البحث عن السلام السيبراني

الاتحـــــاد الدولـــــي للاتصـــــالات

البحث عن السلام السيبراني

بقلم

حمدون إ. توريه

الأمين العام للاتحاد الدولي للاتصالات

و

فريق الرصد الدائم لأمن المعلومات

الاتحاد العالمي للعلماء

يناير 2011

إشعار قانوني

إخلاء مسؤولية

الفصول الواردة في هذا المنشور تمثل آراء المؤلفين كل على حدة، ولا تؤيدها المنظمات التي يعمل بها المؤلفون أو ينتمون إليها، ولا يُقصد منها أن تُمثل آراء هذه المنظمات. ولا يعني ذكر أسماء محددة لبلدان أو شركات أو منتجات أو مبادرات أو خطوط توجيهية أو الإشارة إليها تأييداً أو استحساناً بأي شكل كان من جانب الاتحاد الدولي للاتصالات أو المؤلفين أو أي منظمة أخرى ينتمي إليها المؤلفون، على حساب غيرها من البلدان أو الشركات أو المنتجات أو المبادرات أو الخطوط التوجيهية ذات الطابع المشابه التي لم تُذكر في المنشور.

شكر وتقدير

يود الأمين العام للاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء تقديم الشكر إلى جودي ويستبي، وهنينغ فيغنر وجميع المؤلفين الذين جعلوا من الممكن تجميع آرائهم بشأن هذا الموضوع العالمي الناشئ الذي يثير الاهتمام. ويُعرب الأمين العام أيضاً عن امتنانه للبروفسور أنطونينو زيكيكي، رئيس الاتحاد العالمي للعلماء، وأن يُقدم شكره الخالص إلى رئيس شعبة الاستراتيجية المؤسسية في الاتحاد ألكسندر نوتوكو، وخاصة إلى جونغ هي كيم، التي تولت الإشراف على هذا المنشور وتنسيقه؛ وإلى ربيكا لويس، وديبتي فانكاتيسوار وبريتام مالوور وماركو أوبيسو وإليزابيث آشينبرينار؛ وإلى كلود بريان وفريقها؛ وإلى كثيرين غيرهم في الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء الذين لم يكن من الممكن إصدار هذا المنشور بدون مساهمتهم.

إذا كان لديكم أي تعليقات، يُرجى الاتصال بشعبة الاستراتيجية المؤسسية في الاتحاد الدولي للاتصالات على العنوان التالي: strategy@itu.int.

جدول المحتويات

الصفحة

الصفحة

جدول الاختصارات

AIS	نظم المعلومات الأوتوماتية (*Automated Information Systems*)
ARPA	وكالة مشاريع الأبحاث المتقدمة (وزارة الدفاع في الولايات المتحدة) (*Advanced Research Projects Agency (U.S. Department of Defense)*)
C3	القيادة والسيطرة والاتصالات (*Command, Control & Communications*)
CoE	مجلس أوروبا (*Council of Europe*)
COP	مبادرة حماية الأطفال على الخط (*Child Online Protection Initiative (ITU)*)
CRS	دائرة الكونغرس للأبحاث (الولايات المتحدة) (*Congressional Research Service (U.S.)*)
CSCW	العمل التعاوني المدعوم بالحاسوب (*Computer Supported Cooperative Work*)
DARPA	وكالة مشاريع الأبحاث الدفاعية المتقدمة (وزارة الدفاع في الولايات المتحدة) (*Defense Advanced Research Projects Agency (U.S. Department of Defense)*)
DNS	نظام أسماء الميادين (*Domain Name System*)
ECOSOC	المجلس الاقتصادي والاجتماعي (*Economic and Social Council (UN)*)
ESCAPE	منصة تطبيق التعاون المؤمن إلكترونياً للخبراء (منظمة شراكة إمباكت) (*Electronically Secure Collaboration Application Platform for Experts (IMPACT)*)
EU	الاتحاد الأوروبي (*European Union*)
FG Smart	الفريق التخصصي لشبكة التغذية الذكية (*Smart Grid Focus Group*)
FTC	لجنة التجارة الاتحادية (الولايات المتحدة) (*Federal Trade Commission (U.S.)*)
GCA	برنامج الأمن السيبراني العالمي (*Global Cybersecurity Agenda (ITU)*)
GRC	مركز الاستجابة العالمية (شراكة إمباكت) (*Global Response Center (IMPACT)*)
HRC	اللجنة المعنية بحقوق الإنسان (*Human Rights Committee (HRC)*)
ICT	تكنولوجيا المعلومات والاتصالات (*Information and Communication Technology*)
IGF	منتدى إدارة الإنترنت (*Internet Governance Forum*)
IMPACT	الشراكة الدولية المتعددة الأطراف لمكافحة التهديدات السيبرانية (إمباكت) (*International Multilateral Partnership Against Cyber Threats (Malaysia)*)
IP	بروتوكول إنترنت (*Internet Protocol*)
ISOC	جمعية الإنترنت (*Internet Society*)
IT	تكنولوجيا المعلومات (*Information Technology*)
ITR	لوائح الاتصالات الدولية (*International Telecommunication Regulations (ITU)*)
ITU	الاتحاد الدولي للاتصالات (*International Telecommunication Union*)

ITU-T	قطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات (*ITU Telecommunication Standardization Sector*)
LOAC	قوانين النزاع المسلح (*Laws of Armed Conflict*)
MIT	معهد ماساتشوسيتس للتكنولوجيا (*Massachusetts Institute of Technology*)
NATO	منظمة معاهدة شمال الأطلسي (*North Atlantic Treaty Organization*)
NEWS	نظام إنذار الشبكة المبكّر (شراكة إمباكت) (*Network Early Warning System (IMPACT)*)
NPT	معاهدة منع انتشار الأسلحة النووية (*Non-Proliferation of Nuclear Weapons Treaty*)
NSF	المؤسسة الوطنية للعلوم (*National Science Foundation*)
RFID	التعرف بواسطة الترددات الراديوية (*Radio-Frequency Identification*)
PDA	المساعد الرقمي الشخصي (*Personal Digital Assistant*)
PMP	فريق الرصد الدائم لأمن المعلومات (الاتحاد العالمي للعلماء) (*Permanent Monitoring Panel of Information Security (WFS)*)
SCADA	المراقبة الإشرافية وحيازة البيانات (*Supervisory Control and Data Acquisition*)
SOA	المعماريات الموجهة نحو الخدمة (*Service Oriented Architectures*)
TCP	بروتوكول مراقبة الإرسال (*Transmission Control Protocol*)
UN	الأمم المتحدة (*United Nations*)
UNCPCJ	مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية (*United Nations Congress on Crime Prevention and Criminal Justice (UN)*)
UNESCO	منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) (*United Nations Educational, Scientific, and Cultural Organization (UN)*)
UNODC	مكتب الأمم المتحدة المعني بالعقاقير والجريمة (*United Nations Office of Drugs and Crime (UN)*)
URL	عنوان السجلات الموحد (*Uniform Record Locator*)
WFS	الاتحاد العالمي للعلماء (*World Federation of Scientists*)
WSIS	القمة العالمية لمجتمع المعلومات (*World Summit on the Information Society*)

عن الاتحاد الدولي للاتصالات
وبرنامج الأمن السيبراني العالمي

الاتحاد الدولي للاتصالات هو وكالة الأمم المتحدة الرائدة في قضايا تكنولوجيا المعلومات والاتصالات ونقطة التنسيق العالمية للحكومات والقطاع الخاص بشأن تطوير الشبكات والخدمات.

وكان أحد الأدوار الأساسية التي أُنيطت بالاتحاد الدولي للاتصالات في أعقاب القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين لعام 2006 يتمثل في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات. فقد قام رؤساء الدول والحكومات وغيرهم من قادة العالم المشاركين في القمة العالمية لمجتمع المعلومات، وكذلك الدول الأعضاء في الاتحاد، بتكليف الاتحاد باتخاذ خطوات ملموسة للحد من التهديدات وانعدام الأمن فيما يتصل بمجتمع المعلومات. ولتحقيق هذه الولاية أطلق الأمين العام للاتحاد الدكتور حمدون إ. توريه برنامج الأمن السيبراني العالمي في عام 2007 ليكون إطاراً للتعاون الدولي.

ويهدف هذا البرنامج إلى تعزيز الثقة والأمن في مجتمع المعلومات. وقد وُضع بحيث يحقق التعاون والكفاءة ويشجع التنسيق بين جميع أصحاب المصلحة المعنيين ويستفيد من المبادرات القائمة لتجنب ازدواج الجهود. والبرنامج هو أول تحالف عالمي حقاً بين أصحاب المصلحة والقطاعين العام والخاص لمكافحة التهديدات السيبرانية. وفي عام 2008 وقع الاتحاد الدولي للاتصالات والشراكة الدولية المتعددة الأطراف لمكافحة التهديدات السيبرانية (إمباكت) (IMPACT) مذكرة تفاهم رسمياً بعدها أصبح مقر شراكة إمباكت في سايبر جايا بماليزيا، الذي يضم أحدث ما توصلت إليه التكنولوجيا، المقر الفعلي للبرنامج. وإمباكت هي مبادرة دولية مشتركة بين القطاعين العام والخاص لتعزيز قدرة المجتمع الدولية على منع الهجمات السيبرانية والدفاع ضدها والتصدي لها. ويوفر هذا التعاون للدول الأعضاء في الاتحاد البالغ عددها 192 دولة وغيرها من الجهات الخبرات الفنية والتسهيلات والموارد اللازمة لتعزيز قدرات المجتمع العالمي تعزيزاً فعالاً وزيادة القدرة على منع الهجمات السيبرانية والدفاع ضدها والتصدي لها. وقد جذب هذا البرنامج منذ إطلاقه دعم واعتراف الزعماء وخبراء الأمن السيبراني في أنحاء العالم. ويعمل برنامج الأمن السيبراني العالمي برعاية كل من فخامة الدكتور أوسكار آرياس سانشيز، رئيس جمهورية كوستاريكا السابق والحائز على جائزة نوبل للسلام وفخامة الرئيس بليز كامباوري، رئيس بوركينا فاصو.

ويرعى برنامج الأمن السيبراني العالمي مبادرات مثل حماية الأطفال على الخط وبوابة الأمن السيبراني ويقوم حالياً بالشراكة مع إمباكت وبدعم من اللاعبين العالميين الرئيسيين بنشر حلول الأمن السيبراني في بلدان العالم. ويود الاتحاد الدولي للاتصالات أن يتوجه بالشكر إلى فخامة السيدة لورا شينشيلا رئيسة كوستاريكا لدورها في رعاية مبادرة الاتحاد لحماية الأطفال على الخط (COP).

عن الاتحاد العالمي للعلماء
وفريقه المعني بالرصد الدائم لأمن المعلومات

في عام 1973 قامت مجموعة من العلماء البارزين بقيادة إيزيدور إيزاك رابي وأنطونيو زيكيكي بإنشاء الاتحاد العالمي للعلماء في إيرتشه بجزيرة صقلية. ومنذ ذلك الحين انضم كثير من العلماء الآخرين إلى الاتحاد ومنهم ت. د. لي ولاورا فيرمي ويوجين فيغنر وبول ديراك وبيوتر كابيتزا.

والاتحاد تجمع حر أخذ ينمو حتى أصبح يضم أكثر من 10 000 عالم من 110 بلدان. ويتقاسم جميع الأعضاء نفس الأهداف والمثل العليا ويساهمون طواعية في الدفاع عن مبادئ الاتحاد. ويُشجع الاتحاد على التعاون الدولي في العلم والتكنولوجيا بين العلماء والباحثين من كل أنحاء العالم - شماله وجنوبه، شرقه وغربه. ويسعى الاتحاد وأعضاؤه إلى تحقيق حرية تبادل المعلومات كهدف مثالي، بحيث لا تكون الاكتشافات والتقدمات العلمية قاصرة على قلة مختارة. والهدف هو تقاسم هذه المعارف بين شعوب كل الدول ليتمتع كل شخص بفوائد تقدم العلم.

وكان إنشاء الاتحاد العالمي للعلماء ممكناً بفضل وجود مركز للثقافة العلمية أُقيم في إريتشه لتخليد ذكرى عالم الفيزياء إيتوري مايورانا باسم "***مؤسسة إيتوري مايورانا ومركز الثقافة العلمية*** (المركز). وأصبح، هذا المركز الذي أُطلقت عليه تسمية "جامعة الألفية الثالثة" قوة تعليمية عالمية. وقام هذا المركز منذ إنشائه في عام 1963 بتنظيم 123 مدرسة و1 497 دورة دراسية حضرها 103 484 مشاركاً (منهم 125 من الحاصلين على جائزة نوبل) من 932 جامعة ومختبراً في 140 دولة.

وكان مركز إيتوري مايورانا هو الكيان الذي تولد عنه الاتحاد العالمي للعلماء ببرنامج عمله لتخفيف حالات الطوارئ الكوكبية. وسارع الاتحاد العالمي للعلماء إلى تحديد 15 فصلاً دراسياً لأغراض **الطوارئ الكوكبية** وبدأ تنظيم أعمال مكافحة هذه التهديدات. ومن بين الإنجازات الرئيسية للمعهد وضع **بيان إيريتشه**، في عام 1982 الذي قام بصياغته بول ديراك، وبيوتر كابيتزا وأنطونيو زيكيكي، ويعرض بوضوح المثل العليا للاتحاد كما يُقدم مجموعة من الاقتراحات لترجمة هذه المثل العليا إلى واقع عملي. وكانت إحدى العلامات البارزة الأخرى هي انعقاد سلسلة من الحلقات الدراسية الدولية بشأن الحرب النووية أثرت بشكل هائل على تقليل خطر وقوع كارثة نووية تعم الكوكب بأكمله وساهمت في نهاية المطاف في إنهاء الحرب الباردة. وفي عام 1986، ومن خلال عمل مجموعة من العلماء البارزين (ومعظمهم أعضاء في الاتحاد) تم تأسيس **المختبر العالمي التابع للمركز الدولي للثقافة العلمية** في جنيف للمساعدة على إحراز الأهداف المعروضة في بيان إيريتشه.

وفي عام 2001 أنشأ الاتحاد العالمي للعلماء فريق الرصد الدائم لأمن المعلومات. وكان تقرير هذا الفريق، المعنون *نحو نظام عالمي للفضاء السيبراني: إدارة التهديدات من الجريمة السيبرانية إلى الحرب السيبرانية*، هو إحدى الوثائق الرئيسية التي قدمها المجتمع المدني إلى القمة العالمية لمجتمع المعلومات التي عقدتها الأمم المتحدة

أولاً في جنيف في 2003. وقد نشر فريق الرصد ورقات عديدة بشأن الأمن السيبراني والحرب السيبرانية ويتناول بانتظام قضايا أمن المعلومات باعتبارها موضوعاً من موضوعات الطوارئ الكوكبية الحرجة أثناء الدورات العامة للاتحاد العالمي للعلماء التي تنعقد في شهر أغسطس من كل عام في إيريتشه. وفي أغسطس 2009، أعرب فريق الرصد عن قلقه من إمكانية وقوع حرب سيبرانية تُعطل المجتمع وتُسبب ضرراً لا داعي له ومعاناة لا لزوم لها ولذلك عمد إلى صياغة **إعلان إيريتشه لمبادئ الاستقرار السيبراني والسلام السيبراني**، الذي اعتمدته الجلسة العامة للاتحاد بمناسبة الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ الكوكبية في إيريتشه يوم 20 أغسطس 2009. وتم توزيع هذا الإعلان على كل الدول الأعضاء في الأمم المتحدة.

ويشترك في رئاسة فريق الرصد السفير هيننغ فيغنر من برلين ومدريد والدكتورة جودي ر. ويستبي، الموظفة التنفيذية الأولى لشركة المخاطر السيبرانية العالمية - شركة ذات مسؤولية محدودة، في واشنطن العاصمة. وفيما يلي بيان أعضاء الفريق الذين ساهموا في كتابة هذا المنشور:

أعضاء فريق الرصد الدائم المساهمون في المنشور

وليم أ. بارليتا

وليم أ. بارليتا هو المدير التنفيذي لمدرسة تسريع الجُسيمات في الولايات المتحدة، وهي برنامج وطني للخريجين. وهو أستاذ مساعد للفيزياء في معهد ماساتشوسيتس للتكنولوجيا وجماعة كاليفورنيا في لوس أنجلوس. وهو أيضاً أستاذ اقتصاد زائر في جامعة لوبليانا بسلوفيينيا حيث يقوم بتدريس الإدارة الاستراتيجية، ومن كبار مستشاري رئيس شركة معامل سينكروتروني في تريبستا بإيطاليا. وهو زميل الجمعية الفيزيائية الأمريكية وعضو في فريق الشؤون العامة بالجمعية ونائب رئيس منتدى الفيزياء الدولية التابع للجمعية ونائب رئيس شعبتها لفيزياء الأشعة. وهو مؤلف ومحرر خمسة كتب ومؤلف أكثر من 150 مقالة تُغطي مجموعة واسعة جداً من الموضوعات التكنولوجية. barletta@mit.edu

فلاديمير بريتكوف

فلاديمير بريتكوف (دكتوراه في الفلسفة) هو رئيس مختبر نمذجة المعلومات في معهد تحليل النظم في الأكاديمية الروسية للعلوم في موسكو، في روسيا. وهو أستاذ مساعد لتحليل النظم ونمذجة النظم في معهد موسكو للفيزياء والتكنولوجيا (الجامعة الحكومية). وتشمل مجالات أبحاثه الرئيسية النمذجة والمحاكاة المحوسبة وتطبيق الأنظمة المستندة إلى المعارف لدعم القرارات. وقد عمل عضواً في مجلس مديري جمعية إدارة الطوارئ الدولية. وهو عضو في مختلف هيئات تحرير المجلات العلمية في ميدان النمذجة والمحاكاة ومختلف أفرقة العمل الدولية. وهو عضو في فريق الرصد الدائم لأمن المعلومات التابع للاتحاد الدولي للعلماء منذ عام 2003: britkov@gmail.com

جاك بيس

جاك بيس استشاري مستقل في *Digitrust.EU*، ويعمل في مجال الثقة والأمن في تكنولوجيا المعلومات والاتصالات وهو زميل أبحاث في جامعة لكسمبرغ. وبعد 12 سنة من البحث في الرياضيات بدأ يُركّز على إدارة الأبحاث وظل يعمل لأكثر من 20 عاماً في برنامج أبحاث تكنولوجيا المعلومات والاتصالات في الاتحاد الأوروبي. وكان يعمل في السنوات الست الأخيرة منها رئيساً لوحدة *الثقة والأمن في تكنولوجيا المعلومات والاتصالات*. وهو عضو في فريق الرصد الدائم التابع للاتحاد العالمي للعلماء. وهو يكتب ويحاضر في قضايا الثقة والأمن والخصوصية وإدارة الهوية. http://www.digitrust.eu

أكسل ليمان

أكسل ليمان أستاذ في قسم المعلوماتية في جامعة بوندسفير في ميونيخ حيث يشغل كرسي النمذجة والمحاكاة. وهو أيضاً رئيس معهد النظم الذكية في الجامعة. وتتراوح مجالات أبحاثه الرئيسية من النمذجة والمحاكاة الحاسوبية وتطبيق الأنظمة القائمة على المعارف للتشخيص ودعم القرارات إلى تصميم معماريات حاسوبية ابتكارية. وهو الرئيس السابق لجمعية النمذجة والمحاكاة الدولية وزميل في جمعية المعلوماتية الألمانية وعضو في مختلف هيئات تحرير المجلات العلمية في مجال النمذجة والمحاكاة، وعضو أفرقة عمل دولية ولجان تقييم، مثل الاتحاد الأوروبي. وهو عضو في فريق الرصد الدائم التابع للاتحاد العالمي للعلماء منذ 2001. axel.lehmann@unibw.de

