والقوانين الدوليّة، مع التأكيد على أنّ ذلك ينطبق بحذافيره على الحروب السيبرانية بالقدر نفسه الذي ينطبق فيه على حروب البنادق والمدافع والصواريخ.

في هذا الإطار ترتفع الخشية من تفاقم الاعتداءات السيبرانية التي باتت تشهد اتساعًا هائلاً على الرغم من جهود مكافحتها. ومنذ أشهر قليلة أصدر موقع «أسبوع الأمن (Security Week الأميركي ما أسماه «البعض» ب- «اللائحة السوداء»، وتضمّن تعدادًا لبعض أسوأ خروقات البيانات المخزنة في العالم السيبراني، التي شهدها العام 2014 فقط، حيث بلغت نسبة ارتفاع هذه الخروقات 25% عن مثيلاتها في العام الذي سبق (2013).

وجاء التقرير في عدة صفحات أجتزئ منه بعض خطوطه العامة كما يلي:

اختراق مواقع كثيرة جدا منها على سبيل المثال مواقع : المزاد العالمي الإلكتروني - Ebay، مؤسسة JP Morgan Chase» المالية

ص: 147

الرائدة Home Depot»، شركة SONY وغير ذلك كثير . هـذا إضافـة إلى إختراق أنظمة مستشـفيات وبطاقات دفع للمال. لكن تهديدات إرهابيـة ومحاولات اختراق اسـتهدفت معلومات تتعلق بحوادث 11 /أيلول سبتمبر 2001، دفعت مكتب التحقيقات الفيـدرالي الأميركي (FBI) إلى التدخل في الأمر وفتح تحقيق للوقوف على طبيعة وحجم ما جرى. لكنّ أي مصدر لم يُعلن نتيجة تلك التحقيقات.

اختراق موقع القيادة المركزية الأميركية (CentCom) من قبل قراصـنة ينتمون إلى تنظيم «داعش»، من دون معرفة نتائج ذلك الاختراق وما إذا كان تسبب بأضرار أم لا.

وفي هذا المجال تجدر الإشارة إلى أنّ أوّل عمليّة اقتحام سيبراني ذات طابع سياسي تعود إلى العام 2010، عندما تم اكتشاف برمجية خبيثة نشـرت على أجهزة كمبيوتر إيرانية بهدف إلحاق الضـرر بأجهزة الطرد المركزي المخصـصة لتخصـيب اليورانيوم في بعض المنشآت النووية الإيرانيـة. ويومها رست الاتهامات على الولايات المتحدة الأميركية وإسـرائيل، من دون أن يعترف أحد. وكملاحظة أخيرة في هذا السـياق، فلقـد ساهمت اللجنـة الدوليـة، بصـفة مراقب في مناقشات الخبراء الذين صاغوا دليل «تالين»، وضـمنت انعكاس القانون الدولي الإنساني القائم في الدليل بأقصى قدر ممكن، وتعزيز الحماية التي يوفّرها هذا الفرع من القانون لضحايا النزاعات المسلّحة. وتعكس القواعد الخمس والتسعون المدرجة في

الدليل النصوص التي حظيت بإجماع الرأي بين الخبراء.

ص: 148

3. انقلاب مفاهيم القوّة والتحكّم

لو راقب المرء مسيرة الشعوب والحروب عبر التاريخ لظهرت أمامه جليّة القاعدة المنطقيّة في تعامل القوى الفاعلة في العالم و هى القاعدة التي ما برحت على حالها منذ القدم: كلما ازددتَ معرفة، ازددت قوّة وسيادة وسيطرة. ومع ارتفاع مستويات معرفتك بشؤون الآخر ونقاط قوته وضعفه، ترتفع بالمقابل عناصر ومقومات قوتك أمامه، وتغدو بالنتيجة أكثر استعدادًا لتأمين مكانك وملكيّتك والتفوّق عليه؛ لذلك لم يعترض أيّ مفكر منذ فجر التاريخ على قيمة المعرفة وأهميّتها وجدواها فهي تبني المناعة والغنى وترسم هيكل القوّة والسيادة، وتوسّع مساحات السيطرة وفعاليات التحكم. وعلى مرّ الأزمان ارتبط المفهوم التقليدي للأمن والسيادة الوطنية بعوامل القوّة التقليدية التي لها صلة وثيقة بالوفرة والجغرافيا والعديد البشري والكفاءات القتالية. وفي مرحلة متقدمة بات قصب السبق للجيوش المجهزة والمعدّات الحديثة والأعتدة المتطورة والاقتصاد المليء والمتين. وعلى هذه المقاييس اندلعت الحروب ووُقِّعت معاهدات الصلح والتفاهم، وصيغت وثائق الاستسلام والرضوخ. وبعد قنبلتي (هيروشيما ونغازاكي تجاوزت البشريّة مرحلة القوّة بالسلاح والأعتدة التقليدية والجيوش المجيّشة، لتدخل مرحلة السيادة بالسلاح غير التقليدي» الذي قام على أكتاف الرعب النووي وأشباهه . هكذا دخل مصطلح «الدول العظمى» في قاموس التداول، وصار الهمّ الأبرز لدى هذه الدول «النووية» يكاد يقتصر (ويا للغرابة) ليس على تجنيب البشرية كوارث نووية مما ضُربت

به اليابان، بل... منع الآخرين من امتلاك هذا السلاح والدخول إلى نادي «عُظماء العالم من خلال استخدام الشعار الإنساني الفضفاض الحدّ من انتشار السلاح النووي» وكأنّ القصد منه كان الحد من انتشار السلاح النووي لدول غير دولهم».

ثمّ كان العصر الراهن. وكأنما بطريقة سحرية لم ترافقها (بعد) الضجة الهائلة التي تستحق أضعافها، تسلّلت العلوم الرقمية وتكنولوجيا المعلومات على قفزات علوم التواصل وتقنيات الاتصالات في الربع الأخير منذ القرن العشرين، واحتلت الواجهة وباتت في عُرف العارفين السلاح الأمضى والقوّة الأعتى والأداة الأفعل في عالم اليوم.

والبداية من «الفضاء الإلكتروني أو السيبيري». فثمة فضاء إلكتروني واحد فقط يتقاسمه العالم أجمع، أفراداً وجماعات، مؤسسات وشركات ودول، إدارات مدنيّة وعسكرية وأمنية ومالية واقتصادية... إلى كلّ ما هناك من إدارات. والفضاء «السيبيري يستضيف معلومات هذه الأطراف جميعها حيث يجري تخزينها فيه، ويمكن لأصحابها – مبدئيا – الدخول إليها دون غيرهم، في حين أن الدخول إلى المعلومات من قبل غير أصحابها يكون ممنوعًا قانونيا وشديد التعسّر عمليّا، حيث أنّ كلّ طرف يعمل على حماية معلوماته وتحصينها ببرامج تكون مخصصة لصونها ومنعها على الآخرين وتعطيل الهجمات الإلكترونية التي قد تحصل عليها من قبل أي طرف. لكن هذه الحمايات والتحصينات يمكن في ظروف ما أن تفشل أمام هجمة من

هنـا أو قرصـنة من هنـاك، فتصـبح المعلومـات عُرضـة للانتهاك. وهـذا هو التحـدّي الأساس اليوم: جعل المعلومات المخزنـة في الفضاء الإـلكتروني منيعـة على أي اختراق. وهـذا ما لا يمكن تحقيقه بشـكل تام، ما يسـتدعي مواصـلة العمل على تطوير برامـج الحمايـة مقابل تحديث برامج الاقتحام والقرصنة.

4. القوة الناعمة

لعله منذ قيام ما سُـمّي توازن الرعب النووي الذي ما انفك يمنع أي دولة عظمى ولو كانت الولايات المتحدة الأميركيّة) من المغامرة بضرب أي دولة نووية أخرى، ولو كانت ضـعيفة أو فقيرة أو شبه معزولة ولو كانت كوريا الشمالية لعلّ هذا النوع من التوازنات الإكراهيّة والثقيلة على كاهل القوى العالمية الجبّارة والمتغطرسة، هو ما شـجّع أهل العلم والتقانة ع-ل-ى التفكير بسبيل جديد يتيح لها الهيمنة من دون أن تجد نفسـها ملزمة بتوازن جشـعها ورعبه-ا م-ن الأضـرار المحتملة التي قد تصيبها جراء أي حرب غير تقليدية تشنها . وفي هذه الظروف، دخلنا العصـر الراهن عصـر التقنيات الرقمية والإلكترونية السـيبرانية التي ما انفكت تستعرض أمامنا «معجزاته-ا غ-ي-ر المسبوقة. وكأنما بطريقة سحرية لم ترافقها (بعد) الضجة الهائلة التي تستحق أضعافها، تسلّلت هذه العلوم الرقميّة وتكنولوجيا المعلومات على قفزات علوم التواصل وتقنيات الاتصالات في الربع الأخير منذ القرن العشرين، فاحتلت الواجهة وباتت

في عُرف العـارفين السـلاح الأمضـى، والقوة الأـعتى والأـداة الأفعـل، للتقـدّم والتطوّر ، وتحقيق السـلطة والسـيادة على العـدوّ والمنافس، والصديق والحليف، على السواء، وبكلّ ما يمكن من الهدوء والنعومة.

البدايـة تكون من الفضاء الإلكتروني أو السـيبراني»، هـذه «المغارة التي أين منها مغارة علي بابا!)، حيث الإنجازات والإمكانات تبـدو مثل السحر، بل في أحيان معينة، أكثر من السحر هولاً وإدهاشًا.