حمدون إ. توريه

دكتور حمدون إ. توريه هو الأمين العام للاتحاد الدولي للاتصالات منذ يناير 2007، وقد أُعيد انتخابه لفترة ثانية في مؤتمر المندوبين المفوضين للاتحاد الذي عُقد في غوادالاخارا بالمكسيك في أكتوبر 2010. وعمل مديراً لمكتب تنمية الاتصالات في الاتحاد من عام 1998 حتى عام 2006 ويملك خبرة مهنية واسعة في كلا القطاعين العام والخاص. وقد وُلد دكتور توريه في عام 1953 وهو حاصل على درجة الماجستير في الهندسة الكهربائية من المعهد التقني للإلكترونيات والاتصالات في لينينغراد (اتحاد الجمهوريات الاشتراكية السوفياتية) ودكتوراة الفلسفة من جامعة الإلكترونيات والاتصالات والمعلوماتية بموسكو (روسيا). ويكرس نفسه لكي يكون الاتحاد منظمة ابتكارية ومتطلعة إلى المستقبل ومتكيفة لمواجهة التحديات الناشئة عن سرعة تغير تكنولوجيا المعلومات والاتصالات ومواصلة قيادة الاتحاد نحو تنفيذ قرارات القمة العالمية لمجتمع المعلومات وإنجاز الأهداف الإنمائية للألفية. hamadoun.toure@itu.int

فيتالي تسيغيشكو

دكتور ف. ن. تسيغيشكو، كولونيل متقاعد في الجيش الروسي، وعضو متفرغ في الأكاديمية الروسية للعلوم الطبيعية وكبير الباحثين في معهد تحليل الأنظمة في الأكاديمية الروسية للعلوم منذ عام 1985. وهو الآن خبير وزارة الشؤون الخارجية في الاتحاد الروسي بشأن مشاكل أمن المعلومات. وعمل منذ عام 1967 في معهد

الأبحاث المركزي لوزارة الدفاع وعمل في المحاكاة الرياضية للعمليات العسكرية. ورأس مركز أبحاث مشاكل الأمن القومي، وهو مركز مستقل، في الفترة 1988-1991. وتشمل الاهتمامات العلمية للدكتور تسيغيشكو المشاكل المنهجية والنظمية لنمذجة العمليات الاقتصادية الاجتماعية ونظرية القرار؛ وتحليل النظم التطبيقية؛ ونظرية وأساليب التنبؤات الاجتماعية الاقتصادية؛ وكفالة الأمن القومي والاستقرار الاستراتيجي؛ ومشاكل أمن المعلومات؛ والمشاكل الجيوسياسية. وقد ألّف أكثر من 200 ورقة وثمانية كتب. وهو مؤلف دائم في الصحف مثل الفكر العسكري والنشرة العسكرية والمجلة العسكرية المستقلة وعدد من المنشورات الأجنبية. وهو خريج مدرسة ريازان العسكرية للمدفعية، وأكاديمية دزيرزنسكي العسكرية وحاصل على درجة الدكتوراه في العلوم (الهندسة) والأستاذية. vtsygichko@inbox.ru

هينينغ فيغنر

هينينغ فيغنر هو سفير سابق لألمانيا. وعمل سفيراً في هيئة نزع السلاح بجنيف (1981-1986)، ومساعد للأمين العام للشؤون السياسية في منظمة حلف شمال الأطلسي (1986-1991) ثم سفيراً لدى إسبانيا. وكان السفير فيغنر رئيساً (2001-2009) لفريق الرصد الدائم لأمن المعلومات التابع للاتحاد العالمي للعلماء وهو الآن رئيساً مشاركاً للفريق. وظهرت أعماله في منشورات عن السياسة الخارجية والأمنية بما في ذلك الأمن السيبراني. ومن بين الدرجات الأخرى التي حصل عليها السيد فيغنر درجة الدكتوراة في العلوم القضائية من كلية القانون في جامعة ييل. henningwegener@hotmail.com

جودي ر. ويستبي

جودي ر. ويستبي هي الموظفة التنفيذية الرئيسية في شركة المخاطر السيبرانية العالمي - شركة ذات مسؤولية محدودة، ومقرها في واشنطن العاصمة، وتعمل أيضاً كزميل متميز مساعد في معهد كارنيجي ميلون السيبراني. وتقدم السيدة ويستبي خدمات استشارية وقانونية للعملاء من القطاعين العام والخاص في أنحاء العالم في مجالات الخصوصية والأمن والجريمة السيبرانية وحماية البنية التحتية الحرجة والتجسس الاقتصادي. وهي رئيسة لجنة الخصوصية والجريمة الحاسوبية (قسم قانون العلم والتكنولوجيا) في رابطة المحامين الأمريكية وتمثل الرابطة في المؤتمر الوطني للمحامين والعلماء. وكانت السيدة ويستبي عضواً في فريق الخبراء الرفيع المستوى التابع للأمين العام للاتحاد الدولي للاتصالات وقادت عملية صياغة *مجموعة أدوات الاتحاد الدولي للاتصالات لتشريعات الجريمة السيبرانية*. واشتركت في رئاسة فريق الرصد الدائم لأمن المعلومات التابع للاتحاد العالمي للعلماء. واشتركت السيدة ويستبي في تأليف وتحرير أربعة كتب عن الجريمة السيبرانية الدولية والأمن السيبراني والخصوصية، ونشرت العديد من المقالات. وهي تلقي محاضرات في كل أنحاء العالم عن هذه الموضوعات. westby@globalcyberrisk.com

تقديـــم

إننا نتمتع في عالم سنة 2011 بفوائد مجتمع معلومات عالمي بدون حدود، ولكن هذه الفوائد تأتي مقترنة بتهديد الهجمات السيبرانية. ويمكن أن تنشأ هذه التهديدات في أي مكان وفي أي وقت وأن تسبب ضرراً هائلاً في طرفة عين. وهذا الضرر المحتمل يتزايد بصورة مضطردة مع ربط تكنولوجيا المعلومات والاتصالات بالبنية التحتية القومية ذات الأهمية الحيوية.

ولذا وجب علينا أن نعمل الآن للقضاء على هذا التهديد المتزايد.

وفي القمة العالمية لمجتمع المعلومات كلف زعماء العالم وحكوماته الاتحاد الدولي للاتصالات بمهمة تنسيق آلية لبناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات. وبعد ذلك أطلق الأمين العام توريه برنامج الأمن السيبراني العالمي، وظل الاتحاد الدولي للاتصالات يتابع بنشاط أداء هذه الولاية من خلال عدد من المبادرات. وفوق أي اعتبار آخر يشعر الاتحاد الدولي للاتصالات بالقلق العميق من الهجمات السيبرانية بين دوله الأعضاء.

ويُعزز الاتحاد العالمي للعلماء التعاون الدولي في العلم والتكنولوجيا بين العلماء والباحثين من كل أنحاء العالم. وهو يسعى إلى النهوض بتبادل المعلومات بحرية بحيث يستطيع كل شخص أن يستفيد من تقدم العلم. وفي عام 2009، قام فريق الرصد الدائم لأمن المعلومات التابع للاتحاد العالمي للعلماء بصياغة إعلان إيريتشه لمبادئ الاستقرار السيبراني والسلام السيبراني، وهو إعلان يدعو إلى تضافر العمل العالمي لكفالة بقاء شبكات وأنظمة المعلومات على حالة الاستقرار والموثوقية والتوفر والثقة. واعتمدت الجلسة العامة للاتحاد العالمي للعلماء هذا الإعلان في مناسبة الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ الكوكبية في إيريتشه (صقلية) يوم 20 أغسطس 2009، وتم توزيع البيان على جميع الدول الأعضاء في الاتحاد الدولي للاتصالات.

ويتسم التعاون بين الاتحاد الدولي للاتصالات وأعضاء مجتمع العلم والتكنولوجيا بالأهمية الحاسمة في تحقيق الهدف المشترك لكفالة السلام السيبراني. ولا نستطيع أن نحقق الفعالية في مواجهة تهديد الحرب السيبرانية بدون مشاركة أصحاب المعارف المتخصصة والفهم العميق للتكنولوجيات التي تغير الصورة على المسرح العالمي.

وهذا المجلد يتضمن التعبير عن آراء هذا المجتمع. وهو يمثل خطوة ضرورية في عملية بناء التعاون الدولي للتصدي لهذه التحديات. ونشعر بالامتنان لإتاحة هذه الفرصة لعرض جميع آرائنا بشأن هذه القضية الحرجة.

حمدون إ. توريه
الأمين العام
الاتحاد الدولي للاتصالات

أستاذ د. أنطونينو زيكيكي،
رئيس
الاتحاد العالمي للعلماء

1 مقدمة

بقلم جودي ر. ويستبي

يهدف هذا المنشور إلى الترويج لمفهوم السلام السيبراني العالمي بالعمل على ما يلي:

- فحص الطريقة التي تعمل بها تكنولوجيا المعلومات والاتصالات على دعم الحياة اليومية؛
- تقييم التهديدات السيبرانية والاتجاهات الجارية؛
- تحليل آثار الجريمة السيبرانية والنزاع السيبراني؛
- تقييم صحة الأطر القانونية الجارية؛
- تعريف مفهوم السلام السيبراني، وتثبيته باعتباره مبدأً إرشادياً مهيمناً للسلوك السلمي في الفضاء السيبراني؛
- رسم مسار العمل في المستقبل.

لقد أصبحت الإنترنت هي الجهاز العصبي المركزي في المجتمع. ولنتأمل كيف أن كل قطاع من قطاعات البنية التحتية الحرجة يتوقف على تكنولوجيا المعلومات والاتصالات. فهذه القطاعات تخضع لسيطرة أنظمة الرقابة الإشرافية وحيازة المعلومات وغير ذلك من عمليات تكنولوجيا المعلومات المعقدة التي تتصل بطريقة أو بأخرى بالإنترنت. وعلى سبيل المثال، تستخدم المستشفيات والمراكز الطبية تكنولوجيا المعلومات والاتصالات في كل الأمور بدءاً من التحرك في حالات الطوارئ ووصولاً إلى أنظمة دعم الحياة. وقطاعات النفط والغاز والنقل تستخدم أنظمة ملاحية وأنظمة عمليات معقدة محوسبة بالكامل كما أن الشركات المالية تعمل من خلال أنظمة المدفوعات الإلكترونية والتجهيز الإلكتروني. وتعتمد الحكومات على تكنولوجيا المعلومات والاتصالات لتقديم الخدمات وإدارة العمليات عبر مناطق جغرافية متنوعة والحفاظ على السلامة العامة وحماية أراضيها. ويعتمد قطاع الأعمال على الأنظمة الحاسوبية التي تُدير سلسلة التموين وعلاقات العملاء والتدفقات المالية وتؤدي وظائف الصناعة التحويلية. ونظم الاتصالات وشبكات المرافق هي الأخرى عناصر بنية تحتية "ذات أهمية حرجة فائقة" ويتوقف عليها كل ما عداها.

وقد أصبحت الإنترنت الآن تتصل اتصالاً عضوياً بكل وظائف الحياة اليومية وبحياة الأفراد. وتؤدي تكنولوجيا المعلومات والاتصالات دورها سواء كان ذلك على صعيد العمل أو التعلم أو اللهو. وتمكن الإنترنت من نشر المعارف والمعلومات بشكل غير مسبوق في تاريخ العالم. كما أن قوة التشابك الاجتماعي تربط بين السكان وتؤثر عليهم بطرق منفصلة تماماً عن الحكومات وبطريقة لا تتوقعها هذه الحكومات بالمرة. فقد أتاحت تمكين الفرد والتوسع الذاتي ونشر أفكار غير مألوفة عن طريق آلية لا تتأثر في معظمها بالحدود أو بالاعتبارات الدبلوماسية أو السياسية. واليوم يستطيع أي فرد أن يؤثر بسرعة على المفاهيم والقيم والأفكار والتحيزات من خلال قدرتهم على إنشاء محتوى وتوزيعه على صعيد عالمي.

ولكن شيوع الإنترنت قد أنجب أيضاً أنشطة إجرامية وأنشأ طرائق جديدة لجمع معلومات الاستخبارات والنزاع. وتفتح نقاط الضعف التي تنطوي عليها أنظمة التشغيل والبرمجيات والأوضاع الأمنية الباب لإمكانية القيام بأعمال تهدد الخدمات الأساسية المقدمة للسكان المدنيين وتسهل التجسس الاقتصادي وتؤثر على عمليات الحكومة. فهناك الفيروسات والديدان وهجمات منع الخدمة الموزعة وسرقة البيانات المشمولة بحقوق الملكية والرسائل الاقتحامية والتدليس، وكلها تقوض مصداقية تكنولوجيا المعلومات والاتصالات وقدرة المجتمعات والاقتصادات على العمل.

وتحسّن برامج الأمن الفعّالة قدرة الأنظمة على استعادة الحيوية وتساعد في اكتشاف هذه الإجراءات ومنعها والتخفيف من آثارها. وتساعد الإضافات التكنولوجية والابتكارات الجديدة على صد وتتبع الهجمات كما أن القوانين المنسقة بشأن الجريمة السيبرانية تنهض بالتحقيقات وتقديم المجرمين السيبرانيين إلى القضاء. ويتعين القيام بالكثير من العمل في كل مجال من هذه المجالات ولكن المشكلة الأكثر خطورة والتي قد تنطوي على أكبر قدر من التدمير هي قيام الدول باستخدام هذه التكتيكات لشن نزاع سيبراني.[1] وهناك الآن أمثلة عديدة توضح كيف يمكن أن تمتد النزاعات السياسية والعسكرية إلى الفضاء السيبراني وبذلك تقوض فعلياً الثقة في تكنولوجيا المعلومات والاتصالات وتثير مخاطر جدية. ويرد وصف بعض هذه الأمثلة في الفصول التالية من هذا المنشور.

وقبل ظهور مجتمع المعلومات كانت القوة والقيادة عادة من نصيب أصحاب السلطة السياسية والتفوق العسكري والهيمنة الاقتصادية. وكانت الدول والمنظمات الدولية تفرض القواعد والقيم الاجتماعية كما كانت النزاعات المسلحة تحكمها قوانين ومعاهدات تستند إلى وحدة الأراضي والقدرات الدفاعية براً وجواً وبحراً. أما اليوم فقد غيرت الإنترنت جذرياً من هذا التوازن في القوة. وتاريخ الإنترنت نفسها يوضح أكثر من غيره هذه النقطة.

إن الأحداث العالمية يمكن أن تشكل عوامل حفز هامة. ففي أعقاب الحرب العالمية الثانية كانت أمريكا تواجه نوعاً جديداً من الأعداء: الحرب الباردة والشيوعية وتهديدات الضربات النووية. واستجابة للقلق بشأن التفوق العلمي السوفيتي بعد إطلاق القمر الصناعي سبوتنك، وهو أول ساتل صناعي حول الأرض، قام الرئيس آيزنهاور بإنشاء وكالة مشاريع الأبحاث المتقدمة في وزارة الدفاع لتنسيق كل الأعمال البحثية التكنولوجية للولايات المتحدة.[2] وتم تعيين ج. س. ر. ليكلايدر من معهد مساتشوستس للتكنولوجيا لرئاسة برنامج الأبحاث الحاسوبية في وكالة مشاريع الأبحاث المتقدمة. وقبل ذلك ببضعة أشهر كان ليكلايدر

---

[1] يُقصد بمصطلح النزاع السيبراني أن يشمل سيناريوهات يمكن وصفها تحت عنوان "الحرب السيبرانية".

[2] A Brief History of the Net," *Fortune* 9 أكتوبر 2000 ص. 34، http://money.cnn.com/magazines/fortune/fortune_archive/2000/10/09/289297/index.htm (hereinafter "Fortune"); *see also* Dave Krisula, "The History of the Internet," Aug. 2001 (expanded 2009), www.davesite.com/webstation/net-history1.shtml (hereinafter "Krisula").

قد نشر سلسلة من المذكرات التي تُناقش "شبكة كونية" من الحواسيب ذات التوصيل البيني تمكن من النفاذ المشترك إلى البرامج والملفات. وبعد ذلك لاحظ فينت سيرف وبوب كاهن وبعض "آباء الإنترنت" الآخرين أن "هذا المفهوم يتشابه كثيراً في روحه مع إنترنت العصر الحاضر."[3]

وفي نفس ذلك الوقت تقريباً طلبت القوات الجوية، التي كانت مهتمة بقدرتها على الحفاظ على عمليات القيادة والسيطرة بعد حدوث هجمة نووية، من شركة راند القيام بدراسة عن إنشاء شبكة عسكرية قابلة للبقاء وتستطيع توفير "الحد الأدنى من الاتصالات الجوهرية".[4] واختتمت راند أعمالها (1962-1965) بتقرير كتبه بول باران يصف فيه كيف يمكن لشبكة حاسوبية مبدلة بالرزم أن توفر هذه القدرة.[5] وفي الوقت نفسه (ودون أن يعرف فريق مؤسسة راند) قام ثلاثة مهندسين من معهد ماساتشوستس للتكنولوجيا بمناقشة مفهوم الحواسيب المربوطة شبكياً وتبديل الرزم.[6] وفي أواخر 1966، انتقل أحد هؤلاء المهندسين، وهو لورانس روبرتس، إلى العمل في وكالة مشاريع الأبحاث المتقدمة "من أجل تطوير مفهوم شبكة حاسوبية".[7]

وقد أصبح ما حدث بعد ذلك تاريخاً معروفاً. ففي عام 1971 أصبح لدى شبكة آربا (ARPANET)، أو كما كانت الإنترنت تُعرف في البداية، 23 مضيفاً لربط مراكز الأبحاث الحكومية والجامعات عبر الولايات المتحدة. وبحلول عام 1981، أُطلق عليها اسم إنترنت، وبحلول عام 1991 ظهرت الشبكة العنكبوتية العالمية التي كان سير تيموثي بيرنرز-لي،[8] قد قام بتطويرها في المنظمة الأوروبية للأبحاث النووية (التي تعرف أيضاً باسم CERN). وأطلق الجمع بين الإنترنت والشبكة العنكبوتية (الويب) أفكار الاستعمال التجاري، ولكن الشركات مُنعت من الوصول إلى الشبكة الرئيسية من خلال شبكة مؤسسة العلوم القومية (NSFNET).

---

[3] باري م. لاينر وفينتن ج. سيرف ودفيد د. كلارك وروبرت أ. كاهن وليونارد كلاين روك ودانيل س. لينش وجون بوستل ولاري ج. روبرتس وستيفن وولف، "A Brief History of the Internet," جمعية الإنترنت (ISOC) All About the Internet, www.isoc.org/internet/history/brief.shtml (hereinafter "A Brief History of the Internet")؛ ونشر ليكلايدر سلسلة مذكراته المعنونة "الشبكة الكونية" في أغسطس 1962 وبدأ العمل في وكالة مشاريع الأبحاث البحثية المتقدمة في أكتوبر 1962.

[4] كريسولا: *انظر أيضاً* Fortune; Stewart Brand, "Founding Father," *Wired*, Mar. 2001 at 148, www.wired.com/wired/archive/9.03/baran_pr.html (ويشار إليه فيما بعد باسم "براند").

[5] براند في صفحة 145-153؛ *انظر أيضاً* كريسولا.

[6] A Brief History of the Internet؛ *انظر أيضاً* براند في صفحة 146؛ كريسولا.

[7] A Brief History of the Internet.

[8] إليزابيث د. هووفر، The Inventor of the World Wide Web," *AmericanHeritage.com,* 12 Nov. 2005, www.americanheritage.com/articles/web/20051112-internet-world-wide-web-tim-berners-lee-computer-geneva-cern-enquire-html-url-world-wide-web-consortium.shtml.