الفضاء الإلكتروني أو السـيبراني ليس سوى «مكان» افتراضـي واحد فقط يتقاسمه العالم أجمع أفراداً وجماعات، مؤسسات وشركات ودول إدارات مدنيّـة وعسـكرية وأمنية، ومالية واقتصادية... إلى كلّ ما هناك من إدارات–كما أسـلفنا–. ولكي لا يبدو الأمر مبهما . نسـتذكر أجهزة اللاسـلكي؛ فالتواصـل على موجـات اللاسـلكي لا يتم عبر أسـلاك تصل بين المتخاطبين، بل يتم عبر الجوّ » أو « الهواء» أو «الفضاء» من خلال الذبـذات الكهربائيـة في الجو... بمعنى أنّ هذا التواصل يمتطي خيولاً غير مرئيّة هي ما نسـمّيه الموجات وهذه الموجات تنتشـر في الفضـاء الـذي هو ذاته الفضاء الإلكتروني أو السـيبراني. لكن الأمر هنا متقـدّم كثيراً على ما كان اللاسـلكي يوفّره؛ فالتواصل بين الناس من أقاصـي الكوكب إلى أقاصـيه في الطرف المقابل، يتم مبـدئيًا بيسـر وسـهولة من خلال الفضاء السـيبراني». وفي هذا الفضاء ذاته يجري فتح خزائن هائلة السعات لاستضافة المعلومات

ص: 152

أي معلومات كانت ومن أي صـنف ولون، ولكلّ من يريد. وبعد تخزين كلّ راغب لمعلوماته، يجعلها في ظلّ حماية ينبغي أن تكون منيعة ضـدّ الفضوليين والحُشـريين الـذين يمكن أن يحـاولوا الـدخول إليها والاطلاع عليها وربما اسـتغلالها. فالكثير من المعلومات هي أسـرار للأطراف التي تختزنها، وليس من صالح هذه الأطراف أن تجعل معلوماتها مُشاعة.

ص: 153

ص: 155

الفصل الثاني عشر: المعلومات المخزّنة

اشارة

تنقسم المعلومات المخزّنة ضمن نطاق الفضاء السيبراني، إلى عدة أنماط أحدها يمكن لأصحابها – مبدئيًا– الدخول إليها دون غيرهم، إذ تكون محمية بكلمة مرور أو ببرنامج حماية خاص ممّا يختاره صاحبها. أما دخولها من غير أصحابها فلا يكون إلا عنوة (من خلال اقتحام أسوار حمايتها الإلكترونية)، وهذا أمر ممنوع قانونيًا وشديد التعسّر عمليًا، حيث أنّ كلّ طرف يعمل على حماية معلوماته وتحصينها ببرامج تكون مخصصة لصونها ومنعها عن الآخرين، وتعطيل الهجمات الإلكترونية التي قد تحصل عليها من قبل أي طرف. وكلّما كان الطرف أكبر وأهم ، تزداد معلوماته خطورة، وترتفع بالمقابل أسوار الحماية التي تُقام حولها لإبقائها في أمان ما أمكن. لكنّ هذه الحمايات والتحصينات يمكن في ظروف ما، أن تفشل أمام هجمة من هنا أو قرصنة من هناك، فتصبح فتصبح المعلومات عُرضة للانتهاك. وهذا هو التحدّي الأساس اليوم: جعل المعلومات المخزنة في الفضاء الإلكتروني منيعة على أي اختراق. وهذا ما لا يمكن تحقيقه بشكل تام ما يستدعي مواصلة العمل على تطوير برامج الحماية مقابل تحديث برامج الاقتحام والقرصنة.

وهناك نمط آخر من المعلومات يكون مُباحًا ومُتيسرًا لمن يرغب وهو على العموم معلومات معرفية يستفيد منه الدارسون والباحثون والطلاب. وهذه تتوافر عادة في محركات البحث على الشبكة (مثل محرّك غوغل)، وفي أرشيف المؤسسات الدراسية والبحثيّة والصحافية وما يشابهها.

ص: 156

وهذه المعلومات جميعها هي مواد قوة ومعرفة وأمان، على أساس أنّ المعرفة هي سبيل مضمون لاكتساب القوة والسلطان.

لابـدّ من الاـعتراف بأنّ تكنولوجيا المعلومات أحـدثت تغيرات هائلـة في مفهوم القوّة والأمن؛ فقـد انتقلت نقاط القوة والمنعـة من العـديد البشري والكفاءات العسكرية غير التقليدية والخصوصيات الاقتصادية والجغرافية للبلد، لتتحوّل إلى ما يتصل بالفضاء السيبراني والإمكانات المتاحـة فيه لهـذا الطرف أو سواه، ولاـ سـيّما مـا يتعلّق بعولمـة الاتصالاـت وتبـادل المعلومات، وسـهولة انتقالها بشـكل عابر للجغرافيا. والمشـكلة المحرجـة هي أن لا غنى للعالم (في تقـدّمه وتطوّره) عن السـيبرانية والفضاء السـيبراني فمن هـذا النطاق ينفذ العالم إلى ميادين المزيد من التقدم والتطوّر وتعزير الإنتاج وتعميم الرفاهية. ومن هذا النطاق ذاته أيضًا تهبّ ريح السموم ومخاطر الاقتحامات والاجتياحات الإلكترونيـة المعيقـة والمُكلفـة والمـدمّرة. وبـالنظر إلى الأهمّيّـة القصوى للمعلومات، سواء بالنسـبة إلى أصـحابها، وهي ثروتهم الحيوية وسواعد حياتهم وقواهم وإنتاجهم وصـيرورتهم، أم بالنسبة إلى الآخرين من منافسين ومضاربين وشركاء وأخصام وأعداء... فقد فرض الأمن السيبراني وجوده كواحد من أوّل وأهم وأبرز الحاجات المُلِحّة للإنسان الحديث.

ص: 157

1. «كعب آخيل»

من هنا يبدو واضحًا أنّ مصدر القوّة الاستثنائية هذا ذاته ما هو يمكن أن يكون نقطة الضعف الخطيرة لصاحبها، وربما مقتله أيضًا. يحصل ذلك إذا تمكّن عدوّ أو خصم أو منافس أو حتّى شريك من اقتحام معلومات طرف آخر (شخص أو شركة أو دولة مُخزّنة الفضاء الإلكتروني، ومن الاطلاع عليها (أي على خصوصيات صاحبها وأسراره ونقاط قوته وضعفه ...). ويتعرض بالتالي إلى خطورة إباحة المعلومات ليستفيد منها غير صاحبها وعلى حساب هذا الأخير. فضلاً عن ذلك فإنّ الأخطار اللاحقة يمكنها أن تكون أدهى وأشدّ؛ فقد يقوم المتسلّل إلى المعلومات الذي اخترق برامج حمايتها، بحبس هذه المعلومات بحيث يستحيل على صاحبها بلوغها، وقد يقوم باستغلالها ضد مصالح صاحبها، وقد يبتزه على أساسها، وقد. وقد.... وكلّ ذلك يؤدّي إلى نقل مقوّمات القوة والسيطرة إلى الطرف الذي حصل على المعلومات وحبسها عن الطرف الذي يمتلكها . إنّ استحواذ طرف غريب» على معلومات طرف آخر هو بمثابة تجريد لهذا الطرف الآخر من مقومات معرفته وتنظيمه وقواه فكيف بالحريّ سيكون وضعه إذا ما استخدمت هذه المعلومات ضده؟

هنا موضع القوّة والسيادة والتحكّم، لكنّه بمثابة كعب آخيل» أو نقطة المقتل أيضًا. وكلّ من يعرف ما لا ينبغي أن يعرفه، يمتلك قوة استثنائية.

ص: 158

2. تبدل المفاهيم

تشكل العلوم السيبرانية مجال قوّة أساسية في عالم اليوم بعد أن تغيرت المفاهيم التي سادت أجيالاً طويلة. فمع تطوّر الاتصالات خلال الربع الأخير من القرن العشرين وصاعدا، حدثت تغيرات هائلة ونوعية في مفاهيم القوّة في العالم المعاصر. إنّ العلوم السيبرانية بما فيها من أنظمة وما تتيحه من إمكانات يستحيل حصرها أو الإحاطة بها، باعتبارها تشمل جملة الحياة برمتها تشكل القوّة الحقيقية والأساسيّة لإنسان اليوم بما هو مجموعة صغيرة أو كبيرة من أصحاب العمل والدائرين في مختلف مناحي الحياة والإنتاج والإنفاق...، من حانوت في قرية نائية إلى مؤسسة إنتاجية أو شركة كبيرة أو دولة ... إنّ توافر معلومات الجهة المعنية ضمن الفضاء الإلكتروني هو ما يسمح لهذه الجهة بتنفيذ ما ينبغي عليها تنفيذه من أعمال ومهام وخدمات وبالكميّات المطلوبة وبالسرعات المناسبة، ويتيح لها مقومات القوة والسيطرة بالتالي إلى حدّ ما على مصيرها. وهذا هو التجلي الأعلى لمفهوم القوة. فطالما تسير الأمور على هدي هذه المعلومات المحفوظة والمحمية والتي هي لصالح الجهة صاحبتها، يكون العمل منتظماً ومُنتجًا وناجحًا كما يريد له المبرمجون. أما إذا استطاع طرف آخر اقتحامها والاستحواذ عليها وتسخيرها لمصلحته على حساب الجهة المالكة لها، فعندها يحصل ما هو أسوأ من أسوأ الكوابيس. فسواء من حيث عولمة الاتصالات وسهولة تبادل المعلومات وانتقالها بشكل عابر للجغرافيا، أو انتقال مراكز القوّة وأدوات التحكم والسيطرة

من الأرض والجغرافيا إلى الفضاء الإلكتروني ومقدراته، بات من الصعب القطع بفكرة السيطرة المطلقة من دون أخذ الاعتبار للمعلومات والإمكانيات التي يمكن استخدامها واستثمارها و... حجبها أو تعطيلها. وفي ظلّ الارتباط والاندماج بين المعلومات من جهة والشبكة الدوليّة التي تستضيفها من الجهة المقابلة (الإنترنت) انقلب الفضاء السيبراني من موئل ومضافة ومخزن إلى ساحة مواجهات... وربما ميادين معارك وحروب من النوع الذي لا تُسمع فيه ولا حتى طَلقة رصاص.

فالمعروف أن مختلف شؤون ومقومات الحياة والإدارة والقوّة والإمكانات في عصرنا الحالي، وفي مختلف أنواع وأحجام المؤسسات والإدارات والدوائر تعمد إلى الفضاء الإلكتروني أو السيبراني، فتخزن فيه أصولها وتفاصيلها ومخططاتها واستراتيجياتها... وتجعلها بالأشكال التي تتيح لها بلوغها واستخدامها ومعالجتها بما يخدم مصالحها. وهذه المعلومات تنتظم إلكترونيًا من خلال محركات كومبيوترية هائلة السعة والسرعة في المعالجة، وتتضمن مجموع المعلومات كافة مختلف عن المقوّمات والثروات والعمليات الضرورية لتغذية المواطنين ومدهم بالماء والكهرباء وأصناف الأغذية والأدوية والألبسة... إلى ما هنالك من حاجات حياتية وحيوية لا غنى عنها . وإلى المعلومات المتصلة بشؤون الحياة والغذاء والإنتاج والإنفاق، والتصنيع والاستيراد والتصدير ...، هناك أيضًا المعلومات العسكرية والأمنية، والمقصود هنا الأسرار والمعارف التي ينبغي الاحتفاظ بها خارج نطاق الشيوع

ص: 160

والانتشار، باعتبارها أمان لسلامة البلاد ومنعتها وقوتها واستقرارها وكلّ ما ينبغي أن يبقى في تصرف المعنيين به من المسؤولين الوطنيين، أصحاب الوظائف العليا وما دونها والمختصين، من دون أن يخرج أبدًا إلى النطاق العام. هذه الملفّات المعلوماتية الهائلة المختزنة في الفضاء الإلكتروني، تكون محمية ببرامج وسدود وحصون تحجبها عن العدوّ وعن الخصم، وعن المنافس، وعن كلّ طرف غير معني رسميًا ببلوغها، وعن كلّ شخص غير مكلف بإدارتها ورعايتها وانتظام حركاتها. وأي خلل على هذا المستوى أو اجتياح أو اقتحام...من شأنه التسبّب بمشكلة ، غالبًا ما يكون ثمنها باهظ التكاليف.

إنّ سياقات تطوّر المجتمعات البشرية غالبًا ما مرت بمنعطفات تاريخيّة حدّدتها الابتكارات ومدى أهميتها وجدواها العمليّة. فبعد عصور الحجر ثمّ المعدن ثمّ عبقرية العجلة، ومن ثم الدمج بين الخشب والمعدن لتصنيع الأدوات المختلفة لتلبية الحاجات اليومية للمخلوق المنتصب حافظت التجمعات البشرية على خطوات تقدّمها على سلّم الترقي والتحضر، حتى بلغت قفزة البخار والآلة البخاريّة، ومنها إلى الثورة الصناعية التي تركت انعكاساتها آثاراً بالغةً على مختلف الأصعدة الاجتماعية والثقافية والأخلاقية والفلسفية، وحتّى شكل السلطة وطبيعتها في جميع المجتمعات التي عرفتها وعاشتها. ومن ثمّ جاء عصر التكنولوجيا وتطور وسائل الإنتاج المتاحة وانعكاسات كلّ ذلك على البنى الفاعلة في المجتمعات التي تطوّرت حتّى الدخول في عصر العلوم والتقنيات الرقمية التي ما برحت تواصل مسيرتها بإنجازات لا تتوقّف.

المعروف أنّه عندما تمّ استطلاع خبراء الأمن السيبرانيّ خلال مؤتمرهم السنويّ في «بلاسهات» ب«لاس فيغاس» حديثا، قال 60 % منهم إنّهم يتوقعون أن تتعرّض الولايات المتحدة لهجوم ناجح ضدّ بنيتها التحتيّة الحيوية (أي السيبرانيّة) في العامين القادمين(1). وما تعتبر الولايات المتحدة معرّضة له، هو ذاته ما تتعرض له كلّ دولة أخرى، ولا سيّما الدول المسماة ب–«العُظمى» كما الدول التي تستهدفها القوى الغربية عمومًا. ولا تزال السياسة الأميركية تعاني بسبب تداعيات ما سمي بالتدخل السيبراني الروسي في الانتخابات الرئاسية العام 2016. وهذا يُبرّر طرح تساؤلات مشروعة عما إذا كانت الهجمات الإلكترونية تهدّد المستقبل فعلاً، أم أنه بالإمكان وضع قواعد للتحكّم في الصراع السيبراني الدولي القائم.

فالقوّة التكنولوجية باتت ذات أهمية قصوى في تطوّر الدولة وقدراتها في المجالات والأصعدة كافّة، من العسكرية والاقتصادية والإدارية إلى الصناعيّة والصحية والمالية (...). وبعد أن خطت الدول المتقدّمة خطوات واسعة وسريعة في تحقيق التقدّم التكنولوجي، وامتلاك ناصيته التي أوصلتها إلى غزو الفضاء وقهر الأزمات التي تتعرّض لها أصبحت التكنولوجيا من وسائل القوّة والسيادة للدولة، محاولة بذلك فرض إرادتها على المجتمع الدولي حتى بالنسبة للدول النامية مثل كوريا الشمالية.

لم تعد شبكة الإنترنت تلك الشبكة البدائيّة التي تربط مجموعة العلماء في عدة جامعات مختلفة في تلك المدينة أو هذا البلد،

1- http://www.aljazeera.net/knowledgegate/opinions/2017/8/9/.

كما كانت في بادئ الأمر وحسب، بل أصبحت بعد مرور أربعة عقود على انطلاقتها الشبكة الأوسع على الإطلاق في تاريخ البشرية؛ حيث باتت تهيمن على جميع المجالات الحيويـة التي تهم الإنسان، وينظر إليها على أنّها الأداة المثلى لتحقيق الازدهار الاقتصادي والاسـتقرار والتقدّم، وكذلك لشن الحروب وصيانة السلطان والمصالح.

وربما من الخطير حقًا أنّ أضـرار استخدام الفضاء السيبراني يمكن أن تحدث من دون أن يكون بالإمكان نسبة أي خطأ إلى الدولة المسؤولة مبدئيًا عن فضاء البلد السـيبراني. فمن الصعب بمكان أنْ يكون للبرامج المعلوماتية الخبيثة مظهر خارجي يدلُّ على صفاتها وجنسيّتها، ممّا يُعقد عمليّة الإثبات، وبخاصة تلك التي تكون الدولة قد اشترتها من الأفراد أو شركات تكنولوجيا المعلومات المنتجة لهذه البرامج(1). فهل تتحمل كل دولة طرف تُنتج أو تَسْـمَح بإنتاج أي برنامج معلوماتي خبيث في الفضاء السيبراني، أو يُستخدَم إقليمها أو منشآتها لعملية إطلاق من هذا النوع، مسؤوليّةً دوليّةً عن الأضـرار التي تُسبّبها هذه البرامج أو أيّ من تداعياتها أو آثارها، على الأرض أو في الجو أو في البحر، لأيّ دولـة طرف أو لأي شـخص من أشخاصـها الطبيعيين أو المعنويين؟ وهل تحتفظ الدولة الطرف، أَنْتَجَت أو أَطْلَقَت برنامجًا معلوماتيًا خبيثًا، بالولايـة والرقابـة عليه خارج حـدود الولايـة الوطنيـة للدولـة؟ وبعبارة أوْضَـح هل تتحمل الدولة الطرف، التي أطلقت أو سَـمَحَت بإطلاق البرنامج

1- https://cyborgstechnology.wordpress.com/2015/ 11/ 29/.

الخبيث من أرضـها أو سّـمَحت بتمريره أو بعبور شـبكتها المعلوماتية، بالمسؤولية الدولية عن جميع الأضرار التي تنزل بالآخر؟ وهل تبقى للشركة المصنّعة مُلكيّة مثل هذه البرامج؟ وبسؤال موجز: من يتحمّل المسؤوليّة فى هذه الحالة؟ وما هو أساس هذه المسؤولية؟

ذكر تقرير صادر عن مكتب مـدير أجهزة الاسـتخبارات الأميركية أنّه في العام 2016 ، تمّ جمع معلومـات عن 151 مليون مكالمة هاتفية بتصـريح من المحكمة السرّية الخاصة لشؤون مراقبة الأجانب. FISA وجمعت وكالـة الأمن القومي الأميركية على نطاق واسع معلومات وصـفية عن توقيت وعناوين ومـدة المكالمات الهاتفيـة بعـد هجمات 2001/9/11 وكشف عميل الاسـتخبارات الأميركيـة السابق إدوارد سنودن عام 2013 النقاب عن وجود برنامـج واسع النطاق للتنصت، ما دفع الكونغرس إلى تبنّي قانون يقيّـد قـدرة وكالـة الأمن القومي في حفظ قواعد البيانات الوصفية المرتبطة بالمواطنين الأميركيين أو القيام بعمليات بحث فيها.

ومع ذلك لم تصادف وكالـة الأمن القومي الأميركيـة في مجال رصـدها طيلة تلك الفترة إلا 42 مشـتبها بهم في الإرهاب، من بينهم مواطن أميركي واحـد فقط، كشف نتيجـة مراقبـة لا علاقة لها بأهداف اسـتخباراتية، بحسب التقرير الذي لم يحدد عدد المواطنين الأميركيين الذين وقعوا في شباك التنصت بالعلاقة مع نشاط استخباراتي فعلي.

ص: 164

3. الأسباب والموجبات

لعلّ أحد الأسئلة الكبيرة المطروحة هو ما يتصل بالأسباب والموجبات التي عملت على تنامي قوى وفعاليات العالم السيبراني وجعلها في طليعة مقوّمات القوّة والسيادة لمن يحسن استخدامها على مختلف المستويات الشخصية والتجارية والسياسية والأمنية وحتى على صعيد الدول بمختلف مراتبها على سلّم القوّة والتحكّم .