وفي عام 1995 أذعنت مؤسسة العلوم القومية ونقلت إمكانية النفاذ إلى الشبكة الأساسية للإنترنت إلى أربع شركات تجارية، وبحلول عام 1996 كان هناك قرابة 10 ملايين مضيف على الخط وانتشرت الإنترنت في أنحاء العالم. وفي خلال ثلاثة عقود نمت الإنترنت "من مفهوم للحرب الباردة من أجل السيطرة على الأجزاء الممزقة من مجتمع ما بعد حرب نووية لتُصبح طريق المعلومات فائق السرعة."[9] وتغلغلت الإنترنت المقترنة بالشبكة العنكبوتية العالمية (الويب) في الاقتصادات والمجتمعات في جميع الطبقات وخلقت تحولاً اجتماعياً لم يكن من الممكن توقعه قبل 20 سنة. واليوم يوجد حوالي ملياري مستعمل على الخط ولا توجد حدود جغرافية مفروضة على الإنترنت. وتشمل إدارة الإنترنت اليوم القضايا التقنية وقضايا السياسة العامة معاً ويدخل فيها جميع أصحاب المصلحة والمنظمات الدولية والمنظمات الحكومية الدولية ذات الصلة.

والمفارقة أن هذه الفكرة التي وُلدت في عصر الحرب الباردة واقترنت بتدويل العلم الذي أدى إلى ظهور الويب، أصبحت تُمثل الآن واحدةً من أكثر التحديات الحاسمة التي تواجه السلام العالمي. ورغم أنه لا يزال يجب إيلاء وزن كبير للاعتبارات الجيوسياسية[10] عند تحليل مصالح الأمن القومي والأمن الاقتصادي فقد غيرت الإنترنت التحليل التقليدي للسياسة الخارجية. وتؤثر الأبعاد الجيوسيبرانية تأثيراً متزايداً على سلوك الدول وتعمل التكتلات الجغرافية السياسية على فرض ظهور نموذج جديد.

ولم يعد السؤال هو احتفاظ الولايات المتحدة "بالحد الأدنى الجوهري من الاتصالات": إذ أصبحت المسألة هي طريقة تمكُّن جميع البلدان في أنحاء العالم من الحفاظ على الاستقرار الجيوسيبراني وكفالة عدم استعمال البنية التحتية الحرجة للاتصالات سلاحاً ضد المدنيين العُزل والأبرياء، بما يؤدي إلى معاناة وتدمير لا داعي لهما.

ويُعرِّف المؤلف "الفضاء الجيوسيبراني" بأنه العلاقة بين الإنترنت والجغرافيا والديمغرافيا والاقتصاد والسياسة للدولة وسياستها الخارجية. ويُعرِّف "الاستقرار الجيوسيبراني" بأنه قدرة جميع البلدان على الاستفادة من الإنترنت لتحقيق فوائد اقتصادية وسياسية وديمغرافية مع الامتناع عن أنشطة يمكن أن تُسبب معاناة ودماراً لا لزوم لهما.[11]

---

[9] Krisula ؛"Life on the Internet: Net Timeline," PBS, www.pbs.org/opb/nerds2.0.1/timeline/ *انظر أيضاً*.

[10] تُعرف الجغرافية السياسية بأنها "(1) دراسة العلاقة بين السياسة والجغرافيا والديمغرافيا والاقتصاد، وخاصة في صدد السياسة الخارجية للدولة، (2) أ - سياسة حكومية تستعمل علم الجغرافية السياسية. ب - مبدأ نازي يرى أن الاحتياجات الجغرافية والاقتصادية والسياسية لألمانيا تُبرر قيامها بغزو أراض أخرى والاستيلاء عليها، (3) مجموعة من العوامل الجغرافية والسياسية المتصلة بدولة ما أو منطقة ما وتؤثر عليها." قاموس أمريكان هيريتدج (American Heritage Dictionary)، 2000، www.dictionary.com/search?q=geo-political.

[11] عُرض هذا التعريف للمرة الأولى في مؤتمر معهد الأمن الداخلي التابع لشركة الخدمات التحليلية (ANSER)، المعنون "Homeland Security 2005: Charting the Path Ahead"، جامعة ميريلاند، محاضرة قدمتها جودي ويستبي، "A Shift in Geo-Cyber Stability and Security"، 6-7 مايو 2002.

واليوم يواجه العالم بأكمله تهديدات جديدة من الإنترنت، وقدرة كل دولة على الحفاظ على اتصالاتها وقيادتها وسيطرتها وقدراتها الحاسوبية ضد الهجمات من الإرهابيين وعصابات الجريمة المنظمة وغير ذلك من الدول لم تعد مؤكدة. وتُثير تكنولوجيا المعلومات والاتصالات أمام البلدان تحديات غير مسبوقة للأمن القومي والاقتصادي. ويستطيع الأفراد الآن إحباط السلطة وإجراء هجمات غير منتظمة ممكن أن تؤدي إلى شلل البنية التحتية بأكملها وتعطيل الاتصالات، ويمكن الآن أن تُمثل الأنظمة الأضعف تهديداً لأمن أكبر الدول.

ويمكن أن يتمخض النزاع السيبراني عن عواقب تُهدد الحياة في حالة إفساد البنية التحتية للمعلومات ذات الأهمية الحرجة. ويمكن أن تؤدي أيضاً إلى عمليات معلوماتية تؤثر على حقوق الإنسان الدولية وتدفع على العنف وتُسبب ضرراً اقتصادياً خطيراً. والمخاطر التي يتعرض لها الأفراد والدول مخاطر هائلة - وغير مقيدة بالأطر القانونية الجارية التي لا تستوعب العصر السيبراني بالقدر الكافي.

وهناك حاجة عاجلة في الوقت الحاضر. فالخطى السريعة التي تُقيم بها البلدان القيادات السيبرانية وتوسع قدراتها العسكرية لتشمل النزاع السيبراني يجب أن تتوازن باتفاق بين الدول يعترف بوجود مستوى جديد من "الحد الأدنى الجوهري من الخدمات" التي تحظى بالحماية من النزاع. وهذا الإجراء سيمنع التدمير والمعاناة بدون داع بين المشاركين في النزاع وسيؤدي إلى حماية البلدان الأخرى غير المشاركة من الضرر. ووجود هذا المستوى من الاستقرار الجيوسيبراني أمر حيوي، لكي لا تضيع فوائد الإنترنت في خضمّ قوى التكنولوجيا المدمرة.

والمنظمات المتعددة الجنسيات هي نقطة البداية المنطقية. ويجب عليها أن تبدأ بتحديد المستوى الأدنى من استقرار البنية التحتية والاتصالات المطلوب لحماية المدنيين الأبرياء والحفاظ على الوظائف المجتمعية الأساسية، وكفالة ذلك من خلال اتفاقات دبلوماسية وسيادة القانون. وسوف يتطلب ذلك مدخلات من مجموعة واسعة من أصحاب المصلحة، بمن فيهم الأفراد والصناعة والمجتمع المدني والدوائر الأكاديمية والمحامون وخبراء السياسة العامة والجهات المستجيبة الأولى وجهات إنفاذ القانون. وبهذه الطريقة يُمكن أن توفر تكنولوجيا المعلومات والاتصالات والإنترنت إطاراً دولياً إيجابياً للتعاون بين البلدان وأن تؤديا إلى تحسين الفهم وقبول قيم ثقافية واجتماعية مختلفة في أنحاء العالم.

ويقوم هذا الكتاب على مفهوم السلام السيبراني باعتباره مبدأً موجهاً للسلوك في الفضاء السيبراني. ولذلك ينبغي أن يكون السلام السيبراني هدفاً تبحث عنه جميع الدول. ومزايا السلام السيبراني ترجح بكثير العواقب المدمرة للنـــزاع السيبراني.

وهذا المنشور، الذي اشترك في تأليفه حمدون إ. توريه، الأمين العام للاتحاد الدولي للاتصالات، وأعضاء فريق الرصد الدائم لأمن المعلومات التابع للاتحاد العالمي للعلماء، يهدف إلى أن يكون دعوةً للعمل من جانب جميع أصحاب المصلحة لبذل الجهود من أجل كفالة الحد الأدنى من الاستقرار في الإنترنت وفي بنيتهم التحتية والنهوض بمفهوم السلام السيبراني العالمي.

2 الفضاء السيبراني وتهديد الحرب السيبرانية

بقلم جدون إ. توريه

أصبحت تكنولوجيا المعلومات والاتصالات جزءاً لا يتجزأ من الحياة اليومية لكثير من الأشخاص في أنحاء العالم. والاتصالات الرقمية والشبكات والأنظمة تقدم موارد حيوية وتمثل بنية تحتية لا غنى عنها في كل جوانب المجتمع العالمي، وهي ضرورات لا يمكن لكثير من سكان العالم الازدهار أو حتى البقاء بدونها. وهذه الهياكل والأنظمة تمثل ميداناً جديداً تقترن به تحديات جديدة للحفاظ على السلام والاستقرار. وبدون آليات كفالة السلام فإن مدن العالم ومجتمعاته ستكون عرضة لهجمات تتسم بتنوع غير مسبوق وغير محدود. وهذه الهجمات يمكن أن تأتي دون مقدمات. فالحواسيب والهواتف الخلوية تتوقف عن العمل فجأة كما أن شاشات آلات صرف النقد والآلات المصرفية تنطفئ في وجه العملاء وتتعطل أنظمة مراقبة الحركة الجوية والسكك الحديدية وحركة السيارات وتعم فوضى الطرق السريعة والجسور والممرات المائية وتتوقف السلع غير المعمرة بعيداً عن السكان الجائعين. ومع اختفاء الكهرباء تهوي المستشفيات والمساكن والمراكز التجارية بل ومجتمعات بأكملها في غياهب الظلام. ولن تستطيع السلطات الحكومية معرفة مدى الضرر أو الاتصالات ببقية العالم لإبلاغه بالكارثة أو حماية مواطنيها الضعفاء من الهجمات التالية. وهذه هي المحنة القاسية التي يواجهها مجتمع تعرض للشلل بسبب ضياع شبكاته الرقمية في لحظة واحدة. وهذا هو التدمير الذي يُمكن أن ينجم عن نوع جديد من الحروب هي "الحرب السيبرانية".

ميدان جديد: الفضاء السيبراني والأمن والحرب

يلوح شبح التهديد بالحرب السيبرانية أكبر من أي وقت مضى. واليوم أصبحت التقدمات التكنولوجية والبنية الرقمية المتنامية تربط مجتمعات بأكملها بعجلة أنظمة معقدة ومتشابكة. والطلب على الإنترنت والتوصيلية الرقمية يستدعي تكاملاً متزايداً باستمرار لتكنولوجيا المعلومات والاتصالات واندماجها في منتجات كانت تعمل من قبل بدونها، مثل السيارات والمباني بل وأنظمة المراقبة لشبكات الطاقة والنقل الشاسعة. فشبكات إمدادات الكهرباء وأنظمة النقل والخدمات واللوجستيات العسكرية - أي كل الخدمات المعاصرة تقريباً تتوقف على استعمال تكنولوجيا المعلومات والاتصالات واستقرار الفضاء السيبراني. و"الفضاء السيبراني" هو العالم المادي والمفاهيمي الذي توجد فيه جميع هذه الأنظمة. ولذلك فإن

"الحرب السيبرانية" يمكن أن تُفهم بصورة عريضة على أنها حرب تجري في الفضاء السيبراني باستعمال واستهداف تكنولوجيا المعلومات والاتصالات.[12] والاعتماد المتزايد بسرعة على الشبكات الذكية وغيرها من أنظمة المراقبة والرصد عن طريق الإنترنت تضع مركز موارد الطاقة والنقل والدفاع في متناول هؤلاء الذين يسعون إلى إحداث الفوضى في الحكومة وبين السكان المدنيين.[13] وهكذا فإن تعزيز الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات تمثل الآن عناصر حيوية في أمن كل دولة ورفاهها الاقتصادي.

ومع تزايد الاعتماد العالمي على تكنولوجيا المعلومات والاتصالات تزايد أيضاً التعرض للهجمات على البنية التحتية الحرجة من خلال الفضاء السيبراني. ورغم أن المعالم الدقيقة لأي "حرب سيبرانية" لا تزال غير محددة فإن الهجمات الكبيرة ضد البنية التحتية للمعلومات وخدمات الإنترنت في العقد الأخير تُعطي صورة ما عن الشكل والنطاق المحتملين للنزاع في الفضاء السيبراني. وقد رُبطت هجمات في جورجيا[14] وإستونيا[15] وكوريا الجنوبية والولايات المتحدة[16] بالحرب السيبرانية. ورُبطت انقطاعات الكهرباء المتعددة في البرازيل بهجمات سيبرانية، وفي عام 2008 تمكّن القراصنة من الدخول إلى الموقع الشبكي للحكومة والسيطرة عليه لمدة تزيد عن أسبوع.[17] وتوضح انقطاعات الكهرباء في البرازيل الاتساع المحتمل للأنواع الجديدة من الهجمات

---

[12] ستيفن إليوت، "Analysis on Defense and Cyberwarfare," *Infosec Island*, 8 July 2010, https://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html (hereinafter "Elliot").

[13] إلن مسمر، "Cyberattack Seen as Top Threat to Zap U.S. Power Grid," *NetworkWorld*, 2 June 2010, www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html (وجاء فيها أن خطر الهجوم السيبراني المنسق الذي يمكن الجمع بينه وبين هجوم فعلي مادي يعتبر التهديد الأكثر إلحاحاً "مرتفع التأثير ومنخفض التردد" على إمدادات الكهرباء في أمريكا الشمالية) (ويُشار إلى هذا المرجع أدناه باسم "مسمر").

[14] توماس كلابورن، "Under Cyberattack, Georgia Finds 'Bullet-Proof' Hosting With Google And Elsewhere," *InformationWeek*, 12 أغسطس 2008، www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210002702.

[15] جوشوا دافيس، "Hackers Take Down the Most Wired Country in Europe," *Wired*, 21 Aug. 2007, www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[16] شو سانغ هون وجون ماركوف، "Cyber attacks Jam Government and Commercial Web Sites in U.S. and South Korea," صحيفة نيورك تايمز، 8 يوليو 2009، www.nytimes.com/2009/07/09/technology/09cyber.html; Jack Date, Jason Ryan, Richard Sergay, and Theresa Cook, "Hackers Launch Cyberattack on Federal Labs," *ABC News*, 7 Dec. 2007, http://abcnews.go.com/TheLaw/Technology/story?id=3966047&page=1.

[17] مايكل مايلريا، "Brazil's Next Battlefield: Cyberspace," *Foreign Policy Journal*، 15 نوفمبر 2009، http://foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace (hereinafter "Mylrea").

السيبرانية: وجاء في التقارير تشبيه المشهد بفيلم من أفلام الخيال العلمي حيث توقفت تماماً قطارات الأنفاق وإشارات المرور وثاني أكبر محطة إنتاج قوى كهربائية وهو سد إيتايبو، وتأثر أكثر من 60 مليون شخص.[18]

ويمكن أن تشمل الحرب السيبرانية القطاع الخاص. وقد عانت خدمات الويب العملاقة مثل *غوغل*[19] و*تويتر*[20] بالفعل من هجمات في عام 2009، بل وقد أُطلقت هجمات منع الخدمة في زمن بعيد يصل إلى عام 2000 ضد شركات معروفة مثل *سي إن إن (CNN)* و*إي باي* و*أمازون*.[21] ونتيجة لذلك لم تتوفر بعض الخدمات عدة ساعات بل وعدة أيام. واستهدف القراصنة أنظمة مراقبة المطارات مما أدى إلى تعطيل معدات حرجة مثل الخدمات الهاتفية وأنوار المَدْرجات.[22] وكما جاء في بعض التقارير عانت أكثر من ستة بلدان هجمات سيبرانية في السنوات الثلاث الماضية وهُوجمت 34 شركة خاصة على الأقل في الأشهر الأولى من سنة 2010 وحدها.[23] ورغم أن هذه الانشغالات الأمنية هي انشغالات خطيرة فلا تزال هناك فسحة من الوقت للتغلب على سيناريوهات تنطوي على أبعاد كارثية من خلال إنشاء منتجات وممارسات ومعايير أكثر أمناً عن طريق جهد دولي تعاوني.[24] وزيادة أمان الإنترنت وحماية تكنولوجيا المعلومات والاتصالات من الاضطرابات والتدمير يجب أن تكون من بين الأولويات إذا كان لنا أن نحمي السكان المدنيين ونكفل التسيير الفعّال للهياكل الأساسية ونعمل على استمرار تطوير الخدمات الجديدة.

الحرب السيبرانية كتهديد للبنية التحتية الوطنية

يشمل مفهوم الحرب السيبرانية استهداف لا للقدرات والأنظمة العسكرية وحسب ولكن أيضاً استهداف البنية التحتية الحيوية للمجتمع - بما في ذلك الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات (SCADA) - التي تسمح لها بالعمل والدفاع عن نفسها. وفي حين أن استخدام وسيط مختلف (الفضاء

---

18 *المرجع نفسه*.

19 أندرو جاكوب وميغيل هيلفت، "Google, Citing Attack, Threatens to Exit China," *The New York Time*، 12 يناير 2010، www.nytimes.com/2010/01/13/world/asia/13beijing.html.

20 إليوت فان بوسكيرك،"Denial-of-Service Attack Knocks Twitter Offline (Updated)," Wired.com، 7 أغسطس 2007، www.wired.com/epicenter/2009/08/twitter-apparently-down/.

21 انظر أبراهام د. سوفاير وسيمور ي. جودمان، *The Transnational Dimension of Cyber Crime and Terrorism*, 2001 at 14, http://media.hoover.org/documents/0817999825_1.pdf.

22 *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*, United States Government Accountability Office, Sept. 2007, GAO-07-1036, www.gao.gov/new.items/d071036.pdf. In 1997 (hackers attacked the Worcester Airport in the U.S., disabling phone services to the airport tower and shutting down the control system managing the runway lights).

23 إليوت.

24 جوشوا بينل، "Securing the Smart Grid: The Road Ahead," at 2, *NetworkSecurityEdge.com*، 5 فبراير 2010. http://www.networksecurityedge.com/content/securing-smart-grid-road-ahead.

السيبراني وتكنولوجيا المعلومات والاتصالات العاملة فيه) فإن الأعداء يستطيعون مع ذلك نشر أسلحة والدخول في نزاع هجومي دفاعي يُشبه إلى حد بعيد الحرب التقليدية. وتكتيكات الحرب السيبرانية تنطوي نمطياً على جمع البيانات أو التسلل إلى الأنظمة المحوسبة لإحداث الضرر في الأنظمة الحرجة.[25] وتشمل الأسلحة السيبرانية المحتملة: الفيروسات والديدان الحاسوبية وعمليات جمع البيانات السيبرانية وأجهزة تشويش اتصالات البيانات اللاسلكية وبرمجيات الحاسوبية المزيفة المشبوهة وأسلحة النبض الكهرمغنطيسي وأدوات استطلاعات الحاسوب والشبكات والقنابل الزمنية الطروادية المدمجة.

وتزايد الأزمات على الشبكات الذكية يزيد من تعرض إمدادات الكهرباء للبلدان بالذات للهجوم. إذ إن شبكات التغذية الذكية هي أنظمة مرقمنة تربط إمدادات لمرافق بشبكات رصد مركزية تُسمى في العادة شبكة سكادا (SCADA). وهذه الشبكات تجمع معلومات عن استخدام الطاقة وإمداداتها بينما تتيح الشبكات الذكية قناة رقمية لانسياب هذه المعلومات بين المستهلك والمورد.[26] وهذه التكنولوجيات تُستعمل الآن في مجموعة واسعة من العمليات والأنظمة بما في ذلك: أنظمة إدارة المياه وخطوط أنابيب الغاز ونقل وتوزيع القوى الكهربائية وأنظمة القوى الهوائية وأنظمة الاتصالات الجماهيري والصناعة التحويلية والإنتاج وأنظمة النقل العام وأنظمة المراقبة البيئة ومراقبة الحركة الجوية وإشارات المرور.[27] ويتزايد قيام الموردين بربط الشبكات الذكية بالإنترنت من أجل إتاحة النفاذ عن بُعد وزيادة الاستفادة من الوظائف.