فما هي أبرز الأسباب الموضوعية المباشرة التي ساهمت في رفع هذا العالم الافتراضي لتجعل منه مصدرًا حقيقيًّا للقوة والسيادة والتحكم ؟

الحقيقة أنّها أسباب كثيرة، وربما تبدو بسيطة للوهلة الأولى، لكنّها ذات فاعلية وجدوى؛ ومن أهمها ما يأتي:

تزايد ارتباط العالم بالفضاء الإلكتروني. لقد أصبحت معلوماتنا جميعها تقريبًا مخزونة في هذا الفضاء. وهذا يُعتبر بحدّ ذاته وسيلة الرفع نسبة الخطر على هذه المعلومات التي تحفظ وتنظم وتدير كامل البنى التحتية لمختلف الإدارات والجهات على مستوى العالم أجمع، وأيّ عبث بمعلومات أي جهة، لا بد أن ينعكس وبالاً على هذه الجهة. كلّ هذا يُضاف إلى الخطر الكبير الناتج عن دخول أشكال الإرهاب العالمي على الخط. فإذا كانت مشاعية بعض مخازن المعارف في الفضاء السيبراني، هي الوسيلة الناجعة لتيسير هذه المعارف لكلّ من يطلبها وعلى أوسع مدى، فإنّ اقتحام خزانة معلومات لشخص أو شركة أو إدارة رسمية، من شأنه أن يعرّض

للخطر هذا الشخص أو الشركة أو الإدارة، سواء بكشف أسراره أو باستثمارها أو حتى بشطبها وإلغائها بالمرة.

تراجع الدور الحمائي للدولة (وغالبًا أيضًا للقانون) في ظلّ العولمة المكتسحة، وانسحابها من بعض القطاعات الاستراتيجية المصلحة القطاع الخاص، ما أدّى إلى حلول «السلطات السيبرانية» مكانها بطريقة أو بأخرى. في الوقت عينه، تصاعدت أدوار الشركات متعدّية الجنسية، وبخاصة العاملة في مجال التكنولوجيا، كفاعل مؤثر في الفضاء الإلكتروني، لا سيّما مع امتلاكها قدرات تقنية تفوق القدرات المتوافرة للحكومات في أغلب الأحيان.

ولا يصح تجاهل حقيقة أن تطور وسائل الاتصالات ووسائطها ساهم في زَعْزَعَة الوظيفة التوجيهية للدولة في كل ما يتعلق بالتحكّم بالفضاء السيبراني، بحيث أضحى مفهوم الحدود السياسية والجغرافيّة، وكذلك مفهوم السيادة ومفهوم الاستقلال عن الآخرين، من المفاهيم الغابرة التي لا يمكن الاعتداد بها.

نشوء نمط جديد من إمكانيات إحداث الضرر لدولة ترى فيها الدولة الفاعلة منافسًا أو عدوا... وهذا النمط الجديد يُبتنى على خلفية هجمات إلكترونية يمكن أن تلحق أفدح الأضرار بالطرف المستهدف من دون الحاجة للدخول المادّي إلى أراضيه؛ ذلك أنّ تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية، جعل هذه الأخيرة عرضة للهجوم المزدوج، لما لها من سمات مدنية وعسكرية متداخلة، لا سيّما أنّ الثورة التكنولوجية

الحديثـة تمخضت عنها ثورة أخرى في المجالات العسـكرية، ساهمت إلى حدّ بعيد في تطوير تقنيات يمكن اسـتخدامها بفعالية عالية في الحروب(1).

لقد صار بإمكان دولة صغيرة مُستضعَفة أن تواجه مُنفردة دولة مُتفوّقة عسكريًا. ويمكن تحقيق ذلك من قبل الدولة الضعيفة من خلال قيامها بإنتاج برامـج معلوماتيـة متعـددة الغايات والأغراض اسـتطلاع قواعـد معلومات الخصم الإلكترونيـة وتحديد نقاط ضَـعفها والتسـلُّل إليها واسـتنساخها أو تغييرها أو إتلافها، وتشويش الاتصالات السـلكيّة واللاسلكيّة لنظم تشغيل مرافق الدولة، وتوفير المعلومات اللازمة لتوجيه العمليات العسكرية، وتعقب الأهداف الجوّيّة المتنوعة). وستُحرِّر، إذا ، تكنولوجيا الفضاء السيبراني الدول الصغيرة، حَسَنة التنظيم والتدبير نسبيا، من الاعتماد على حلفائها الإقليميين.

قلّـة تكلفـة الحروب السـيبرانية، مقارنة بنظيراتها التقليدية. فقد يتم شنّ هجوم إلكتروني على دولة أخرى بما يعادل عدّة ألوف من الدولارات فقط، أو ربما بمقـدار تكلفـة دبّابة. فالإمكانات السـيبرانية الحديثة تكلّف مالاً، سواء لشـرائها أو لتصـنيعها (برمجتها)، وهي تصـبح أسـلحة إلكترونية جديدة أو تفتح إمكانات هائلة للأسلحة

1- راجع ما أورده الموقع الإلكتروني للجنة الدولية للصـليب الأحمر حول موضوع: "Round table on new weapon technologies and IHL – conclusions" في 13 / 09 / 2011 ، المرجع السابق. وهـذا ثبت بالجملـة الإنكليزية: In cyber space on the other hand, allocation of responsibility does» appear to present a legal challenge if anonymity is the rule rather than the exception». تصفح بتاريخ 2014/04/9 .

التقليدية بمجرّد توافر المهارات البشرية المناسبة. علاوة على أنّ هذا الهجوم قد يتم في أي وقت، سواء أكان وقت سلم أم حرب أم أزمة، ومن دون لفت انتباه الخصم إلا بعد فوات الأوان. وغالبًا ما لا يتطلّب تنفيذ ذلك أكثر من وقت قليل ومحدود.

تحوّل الحروب السيبرانية إلى إحدى أدوات التأثير في المعلومات المستخدمة في مستويات ومراحل الصراع المختلفة، سواء على الصعيد الاستراتيجي أم التكتيكي العملياتي، بهدف التأثير بشكل سلبي في هذه المعلومات، ونظم عملها.

توظيف الفضاء الإلكتروني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوّق أو تأثير في البيئات المختلفة، وبالتالي ظهور ما يسمّى «الاستراتيجيّة السيبرانيّة للدول، والتي تشير إلى القدرة على التنمية، وتوظيف القدرات السيبرانية لتشغيل الآلات والأجهزة بواسطة الفضاء الإلكتروني، وذلك بالاندماج والتنسيق مع المجالات العملياتية الأخرى.

أدى تصاعد المخاطر والتهديدات في الفضاء الإلكتروني إلى بروز تنافس بين الشركات العاملة في مجال الأمن الإلكتروني بغرض تعزيز أسواق الإنفاق العالمي على تأمين وحماية البنى التحتية السيبرانية للدول، من خلال برامج حماية أكثر صلابة وكلفة، وبخاصة بعد بروز فاعلين آخرين من شبكات الجريمة المنظمة والقراصنة، وغيرهم، مااستدعى رفع الإنفاق في الميدان السيبيريّ بغية حماية المعلومات والتمكن من خرق حمايات الخصم أو العدو.

ص: 168

اتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون، سواء من الدول أم من غير الدول في الحرب السيبرانية؛ فقد تشنّ الدول الهجمات الإلكترونية عبر أجهزتها الأمنية والدفاعية، كما قد تلجأ إلى تجنيد قراصنة موالين لها أو مأجورين تشتري مهاراتهم لشنّ هجمات ضدّ الخصوم من دون أي ارتباط رسمي. وعلى الرغم من عدم تطوير الجماعات الإرهابية، كفاعل من غير الدول لقدراتها في الحرب السيبرانية، مقارنة بممارسة القوة الناعمة على الفضاء الإلكتروني، لنشر الأفكار المتطرّفة، فإنّ هناك مؤشرات على احتمال تطوير تلك الجماعات لقدراتها الهجومية مستقبلاً، ما يضع مسائل أساسية مثل القوة والسيطرة والتحكّم، في مجال الخطر.

4. هجوم بلا أثر

لقد بات واضحًا اليوم أنّ السلاح الأمضى والقوة الأعتى والأداة الأفعل للتقدّم والتطوّر، ولفرض القوّة وتحقيق السلطة والسيادة على العدوّ ومقدّراته، وعلى المنافس والصديق والحليف على حدّ سواء، هو القوى السيبرانية. إنّ الخط الفاصل بين هجوم عسكري وعملية تجسّس ضمن الفضاء السيبراني، تكون أكثر غموضًا في عالم الإنترنت. فالهجوم الإلكتروني عمومًا لا يتطلب تحركا لأجسام مادّيّة على الأرض ولا في البحر أو الجوّ، كذلك فهو لا يعرض جنود المهاجم للخطر ولا للانكشاف. وقد تستخدم وكالات الاستخبارات الثغرة نفسها للتجسّس على عدوّ ، أو كسلاح هجومي لشنّ هجوم مفاجئ عليه، يُعطّل قواه السيبرانية أو جزءً منها.

وبالإمكان استخدام الغموض هذا في سبيل حجب المسؤولية. ومن هنا جاء الإثبات، ولمرّة جديدة أيضًا، لمقولة أنّ المعرفة هي بحد ذاتها قوة، وبالتالي فالأوسع معرفة هو الأكثر قوة وقدرة على السيطرة على العدوّ والمنافس، وعلى الصديق والحليف. وفي حالات أخرى يمكن للأقوى سيبرانيا دفع العدوّ أو الخصم إلى حافة الهاوية ليدمّر ذاته بنفسه. وكلّ ذلك يتأتى من خلال العلوم الرقميّة وتكنولوجيا المعلومات.

وليس هناك شكّ أنّ هناك بعض الدول تستثمر بالفعل أموالاً طائلة في القدرات الإلكترونية التي يمكن استخدامها لأغراض عسكرية. ويبدو للوهلة الأولى أنّ سباق التسلح الرقمي يقوم على منطق واضح وحتمي، لأنّ مجال الحرب الإلكترونية يقدم ميزات عديدة فهي غير تقليدية وغير مكلفة وجميع المزايا تصبّ منذ البداية في الجانب الهجومي.

علاوة على ذلك، فليس هناك رادع فاعل في الحرب الإلكترونية، لأنّ تحديد المهاجم عمليّة صعبة جدًّا، وفيها يكون الالتزام بالقانون الدولي مستحيل تقريبًا . وفي ظلّ هذه الظروف، قد يكون أي شكل من أشكال الردّ العسكري مشكلة كبيرة جدا، من الناحية القانونيّة والسياسيّة.

لكن بدلاً من الحديث عن الحرب الإلكترونية كحرب في حدّ ذاتها – يتم وصف الهجمات الإلكترونيّة الأولى باعتبارها «عمليات تسلّل رقمي أو هجمات 9/11 في العالم الإلكتروني» – وهو

وصف مناسب إلى حدّ كبير للحديث عن الهجمات الإلكترونية كوسيلة من وسائل الحرب. إنّ مخاطر الهجمات الإلكترونية حقيقية وتتطوّر أكثر فأكثر. في نفس الوقت، ليس هناك من داع للخوف، لأنّ هذه التهديدات في المستقبل القريب لن يكون من السهل التنبؤ بها أو السيطرة عليها تماماً.

5. الحكومات يتجسّس بعضها على بعض

الحقيقة أنّه لم يعد سرًا أنّ معظم الحكومات يتجسّس بعضها على بعض، بل على شعوبها أيضًا. فالحكومات تقوم بهذا الإجراء تحت مبررات وذرائع متعدّدة ومتباينة. لكن في كلّ مرة ينجح طرف التجسّس على آخر يكسب أفضليّة على هذا الطرف الآخر. فالمعلومة أيضًا قوّة. وفي عصرنا فإنّ الطريق إلى اكتساب القوّة، تمرّ من خلال كشف الآخر والاطلاع على خصوصياته. وهذا ما يفعله التجسّس الإلكتروني أو القرصنة السيبيرية.

والأمثلة التي اشتهرت عالميًا في هذا الميدان تكاد تكون فضائحيّة. منها مثلاً أنّ عملاق البرمجيات العالمية شركة «مايكروسوفت انتقدت فكرة تخزين المعلومات على شبكة «الإنترنت بغض النظر عن الإجراءات الحمائية التي تتبعها الدول والمؤسسات في هذا الشأن، واعتبرت أنّ هذه المعلومات تظلّ قابلة للسرقة والاختراق مهما بلغت حمايتها. وجاء في بيان صدر عن الشركة) ... ولقد رأينا معلومات مخزنة من جانب وكالة الاستخبارات المركزية الأميركية، وهي تُعرض على «ويكيليكس»،

ص: 171

وهي كناية عن بيانات سُرقت جرت قرصنتها من وكالة الأمن القومي الأميركية، وأضرت بالعملاء حول العالم! وقالت الشركة في بيانها إنّ هجوم فيروس الفدية» بمنزلة «ناقوس خطر» للتحذير من ضعف الإجراءات الحمائية للمعلومات.

كذلك ذكرت صحيفة «نيويورك تايمز» أنّ وكالة الأمن القوميّ الأميركيّة تواجه أزمة بعد أن تمكّن القراصنة (الهاكرز) من اختراقها في العام 2016 وسرقة برامج فيروسيّة تستخدم للتسلّل إلى الأجهزة والشبكات الأخرى حول العالم.

وكانت مجموعة الهاكرز المعروفة بلقب Shadow Brokers قد نشرت كودا برمجيا لبرامج سرقتها من وكالة الأمن القومي، وكانت تستخدم لإنشاء الفيروسات التي تسبّبت بأضرار كبيرة لأجهزة الكمبيوتر في جميع أنحاء العالم.

ولم تعلق الوكالة الأميركية رسميًا على النبأ ولكنّ الصحيفة تعتبر أنّه تمّ الإثبات بالدليل الدامغ أنّ السلاح السيبراني المسروق يعود إلى جهاز الاستخبارات المذكور الذي يُعتبر الإدارة الضاربة في مجال التجسّس الأميركي.

وأكدت الصحيفة أنّها تلقت تأكيدًا من موظفين حاليين وسابقين في المؤسسة الأمنيّة على وجود عواقب كارثية لعمليّة السطو بالنسبة إلى الوكالة، وذلك لأن الحادث وَضَع محلّ الشكّ الكبير قدرتها على حماية الأسلحة السيبرانية القوية.

وقالت إنّ الوكالة، التي تُعتبر المؤسسة الرائدة عالميًا في

اختراق شبكات الكمبيوتر لدى الخصوم، لا تستطيع حماية شبكاتها الخاصة. وشبّهت الصحيفة سرقة الوثائق بالزلزال الذي هزّ وكالة الأمن القومي في أساسها، معتبرة أنّ "عواقب ذلك قد تكون أقوى بكثير من عواقب فرار موظف الاستخبارات السابق إدوارد سنودن. فالأخير كشف اسم برامج المراقبة الإلكترونية الشاملة، أما الهاكرز فقد نشروا شيفرة هذه البرامج، وبالتالي سمحوا باستخدامها من قبل أطراف ثالثة.

واختتمت الصحيفة بأنّ الاستخبارات الأميركية لم تستطع بعد تحديد كيفية حدوث هذا التسرب، وما إذا كان أي من الموظفين متورّطاً فيه.

الأكثر إثارة في ما يتعلّق بموضوع التحكم والسيطرة، هو قدرة دولة معيّنة تحديدًا على منع وصول الإنترنت بشكل كامل إلى دولة أخرى أو إلى إقليم بأكمله، وهذه الدولة هنا هي الولايات المتحدة الأميركية التي تُعتبر المتحكم الفعلي في مجمل الفضاء الإلكتروني. وجدير بالذكر في هذا الخصوص أنّ وكالة الأمن القومي الأميركيّة مارَسَت التنصت على أكثر من 150 مليون مكالمة هاتفية داخل الولايات المتحدة خلال العام 2016 ، على الرغم من القيود التي وضعها الكونغرس على هذا النوع من النشاطات. وهذا يؤكد الأهمّيّة البالغة للفضاء السيبراني في عملية كشف بواطن الآخر (الذي يمكنك التجسّس على معلوماته، وهي ما يُفضي بك في حال نجاحك بالحصول على معلوماته، إلى السيطرة عليه والتحكّم به.

ص: 173

6. منافسة الفضاء التقليدي

في ما يتصل بالسيطرة – وربما أيضًا بالهيمنة – الأميركية على شبكة الإنترنت يمكن قراءة دوافعها انطلاقا من عاملين العامل التاريخي الذي يتعلّق أساسًا بموضوع الأسبقية، حيث أنّ شبكة الإنترنت هي وليدة الأراضي الأميركيّة، والعامل التقني الذي يتعلّق بالبنية التحتية للفضاء الإلكتروني والبروتوكولات الرقمية التي وضعها علماء التكنولوجيا الأميركيون الذين كانوا يعملون ضمن طاقم وكالة مشاريع البحوث المتقدّمة التابعة لوزارة الدفاع الأميركية في بداية ستينيات القرن المنصرم.

هذا التطور الكبير أتاح أسلوبًا جديدًا في التعامل الدولي لم يَكُن قائماً ولا متوقعًا عندما جرى وَضعُ النظم القانونية السائدة. فبعد أن كان التعامل الدولي خلال المنازعات المسلحة يجري على الأرض أو في البحر أو في الجوّ أو في الفضاء الخارجي، أصبح، بفعل التقنية السيبرانية ، يتم بطريقة إلكترونية ضمن نظام معلوماتي يختلف كلّيًا عن أنواع الحروب التقليدية المعروفة؛ الحرب البرية والبحرية والجويّة، إن لجهة اختراق منظومة العدوّ الإلكترونية أو لجهة جمع المعلومات الإلكترونية الحساسة أو نقلها أو تبادُلها(1).

---

1 – Linant de Bellefonds et A. Hollande "Il est important d'opé rer une distinction entre é tats راجع ما كتبه1: informatiques de sortie et é tats informatiques de stockage. Les premiers (hard- copy, listes d'imprimantes, microfilm) constituent une visualisation stabilisé e de l'information. Les maté rialisations sont é videment celles qu'on produira le moment venu. Mais la plupart du temps, ces visualisations auront é té pré paré es de maniè re extemporané e a partir d'une information normalement stocké e

ومع تزايـد الاعتماد على الوسائل التقنيـة الحديثـة في إدارة الأعمال المختلفة، بَرَزَت تحديات قانونية، وطرحت تساؤلات حول إمكان اعتبار التواصل الإلكتروني الافتراضي (Virtual communication) الذي أصبح يتم اليوم بواسطة الإنترنت (Internet) أو الفضاء الإلكتروني أو فضاء السايبر أو الفضاء السيبراني (Cyberspace)، موازيًا للمرافق العامة الدولية التقليدية، وحول ضرورة عقد معاهدات جديدة تنسجم مع التطور التكنولوجي إنْ لم تكن الإمكانية الأولى متاحة أو كافية.