وفي حين أن شبكات التغذية الموصولة تُتيح فوائد هائلة مثل تقليل فاقد الطاقة وزيادة سرعة الاتصال بين المستهلك والمورد فإنها تؤدي أيضاً إلى مركزية البيانات والسيطرة الخاصة بشبكات تغذية الطاقة الضخمة في شبكة اتصالات تضم العديد من نقاط النفاذ. ومع تزايد النقاط النهائية والشبكات الموصولة تُتيح الشبكات الذكية وشبكات سكادا طرائق عديدة للمهاجمين للتسلل إليها.[28] وعلى سبيل المثال يمكن اختراق أي مقياس ذكي (مقياس كهربائي موصول بالشبكة) وتلويثه بسهولة كبيرة إلى حد ما، وبعد ذلك يمكن استعماله لنشر دودة إلى المقاييس الأخرى وبالتالي رفع شدة التيار في شبكة الطاقة أو إغلاقها[29] ورغم أن كثيراً من الشركات تسعى لتأمين شبكاتها بعزل مراكز المراقبة عن الشبكات الأخرى (وهي تقنية تُسمى "الثغرات الهوائية") فإن محاولات عزل بعض المكونات عزلاً كاملاً تواجه الفشل في كثير من الأحيان، وذلك دون علم

---

[25] إليوت.

[26] "Smart Grid"، وزارة الطاقة في الولايات المتحدة, www.oe.energy.gov/smartgrid.htm; "SCADA," *TopBits.com*, www.tech-faq.com/scada.html (ويُشار إلى المرجع باسم "سكادا").

[27] سكادا.

[28] كاتي فهرنباشر, "10 Things to Know About Smart Grid Security," 9 Oct. 2009, Earth2Tech, Gigaom, http://gigaom.com/cleantech/10-things-to-know-about-smart-grid-security/. (ويشار إلى المرجع باسم "فهرنباشر").

[29] *المرجع نفسه*.

مدير النظام غالباً.[30] والقنابل المنطقية هي طريقة أخرى قد يستخدمها المهاجمون لوقف أو حتى تدمير الشبكة الذكية؛ وقد يتسلل القراصنة إلى الشبكة لإخفاء برمجيات خبيثة فيها والانتظار حتى يتم تشغيل هذه القنابل في وقت لاحق من أجل القيام بهجوم منسق أو إحداث انقطاع الطاقة بصورة محدودة.[31] وهذه القنابل تُنشئ مشكلة أمنية إضافية لأنه من الممكن إطلاقها عرضاً أو يُمكن أن يُطلقها قرصان آخر يكتشفها في تاريخ لاحق.[32]

وبالفعل أبلغت البلدان التي استثمرت في الشبكات الذكية عن وقوع محاولات للهجوم والاختراق يبلغ عددها آلاف المحاولات يومياً.[33] وحسب بعض التقديرات، تُمثل الهجمات السيبرانية أكبر خطر على الشبكات الوطنية لتوليد الطاقة.[34] ويُمكن بسهولة توجيه هجوم عن بُعد ليستهدف البنية التحتية المادية مثل مولدات ومحولات الكهرباء بحيث تجعلها تُدمر نفسها من الناحية العملية.[35] ومن المرجح أن أي هجوم من هذا النوع سينطوي على عواقب بعيدة المدى نظراً لأن شركات القوى لا تقوم في العادة بتخزين قطع الغيار الباهظة التكلفة، وقد يستغرق الأمر عدة أشهر لتصنيعها وتسليمها.[36] وأي هجوم على شبكة ذكية لن يحرم العملاء من الطاقة فحسب ولكنه يؤدي أيضاً إلى ضرر مالي ضخم. ويمكن أن تصل مولدات الكهرباء إلى حدود عدة ملايين من الدولارات وقد تبلغ الاستثمارات الشاملة في الشبكات الذكية عشرات المليارات في بعض البلدان.[37]

---

30 "SCADA Security and Terrorism: We're Not Crying Wolf," at 26, BlackHat, www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.

31 شوفان غورمان. "Electricity Grid in U.S. Penetrated By Spies," *The Wall Street Journal,* 8 Apr. 2009, http://online.wsj.com/article/NA_WSJ_PUB:SB123914805204099085.html.

32 إلين ميسمر. "Cyberwar' author: U.S. needs radical changes to protect against attacks," *NetworkWorld*, 7 Apr. 2010, www.networkworld.com/news/2010/040710-clarke-book-review.html (ويُشار إلى المرجع باسم "Radical Change").

33 *المرجع نفسه* (يبلغ عن تعرض شبكات القوى الكهربائية في الولايات المتحدة بالفعل لمئات الآلاف من الاستكشافات يومياً)؛ فهرنباشر (حيث جاء فيه أن 40 مليون مقياس ذكي رُكبت عالمياً قد تعرض بالفعل لعدد من الخروقات الأمنية).

34 ميسمر.

35 ميلريا.

36 "Cyberwar: War in the fifth domain," 7 Jan. 2010, *The Economist*, www.economist.com/node/16478792 ("Fifth Domain" ويسمى بعد ذلك باسم).

37 *Smart Grid: Hardware and Software Outlook*, Zpryme, 2009 at 2, www.zpryme.com/SmartGridInsights/2010_Smart_Grid_Hardware_Software_Outlook_Zpryme_Smart_Grid_Insights.pdf (stating that the U.S. smart grid industry was valued at $21.4 billion in 2009 and will reach an estimated $42.8 billion by 2014); Jonathan Weisman and Rebecca Smith,"Obama Trumpets Energy Grants," *The Wall Street Journal*, 28 Oct. 2009, http://online.wsj.com/article/SB125663945180609871.html (خبر عن إعلان الرئيس أوباما عن تقديم منح حوافز بمبلغ 3,4 مليار دولار لمشاريع الشبكات الكهربائية المتقدمة).

وبالإضافة إلى إمكانية حدوث تدمير مادي واسع وخسارة مالية فورية فإن التهديد بالهجمات السيبرانية في المستقبل يُقوض الثقة في التكنولوجيات القائمة والجديدة مثل الشبكات الذكية، وبالتالي في موثوقية الموارد الإلكترونية والمالية والصحية. وضياع الثقة وحده يمكن أن يُسبب اضطرابات مجتمعية واقتصادية هائلة.[38] وتطوير استعمال الشبكات الذكية مع المفاعلات النووية (ومرافق الأسلحة النووية) يُنشئ مخاطر وأضراراً محتملة أبعد أثراً. فبالإضافة إلى الهجمات التقليدية والاستراتيجيات الدفاعية يمكن أن تستتبع الحرب السيبرانية أيضاً الهجوم على كيان أو على الأنظمة الداخلية للبلد من أجل تشتيت البلد أو عرقلته مؤقتاً وليس الإضرار به بصورة مباشرة.[39] وقد يختار أحد البلدان هذا النوع من الهجوم السيبراني إذا كان يُريد مثلاً أن يشل الدعم المتحالف للعدو المستهدف لفترة تكفي لتحقيق هدف محدد.[40]

السمات الفريدة للحرب السيبرانية وأثرها

رغم أن الحرب السيبرانية يمكن أن تُشبه الحرب التقليدية من عدة جوانب فإن السمات الفريدة للفضاء السيبراني تُنشئ إلى جانب ذلك أبعاداً جديدة وغير متوقعة. ونظراً لأن الأنظمة في الفضاء السيبراني ترتبط بالحواسيب وشبكات الاتصال فإن الاضطراب الذي ينشأ عن هجوم باستعمال تكنولوجيا المعلومات والاتصالات يتجاوز تعطل نظام وحيد بل ويتجاوز الحدود الوطنية في كثير من الأحيان. وتؤثر عمليات كثيرة لنقل البيانات على أكثر من بلد واحد وتستند خدمات كثيرة في الإنترنت إلى خدمات تأتي من الخارج؛ وعلى سبيل المثال قد تعرض مواقع استضافة تقديم الخدمة فضاءً في شبكة الويب للإيجار في بلد على أساس العتاد الموجود في بلد آخر. بل إن الأعطال القصيرة في الخدمات يمكن أن تسبب أضراراً مالية ضخمة في شركات أعمال التجارة الإلكترونية. وشبكات الاتصالات المدنية ليست هي الأنظمة الوحيدة المعرضة للهجوم، إذ إن الاعتماد على تكنولوجيا المعلومات والاتصالات يمثل عنصر مخاطرة كبيراً أيضاً للاتصالات العسكرية. وبعكس المقاتلين التقليديين، لا يحتاج المهاجمون السيبرانيون إلى التواجد في المكان الذي يحدث فيه أثر الهجوم أو حتى في المكان الذي يظهر أن الهجوم ينشأ فيه. ويستطيع المهاجمون أثناء القيام بالهجوم استعمال تكنولوجيا اتصال مجهول الهوية والتشفير لإخفاء هويتهم.[41]

وبالإضافة إلى ذلك، يجري استعمال أدوات البرمجيات المتوفرة على نطاق واسع عبر الإنترنت من أجل شن هجمات أوتوماتية. إذ يمكن بمساعدة هذه البرمجيات والهجمات المركبة سلفاً أن يقوم مهاجم واحد بمهاجمة

---

[38] Fifth Domain.

[39] *انظر على سبيل المثال المرجع نفسه* (حيث جاء فيه أن "الاستعمال الأكثر ترجيحاً للأسلحة النووية قد لا يكون إحداث تدمير إلكتروني شامل ولكن سيكون استعمالها لأغراض حرب محدودة").

[40] *المرجع نفسه*.

[41] *CERT Research 2006 Annual Report*، جامعة كارينجي ميلون، Software Engineering Institute, at 7 *et seq.*, http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

آلاف الأنظمة الحاسوبية في يوم واحد باستعمال حاسوب واحد. وإذا كان المهاجم يملك النفاذ إلى أكثر من حاسوب - مثل النفاذ عن طريق برنامج تسلل روبوتي - فإنه يستطيع أن يزيد من حجم الهجوم إلى درجة أكبر. وعلى سبيل المثال يُشير تحليل الهجمات التي جرت ضد المواقع الشبكية الحكومية في إستونيا إلى أنها تمت من خلال آلاف الحواسيب داخل "برنامج تسلل روبوتي" أو مجموعة من الحواسيب المشبوهة لتشغيل برامج تحت سيطرة خارجية.[42] وبرامج التسلل الروبوتية تجعل أيضاً من العسير تعقب المجرم الأصلي نظراً لأن الآثار الأولية تقود فقط إلى الأفراد الآخرين في برنامج التسلل. ويشير التحليل الجاري إلى أن ما يصل إلى ربع جميع الحواسيب الموصولة بالإنترنت يمكن تلويثها ببرمجيات تجعلها جزءاً من برنامج تسلل روبوتي.

وتؤدي أدوات البرمجيات أيضاً إلى تبسيط الهجمات وتسمح لمستعملي الحاسوب الأقل خبرة أو المجموعات العسكرية الأقل تقدماً بارتكاب هجمات سيبرانية. وبالإضافة إلى ذلك نجد أن الهجمات القائمة على أساس تكنولوجيا المعلومات والاتصالات هي عموماً أرخص من العمليات العسكرية التقليدية بل ويمكن أن تقوم بها الدول الصغيرة. وقد أصبح الآن بمقدور دولة تملك تاريخياً قدرات عسكرية أقل أن توجه ضربة قاصمة إلى البنية التحتية الحرجة من خلال هجمات سيبرانية. وهذا الاختلال المحتمل في التوازن يجعل الحرب السيبرانية جذابة كطريقة استراتيجية لتحقيق درجة من المساواة في الفرص في سيناريوهات ستكون خلاف ذلك *سيناريوهات قوة غالبة ضد قوة ضعيفة*. والخوف من الحرب السيبرانية الذي يُعززه وقوع هجمات سيبرانية فعلية (حتى وإن كانت محدودة) يقوض ثقة الجمهور في تكنولوجيا المعلومات والاتصالات. وهكذا فإن التذبذبات النفسية المحتملة للنـــزاع السيبراني يُمكن أن تنطوي على آثار واسعة الانتشار لتعطيل الاستعمال الفعلي للتكنولوجيات الجديدة وعرقلة التقدم في قطاعات كثيرة.

---

[42] *Understanding Cybercrime: A Guide for Developing Countries*, at 72, International Telecommunication Union, April 2009, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (hereinafter "Understanding")

3 أوجه اعتماد المجتمع والثقة المجتمعية

1.3 اعتماد المجتمعات الحديثة على تكنولوجيا المعلومات والاتصالات والإنترنت

بقلم جاك بيس

لقد بدأنا في استعمال الحواسيب وتكنولوجيا المعلومات منذ النصف الثاني من القرن الماضي بينما بدأت الإنترنت منذ 38 سنة فقط كشبكة اتصال في مشروع آربا (ARPA). ومع ذلك فإن الإنترنت، بفضل اختراع الشبكة العنكبوتية العالمية (وسوف نسمي الجمع بين الإنترنت والويب في بقية هذه الورقة باسم "الإنترنت" توخياً للسهولة) انتشرت في السنوات الخمس عشرة الأخيرة فقط في كل أنحاء الاقتصاد والحياة الاجتماعية بسرعة مذهلة. ونستطيع الآن أن نتمتع بالاتصال والتشابك الاجتماعي في أي وقت وفي أي مكان؛ ونملك الوصول إلى معلومات لا حدود لها عملياً؛ ونستطيع أن نناقش وأن نتواصل اجتماعياً مع أشخاص في كل أنحاء العالم؛ ونستطيع أن نُقارن وأن نطلب خدمات ومنتجات من مقاعدنا الوثيرة في البيت في أي وقت نشاء.

وحسب تقديرات الاتحاد الدولي للاتصالات عن عام 2009 يملك 25,9% من سكان العالم توصيلاً بالإنترنت (وهو ما يعني 1,8 مليار شخص). ويقضي الناس أمام الإنترنت ضعف عدد الساعات التي يقضونها أمام التلفزيون. وهناك 4,6 مليار اشتراك في الهواتف المتنقلة في أنحاء العالم تُمثل 67% من سكان العالم. وكان فيسبوك وحده يضم أكثر من 500 مليون مستعمل ناشط في يوليو 2010، وجذب فيسبوك وماي سبيس وتويتر معاً 220 مليون زائر ناشط في شهر يوليو 2010. ومن أهم التغييرات التي شملت كل أنحاء العالم تحول الهاتف المتنقل إلى هاتف إنترنت وبذلك حل محل الحاسوب الشخصي كجهاز مفضل للتوصيل بالإنترنت. وبالفعل يتمتع 9,5% من السكان في أنحاء العالم بالنطاق العريض المتنقل.

وفي حين أن الإنترنت قد أحدثت فعلاً تغييراً في المجتمع الحديث من جوانب جوهرية وعلى نطاق عالمي حقاً فإن علينا أن ننتظر الكثير في المستقبل. ففي كثير من المنشورات[43] نقرأ سيناريوهات للمستقبل عن شكل العالم بعد 25 سنة من الآن. فسوف يكون من الشائع استعمال أقراص الهوية لركوب وسائل النقل العام والسجلات الصحية والنفاذ إلى الخدمات الحكومية والخدمات الموصولة بالشبكة. وسوف يتسع التشابك الاجتماعي مع اكتشاف تطبيقات جديدة أكثر فعالية وأكثر إثارة. وسوف يحقق ربط البيانات وجود خدمات معلوماتية جديدة تُساعد الباحثين على القيام بالأبحاث بفعالية أكبر وتُساعد المسافرين على زيادة تمتعهم برحلاتهم وتُساعد المواطنين على فهم قواعد الإدارات وبواعث السياسيين، وما إلى ذلك. وسيكون

[43] Trust in the Information Society: *A Report of the Advisory Board RISEPTIS,* http://www.think-trust.eu/; David-Olivier Jaquet-Chiffelle, ed., *Identity Revolution: Multidisciplinary Perspectives,* FIDIS, May 2009, http://www.fidis.net/resources/identity-revolution/.

هناك وكلاء وعمليات تستند إلى السياسات العامة تُخفف عنّا كثيراً من عبء العمل الإداري، مثل تحديد المواعيد والتجهيز للاجتماعات والامتثال للتشريعات.

وسوف تؤدي الثورة المجتمعية القائمة على تكنولوجيا المعلومات والاتصالات إلى تغييرات جوهرية في توازن القوى على الصعيد الوطني حيث يحصل المواطنون على معلومات غزيرة عن العمليات السياسية التي سوف تُستعمل في العملية الديمقراطية، وكذلك على المستوى الدولي أيضاً. وسيمكّن النفاذ إلى الإنترنت المواطنين من تحسين إدماجهم في الحياة الاقتصادية والسياسية وفهم أحوال وطرق الحياة في ثقافات أخرى. وقد شهدنا كيف استعمل الرئيس أوباما رئيس الولايات المتحدة الشبكات الاجتماعية في حملته الانتخابية ولنا أن نتوقع أنشطة مشابهة في المستقبل لدعم صنع القرارات الحكومية.

وتسمح تكنولوجيا المعلومات والاتصالات أيضاً للشركات الدولية بتنظيم نفسها بطرق تُحقق الاستخدام الأمثل للفرص المتاحة في كل أنحاء العالم. ويُمكن أن يؤدي كل ذلك إلى تعزيز التنمية الاقتصادية والنمو عالمياً وخاصة في البلدان منخفضة التكاليف. ونشهد بالفعل كيف أخذت بلدان نامية كبرى تستفيد من هذا الموقف وأصبحت من اللاعبين الهامين اقتصادياً وسياسياً.

ومع ذلك، وكما يحدث في حالة كل ثورة في التاريخ، تقترن الفرص والمزايا دائماً بجانب سلبي.

لقد أصبحت البنية التحتية للمعلومات والاتصالات وخدماتها جانباً حرجاً في اقتصاداتنا. ولكنها ضعيفة للغاية وفقاً لما تُثبته أنباء الهجمات الكثيرة التي تحدث يومياً تقريباً. ومعظم البنية التحتية الحرجة الأخرى، مثل الطاقة والمياه والنقل والأنظمة المالية، تعتمد اعتماداً كثيفاً على تكنولوجيا المعلومات والاتصالات من أجل القيام بعمليات الاتصال والمراقبة. ولذلك يوجد خطر مرتفع من وقوع حوادث أو هجمات متعمدة على هذه البنية التحتية الحرجة، وهي هجمات قد تؤدي إلى الفوضى وإلى خسائر اقتصادية هائلة. ويشمل ذلك عمليات التطفل والهجوم على الأنظمة وقواعد البيانات الخاصة بوكالات الأمن القومي.

وهذا الضعف في بنيتنا التحتية المجتمعية لتكنولوجيا المعلومات والاتصالات يجعل منها هدفاً سهلاً أمام "الحرب السيبرانية" أو "الإرهاب السيبراني" ويُنشئ تهديداً للاستقرار الجيوسياسي. والقيام عن عمد بتنظيم هجمات على الأنظمة الحرجة لمجتمع إحدى الدول بموافقة دولة أخرى أو دعمها أو سيطرتها يُسمى أحياناً "الحرب السيبرانية". وينبغي أن يكون واضحاً رغم ذلك أن كلمة "الحرب" في هذا السياق قد تُثير البلبلة نظراً لأنها لا يمكن أن تُقارن من أوجه كثيرة بما يجول بخاطر كثير من الناس عند التحدث عن الحرب: أي التدمير الطويل الأجل في البنية التحتية المادية والخسائر الباهظة في الأرواح.