لقد أصـبح الفضاء السيبراني مُنافسًا حقيقيًا للنطاق الدولي التقليدي (من برّ وبحر وجوّ وفضاء خارجي). على الرغم من ذلك لا يجوز القفز فوق المرحلـة الانتقاليـة واعتبارها غير موجودة؛ فهي مرحلـة ضـرورية لا بـدّ من المرور بها في سبيل بلورة الوضع القانوني الخاص بالفضاء السـيبراني والـذي يلتزم به الجميع. ومن معالم هـذه المرحلـة أنّ الثقافـة القانونيـة التي لا تزال إلى حد بعيد مُشـبعة بمفهوم النطاق الدولي التقليـدي (أو) الواقعي أو الحقيقي)، تميـل إلى جَعْل الوضع القانوني لهـذا الأخير مقياسًا لنجاح ونجاعـة قوانين الفضاء السـيبراني، بمعنى آخر، كلّما تم التصديق على معاهدات أو ترسخت مواقف اجتهاديّة أو ظهرت آراء فقهيّة تذهب إلى إعطاء الفضاء

sous la forme magné tique. C'est donc, en fin de compte, la valeur de l'enregistrement magné tique en tant que mode de preuve, qui doit e ̂tre appré cié e" (Droit de l'informatique et de la té lé matique, J. Delmas et cie, (2è me é dition, p. 141

ص: 175

السـيبراني وضـعا قانونيا، فإنّها تتّخـذ من النطاق الدولي التقليدي مثالاً تحتذيه لجعل الفضاء السـيبراني قابلاً للانضـمام إلى النظم القانونية السائـدة أو المعروفـة. وبصـرف النظر عن منسوب الصـحة والخطـإ في هـذا الوضع، ، فقـد بـات من الممكن اعتبار أنّ الأقوى في الميـدان السيبراني هو الأقوى في التحكم بمعلوماته وحمايتها، والأقدر على تهديد الآخرين.

والواقع أنّ الفعّاليّات السـيبرانية تتجاوز مجرد كون الفضاء السـيبراني أداة تكنولوجيـة ومهنية أو مخزنا هائلاً للمعلومات والعمليّات التبادلية السـريعة لهـا، وتطوّراتهـا المتلاحقـة إلى فعاليات متعـدّدة ومركبـة المسـتويات والفعّاليّات، جغرافيا وديموغرافيا، واقتصاديا وماليا وشـعبياً واجتماعيـا وسـلوكيا وصـحيا وثقافيا ونفسـيا، وسياسـياً وعلميا ، وأمنيًا وعسـكريا، وداخليا وخارجيا، وعلى المسـتويات الرأسـية والأفقيـة، والاستراتيجية والتكتيكية، والسرّية والبنية التحتية والفوقية كافّة.

من هذه الخصوصية المتعدّدة والمركبة تصاعدت أهميّتها الخطيرة إلى استهداف الوصول إلى ماهية التملك والتحكم والسيطرة والاستحواذ، والتغلغـل والتلاـعب والفوضـى والاـختراق والتسـلّل، والتصـيّد ،والإخفاء، والمراقبـة والتجسّـس، والتشويه والتضـليل والخـداع والحرمان والاسـتباق والتجـاوز الجغرافي والمادي، وأصـبحت هـذه الفعّاليّات تشـكل ديناميات الحرب السـيبرانية التي تسـتهدف تخريب كلّ هـذه المستويات والفعاليات المركبة وتعطيلها وسرقتها والتحكم فيها اعتمادًا على السيطرة والتحكم الواسع النطاق

ص: 176

الفضاء السيبراني بكل تطوّرات التقنية المستمرة، وبما يحقق المستهدف من شنّ الحروب السيبرانية وعسكرة الفضاء السيبراني.

7. تغييرات في مفاهيم السيادة

لم يعد خافيًا أنّ مختلف وسائل السيطرة والتحكّم في مُعظم العمليات الحيوية الموجودة على الأرض قد انتقلت إلى الفضاء في صورة أقمار صناعية ومحطات فضائية، كما انتقل أيضًا قطاع واسع من الحروب والمعارك والحوارات والثورات إلى العالم الافتراضي الذي بناه الإنسان باختراعه الكومبيوتر والذاكرات الإلكترونية وشبكات المعلومات، وأنشأ داخله جغرافيا افتراضية جديدة(1).

لكلّ ذلك، فإنّ المقدرة على اقتحام قرصنة) الفضاء السيبراني لدولة ما، يتيح التحكّم بتلك الدولة والسيطرة على مقومات قواها وغناها وقدراتها، وبالتالي الهيمنة على قراراتها، من دون أن تملك تلك الجهة (الدولة) إمكانيّة الرفض أو التمرّد. لذلك، ومن باب ولى، تعمل الجهات جميعها من الشركات الصغيرة والمؤسسات الناشئة إلى الدول والشركات العابرة للقارات على حماية معلوماتها التي تكون قد خزنتها ضمن الفضاء الإلكتروني وأحاطتها بكلّ وسائل وسُبل الحماية والتحصين.

ومن هذه الخصوصية المتعدّدة والمركبة تتأتى أهمية السيادة السيبرانيّة وتوجهاتها الاستراتيجية نحو استهداف الوصول إلى ماهيّة التملك والتحكّم والسيطرة والاستحواذ، والتغلغل والتلاعب

1- https://www.lebarmy.gov.lb/ar/content.

والفوضـى والاختراق والتسلّل والتصيّد، والإخفاء والمراقبة والتجسّس، والتشويه والتضليل والخداع والحرمان، والاستباق والتجاوز الجغرافي والمادّيّ. وتشـكل هذه الفعاليات بمجموعها ديناميات الحرب السـيبرانية التي تسـتهدف تخريب كلّ هذه المسـتويات والفعاليات المركبة وتعطيلها وسـرقتها والتحكم بها، اعتمادًا على السـيطرة والتحكّم واسع النطاق في محتويات الفضاء السـيبراني، وكذلك بمختلف التطوّرات التقنية المسـتمرة، بما يحقق الهدف. هكذا شـهد مفهوم الأمن الوطني تطوّرًا بدا أنه على صـلة وثيقة بمستوى المعلومات ومدى القدرة على التحكم بها والسـيطرة عليها وحمايتها واسـتخدامها لصالح الطرف الذي يمتلكها. وهنا تضاعفت أهمّيّة وقيمة السـيادة السيبرانية التي تؤطّر معايير السـيادة في عصر المعلومات، وبخاصّة بعد تفاقم خطر التهديد السيبراني والحروب السيبرانية، ومسارعة الدول المتقدّمة إلى تشكيل قيادات عسكريّة تُوضع في تصرفها كفاءات سيبرانية مختصة في التخطيط، لصد هجمات القراصنة (Hackers) وشن حروب إلكترونية ضدّ المنافسين والخصوم الاستراتيجيين.

والحقيقـة أنّ المعلومات وكلّ ما يجري وما يمكن تنفيـذه على مختلف المسـتويات، ضـمن ومن خلال الفضاء السـيبراني، أحدث تغيرات هائلـة في مفهوم القوّة والسـيادة والأـمن في العالم، وفي كيفيات تحقيق السـيطرة والتحكّم والإخضاع. فقـد انتقلت نقاط القوّة والمنعـة من العديد البشري والكفاءات العسكرية التقليدية والخصوصيات الاقتصادية والجغرافية للبلد، لتتحوّل إلى ما

يتصل بالفضاء السيبراني والإمكانات المتاحة فيه لهذا الطرف أو سواه، ولا سيّما ما يتعلّق بعولمة الاتصالات، وتبادل المعلومات، وسهولة انتقالها بشكل عابر للجغرافيا. بالنظر إلى الأهمّيّة القصوى للمعلومات المخزنة أو المتبادلة في الفضاء السيبراني ومن خلاله، سواء بالنسبة إلى أصحابها وهي ثروتهم الحيوية وسواعد حياتهم وقواهم وإنتاجهم وصيرورتهم، أو بالنسبة إلى الآخرين من منافسين ومضاربين وشركاء وأخصام وأعداء... فقد فرض الأمن السيبراني وجوده، كونه واحدة من أوّل وأهم وأبرز الحاجات الملحة للإنسان الحديث، بمعنى أنّ فقدان هذا الأمن بالنسبة لأيّ طرف شخص مفرد أو مؤسسة أو شركة كبرى أو دولة...) يُفضي إلى جعل هذا الطرف رهينة لمن قام بعمليّة خرق الحمايات واقتحام المعلومات. فطالما أن تجريد أي جهة من معلوماتها المخزنة في الفضاء الإلكتروني، هو مثابة تجريد لها من مقوّم حياتها الأوّل والأساسي الذي لا غنى لها عنه ولا بديل، فكيف بالحري سيكون حال تلك الجهة فيما لو استخدمت جدائل معلوماتها ضدها... ولصالح الآخر الذي ربما يكون عدواً أو منافسًا أو قرصانا يبحث عن فدية...؟

إنّ تاريخ وتطوّر المجتمعات البشرية غالبًا ما يمر بمنعطفات تاريخيّة تحدّدها الثورات المناخيّة أو الشعبيّة أو الثورات الصناعية والعلمية والتكنولوجيّة. وعلى سبيل التحديد، فإنّ تطور وسائل الإنتاج المتاحة بفضل العلوم والتكنولوجيا سوف يترك انعكاساته على البنى الاجتماعيّة، وكذلك على البنى السياسية للدول، بحيث

أنّ الدولـة الأكثر تقـدّمًا علميًا وصـناعيا وتكنولوجيا سوف تكون الأقـدر على فرض احترام قواها على الصـعيد الدولي، والأقدر كذلك على الدفاع ضدّ الأعداء، والسـعي إلى إخضاعهم لقواها بما يجعلها تُسـيطر وتسود عليهم. ولعلّ هذا ما يمكن ملاحظته على المسـتوى الدولي اليوم، حيث أنّ دول الغرب المتقدمـة باتت هي الأغنى والأقوى أيضًا. فالمجتمع الـدولي يُفسـح مقاعد الصـفوف الأولى للأقوى والأغنى، ولهذا تكون السلطة والسيادة والسيطرة بأيديهم.