وفي السنوات القليلة الماضية وقعت عدة هجمات استُخدم فيها مصطلح "الحرب السيبرانية"؛ في إستونيا،[44] وجورجيا وكوريا الجنوبية والولايات المتحدة على سبيل المثال. وقد بدأت هذه الهجمات أحياناً بشن

---

[44] انظر أيضاً كيرتو روس، "Cyber War I: Estonia attacked from Russia," *European Affairs*, Vol.9, No1-2, 2008, http://findarticles.com/p/articles/mi_7054/is_1-2_9/ai_n28550773/.

"حرب" نفسية من جانب الهواة بأهداف دعائية، ثم تحولت في مرحلة ثانية لتشمل متخصصين في الهجمات السيبرانية (من المجرمين أو غير المجرمين) في حملة كاملة عن طريق برامج التسلل الروبوتية التي تُطلق هجمات منع الخدمة الموزعة على البنية التحتية الاجتماعية والاقتصادية. وفي حالات أخرى تم تنفيذ الهجمات السيبرانية قبل أعمال الحرب الحركية مباشرة أو أثناءها. وحتى الآن كان التدمير الناشئ عن الهجمات السيبرانية محدوداً في معظم الحالات وأمكن استعادة القدرة بعد بضعة أيام، دون أي ذكر لخسائر في الأرواح تعود مباشرة إلى الهجمات السيبرانية.

ولا يوجد في معظم الحالات ما يُثبت الأدوار التي قامت بها الدول في هذه النزاعات. ولكن ذلك يُبرهن على الحاجة العاجلة للتوصل إلى اتفاقات بشأن كوابح الهجمات السيبرانية والدفاع ضدها وللدخول في تعاون دولي لوضع هذه الهجمات تحت السيطرة. ومن الواضح أن مبدأ الردع القديم الذي ساد أثناء الحرب الباردة لا ينطبق بسهولة في الفضاء السيبراني. والعناصر التي يتألف منها هذا الردع ليست مفهومة بصورة واضحة، والأهم من ذلك أن العدو يصعب تحديد هويته (عدم إمكانية نسبة الهجوم واستعمال مخدمات وكيلة).

وإذا نحّينا جانباً المناقشة السياسية بشأن مصطلح "الحرب السيبرانية" فليس هناك شك في أن الجريمة السيبرانية تتحول الآن إلى قضية تُسبب قلقاً جديداً. ويتزايد عدد التهديدات الخبيثة والإجرامية تزايداً هائلاً. ففي عام 2008 وحده اكتشفت خدمة سيمانتك 1,6 مليون تهديد، وهي تُمثل 60% من مجموع التهديدات المكتشفة في جميع السنوات السابقة لعام 2008. ووقع أكثر من 8 مليون شخص مقيم في الولايات المتحدة ضحية لسرقة الهوية. وقُدر متوسط تكلفة خروقات البيانات في الولايات المتحدة بمبلغ 6,7 مليون دولار أمريكي. وفي فبراير 2010 أصبح من المعروف أن 750 000 نظام حاسوبي للشركات في أنحاء العالم أُصيبت واستولت عليها برامج التسلل الروبوتية. ويُشير آميت يوران، وهو مسؤول سابق في الولايات المتحدة، إلى أن الشركات ليست مستعدة بالمرة للدفاع عن نفسها، رغم أن الصناعة الأمنية في الولايات المتحدة قللت من هذا الخطر بعد ذلك.

ومع إقرار هوارد شميت، (المساعد الخاص لرئيس الولايات المتحدة ومنسق الأمن السيبراني) بتزايد مشكلة الاستعمال الخبيث للإنترنت فإنه عرض أولويات واضحة. فهو يرفض مصطلح "الحرب السيبرانية" باعتباره "مفهوماً فظيعاً". وهو لا يرى أن هناك أي جهة يمكن أن تكون هي الرابحة في هذه البيئة واقترح التركيز على الجريمة والتجسس عبر الإنترنت.

ورغم اختلاف الآراء فهناك اتفاق عام على أنه لا يوجد سبب للانزعاج من الأمن والثقة في الإنترنت. والاتجاهات الجارية تنطوي على خطر زيادة خوف المواطنين على العالم الرقمي الجديد ورفضهم له. وقد ينطوي ذلك على آثار اقتصادية ضخمة إذا لم تتمكن السياسة والتكنولوجيا من التعامل مع هذه التطورات المجتمعية السلبية.

وشددت هيلاري كلينتون، وزيرة خارجية الولايات المتحدة في كلمة لها في 21 يناير 2010 على أهمية انفتاح وحرية الإنترنت من أجل التعاون والتنمية على الصعيد العالمي. وأشارت إلى "الحريات الأربع" التي حددها روزفلت - وهي حرية التعبير والعبادة والتحرر من العوز والخوف - والأثر الهام للإنترنت على هذه

الحريات، وخاصة حرية التعبير. وقد أدت الإنترنت إلى ثورة في تبادل المعلومات والتشابك الاجتماعي. وهي تنطوي على إمكانات هائلة لخلق مزيد من الثروة لكل شخص، وخاصة في حالة الاعتراف الكامل "بحرية التوصيل". ولكنها أدت أيضاً إلى زيادة الجريمة العالمية وإثارة الخوف، وهو خوف لا بد من احتوائه.

وقد اعترف السياسيون بوضوح بالأهمية الهائلة للإنترنت في الساحة الجيوسياسية العالمية. وهم يفهمون أن المواطنين يتوقعون من الحكومات أن توفر لهم السلامة والحماية في حين أن التشريعات الوطنية والحدود الوطنية لم تعد توفرهما كما كانت تفعل من قبل. وقانون المستهلك الذي يُطبق في الوقت الحاضر في بلدان كثيرة، وكذلك المسؤولية المصاحبة للمنتجات والخدمات، لا تعمل بصورة فعالة في عالم يشهد انفصال العميل والمورد في منطقتين قضائيتين مختلفتين غير متعاونتين وحيث يتم توصيل الخدمات من خلال سلاسل مخصصة للخدمات الفرعية باستخدام بيانات من حواسيب سحابية منتشرة في أنحاء العالم.

ويواجه زعماء العالم تحديات هائلة لا مثيل لها. ويتعين إيلاء الاهتمام السياسي إلى تغير المناخ وإلى التغيرات السريعة الحاصلة في القوى الاقتصادية العالمية وإلى أمن الطاقة، من بين قضايا أخرى كثيرة، وكذلك المخاطر الناشئة عن التوصيل الرقمي العالمي. وسوف نحتاج إلى قيادة عالمية قوية تملك رؤية مستقبلية لحل كل هذه المشاكل.

والأهم في كل ذلك هو استعمال ما تعلمناه من التاريخ عن الهياكل والقيم المجتمعية والأمن والثقة والعلاقات الدولية. ويجب أن ندخل في عملية تحوّل عالمية لنقل ثقافاتنا وقيمنا المجتمعية ونقاط قوتنا الاجتماعية وعمليات التعاون الدولي لكي يمكن الاستفادة منها في عالم يعترف بواقع يتشابك رقمياً.

ضرورة الثقة

مفهوم الثقة ودورها في المجتمع

"تغمر الثقة حياتنا اليومية. وإذا أخذنا عينة صغيرة فقط من المجموعة الهائلة من المناسبات فسوف نرى بالتأكيد أن الثقة هي أكثر الظواهر الاجتماعية حيوية. ولكن هذه المحورية تقترن بمشاكل لدراسة الثقة - كيف يستطيع المرء أن يبدأ مجرد البدء في فهم هذه القوة الاجتماعية المتقلبة؟" [45]

الثقة والجدارة بالثقة مفهومان من المفاهيم الأساسية في الوجود الإنساني. ونحن نستعملهما بصورة غريزية ويتوقف تقييمهما على السياق في كل حالة بدون استثناء. ولكن عند نقل هذه المفاهيم إلى البيئة الرقمية فإننا نواجه فوراً بعض المشاكل.

---

[45] كيرون أوهارا، *Trust: From Socrates to Spin*, Icon Books, Cambridge, 2004 at page 10, http://eprints.ecs.soton.ac.uk/9361/.

ويوضح لوهمان[46] أن الثقة كآلية تُقلل التعقيد وتمكّن الأشخاص من التعامل مع مستويات مرتفعة من الشكوك والتعقيد في الحياة (المعاصرة). وهكذا فإن الثقة توسع قدرة الناس على الاتصال بنجاح بعالم حقيقي تزيد درجة تعقيده وعدم القدرة على التنبؤ به كثيراً عما نستطيع استيعابه. وبهذا المعنى تُصبح الثقة آلية ضرورية لكي يعيش الأشخاص حياتهم: في الاتصال والتعاون وإجراء المعاملات الاقتصادية، إلخ. والثقة تُثري حياة الفرد حيث تشجع النشاط والجرأة والمغامرة والابتكار وحيث تثري علاقات الفرد بالآخرين.

وإذا نظرنا إلى الثقة من منظور آخر فسوف يكون من الممكن أن نقول إن الثقة هي توقع السلوك الطيب تجاه الطرف الذي يمنح الثقة، في أي حالة معينة. وكما يوضح هاردن:[47] "تندرج الثقة في الفئة المعرفية مع المعارف والمعتقدات. فعندما أقول إنك موضع ثقتي فإن هذا لا يعني أكثر من أنني أعرف أو أعتقد بعض الأشياء عنك، وهي تجعلني أعتقد أنك تستحق ثقتي وأنك سوف تتصرف "تصرفاً حميداً" حتى في الظروف غير المتوقعة."

والثقة هي علاقة ثلاثية (*ألف* يثق في *باء* ليفعل *سين*). وتقييم ثقة *ألف* في *باء* ليفعل *سين* يؤدي دوراً هاماً في قرار *ألف* للمشاركة في أي معاملات أو مبادلات أو اتصالات مع *باء*. والثقة تقلل التعقيد والمخاطر المتصورة وبذلك تُسهل فعلاً النشاط الاقتصادي والإبداع والابتكار. والثقة تتوقف على السياق توقفاً كبيراً. وهي مشروطة: الوقت (إذ إن المرء يستطيع بسهولة أن يفقد الثقة في شخص ما، ولكن المفهوم يتغير أيضاً مع مرور الوقت)؛ والتاريخ والذاكرة؛ والمكان والموقف؛ والثقافة؛ والدور (الخاص أو المهني)؛ والمشاعر؛ وبعدد من المتغيرات الأخرى (على سبيل المثال الاعتبارات السوسيولوجية من قبيل الشهرة والتكرار والتوصية).

ومن الواضح مما سبق أن الثقة مفهوم يمكن تعزيزه بصورة متصاعدة في حالة بعينها وبين طرفين بعينهما. ويمكن أن تُعزز المعلومات الإضافية الثقة، وهي معلومات قد يتم الحصول عليها من خلال أدوات استشعار أخرى أو من خلال العلاقات، وكذلك مع طول مدة العلاقة الناجحة.

وعموماً ينبغي في هذه المناقشة أن نعتبر الطرفين *ألف* و*باء* من أفراد البشر. وهذا لا يمنع إمكانية تصرف هؤلاء البشر نيابة عن منظمات أو مجموعات. ولكن كثيراً من الناس في الممارسة العملية سيتحدثون أيضاً عن الثقة في كيانات أخرى، مثل الثقة في حكومة أو شركة أو نظام أو خدمة أو قاعدة بيانات أو خدمة معلومات (مثل ورقة بحثية أو تدوينة تكنولوجية)، أو ربما كيان افتراضي مثل وكيل البرمجيات. ويسمى هاردن ذلك "الثقة في أفعال الكيان أو سلوكه أو استقامته". ويمكن خلق هذه الثقة مثلاً من خلال المساءلة والشفافية والتأكيد والتبعة والتدقيقات والشهرة أو المعرفة عن نوايا الكيان.

---

[46] نيكلاس لوهمان، "*Trust: A Mechanism for the Reduction of Social Complexity*", *Trust and Power*, New York: Wiley, 1979 at 4-103

[47] راسل هاردن، *Trust and Trustworthiness*; Russell Sage Foundation Series on Trust, Vol. 4, 2002.

وقد قام فوكوياما[48] وبوتنام[49] وخبراء آخرون بمناقشة وتطوير مفهوم الثقة كرأس مال اجتماعي أو "الثقة الاجتماعية". وهذا المفهوم مفهوم إحصائي يُعبر عن رأي الأشخاص في جدارة مجتمعهم بالثقة في كل جوانبه، أو ربما، وبصورة أدق: ثقة الأشخاص في حكومة المجتمع أو مؤسساته أو قوانينه أو أنظمته، إلخ. ويبدو أن هناك تناظراً قوياً بين الثقة الاجتماعية العالية وارتفاع النمو الاقتصادي والرخاء.

وسوف نستخدم كلمة "الثقة" في أغلب الأحيان أيضاً في المواضع التي تسميها هاردن "الطمأنينة". ومع ذلك، فمن المهم لمواصلة المناقشة أن نُميّز الثقة بين الأشخاص الذين يستخدمون الأنظمة والخدمات الرقمية عن طريق الشبكة في معاملاتهم والثقة أو الطمأنينة لدى الشخص في كيان غير إنساني أو مؤسسة.

وقد أدى إدخال التكنولوجيا الرقمية إلى إحداث ثورة في الاتصال والتعاون بين البشر من خلال إدخال وسيط جديد يتألف من مجموعة معقدة من "المؤسسات" القائمة على التكنولوجيا (بما فيها الشبكات والخدمات الرقمية وقواعد البيانات والشبكات الاجتماعية). ولذلك يجب عند التعامل مع الثقة بين الفعاليات البشرية أن نبحث أيضاً جانب الثقة (الثقة أو الطمأنينة) في هذه البنية التحتية التكنولوجية.

ويُناقش نيسينباوم[50] فقط الثقة بين الأشخاص الذين يستخدمون الأنظمة الرقمية المربوطة بالشبكة للاتصال فيما بينهم ويذكر قائمة بالعوامل التي تستجيب لها اتجاهات الثقة (أو عدم الثقة) بصورة منهجية:

1. التاريخ والشهرة.
2. الاستنتاجات المستخلصة على أساس الخصائص الشخصية: مثل الفضيلة والحذر والوفاء والرغبة في الحصول على رأي طيب لدى الآخرين والسلوك والملابس.
3. العلاقات: التبادل والمعاملة بالمثل والأسرة والاشتراك في نفس الحالة والاشتراك في الأهداف.
4. أداء الأدوار (قائد الطائرة أو السفينة، سائق الحافلة).
5. عوامل السياق (المجموعات والمجتمعات - الدعاية؛ المكافأة والعقاب؛ القواعد؛ تأمين الثقة أو شبكات الأمان مثل المسؤولية أو قوانين المستهلك).

وينطوي عدد من هذه القضايا، وخاصة المذكورة في 1 و3، على جوانب "الثقة باعتبارها مصلحة مختصرة في شكل كبسولة" كما تُعرفها هاردن.[48] ومن مصلحة الشخص موضع الثقة أن يتصرف بطريقة حميدة بحيث لا يفقد مثلاً السمعة التي يمكن أن تؤدي إلى إنهاء العلاقة من جانب الشخص الذي يُعطي الثقة (مثل

---

[48] فرانسيس فوكوياما، *Trust: The Social Virtues and the Creation of Prosperity*, Free Press, 1995.

[49] روبرت د. بوتنام وروبرت ليوناردي ورافاييل واي. نانيتي، *Making Democracy Work: Civic Traditions in Modern Italy*, Princeton University Press, 1993.

[50] هيلين نيسينباوم، "Securing Trust Online: Wisdom or Oxymoron?" Boston University Law Review, Vol. 81, No. 3, June 2001 at 635-664, www.nyu.edu/projects/nissenbaum/main_cv.html.

قائد الطائرة قد يفقد وظيفته بعد أن يفقد سمعته). وتذكر هاردن أيضاً قائمة بالعقبات التي تعترض الثقة على الخط:

1 عدم وجود بيانات الهوية (ولكن يُلاحظ الحق في إخفاء الاسم).

2 عدم وجود الخصائص الشخصية (ولكن يُلاحظ الحق في الخصوصية).

3 السياقات التي يصعب فهمها (المجهولة والمشوشة التي تؤدي إلى الغموض ولكن أيضاً إلى التحرر).

وهذه النقطة الثالثة يمكن أن ينظر إليها باعتبارها مجرد مرحلة متقدمة في التعقيد على الخط. فهي تسمح بزيادة الحرية طبعاً ولكن الأمر يتطلب في الوقت نفسه، من أجل إجراء معاملة صحيحة أو اتصال صحيح، بناء قدر أكبر من ذلك من الثقة وبالتالي من إمكانية الوثوق. وتُلاحظ نيسينباوم أيضاً أن الأمن لا يعني الثقة. فإذا كان هناك أمن فليست هناك ضرورة للثقة. ومع ذلك فإن الثقة تمكّن الناس من الحياة في عالم غير آمن وغني بالتعقيد وزيادة الأمن يُقلل هذا الثراء والتعقيد. ويُعتبر مؤلفون آخرون أن الأمن يوجد في كفة من كفتي ميزان الثقة وفي الكفة الأخرى توجد الثقة غير المبررة بالمرة (الساذجة).

ومن خلال البنية التحتية العالمية للمعلومات تتزايد الثقة (بأشخاص غرباء) مع الحصول على المزيد من المعرفة (عن هؤلاء الغرباء)، وهذا هو ما جعل مجلة الإيكونوميست تُعلن: "أن رغبة الكثيرين، إذا أُتيحت لهم الفرصة، [...] للعيش في بلدان خلاف بلدهم تُلغي توافق الآراء القائم منذ زمن طويل في السياسة والفلسفة على أن الحيوان البشري يعيش أفضل ظروفه في موطنه."[51] والأكثر من ذلك: "لقد كان خطأ الفلسفة هو افتراض أن الإنسان ينبغي أن ينتمي، لأنه حيوان اجتماعي، إلى مجتمع بعينه."[52] ومع ذلك فإن هذا يمكن أن يكون تعميماً سريعاً أكثر مما ينبغي لسلوك أقلية من الناس، نظراً لأن معتادي السفر والمسافرين مسافات أطول من مجرد رحلات الإجازات المضمونة والموثوقة التي يُنظمها وكلاء سفر مسؤولين في بلد المسافر لا يزالون يمثلون أقلية صغيرة جداً.

ومع ذلك فإن العولمة، التي تدفعها بوضوح تكنولوجيا المعلومات والاتصالات الجديدة وشبكة الويب، تخلق التفاهم وبالتالي تخلق مزيداً من الثقة عن طريق نشر المعلومات عن تاريخ وسمعة المجتمعات، وخصائص المجتمعات وحياة الأشخاص الذين يعيشون في بعض المجتمعات، وتسمح بسهولة الاتصال في كل أنحاء العالم. وقد يؤدي ذلك بالفعل إلى زيادة تآكل مفهوم "أفضل مكان للحيوان البشري هو موطنه". وقد تؤدي أيضاً إلى ضرورة التوصل إلى آراء جديدة بشأن المجتمعات وتماسكها والدور الذي يجب أن تؤديه الثقة في كل ذلك.

---

[51] "The Others", *The Economist*, 17 december 2009, www.economist.com/node/15108690.

[52] *المرجع نفسه*.

الثقة في المجتمع الرقمي

كما ذكرنا أعلاه يجب أن نُميز بين ما يلي:

- الثقة بين الأشخاص في مجتمع يستعمل على نطاق واسع التكنولوجيا الرقمية لأغراض الاتصال والمعاملات.
- الثقة أو الطمأنينة لدى الأشخاص إزاء البنية التحتية للشبكات والأنظمة الرقمية التي يستخدمونها لأغراض الخدمات والاتصال وتخزين البيانات والحوسبة، إلخ.