ص: 180

الخاتمة:من يحكم الإنترنت؟

ص: 181

الخاتمة:من يحكم الإنترنت؟

يمكن النظر إلى مسألة من الذي يحكم شبكة الإنترنت أو يتحكّم بها على مستويين اثنين:

المستوى الأوّل: يتصل بالعلاقة البينية للدول بعضها مع بعض داخل النظام الدولي. وهنا توجد وجهتا نظر متضاربتان:

الأولى تتمحور حول المبادئ الليبرالية المتعلقة بالمحافظة على خاصية الانفتاح واللامركزية اللتين تتصف بهما شبكة الإنترنت، حيث يجري التنظير للشبكة حسب وجهة النظر هذه على أنّها الأداة التي من شأنها دعم التوجهات الديمقراطية وحقوق الإنسان، وتعزيز فرص التقدم والازدهار الاقتصادي. وتُعتبر الولايات المتحدة الأميركيّة رائدة هذا التوجه، تدعمها إلى حد كبير الدول الأوروبية.

والثانية تتعلّق بالدول التي تسعى إلى تحدّي وجهة النظر الليبرالية بالدعوة إلى اتفاقية دولية متعدّدة الأطراف، وذلك من أجل كسر احتكار وهيمنة الولايات المتحدة على مصادر التحكّم والسيطرة التابعة لشبكة الإنترنت. وتُعتبر الصين وروسيا وبعض الدول الكبرى في العالم الثالث كالبرازيل وإيران من أعلى الأصوات

العالميّة التي تتبنّى وجهة النظر هذه.

أمّا المستوى الثاني: فيتعلّق بمدى سيطرة الدولة على الإنترنت ضمن حدودها السياديّة. وهنا يبرز إلى الواجهة ذلك التضارب بين عالم الشبكة العنكبوتية من ناحية، وهو الآخذ في التنامي كظاهرة من ظواهر العولمة وأداة فاعلة لها، وبين سيادة الدولة التي يجادل كثيرون بأنّها آخذة في التآكل من الجهة المقابلة. هذا ما دفع بعض المختصين إلى طرح مسألة بروز الطلائع الأولى لحقبة جديدة من النظام الدولي، يتلاشى فيها النظام السابق القائم على مبدأ «الدولة – الأمة كما هو متعارف عليه منذ اتفاقية وستفاليا في القرن السابع عشر ليحل محله نظام يتمتّع باللامركزية بشكل أكبر.

فالشبكة بوضعها الحالي تتحدّى بشكل لافت مبدأ المركزية الذي تتصف به ،الدول، وقد باتت الدولة – على سبيل المثال – عاجزة في أحيان كثيرة عن فرض سيطرتها على كثير من مظاهر السيادة، كالتحكم بتدفّق المعلومات والتعاملات التجارية والتواصل بين الشعوب عبر الحدود كذلك فإنّ الشركات العملاقة أصبحت قادرة على توجيه اقتصادات الدول من خارج حدودها؛ وهذا كله من جملة عوامل السيطرة. ولا يصحّ التغاضي عن واقع أنّ بعض الدول أصبحت قادرة على توجيه الرأي العام في دول أخرى بما يخدم مصالحها هي، وذلك

من خلال بعض منصّات الفضاء الإلكتروني، وهذا يتيح لها من بين ما يتيحه – ، إثارة القلاقل في الدولة المستهدفة وتحريك شارعها خارج المصلحة الوطنية. ولعلّ الكثير من أحداث ما عُرف ب– «الربيع العربي قدّم الدليل على ذلك. وربما يمكن اعتبار الانتخابات الأميركية الأخيرة وما رافقها من تضليل للرأي العام الأميركي (من الداخل والخارج من خلال الآلاف من الحسابات الوهمية والأخبار المزيفة على شبكة «الفيسبوك» و«تويتر»، مثال آخرعلى ذلك.

وعلى أيّ حال يبقى الحديث عن تهاوي أو تلاشي سيطرة الدولة محلّ جدل كبير.

فما زالت الحكومات قادرة على فرض القيود الشديدة على شبكة الإنترنت سواء من خلال منعها لبعض المواقع المناوئة لها، أم من خلال برامج التجسّس والمراقبة التي تحدّ من خصوصية المواطنين، أو حتى من خلال التهديد بفرض عقوبات من نوع ما، على شبكات تزويد المعلومات في الفضاء الإلكتروني. وفي هذا الصدد يبرز النزاع الذي جرى بين الصين وبين شركة (ياهوو» كمثال على استمرار قدرات الدولة على فرض سيادتها على شؤونها الداخلية.

يعود بنا هذا المثال للتأكيد على فرضية في غاية الأهمية تتعلق

بالأسـطورة التي تتحدّث عن لامركزية شبكة الإنترنت وأنّ الفضاء الإلكتروني غير خاضع – من حيث المبدأ – للسيطرة. مثل هذه المفاهيم المغلوطة ترتكز غالبًا على شـيء من الصواب، مقابل الكثير من الوهم أيضًا. فشـبكة الإنترنت من حيث الوصول والاستخدام تتمتّع بخاصية الانفتاحيّـة واللامركزيـة ولكن من ناحيـة السـيطرة والتحكّم فهي بالتأكيـد مركزيّة إلى حدّ يثير الدهشة، وهذا يعني أنّ هنالك مصدرًا معيّنا يفرض قوانين صارمة في ما يخص بنية شبكة الإنترنت وطبيعة العمليات التي تجري فيها.

فالشـبكة تعمل على دفع حركة المواطن من خلال المساعدة على تقوية التنظيم السياسـي والشـرعيّة السياسـية، وتعزيز قدرة الحصول على الـدعم الشـعبي، والقدرة على تحديد الهدف، ووضع استراتيجية للحركة، وتعزيز القدرة على القيادة؛ كلّ ذلك يتحرك في شـكل مُخرجات يقودها المواطن، وتظهر في عمله على إحـداث التغيير السياسـي التـدريجي أو الجـذري، والقدرة على تقييم مُعدّلات المكسب والخسارة والمشاركة في الانتخابات ودعم الإعلام ونقل المعلومات.

وفي حركـة موازيـة لحركة المواطن تدفع شـبكة الإنترنت إلى القيام بعملية نقل المعلومات، وتعبئة وحشد الرأي .العام. وبهذا يكون الفضاء الإلكتروني بمثابة آلية مهمة في عملية

ص: 185

التأثير على الرأي العام. وتتميّز في ذات الوقت بعدد من الخصائص حيث أنها قد تكون أداةً لنشر رأي عام ذي طابع فردي مُعين، وذلك بنشر معلومات موجهة من خلال مجموعة من البرامج والأدوات، والمقالات والأخبار والصور، والتفاعلات الإعلامية المتنوعة والتي تخدم بشكل غير مباشر، ومن حيث لا يشعر المتلقي، ذلك الرأي.

ويتميّز التواصل الإلكتروني بوجود حالة من الانفتاح على الخارج وما يحمله من قيم مغايرة عن قيم الداخل إلى أن تكون هناك عمليّة تغيير معرفي وقيمي عبر عملية طويلة تتنوع فيها جزيئات التكوين المعرفي الجديدة التي يُراد إحلالها محلّ المعرفة القديمة.

ومن الآليـات التي ينتهجهـا مرتـادو الفضاء الإلكتروني في التأثير على الرأي العام، يمكن ذكر الانحياز إلى بعض الآراء وإبرازها للجمهور، والتركيز عليها بأكثر من ،طريقـة، سواء أكانت مُباشـرة أم غير مباشـرة ، والاحتفاء بها، والحديث عن إيجابياتها، والتقليل من شأن سـلبيّاتها، وفي المقابل تقوم بتشويه الآراء الأخرى، وإبراز سـلبياتها ،وتضـخيمها وافتعال الإشـكالات حولها، ويصل الوضع أحيانًا لحدّ تجاهُل تلك الآراء وحجبها عن الجمهور.

ص: 186

القرصنة

القرصـان هو اللقب الـذي يُطلق على لص البحـار. وهـذا ينبغي أن يكون خارجًـا على القوانين المتعارف عليها . يقتحم السـفن في أعالي البحار ويحوّل اتّجاهها نحو ملاذات خاصة به، ويعمل على سلب حمولاتها وقتل أفراد طواقمها إن رأى في ذلك مصلحة له.

هـذا هو قرصـان البحـار؛ أما قرصان الكومبيوتر (هاكر Hacker) فهو شـخص مختص بالعلوم الإلكترونيـة ومبرمـج متمكن من المهارات العالية في مجال الحوسبة والمعلوماتية والبرمجيات. يقتضي عمله بأن يقتحم حسابات الآخرين على الإنترنت أشخاصًا أو شركات أو دولاً، ويصل إلى المعلومات المخزنـة لهـذا الطرف أو ذاك. دخوله إلى تلك المعلومات (المحميـة كما ينبغي) ينفّذه بطرق غير مصـرّح بها، ومن دون الإذن من مصدرها، مسـتخدمًا معارفه ومهاراته وربما أيضًا برامج يبتكرها أو يحوز عليها، فيفتح ثغرات في حصون الحماية الإلكترونية للمعلومات التي يطلبها تتيح له الدخول والخروج من دون إعاقات، ويعمد إلى التصرف بالبيانات التي يتحصل عليها، فإما أن يوجه الأموال التي تتحكّم بها إلى حسابات مصـرفية سرية له أو لزبونه، أو إنّه يبتز أصحاب البرامج فيمنعها عنهم إلى أن ينال منهم ،مُراده، أو يضطرهم إلى الخضوع لمتطلبات الطرف الذي يُشغله لقاء أجر.

ص: 187

وفي هذا السياق، يمكن تقديم أحد الأدلة التي تُثبت أنّ التجسّس على معلومات الجمهور الواسع باتت في هذا العصر، نوعًا من القاعدة، ويجري اعتمادها لمجرد الشك، فتُتيح فضح أسرار المواطن من دون أن يكون على دراية بما يحصل. فبعد الحادثة بسنوات، كشفت الصحافة الأميركيّة، على سبيل المثال، أنّ وكالة الأمن القومي الأميركية تنصتت على أكثر من 150 مليون مكالمة هاتفية داخل الولايات المتحدة خلال العام 2016 ، على الرغم من القيود التي وضعها الكونغرس على هذا النوع من النشاطات(1).