تتصل مشاكل الثقة (بين الأشخاص) في المجتمع الرقمي مقابل "المجتمع القديم" بما يلي بالتحديد:[53]

- التغير التحويلي في طريقة جمع البيانات وتخزينها وتجهيزها وإتاحتها وحمايتها. ولا يقتصر جمع وتخزين البيانات على البيانات التي ينتجها أشخاص بغرض تبليغها وتخزينها، ولكن ذلك يشمل بالتحديد البيانات المجموعة عن السلوك عن طريق المراقبة (من مراقبة السير في الشارع إلى زيارة مواقع الويب أو فتح إعلانات شبكة الويب).
- في الإنترنت تعني مصطلحات تحديد الهوية والسمعة والتصديق والمساءلة شيئاً آخر. إذا تعين على الشخص أن يُثبت الخصائص وتقديم أسرار أو معلومات بيومترية لإقناع شخص آخر بهوية مقدم البيانات. ويمكن بسهولة تدمير السمعة من خلال نشر معلومات محرجة أو زائفة ويكون من الصعب للغاية تصحيح هذه المعلومات. وإمكانية الاختفاء في ولاية قضائية أخرى تقوض المساءلة والشفافية إلى درجة كبيرة في حالة عدم وجود اتفاقات دولية بشأن إنفاذ القانون وتسليم المجرمين.
- أدت زيادة التعقيد والتكنولوجيا غير المفهومة مع عدم وجود ضمانات كافية عن طريق إصدار الشهادات والتقييس، والافتقار إلى الشفافية في عمليات وأساليب جمع البيانات واستخدامها إلى خلق سياق يصعب فهمه، وهو ما يقوض الثقة التي يتعين إقامتها بين الأشخاص في البيئة الرقمية. وقد يشعر الناس بالحيرة إزاء ما يحدث حولهم وهم لا يعرفون في كثير من الأحيان أي شيء عن البيانات التي يتم تجميعها عنهم وكيفية استخدامها.

ومن الأيسر إقامة الثقة عندما تكون الهوية و/أو معلومات إثبات الصحة (أوراق الاعتماد أو الخصائص أو الادعاءات) عن الطرف الثالث معروفة أو يمكن تأكيدها (ربما عن طريق طرف ثالث موثوق). وقد تعطي الثقة السمعة وغيرها من المعرفة المتجمعة من شبكة الويب أو من الأصدقاء في الشبكات الاجتماعية ثقة إضافية. وبالإضافة إلى ذلك سيشعر المواطنون بدرجة أكبر من الثقة في التعامل مع طرف ثالث إذا كان لديهم السيطرة على الكشف عن بياناتهم لهذا الطرف الثالث وتبادل هذه البيانات معه. وتزيد أيضاً الثقة من خلال شفافية عمليات جامعي البيانات والقائمين بتجهيزها ومن خلال سمعة هذه الكيانات.

---

[53] انظر نيسينباوم.

ولكن، وهذا ما يجعلنا نصل إلى النقطة الثانية، لا يمكن الحصول على الثقة بين الأشخاص في عالمنا التكنولوجي إلا إذا أمكن الشعور بالثقة في الأنظمة المستعملة لتبليغ وتبادل البيانات أو تأكيد الهوية أو غيرها من المعلومات مثل السمعة أو وثائق الاعتماد. ولكي يستعمل المواطنون الإنترنت يجب أن تتوفر لديهم الطمأنينة إزاء الأدوات والأنظمة والبنية التحتية التي يستعملونها في معاملاتهم واتصالهم. ونحن نصف أي نظام أو خدمة بجدارة الثقة إلى درجة معينة إذا كان الشخص يملك درجة معينة من الثقة المبررة بأن النظام أو الخدمة سيؤديان واجبهما وفقاً لأوصافهما أو وعودهما، وأن النظام أو الخدمة لن يؤديا أعمالاً غير موصوفة في مختلف الظروف. ويمكن الشعور بالثقة المبررة من خلال المساءلة (مسؤولية المنتجات) أو شفافية تجهيز البيانات وتخزينها أو شهادات النظام التقني والقدرة على تدقيق الحسابات لاحقاً. ويمكن أيضاً تعزيزها من خلال توفير أدوات وآليات مفهومة ومفيدة تُمكّن من تأكيد الادعاءات بشأن الاعتماد أو السمعة أو الهوية. والناس يحتاجون إلى خدمات وأدوات تساعدهم على إنشاء وتعزيز الثقة في نوعية الخدمة والأمن والمرونة وحماية البيانات والخصوصية، وفقاً لسياسات محددة سلفاً ويسهل فهمها. ويمكن توفير ذلك من خلال مقدمي الخدمات الآخرين وكذلك من خلال السلطات العامة.

وكما يقول فيتالي تسيغشكو[54]، تؤدي أنظمة المعلومات الأوتوماتية دوراً هاماً بصفة خاصة في المجتمع الحديث، وهي أنظمة يتزايد إدماجها في نظم الإدارة العامة عبر كل قطاعات الاقتصاد الوطني. وتُشكل أنظمة المعلومات الأوتوماتية جوهر أنظمة دعم القرارات لكل المنظمات الاجتماعية الاقتصادية تقريباً. وموثوقية أداء نظم المعلومات الأوتوماتية لا يتوقف عليها فقط كفاءة السلطات العامة والاقتصاد والمنظمات الطوعية ولكن أيضاً الأمن القومي.

ومن الواضح أنه من المهم للغاية دراسة جدارة هذه الأنظمة بالثقة. ويتصل ذلك أساساً بصحة نماذجها الأساسية وموثوقية برمجياتها وعتادها ومستوى المؤهلات المهنية للموظفين الذين يقومون بصيانة النظام وفعالية تدابير الحماية من التهديدات الخارجية.

وتعني متابعة ما يقوله تسيغشكو أن جدارة أنظمة المعلومات الأوتوماتية بالثقة تتطلب تطوير مجموعة من الاشتراطات والمقاييس للأمن والموثوقية (بما في ذلك النموذج الأساسي الذي يعمل كمثال للواقع) وسلامة البيانات. ويمكن استعمال مقياس مخاطر اختراقات الأمن كأحد معايير التقييم. وتعرَّف **إدارة المخاطر** بأنها عمليات تنطوي على تعيين وتحليل المخاطر وصنع القرارات بما في ذلك تعظيم الآثار الإيجابية وتقليل الآثار السلبية لحدوث المخاطر.

وبالإضافة إلى الوسائل التقنية المطلوبة لبناء الثقة نحتاج أيضاً إلى قواعد ولوائح وقبول مجتمعي. وسوف يثق المواطنون في التعامل مع بياناتهم الشخصية داخل مجتمعهم في حالة: احترام لوائح الخصوصية وحماية البيانات الشخصية وإمكانية إنفاذها؛ وامتثال المنظمات لمفاهيم المواطنين لثقافة المساءلة عن طريق حماية المستهلك

---

[54] فيتالي تسيغشكو عضو مساعد في فريق الرصد الدائم لأمن المعلومات وشارك في هذه المناقشات.

الصحيحة ووجود لوائح للانتصاف؛ ووجود لوائح بشأن المراجعة والشفافية؛ ووضوح إسناد المسؤولية في سلسلة الفعاليات في أي معاملة يجري تنفيذها.

وعلى الصعيد السياسة العامة لا يمكن إنشاء بنية تحتية لتكنولوجيا المعلومات والاتصالات تكون جديرة بالثقة ومواصلة تشغيلها إلا مع توزيع صحيح ومنصف للحوافز في كل سلسلة القيم.

ويتعين للشفافية والمساءلة كفالة الإنصاف وإمكانية التنفيذ. ويتعين معالجة المشاكل المتصلة بمسؤولية الأنظمة، وخصوصاً الأجزاء الخاصة بالبرمجيات وسلامة البيانات. ويمكن أن يؤدي ذلك إلى تطوير نظام من تأمين مخاطر خروقات الأمن، وهو ما يؤدي بدوره إلى دعم تطوير مقاييس وأدوات تمكّن من تقييم المخاطر. ويمكن أن يؤدي كل ذلك في نهاية المطاف إلى نظام يتسم بدرجة كبيرة من التنظيم الذاتي والاستدامة.

وهناك شرط جوهري لبناء الثقة بين الناس في استعمال الإنترنت وهو صياغة نظام جدير بالثقة وقابل للتشغيل عالمياً من أجل **تحديد الهوية والاستيقان**. ومن أمثلة الإجراءات التي اتخذتها بلدان كثيرة قيام الحكومات بإصدار بطاقات هوية وجوازات سفر إلكترونية موثوقة وفقاً لمعايير متفق عليها في أنحاء العالم. ولكننا نحتاج لأغراض المعاملات الإلكترونية العالمية إلى عملية إدارة لمستندات الاعتماد والمطالبات قابلة للتشغيل البيني في الإنترنت لتكفل الامتثال لحقوق الخصوصية. والمساءلة مسألة جوهرية في اقتصاد الإنترنت ولا يمكن تحقيقها إلاّ من خلال مسؤولية فعلية للأشخاص والمنظمات عن أعمالهم العامة والتعاقدية. وتتحقق المسؤولية عن الأعمال التعاقدية عادةً من خلال تقديم مستندات اعتماد وإثبات الخصائص أو استعمال أسرار لا يعرفها سوى الشخص نفسه. ويستطيع الشخص أن يستخدم مختلف الأسرار أو مستندات الاعتماد أو الخصائص في حالات مختلفة، وهو ما يقود إلى "هويات" مختلفة. وقد اقترح كاميرون وبوش وراينبيرغ[55] معايير من المستوى الشرحي لإدارة ادعاءات الهوية.

وتتيح الإنترنت، بمختلف شبكاتها الاجتماعية الكثيرة، فرصة للناس والمنظمات لبناء سيرة حياتهم ودوائر أصدقائهم وسمعتهم في مختلف المجتمعات. وإذا استخدمنا مصطلحات مشروع "مستقبل الهوية في مجتمع المعلومات – FIDIS"[56] فإن ذلك يؤدي إلى "هويات جزئية للشخص". وفي المواقف التي تتطلب مساءلة يمكن أن يرتبط ذلك بطريقة تحمي الخصوصية بتعريف الهوية والاستيقان والتوقيعات الرقمية. ويمكن أيضاً أن تُساعد على زيادة الثقة في الإنترنت كآلية للأنشطة الاجتماعية والاقتصادية.

---

[55] كيم كاميرون ورايارد بوش وكاي راينبيرغ، *Proposal for a Common Identity Framework: A User-Centric Identity Metasystem,* Joint 'ICT Security' – 'ICT for Government and Public Services' Workshop on "Identity Management in the Future Digital Society"، 14 أكتوبر 2008، www.identityblog.com/?p=1048.

[56] "About the FIDIS Network of Excellence," www.fidis.net/about/.

ملخص

ناقشنا أهمية الثقة في مجتمعنا والآراء المختلفة بشأنها. وبالتحديد ناقشنا التغيرات والمشاكل التي أخذت تظهر مع تحول مجتمعنا ليتزايد اعتماداً على الاتصال الرقمي والمعاملات الرقمية من خلال الإنترنت. والافتقار إلى تعيين الهوية الكافي بطريقة تحترم ضرورة عدم الكشف عن الهوية في بعض الحالات وعدم وجود تجربة الخصائص الشخصية مع الحاجة إلى حماية الخصوصية وأخيراً وليس آخراً السياق المبهم الناشئ عن البنية التحتية للتكنولوجيا المستعملة في اتصالاتنا أمور أدت جميعها إلى حرمان البشر من الآليات الجوهرية لإنشاء الثقة لتمكينهم من الحياة والإبداع في مجتمع معولم.

ولذلك يجب أن نقوم بصياغة آليات جديدة جديرة بالثقة في البيئة الرقمية لتمكين الأشخاص من بناء الثقة بينهم بغض النظر عن مكان وجودهم أو طريقة اجتماعهم.

ويجب أن نكفل وجود شبكات اتصالات مأمونة وجديرة بالثقة؛ وأنظمة معلومات تضمن الامتثال لحماية البيانات وقوانين الخصوصية؛ وإطار عالمي جدير بالثقة وقابل للتشغيل البيني لتحديد الهوية وإدارة مستندات الاعتماد/الادعاءات؛ وخدمات تحقق معايير المسؤولية الصحيحة وقوانين حماية المستهلك. ويجب تصميم هذه التكنولوجيا وتطويرها مع مراعاة الثقة والأمن والخصوصية، وتمكين قوانين الإنفاذ والشفافية وفي الوقت نفسه يجب صياغة قوانين ولوائح تُراعي اتجاهات التكنولوجيا وإمكاناتها.

ويجب أن يعمل القطاعان العام والخاص معاً على الصعيد الدولي من أجل بناء بنية تحتية للتكنولوجيا تتسم بالتوازن الجيد ووضع قوانين/لوائح تُعطي للمواطنين الثقة في استعمال فرص العالم الرقمي الجديد.

ومن خلال القيام بذلك تستطيع البشرية أن تحصل حتى الآن على فرص لم تكن متوقعة للاتصال والتعاون وأن تقوم بمعاملات اقتصادية على الصعيد العالمي استناداً إلى آليات الثقة، بما يشبه ما عرفته البشرية في الماضي في المجتمعات الصغيرة من خلال التفاعل البشري المباشر. وسوف يُشكل ذلك خطوة حاسمة نحو الاستقرار العالمي.

2.3 الآثار الاجتماعية الاقتصادية للجريمة السيبرانية

بقلم جاك بيس[57]

ينطوي تقديم الخدمات الرقمية، والبنية التحتية الرقمية عموماً التي يجري تطويرها لمجتمعنا، على إمكانات إيجابية هائلة. وفي الوقت نفسه، يمكن أن تُستعمل هذه التكنولوجيا، مثلها مثل كل التكنولوجيات، في أنشطة خبيثة. ويمكن أن نميّز مجالات المشاكل الأربع التالية فيما يتعلق بالقضايا الاجتماعية الاقتصادية:

1 **الطابع العالمي للفضاء الرقمي**: نشأ عن ظهور الخدمات والاتصالات عبر الحدود على الإنترنت عدد من قضايا الثقة الاقتصادية والاجتماعية وقضايا الأمن القومي التي كان يجري معالجتها حتى الآن على مستوى الحدود بين الدول (مراقبة الواردات والصادرات ومراقبة جوازات السفر والجمارك والعدوان بين الدول، وما إلى ذلك) أو داخل الدول على يد الشرطة المحلية أو الوطنية ضد المواطنين المسجلين. والعواقب السلبية لعدم وجود مراقبة على الحدود في الفضاء الرقمي لم تخضع لمناقشة بأي شكل كبير سواء أكان على صعيد الدولة الواحدة أم على الصعيد الدولي. ولكن من الواضح أنها تُسهل الجريمة من ناحية إنشاء نوع من الحصانة للمجرمين التي ترجع في جانب منها إلى أن العمل الذي يجري عن طريق الإنترنت يصعب نسبته إلى فاعله وترجع في جانب آخر إلى وجود الفاعلين في دول تعطيهم الحماية من إنفاذ القانون دولياً.

2 **تعقّد الخدمات**: يتزايد تنظيم المعاملات والخدمات في شبكة الويب باعتبارها سلاسل مخصصة من الخدمات الفرعية التي تنتشر عبر ولايات قضائية وتستعمل بيانات مأخوذة من كل أنحاء "السحب". والخدمات أو البيانات الفرعية يمكن أن تندرج في أنظمة قضائية مختلفة أو حتى متعارضة. ويصعب على المستهلكين إدراك هذه الحقيقة وفهم عواقبها. فلم تعد الدول قادرة على ضمان المسؤولية عن المنتج وحماية المستهلك بالطريقة التي كان يجري بها ذلك حتى الآن. وستحتاج الدول إلى اتفاقات دولية وإلى تعاون في إنفاذ القوانين بالتعامل مع هذا الوضع. وبالإضافة إلى ذلك يتعين أن تكفل الخدمات الشفافية في سلسلة الخدمة وأن تستجيب (آلياً) للشروط التي يضعها المستهلك. والحالة الجارية تفتح، مقترنة بالنقطة 1، الباب واسعاً أمام خداع وتدليس لا يمكن تعقبهما. وفي الوقت الحاضر لا تستطيع الدول أن توفر الحماية من ذلك.

3 **الشبكات الاجتماعية وغرف الدردشة**: وهي تُستخدم في كثير من الأحيان لإجراء اتصالات بدوافع خبيثة تُركّز بالتحديد على الأطفال أو كبار السن. وهذا ليس جديداً. فقد كانت عمليات الاحتيال والغش موجودة دائماً. ومع ذلك فإن ضعف الاستيقان والافتقار إلى الآليات المأمونة والمحصّنة لحماية الخصوصيات من أجل أوراق الاعتماد (مثل الأسماء وبيانات المولد والعمر ونوع الجنس وبيانات العمل وكلمات المرور) تجعل كل ذلك أمراً سهلاً ومربحاً. وقد وصلت الفيروسات أيضاً إلى مواقع الشبكات الاجتماعية حيث يمكن استخدام الثقة في هذه المواقع لنقل الفيروسات. ومعدل نجاح الهجمات باستخدام

[57] يود المؤلف أن ينوه بمساهمة أوبو هيلمبريشت وفريقه من الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA).

الشبكات الاجتماعية مرتفع جداً. والتمويه هو التهديد رقم واحد ضد المصارف ولكن المصارف لا تُقدم بعد خدمات لإثبات نفسها أمام العملاء.

4 **منظمات الجريمة الدولية:** تم التبليغ في كثير من الأماكن في السنوات القليلة الماضية أن الجريمة الدولية لم تنتقل فقط إلى شبكة الويب من أجل تنفيذ نواياها الإجرامية ولكن توجد سوق سوداء دولية تعمل لتوزيع الأدوات الإجرامية (مواقع الاحتيال الروبوتي وأدوات التمويه والفيروسات، وما إلى ذلك) والبيانات المسروقة (المعلومات الشخصية وبيانات بطاقات الاعتماد ومعلومات أسرار الشركات). والجرائم التي تجري على شبكة الويب وباستعمال هذه الشبكة تُحسّن من تنظيمها على الصعيد الدولي بصورة مستمرة وتنتشر بصورة واسعة عبر ولايات قضائية بما في ذلك ولايات قضائية ذات هيئات قضائية ضعيفة جداً، وتُركّز كثيراً جداً على المكاسب المالية. وهناك أمثلة كثيرة لهذا التطور. وقد أغلقت لجنة التجارة الاتحادية في الولايات المتحدة شركة برمجيات ترويع شبه قانونية في مارس بلغ رقم أعمالها السنوي 180 مليون دولار أمريكي. وهناك ضمانات رد ثمن الفيروسات والدعم التقني ومجموعات "التركيب الذاتي" للقيام بأفعال إجرامية في حالة عدم رضاء المشتري. ويُكلف الفيروس الطروادي المصرفي المسمى زيوس (Zeus) 700 دولار أمريكي (4 000 دولار أمريكي لآخر نسخة) في السوق السوداء (ويُستخدم زيوس لإحباط مخططات الاستيقان مثل مخططات العامل المزدوج ومخطط الشفرة الآمنة لماستر كارد). وهناك عدة طبقات من الموردين القانونيين وشبه القانونيين الذين يُحققون أرباحاً من الاقتصاد الخفي.

وتُقدم الدراسات والإحصاءات أحياناً أرقاماً مذهلة عن الخسائر المجتمعية والاقتصادية المتصلة بهذه الأنشطة غير القانونية. وقد ترتفع هذه الأرقام لتصل إلى ترليون دولار أمريكي[58] على الصعيد العالمي، وهو ما يبلغ قرابة 2% من الناتج المحلي الإجمالي العالمي. وتُقدر شبكة بوستن للحوسبة أن قطاع الأعمال الأمريكي خسر أكثر من 7,6 مليار دولار أمريكي نتيجة الفيروسات في الأشهر الستة الأولى من عام 1999. وتُقدر الأرقام الألمانية عن الخسائر المالية للتمويه بمبلغ 15 مليون يورو سنوياً وخسائر بطاقات الائتمان بمبلغ 155 مليون يورو.