من جهة ثانية وبالنظر إلى الأهمية الفائقة للبرمجيات بالنسبة إلى أصحابها من باب أولى، وحاجتهم الحيوية إليها، فإنّ قرصنتها تُعتبر عملاً إجراميًا خطيراً وفادح الضرر. والقانون يعتبر الهاكر دخيلاً تمكن من اقتحام مكان افتراضي لا ينبغي له أن يكون فيه.

وبالنظر إلى خطورة عمليّات القرصنة فقد درجت مُختلف الشركات العملاقة والصغيرة وحتى الأشخاص الذين يُشغلون أجهزة رقمية (كالكومبيوتر المنزلي) إلى اعتماد برامج حماية خاصة تمنع اقتحام أجهزتهم والمعلومات المخزنة فيها وإعاقة عملها. وعمدت شركات عملاقة مثل «مايكروسوفت إلى توظيف قراصنة سابقين يجري

1- عادل عبد الصادق، حروب المستقبل، الهجوم الإلكتروني على برنامج إيران النووي، مجلّة السياسة الدولية، مؤسسة الأهرام، أبريل 2011.

تكليفهم بالعثور على أساليب ووسائل لاختراق أنظمة الشركة ذاتها، المعالجة ذلك مسبقًا، والعثور على أماكن الضعف فيها، وتدبّر سبل للوقاية اللازمة لتجنّب الأضرار التي قد يتسبب بها قراصنة آخرون من صفوف الأعداء أو المبتزين أو الإرهابيين.

عُرفت البرمجيات الخبيثة والمخرّبة واشتهرت باسم الفيروس (Virus)، وبات من شأنها أن تستهدف» أي برنامج آخر يعمل في جهازك المكتبي أو المنزلي أو في الحواسيب الضخمة التابعة للشركات أو للدول، تدخل فيه بواسطة التقنيين المقرصنين، فتسرق منه المعلومات المثبتة، لتعود بها إلى مُشغلها، ولو كان على الطرف الآخر من الكوكب. هذا نموذج كلاسيكي من هجمات القرصنة السيبرانية التي يقوم بها متسلّل قرصان.

فيروسات الفدية وكيف تعمل؟

بات من المفروغ منه منه أنّ جميع قطاعات الأعمال والخدمات والمال والاقتصاد والأمن والأمور العسكرية، وقطاعات النقل والمواصلات والتزويد والتصدير ،والاستيراد ومختلف الشؤون من دون استثناء في معظم الدول، ولا سيّما المتقدمة منها، تشكل القوّة الأساسيّة لأصحابها من أشخاص ومؤسسات وشركات ودول. والحيلولة دون وصول أصحاب الحسابات إلى حساباتهم بأيّ

طريقة كانت يتسبّب بأضرار فادحة لأصحاب هذه الحسابات، بحيث يكون كثيرون منهم، ولا سيّما المؤسسات الكبيرة والدّول، مضطرين لدفع مبالغ كبيرة يحدّدها القرصان»، لإعادة حساباتهم إليهم وفكّ القيود عنها. وهذه المبالغ التي يطلبها القرصان لإعادة تحرير الحسابات الإلكترونية التي يدخلها ويمنعها على أصحابها،

هو مثابة الفدية والتي إن لم يتم دفعها، فإنّ الحسابات المقرصنة تبقى ممنوعة على أصحابها، وقد يلجأ مقرصنها إلى بيعها لطرف يريدها أو يعمد إلى إتلافها.

وثمة أعداد لا حصر لها لها من فيروسات الفدية الموجودة والتي يمكن ابتكارها، إذ يمكن لكلّ ضليع بالإلكترونيات وفنون البرمجة ابتكار وبرمجة «فيروس خبيث قد يتجاوز حصون الحماية للحسابات الإلكترونية، ويقتحمها لتعطيلها، ثمّ يطلب الفدية التي يشاء لإعادتها إلى تصرّف أصحابها. وفي حالات معينة يصعب بل ويستحيل على صاحب الحسابات القضاء على الفيروس المعتدي أو صدّه، ما ينتهي به إلى دفع الفدية صاغراً لاستعادة حساباته المقرصنة. ومن الملاحظ هنا أنّ التطوّر التقني حتى في الدول المتقدّمة، لا يحميها من البرامج الخبيثة ولا من القرصنة الإلكترونية. من هنا، فإنّ طبيعة الأخطار التي تأتي من الفضاء

السـيبراني، تضع الجميع في مواجهـة خطر التهديـد، من دون اسـتثناء، طالمـا أن لا غنى عن المعلومات المخزنـة، ولا بـدّ من العودة إليها والاسـتعانة بها، وربما بشـكل لحظوي متواصل الحاصل أنّ بلدًا فائق التقنية والتطوّر والاسـتعداد، كالولايات المتحدة الأميركية، على سبيل المثال، أصـبحت الدولة الأكثر تعرّضًا لخطر التهديد السـيبراني، بحسب ما أعلنه مسؤولون في وكالة الاستخبارات الأميركية «سي آي إيه»؛ بل إنّ هؤلاء لم يترددوا في اعتبار أنّ التهديـد الأكثر تحـدّيا الـذي تواجهه الولايات المتحدة، يأتي من الفضاء الإلكتروني. وهذا التطوّر في مصادر الخطر والتهديد يفسّـر الزيادات الهائلة في حجم سوق الأمن السـيبراني، الذي يبلغ بحسب إحصاءات عام 2017 ، أكثر من 120 مليار دولار، محققاً زيادات بلغت نحو 13 ضعفًا على مدى السنوات ال- 13 الماضية.

ص: 191

المؤلَف في سطور: محمود برّي.

- صحافي وباحث لبناني في الاستراتيجيات الدولية.

- متخصص في التاريخ والحضارات المعاصرة.

- صحافي ومترجم من العربية وإليها باللغتين الفرنسية والإنكليزية.

- مستشار علمي لعدد من مراكز الأبحاث والمجلات المتخصصة في لبنان والعالم العربي.

- رئيس تحرير مجلة الدفاع الوطني الصادرة عن وزارة الدفاع اللبنانية، (1999-2008).

- شارك في عدد من المؤتمرات التخصصية في لبنان والخارج.

- من أعماله:

1- النانو التكنولوجي - وعود جديدة، مخاطر جديدة صادر عن مؤسسة الفكر العربي - بيروت 2011

2- السيبرنطيقا علمُ القُدرة على التّواصل والتّحكُم والسيطرة - المركز الإسلامي للدراسات الاستراتيجية بيروت 2019م، هذا الكتاب.

- له العديد من الدراسات والأبحاث في مجال الفكر المعاصر، والعلاقات الدولية.

ص: 192

هذا الكتاب: السيبرنيطيقا.

هذه الدراسة التي تدخل كحلقة جديدة ضمن سلسلة مصطلحات معاصرة تعني بمصطلح مستحدث جرى تداوله في السنين الأخيرة في حمى الثورة المعلوماتية عنينا به مصطلح "السيبرنيطيقا.

تحاول الدراسة مقاربة هذا المصطلح كمفهوم يما يعنيه من قدرة الانسانية على التواصل والتحكم والسيطرة في مجمل نواحى حياتها المعاصرة.

من المقدمة

المركزالاسلامى للدّراسات الاستراتيجيّة

http://www.iicss.iq

islamic.css@gmail.com

ص: 193

تعريف مركز

بسم الله الرحمن الرحيم

جَاهِدُواْ بِأَمْوَالِكُمْ وَأَنفُسِكُمْ فِي سَبِيلِ اللّهِ ذَلِكُمْ خَيْرٌ لَّكُمْ إِن كُنتُمْ تَعْلَمُونَ

(التوبه : 41)

منذ عدة سنوات حتى الآن ، يقوم مركز القائمية لأبحاث الكمبيوتر بإنتاج برامج الهاتف المحمول والمكتبات الرقمية وتقديمها مجانًا. يحظى هذا المركز بشعبية كبيرة ويدعمه الهدايا والنذور والأوقاف وتخصيص النصيب المبارك للإمام عليه السلام. لمزيد من الخدمة ، يمكنك أيضًا الانضمام إلى الأشخاص الخيريين في المركز أينما كنت.

هل تعلم أن ليس كل مال يستحق أن ينفق على طريق أهل البيت عليهم السلام؟

ولن ينال كل شخص هذا النجاح؟

تهانينا لكم.

رقم البطاقة :

6104-3388-0008-7732

رقم حساب بنك ميلات:

9586839652

رقم حساب شيبا:

IR390120020000009586839652

المسمى: (معهد الغيمية لبحوث الحاسوب).

قم بإيداع مبالغ الهدية الخاصة بك.

عنوان المكتب المركزي :

أصفهان، شارع عبد الرزاق، سوق حاج محمد جعفر آباده ای، زقاق الشهيد محمد حسن التوكلى، الرقم 129، الطبقة الأولى.

عنوان الموقع : : www.ghbook.ir

البريد الالكتروني : Info@ghbook.ir

هاتف المكتب المركزي 03134490125

هاتف المكتب في طهران 88318722 ـ 021

قسم البيع 09132000109شؤون المستخدمين 09132000109.


مركز القائمية للبحوث والتحريات الكمبيوترية
اصبهان
www
للحصول على المكتبات الخاصه الاخرى
ارجعوا الى عنوان المـركز من فضلـكم
www.Ghaemiyeh.com
www.Ghaemiyeh.net
www.Ghaemiyeh.org
www.Ghaemiyeh.ir
و للايصاءِ من فضلكم
۰۹۱۳ ۲۰۰۰ ۱۰۹