وعموماً فإن معظم الأرقام عن الخسائر الاقتصادية تستند إلى افتراضات قابلة للمناقشة وهي مستنبطة بالضرورة مما هو معروف في حين أن كثيراً من المشاكل لا يتم التبليغ عنها علناً. ومع ذلك يمكن أن نتوصل إلى استنتاج أن التكلفة الاجتماعية الاقتصادية للجريمة السيبرانية كبيرة جداً، ويلجأ كثيرون ممن يتخذون قرارات بشأن الاستثمار في التدابير الأمنية إلى تقليلها في كثير من الأحيان. وينبغي النظر إلى العائد من الاستثمارات الأمنية بطريقة أكثر جدية.

---

58 "McAfee, Inc. Research Shows Global Recession Increasing Risks to Intellectual Property," McAfee Press Release, Feb. 2010, www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html ; see also Unsecured Economies Protecting Vital Information, McAfee, 2009, http://resources.mcafee.com/content/NAUnsecuredEconomiesReport.

وتتطلب مكافحة الجريمة السيبرانية توزيع المسؤولية عن الأعمال الجارية في البيئة الرقمية. ويشمل ذلك الأعمال الفرعية في الخدمة المنتشرة دولياً والناشئة دينامياً. ويتطلب الأمر التعاون القانوني والدبلوماسي على المستويات السياسية العالية الدولية من أجل تحديد سياسات وإجراءات مشتركة تخلق الموثوقية والمسؤولية في الخدمات وفي الأعمال العمومية والاقتصادية.

والمطلوب حدوث تطوير تقني للتوصل إلى حلول تحافظ من ناحية على الشبكة العالمية دون تقسيم ويستطيع أصحاب الأعمال والمستهلكون النفاذ إليها لأغراض العمل والاتصال والمعلومات، أثناء الإقامة والسفر، وبطرق تكفل الامتثال للقوانين المنطبقة على جميع أمثلة النشاط. ومن ناحية أخرى يحق للأشخاص التمتع بالحياة الخاصة على شبكة الويب وبالتالي ينبغي أن تتاح لهم إمكانية العمل في شبكة الويب في حدود دوائر الثقة المأمونة المحدودة التي يختارونها بأنفسهم في بعض الحالات وبضمانات من مقدمي الخدمات بأن ما يقدمونه من بيانات لن يُستعمل في أغراض أخرى.

ولكننا نشهد الآن للأسف تطوراً لاقتصاد البيانات الخاصة يسير في الاتجاه المعاكس. فشركات جمع وتجهيز البيانات تحصل على أرباحها فقط من نموذج تجاري يتمحور حول بيانات العملاء الخاصة. وقد يظن المستهلكون أنهم عملاء لمقدمي هذه الخدمات وأنهم قد يتحملون المسؤولية عن الخدمة. ولكن الواقع هو أن المستهلك لا يدفع شيئاً إلى هذه الشركات إذ إن المستهلكين هم الناتج فقط في الواقع. وشركات التسويق ومحللو البيانات والقائمون بتجميع الملامح الشخصية والمعلنون والشركات الأخرى هم العميل **الحقيقي** الذي تبيع له مواقع الشبكات الاجتماعية ونوافذ الخدمات، إلخ بيانات المستهلكين.

ويبدو في الواقع أن الحياة الخاصة قد وقعت فريسة التطورات في الفراغ الاجتماعي الاقتصادي المتصل بالرقمنة والتشابك. وتتناقص تكلفة تخزين البيانات تناقصاً سريعاً جداً وفي نهاية المطاف سيتم تخزين بيانات بدون حدود من ناحية الكمية والوقت. وسيؤثر ذلك تأثيراً عميقاً على طريقة التفاعل وكيفية خلق جرائم جديدة في المستقبل (خروقات الخصوصية وتحديد الملامح الشخصية بدون إذن والبحث عن البيانات بدون إذن) وكذلك طرق جديدة للسيطرة السياسية. وقد يكون الكثير من ذلك مناقضاً للحقوق الدستورية الموجودة في الوقت الحاضر وقلما نجد مناقشة لتأثير ذلك على الاستقرار الاجتماعي والاقتصادي والسياسي في المجتمع.

وبالإضافة إلى الآثار المحتملة للبيئة الرقمية على الجريمة وحقوق الإنسان، وهي الآثار التي نُوقشت أعلاه، هناك خطر مختلف تماماً على المجتمع والاقتصادات وهو يتصل بالضعف الشديد للبنية التحتية المجتمعية الرقمية في المستقبل. فالمجتمعات قد تواجه ككل خسائر اقتصادية واجتماعية فادحة إذا تعرضت شبكات اتصالاتها أو بنيتها التحتية الحرجة الأخرى للهجوم والأعطال، سواء أكان ذلك من جانب مجرمين (لأغراض الابتزاز) أم من جانب الإرهابيين لبث الخوف والاضطراب، أو من جانب دول أخرى في إطار حرب أو ردع. وإمكانية تصرف الدول ضد هذه الهجمات تقتصر عملياً على أعمال الدفاع. والاستراتيجيات التي تتسم بطابع هجومي أكبر مثل الردع أو الهجوم المضاد يصعب تنفيذها نظراً لأن الهجمات يصعب في كثير من الأحيان نسبتها إلى جهة ما وتبدأ في كثير من الأحيان في أماكن غير معروفة أو في دول مارقة. وسوف يزيد

التطور التكنولوجي، في حالة عدم إيلاء اهتمام كافٍ بالأمن والثقة في الشبكات والأنظمة، من هذه المشاكل بل وقد يؤدي إلى أن تكون النزاعات الوطنية والدولية خارجة عن السيطرة في المستقبل.

وأخيراً تمثل المخاطر طويلة الأجل للمجتمع عنصراً جوهرياً وإضافياً يجب دراسته. وقد تستمر الهجمات لبضع ثوانٍ ولكنها تُحدث آثاراً واسعة إلى حد ما. ولكن الخسارة المجتمعية للثقة في هذه الثواني قد تتطلب سنوات وسنوات لإعادة بنائها. وتقويض الثقة بين الناس وبين الناس وشركات الأعمال وبين المواطنين والدولة وبين الدول نفسها يمكن أن يولد آثاراً مدمرة على المجتمعات وعلى الاستقرار العالمي في الأجل الطويل. وسيكون ذلك عقبة تعترض النمو الاقتصادي الفعّال في المستقبل الذي يتوقف بدرجة كبيرة في اقتصاد ما بعد الأزمة الجاري على نمو استعمال تكنولوجيا المعلومات والاتصالات. ونحن لا نستطيع أن نتحمل تكلفة الركود في هذا المجال بسبب ضياع الثقة.

وأمن الشبكات والمعلومات، بما في ذلك عملية الاستيقان، في البيئة الرقمية يجب أن يكفل سلامة المواطنين (المادية والاقتصادية والخاصة). وسوف تكفل أنظمة تكنولوجيا المعلومات والاتصالات وبنيتها التحتية ومؤسساتها الجديرة بالثقة وجود مستوى من الثقة الاجتماعية في مجتمعاتنا، وهو أمر جوهري من أجل الرخاء الاقتصادي كما تبيّن في كثير من الدراسات.

ومع أنه يصعب قياس عدم الاستقرار في المجتمع والضرر في الاقتصاد (من ناحية النمو الاقتصادي) فإنهما قد يصلان إلى أبعاد كبيرة جداً. ويدعو ذلك إلى التأهب وتوفير حماية قوية، وكذلك الانتعاش السريع وإصلاح الأنظمة ذاتياً.

وتلخيصاً لما سبق نستطيع أن نقول:

إن الطابع العالمي للفضاء الرقمي مقترناً بضعف تعيين هوية المستعملين وعدم كفاية إسناد الأفعال وتعقّد الخدمات المنتشرة دولياً والتطوير العالمي لمواقع الشبكات الاجتماعية وأسواق الجريمة الدولية الناشئة كلها تُثير القلق الجدي من ارتفاع الجريمة السيبرانية وبالتالي استدامة المجتمع المستقر كأساس للتنمية الشخصية والرخاء الاقتصادي.

وضعف البنية التحتية المجتمعية لتكنولوجيا المعلومات والاتصالات وجمع وتخزين البيانات بدون حدود يهددان الحرية الشخصية والاستقرار الدولي.

وثقة المواطنين في المجتمع والحكومة لحماية أمنهم وسلامتهم ورخائهم تتعرض للتآكل بفعل الأخطار والشكوك الناشئة عن التطورات التقنية مع ما ينطوي عليه ذلك من خسائر اقتصادية باهظة.

ولذلك فإننا نحّث على سبيل الاستعجال على اتخاذ إجراءات سياسية عالمية للتصدي لهذه المشاكل استناداً إلى تحليل متماسك للاتجاهات والعواقب التكنولوجية والمجتمعية والاقتصادية والسياسية.

4 اتجاهات التكنولوجيا والتهديدات

1.4 الإمكانيات والاتجاهات والتهديدات في الوقت الراهن

بقلم أكسل ليمان وفلاديمير بريتكوف وجاك بوس

إن القوة المحركة للابتكارات في المنتجات هي حصيلة ما "تزج به" التكنولوجيا وما "تجذبه" الأسواق. وفي هذا الصدد، فإن تحليل الاتجاهات المستقبلية والابتكارات المحتملة في تكنولوجيا المعلومات والاتصالات يقتضي النظر في التطورات التكنولوجية الحالية والمتوقعة فضلاً عن اتجاهات متطلبات المستهلكين أو متطلبات السوق في المستقبل. ولذلك، تتناول المقاطع الثلاثة الأولى من هذا الفصل تلك الاتجاهات والمتطلبات وفقاً لذلك. ويعقبها تحليل للتهديدات الرئيسية وبعض الملاحظات الختامية.

وإذ يُستهل هذا الفصل بموجز من التحليلات والتقييمات التالية، يُفترض أن الابتكارات التكنولوجية المرتقبة لن تقف عند التقدم السريع الذي تحرزه التكنولوجيات الجديدة الميكروية والنانوية، بل ستشمل أيضاً تطوير أجهزة استشعار وحوسبة متكاملة على نطاق واسع، وتطوير تكنولوجيات شبكات واتصالات جديدة، و خدمات وتطبيقات مبتكرة. كما ستفعّل هذه الابتكارات اتجاهين رئيسيين من التطورات:

- تقارب الحواسيب الفردية وهواتف المستخدمين المتنقلة الحالية لتندمج في جهاز واحد للحوسبة والاتصالات محمول متنقل متعدد الاستخدامات؛
- ارتقاء شبكة الإنترنت وتكنولوجيات وخدمات الويب الحالية نحو إنترنت المستقبل. أما "إنترنت الأشياء" التي ستتميز بقدرة هائلة على الاتصال والتنقلية بالنسبة إلى الأفراد وإلى جميع أنواع الأجهزة والأغراض ("الأشياء")، وفيما بينهم، فستخطو خطوة إلى الأمام نحو شبكة إنترنت مستقبلية فعالة وموثوقة وجديرة بالثقة.

وستتعزز هذه التطورات التكنولوجية بمتطلبات السوق والمستهلكين الداعية لتطوير الجديد من خدمات تكنولوجيا المعلومات والاتصالات ومنتجاتها وتطبيقاتها. فوفقاً لدراسة نشرتها مجلة فوربز (Forbes) فإن قطاعات الترفيه والاتصالات والطاقة والرعاية الصحية ستكون، على وجه الخصوص، قاطرات منتجات تكنولوجيا المعلومات والاتصالات المبتكرة، وستشكل ميادينها التطبيقية الكبرى.[59]

وفي هذا المجال، فإن الفصول الفرعية الثلاثة التالية ستُجْمِل أهم عوامل التأثير في مستقبل تطورات تكنولوجيا المعلومات والاتصالات ونتائجها: اتجاهات التكنولوجيا، ومتطلبات السوق والمستهلك، و "إنترنت الأشياء"،

[59] روبرت كريسياك. "الاتجاهات الكبرى في أشباه الموصلات عام 2010"، فوربز، يناير 2010، www.forbes.com/2010/01/04/stmicroelectronics-healthcare-entertainment-technology-cio-network-semiconductors.html.

فيما يرد في الفصلين الفرعيين الأخيرين ملخص للفرص والتهديدات والتحديات الأساسية أمام هذه الابتكارات في تكنولوجيا المعلومات والاتصالات في حياتنا الخاصة والعامة.

اتجاهات التكنولوجيا

لا شك أن التصغير والرقمنة في العقد الحالي قد ساهما إلى حد كبير في قطع شوط طويل نحو "عالم مرقمن" تُخزن فيه جميع أنواع البيانات والمعلومات والمعرفة، وتُرسَل وتعالَج في شكل رقمي. ويبين تحليل اتجاهات ما يستجد من تطورات للتكنولوجيات الأساسية الحالية، ألا وهي أشباه الموصلات، بأن قانون مور (Moore) القاضي "بمضاعفة عدد الترانزستورات لكل بوصة مربعة كل سنتين" ربما سيبقى سارياً لمدة عشر سنوات أخرى على الأقل. إذ إن تقنيات التصميم والتصنيع الراهنة تتيح دمج نحو مليار ترانزيستور في رقاقة واحدة. وحتى إذا حلت تكنولوجيات جديدة، مثل التكنولوجيا الحيوية أو الحوسبة الكمومية، تدريجياً محل تكنولوجيا أشباه الموصلات الحالية على المدى الطويل، ستتواصل هذه الاتجاهات العامة لزيادة التصغير والرقمنة وللتوسع في الخواص الوظيفية والتطبيقية، مفرزةً مزيداً من التوسع في تكنولوجيا المعلومات والاتصالات وفي المنتجات والتطبيقات القائمة على تكنولوجيا المعلومات والاتصالات.

وفي هذا المقام، يتعين النظر في أربعة مجالات رئيسية لمستقبل تطورات النظام الرقمي ومبادئ التنظيم في سياق تطورات العتاد والبرامج الثابتة والبرمجيات:

- أنظمة الحاسوب الواحد والمتعدد.
- شبكات وبروتوكولات وخدمات الاتصالات.
- التكنولوجيات النانوية، وعلوم المواد، وأجهزة الاستشعار، والأنظمة الفاعلة والمدمجة.
- آليات التشغيل والتنظيم اللامركزية للأنظمة الرقمية.

وإذ كان الدمج واسع النطاق جداً للترانزستورات في مساحة الرقاقة بالإضافة إلى رفع ترددات الميقاتية يتسبب بمشاكل فرط الإحماء، فإن **المعالجات الصغرية** الحالية تُصمَم كمعالجات متعددة النوى تعمل بترددات ميقاتية مخفضة ولكن بأداء معزز بفضل المعالجة المتوازية في الرقاقة. وسوف يمكّن تواصل الابتكارات في المعالجات عبر تكنولوجيات أشباه الموصلات متعددة الطبقات وزيادة عدد المعالجات الأساسية وانخفاض استهلاك الطاقة لكل رقاقة. وسيؤدي ذلك إلى تحسينات كبيرة في الأداء من خلال معالجات متعددة النوى، وأنظمة المعالجات المتعددة مما يعزز من زيادة سعات ذاكرة التخزين المؤقت والذاكرة الرئيسية، وتطورات الأنظمة المحتواة ضمن رقاقة. وسترفع هذه الاتجاهات أداء كامل مجموعة الحواسيب بدءاً من الحواسيب في رقاقة واحدة مروراً بمكونات الحوسبة المدمجة ووصولاً إلى الحواسيب العملاقة. وإذ تتقدم شبكات الاتصالات والتبديل كذلك، ستتوفر جميع أنواع هياكل ومعماريات الحواسيب الموصولة بينياً.

بالإضافة إلى ذلك، ستتاح أيضاً أجهزة تخزين خارجية سريعة بسعات تخزين أعلى وأوقات نفاذ مختصرة إلى الحد الأدنى، بفضل تقنيات التصغير المحسنة. وإلى جانب تقدم النُهُج المعمارية والتقنيات البرمجية، سيغدو ممكناً التنفيذ المتوازي الهائل لتطبيقات برمجية معقدة. وفي موازاة ذلك، ستتحسن أو تتيسر كثيراً تنقلية الحواسيب وجميع أنواع أجهزة الحوسبة ومن خلال تطوير الجديد من تكنولوجيات منخفضة الطاقة والبطاريات.

في مجال **شبكات وبروتوكولات وخدمات الاتصالات**، ستتأتى كبرى الابتكارات من التحسينات الدائمة لتقنيات الاتصالات اللاسلكية والساتلية التي تقدم توصيلية أعلى وتوسع عروض النطاق. ويتعلق أحد الاتجاهات الكبرى بالتشكيل الدينامي لشبكات افتراضية، ومثالها شبكات خاصة افتراضية[60]. وهذه التقنية المطبقة بالفعل تقدم في الوقت المناسب تشكيلاً واستخداماً محدوداً للتطبيقات وللشبكات التي تستهدف المستخدم، وهي تتألف من مكونات وخدمات مختارة في الشبكة.

وهناك اتجاه آخر نحو المزيد من المرونة وسهولة الاستخدام في البنى التحتية القائمة للحوسبة والاتصالات، وهو اتجاه يعنى بتشكيل شبكات تراكب. وحالياً، يُنظر إلى هذا النهج التقني، كموضوع بحث رئيسي، على أنه نهج كفء للتغلب على القيود الحالية القائمة في بروتوكولي الإنترنت/التحكم في الإرسال (IP/TCP) وفي الارتقاء من الإصدار الرابع من بروتوكول الإنترنت (IPv4) إلى الإصدار السادس منه (IPv6)، وهي خطوات مهمة نحو توسيع استخدام الإنترنت و"إنترنت الأشياء". والتقدم التقني في كلا الاتجاهين هو شرط أساسي لمزيد من الابتكار في تكنولوجيا الإنترنت وتطبيقاتها. والنمو الهائل للإنترنت الحالية، لا سيما فيما يتعلق بتنوع وعدد الأغراض الموصولة بالإنترنت، يتطلب من جهة توسعاً كبيراً في مساحة العنوان الحالية لأغراض الإنترنت (الإصدار الرابع من بروتوكول الإنترنت) نحو الإصدار السادس من بروتوكول الإنترنت[61]. ولذلك، لا بد من تطوير تقنيات تحويل خاصة تتيح انتقالاً متنوع المقاييس بين هذين المعيارين. ومن جهة أخرى، وعلى نحو متزامن مع الارتقاء من الإصدار الرابع من بروتوكول الإنترنت إلى الإصدار السادس منه، يجب وضع بروتوكولين مقيّسين للإنترنت/التحكم في الإرسال (IP/TCP) في المستقبل لتمكين الاتصالات بين جميع أنواع الأغراض من خلال "إنترنت المستقبل". وعلى الرغم من أن كلا الاتجاهين من البحوث لا يزال بحاجة إلى حلول ملموسة، يمكن افتراض أن تلك الأسس التقنية للإنترنت المستقبلي ستكون قيد الاستخدام في غضون سنوات قليلة من الآن مقدمةً قدرات متطورة وجديدة لتطبيقات الإنترنت،"لإنترنت الأشياء" مثلاً.

---

[60] جيمز هنري كارموش، أسس أمن بروتوكول الإنترنت في الشبكة الخاصة الافتراضية، دار نشر سيسكو، 19 يوليو 2006، www.ciscopress.com/bookstore/product.asp?isbn=1587052075.

[61] س. ديرينغ ور. هندن، "بروتوكول الإنترنت، مواصفة الإصدار 6 (IPv6)"، جمعية الإنترنت، ديسمبر 1998، www.ietf.org/rfc/rfc2460.tx؛ والتر غورلاسكي، "إيضاح الشبكة: كيفية عمل TCP/IP في شبكة حديثة"، سلسلة مورغان كوفمان في الربط الشبكي، 2008، www.freshwap.net/forums/e-books-tutorials/120250-illustrated-network-how-tcp-ip-works-modern-network.html.

وبالإضافة إلى اتجاهات تطور نظام تكنولوجيا المعلومات والاتصالات المذكورة أعلاه، يجب الأخذ بعين الاعتبار سرعة التقدم التقني والإنتاجي في التكنولوجيات النانوية وعلوم المواد والمكونات الرقمية المتخصصة – مثل أجهزة الاستشعار القائمة على أشباه الموصلات والأنظمة الفاعلة أو المدمجة – عند تحليل الاتجاهات والتهديدات المستقبلية في تكنولوجيا المعلومات والاتصالات. وسيسفر هذا التقدم عن مكونات في تكنولوجيا المعلومات والاتصالات من قبيل:

- سطوح بينية ملموسة للمستخدم[62].
- شاشات عرض بوليمرية.
- ملابس مرقمنة (حاسوب يمكن ارتداؤه)[63].
- أجهزة الاستشعار المنفعلة والفاعلة (تكنولوجيات التعرف بواسطة الترددات الراديوية (RFID)[64]).
- الأنظمة "الذكية المحيطة"[65] أو "الحصيفة".

وبمحاذاة هذه التطورات التقنية، سيوفر المحسن والجديد من منتجات و**خدمات البرامج الثابتة/البرمجيات** وآليات التنظيم فرصاً لتحسين وإضافة خواص وظيفية وخدمات. وتتراوح هذه التطورات بين مختلف تكنولوجيات البرمجيات المبتكرة (كتطوير البرمجيات المستندة إلى وكلاء)، أو المعماريات الخدمية (SOA)، أو خدمات ويب جديدة، أو أنظمة إدارة (لتخزين البيانات أو استخراجها بكفاءة، أو من أجل موازنة الحمولة بكفاءة، على سبيل المثال) وصولاً إلى كفاءة استخدام البنى التحتية المتشابكة المشكلة من شبكات ضخمة من موارد الحاسوب والاتصالات الموزعة. ومعظم التطبيقات ذات الصلة وبعيدة المدى هي الحوسبة المتشابكة

---

[62] هيروشي إيشي، "السطح البيني الملموس للمستخدم"، اتصالات *ACM*، المجلد 51، العدد 6، يونيو 2008، http://portal.acm.org/citation.cfm?id=1349026.1349034.

[63] ستيف مان وهال نيدزيكي (Niedzviecki)، سايبورغ: المصير الرقمي والإمكانية البشرية في عصر الحاسوب الذي يمكن ارتداؤه، دار نشر دبلدي الكندية، نوفمبر، 2001.

[64] *اعتماد RFID وآثاره*، المفوضية الأوروبية (المديرية العامة للمؤسسات والصناعة، تكنولوجيا المعلومات والاتصالات من أجل التنافسية والابتكار)، المديرية العامة للمؤسسات والصناعة، مراقبة التجارة الإلكترونية القطاعية، دراسة التأثير رقم 07/2008، التقرير النهائي، سبتمبر 2008، www.ebusiness-watch.org/studies/special_topics/2007/rfid.htm؛ آرون نامبيار، "تكنولوجيا RFID: استعراض تطبيقاتها"، مجريات المؤتمر العالمي للهندسة وعلم الحاسوب 2009، المجلد الثاني، WCECS 2009، 20-22 أكتوبر 2009، سان فرنسيسكو، الولايات المتحدة الأمريكية، www.iaeng.org/publication/WCECS2009/WCECS2009_pp1253-1259.pdf.

[65] إ. آرتس، ر. هارويغ، م. شورمان، فصل "الذكاء المحيط" في كتاب بيتر ج. دنينغ، *المستقبل غير المرئي؛ الدمج السلس للتكنولوجيا في الحياة اليومية*، شركات مغرو هيل، 2001 في الصفحات235-250؛ د. رايت، س. غوتورث، م. فريدولد وغيرهما، *الضمانات في عام الذكاء المحيط*، سبرينغر، 2008، www.springer.com/computer/database+management+&+information+retrieval/book/978-1-4020-6661-0.

أو الحوسبة السحابية[66] التي تفتح عهداً جديداً من تكنولوجيا المعلومات والاتصالات فيما يتعلق باقتصادياتها وأدائها وتوافرها وموثوقيتها.

وعلاوة على كل التطورات التكنولوجية المذكورة أعلاه، يتعين الأخذ بعين الاعتبار اتجاهين رئيسيين أساسيين يتعلقان **بمبادئ التنظيم والتشغيل** عند تحليل الاتجاهات الأساسية لابتكارات تكنولوجيا المعلومات والاتصالات والتهديدات التي تحدق بها، وهما: **الافتراضية واللامركزية**. فقد أدت الزيادة المطردة في الخواص الوظيفية والتوصيلية للمكونات الرقمية غير المتجانسة، من ناحية، والطلب على استخدامها بكفاءة، من ناحية أخرى، إلى تشكيل أنظمة افتراضية وتشغيلها، ومثالها المعالجات الافتراضية أو ذاكرات التخزين الافتراضية أو حتى الحواسيب الافتراضية. زد على ذلك أن التعقيد المتزايد بشكل دائم لأنظمة الحاسوب والاتصالات المربوطة شبكياً واستخدام الشبكات الافتراضية على النحو المذكور أعلاه غالباً ما يحول دون التشغيل الكفء على أساس التحكم المركزي. فبدلاً من ذلك، يجري تطبيق آليات تشغيل تحكم لا مركزي في النظام والتي ثبت أنها أكثر مرونة وفعالية بالمقارنة مع تلك المركزية. ومن أمثلة الآليات اللامركزية، تطبيقات البرمجيات المستندة إلى وكلاء أو نظام التحكم البيولوجي التماثلي.

وقد أفرز تحقيق وتطبيق كلا المبدأين معاً – مبدئي الافتراضية واللامركزية – فرصاً جديدة لكفاءة استخدام الموارد الرقمية المربوطة شبكياً. وهذه الشبكات يمكن أن تشكل "تشابكات"[67]: تشابك حاسوبي يتألف من عقد حاسوبية مربوطة شبكياً، أو تشابك بيانات مكون من أنظمة تخزين موزعة موصلة بينياً، أو تشابكات معدات مشكّلة بأجهزة متخصصة يمكن النفاذ إليها عن بعد. ويمكن في حالة الحوسبة السحابية النفاذ عن بعد إلى تلك الموارد المربوطة شبكياً والموصولة بينياً واستخدامها عن طريق مقدمي الخدمات. وإلى جانب هذه الفوائد الاقتصادية والفوائد من حيث الأداء، لا بد من النظر في المخاطر أيضاً. ويتمثل التحدي العام – والمخاطرة الكبيرة حالياً – في امتلاك ناصية تعقيد تلك الأنظمة، وخاصة فيما يتعلق بالسلامة والموثوقية والأمن. وفيما يتعلق بالحالة الراهنة للعلوم، فإن تلك الأنظمة المربوطة شبكياً الموجودة لدينا فعلاً قيد التشغيل لا يمكن التحقق منها تماماً فيما يتعلق بصحتها ولا الإقرار بصحتها تماماً فيما يتعلق بتطبيقات محددة ولا اختبارها بشكل كامل نظراً للامتداد الهائل لمساحة حالتها. ولم يلق هذا الوضع اهتماماً كافياً حتى الآن على الرغم من أنه يظهر المشكلة الأساسية المتعلقة بابتكارات تكنولوجيا المعلومات والاتصالات[68]. أضف إلى هذا التحدي مخاطر أخرى تنجم عن وقوع الأخطاء والأعطال، وكذلك عن مصادر محتملة لإساءة

---

[66] فلاديمير بريتكوف، :الحوسبة المتشابكة والسحابية"، ورقة مقدمة إلى هيئة المراقبة الدائمة لأمن المعلومات في الاتحاد العالمي للعلماء، مايو 2010 (يشار إليه "بريتكوف" من الآن فصاعداً).

[67] بريتكوف.

[68] فلاديمير بريتكوف وآكسل ليمان، "التحديات الأمنية الناشئة عن الابتكارات في مجال تكنولوجيات المعلومات والاتصالات" *ندوة دولية حول الحرب النووية والطوارئ الكونية*، الدورة الثامنة والثلاثين، مركز إ. ماجورانا للثقافة العلمية، إريس، إيطاليا، 19-24 أغسطس 2007 في الصفحات 503-515.

الاستخدام والتلاعب. فيجب أن تأخذ هذه المخاطر بعين الاعتبار إجراء تقييم شامل لابتكارات تكنولوجيا المعلومات والاتصالات هذه، وهناك حاجة ملحة لمزيد من البحث بشأن التدابير المضادة.

اتجاهات طلبات المستهلكين والسوق

هناك الآن بالفعل مطلب رئيسي للأسواق والمستهلكين يتناول الحوسبة والاتصالات والنفاذ إلى المعلومات في كل مكان، وهو ما يعني استخدام الأجهزة الرقمية وقدرات الربط الشبكي "في كل مكان في أي وقت". إذ إن التنقلية العالية للمستهلكين، من ناحية، والتوزيع والتوافر العالمي للمعلومات والمعرفة، من ناحية أخرى، يُزيدان الطلبات على خصائص وظيفية محسنة أو مضافة لمنتجات تكنولوجيا المعلومات والاتصالات وعلى استخدامها بكفاءة. وستتنامى هذه الطلبات باستمرار وبشكل كبير وستكون وليدة أسواق مختلفة. فعلى سبيل المثال، يزداد الطلب على تعاون موزع محلياً ومستقل عن الزمن في الصناعات والاقتصادات.

وتستند هذه المطالب جميعها ضمنياً إلى افتراض أننا سنحيا ونعمل في عالم رقمي تماماً حيث يمكن تناول واستخدام كل غرض أو أي معلومة في أي وقت ومن أي مكان. وتولد هذه المطالب الاستهلاكية التي يحركها السوق قوة "جذب" كبيرة للابتكارات التكنولوجية، مثلاً من أجل الاستخدام الفعال للوسائط المتعددة أو تطبيقات الفيديو أو النفاذ إلى الويب في كل مكان أو العمل التعاوني بدعم الحاسوب (CSCW) أو استخدام مجموعة كبيرة من الخدمات والتطبيقات (القائمة على الويب). ولكن مكونات ومنتجات تكنولوجيا المعلومات والاتصالات الجديدة والمفيدة، إلى جانب التقدم نحو "إنترنت الأشياء"، قد تتسبب بإشكالات اجتماعية وإدارية جديدة، ناهيك عن التهديدات المحتملة للسلامة والأمن. ولذلك، يتعين أن تحلَل هذه الابتكارات والآثار المترتبة عليها بعناية منذ البداية – أي منذ الآن (انظر الفصل الفرعي التالي).

وكما هو موضح أعلاه، فإن تطورات العتاد والبرامج الثابتة والبرمجيات ستفعّل المنتجات الجديدة والتطبيقات المبتكرة المستندة إلى تكنولوجيا المعلومات والاتصالات وفقاً لما تقدم في ميادين التطبيق المختلفة. ومن أمثلة ميادين التطبيق هذه ما يلي:

- المعيشة الميسرة محيطياً (للمسنين مثلاً)[69].
- أنظمة التحكم الذكية (على سبيل المثال، في مجال النقل والخدمات اللوجستية والملاحة الجوية، وتوفير الطاقة، إلخ).

[69] كيزيتو ساموﻻ موكاسا، آندرياس هولزينغر، آرثر إ. ارشر "السطوح البينية الذكية للمستخدم من أجل المعيشة الميسرة محيطياً"، مجريات المؤتمر الدولي الثالث عشر بشأن السطح البيني الذكي للمستخدم، 2008 ,6-987-59593-1-978 :ISBN، http://portal.acm.org/citation.cfm?id=1378856؛ Fraunhofer IRB Verlag ; ISBN 978-3-8167-7521-8، http://verlag.fraunhofer.de/PDF/English_Publications_2010.pdf.

- المنازل "الذكية"[70].
- الرعاية الصحية.

وفي حين تتركز المطالب في قطاعي الترفيه والاتصالات أساساً على أداء تكنولوجيا المعلومات والاتصالات والجوانب الاقتصادية، فإن ميادين التطبيق الأخرى مثل أنظمة التحكم أو الرقابة في قطاعي الرعاية الصحية والطاقة يتعين عليها تلبية متطلبات السلامة أو الموثوقية أو الأمن في المقام الأول. وكما ذكر في الفصل الفرعي السابق، فإن الزيادة المطردة في أعداد وقدرات الأجهزة الرقمية المستخدمة في هذه التطبيقات، إلى جانب توصيليتها البينية غير المحدودة تقريباً، تؤدي إلى مشكلة "انفجار مساحة الحالة". وتمس الحاجة إلى جهود حثيثة في البحوث الأساسية والتطبيقية لتطوير ما يفي بالغرض من تصاميم وطرائق تحقق وإقرار صحة، فضلاً عن استراتيجيات اختبار لضمان متطلبات الجودة هذه.

"إنترنت الأشياء"

تعبّر "إنترنت الأشياء" عن رؤية مفادها أنه إلى جانب أفراد البشر، يمكن توصيل جميع أنواع الأجهزة والأغراض أو السلع من حياتنا اليومية ("الأشياء") عبر إنترنت المستقبل. ويمكن لهذه "الأشياء" أن تستقبل أو تخزن أو تعالج أو تبعث البيانات والمعلومات من خلال التواصل مع غيرها من "الأشياء" أو الأفراد أو الخدمات. وهذا يتطلب حصول عدد أكبر كثيراً من "الأشياء" على عنوان إنترنت – وهو أمر ممكن في إطار الإصدار السادس من بروتوكول الإنترنت (IPv6) – وأن تخدّم "الأشياء" نفسها أو في شبكات فرعية كمصدر مادي أو مقصد أو نقطة نفاذ للاتصالات والتعاون والحوسبة[71].

ويمكن لتنفيذ تدريجي لهذه الرؤية أن يحقق فكرة "الحوسبة والاتصالات في كل مكان" التي عبر عنها مارك وايزر منذ نحو 20 سنة خلت[72]. ومن الخصائص الرئيسية لهذه الرؤية تطوير الأغراض التقنية لتصبح "أغراضاً ذكية" تملك قدرات محدودة في الحوسبة والمنطق وتتصل من خلال شبكة الإنترنت مع الفضاء السيبراني. ومن

---

[70] ب. راشدي، د. ج. كوك، "إبقاء المقيم على اطلاع: تكييف المنزل الذكي على مقاس المستخدم"، في دورية الأنظمة والإنسان والسيبرانية، الجزء أ: الأنظمة والبشر، مداولات IEEE، سبتمبر 2009، المجلد 39، العدد 5 في الصفحات 949-959، http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?reload=true&punumber=3468؛ مشروع المنزل الذكي CASAS، جامعة ولاية واشنطن، الولايات المتحدة الأمريكية، http://ailab.eecs.wsu.edu/casas/.

[71] إنترنت الأشياء – خطة عمل لأوروبا، مذكرة اتصال من المفوضية إلى البرلمان الأوروبي، والمجلس واللجنة الاقتصادية والاجتماعية الأوروبية ولجنة الأقاليم، http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf؛ التذييل F: إنترنت الأشياء (خلفية)، التكنولوجيات المعطلة: اتجاهات عالمية 2005، هيئة SRI للاستعلامات التجارية الاستشارية، www.dni.gov/nic/PDF_GIF_confreports/disruptivetech/appendix_F.pdf.

[72] مارك وايزر، "الحاسوب للقرن الحادي والعشرين"، مجلة العلوم الأمريكية، سبتمبر 1991، في الصفحات 94-110، www.cim.mcgill.ca/~jer/courses/hci/ref/weiser_reprint.pdf.

أمثلة مثل هذا "الغرض الذكي" جهاز استشعار فاعل يتلقى المعلومات من أغراض أخرى فيعالجها ويتفاعل – استناداً إلى وضعه الحالي – عن طريق إرسال رسائل جوابية إلى الأغراض الأخرى. وسيمكن ذلك التواصل بين الأفراد و"الأشياء"، ولكن أيضاً بين "الأشياء" نفسها متيحاً فرصاً جديدة تماماً للتطبيقات، إلا أنها فرص تنطوي أيضاً على مخاطر فيما يتعلق بالسلامة وأمن تكنولوجيا المعلومات (الخصوصية والأصالة وأمن البيانات).

التهديدات الراهنة

كما ذكر من قبل، فإن حجم عالمنا الرقمي المربوط شبكياً وتعقيده وانفتاحه قد بلغ مستوىً لا يُستغرب معه النمو السريع في الإساءات. ومن شأن الاتجاهات المستقبلية للتوسع في تكنولوجيا المعلومات والاتصالات أن تفاقم من التهديدات المحتملة إن لم يُنظر فيها بعناية.

وهناك العديد من التقارير الصادرة إما عن جهات مهتمة في بيع الحلول الأمنية في تكنولوجيا المعلومات والاتصالات مثل شركات ماكافي (MacAfee)[73] وسيمانتيك (Symantec)[74] وكاسبيرسكي (Kaspersky)[75] أو عن جهات أخرى تناقش القضايا الأمنية الأعم أو تهتم في أمن ما يخصها من أنظمة ومنتجات تكنولوجيا المعلومات[76]. أما فئات أساليب الجريمة السيبرانية التي يغلب تناولها في هذه التقارير فهي كما يلي:

1 **الشفرة الخبيثة أو البرمجيات الضارة:** برمجيات قائمة على النية المبيتة لمبرمجها وليس على أي سمات خاصة. وتشمل البرمجيات الضارة فيروسات الحاسوب والديدان وأحصنة طروادة وبرمجيات التجسس والبرمجيات الدعائية المخادعة والبرمجيات الإجرامية ومعظم الجذور الخفية وغيرها من البرامج الخبيثة وغير المرغوب فيها[77]. وقد رصدت شركة سيمانتيك زيادة التهديدات الخبيثة الجديدة من 624 000 إلى 1 656 000 تهديد ما بين العامين 2007 و2008.

2 **الرسائل الاقتحامية** هي إساءة استخدام أنظمة الرسائل الإلكترونية (بما في ذلك معظم وسائط البث، وأنظمة التسليم الرقمي) لإرسال الرسائل غير المرغوب فيها بالجملة من دون تمييز. وأكثر أشكال الرسائل الاقتحامية شيوعاً هو البريد الإلكتروني الاقتحامي أو رسائل البريد الإلكتروني غير المرغوب

---

[73] مركز McAfee للمشورة الأمنية، http://home.mcafee.com/advicecenter/ ,

[74] " تقرير عن التهديدات المحدقة بأمن الإنترنت" Symantec، www.symantec.com/business/theme.jsp?themeid=threatreport.

[75] Kaspersky، www.kaspersky.co.uk/index.htm.

[76] "مركز تقنيات الأمن"، http://technet.microsoft.com/en-us/security/default.aspx، SANS، www.sans.org/.

[77] للاطلاع على هذا التعريف وعلى المزيد من الإيضاح، انظر: http://en.wikipedia.org/wiki/Malware.

فيها ذات المضمون التجاري والمرسلة بكميات كبيرة. إذ إن انخفاض تكلفة الإرسال يعود بقيمة عالية. بيد أن الرسائل الاقتحامية تُرسَل على نحو متزايد بنية إجرامية فتحوي برمجيات ضارة أو تسعى للإيقاع بالناس لحملهم على أداء دفعات مالية أو الإفشاء بمعلومات وما إلى ذلك (التصيد الاحتيالي). ولإخفاء عنوان المرسل وتمكين حجم عال من الإرسال، كثيراً ما يستخدم المجرمون حواسيب مأمورة (zombies) أو مسيّرة (bots) (حواسيب الآخرين التي تنقاد عن بعد في إطار تحكم خارجي دون علم المالك) أو شبكات من الحواسيب المأمورة (وتدعى أيضاً شبكات الحواسيب المسيّرة (botnets)). وتشير التقديرات إلى أنه في عام 2008، أُرسل ما مجموعه 350 مليار رسالة اقتحامية، 90 في المائة منها عن طريق شبكات الحواسيب المسيّرة. ويشكل ذلك قرابة 85 في المائة من مجموع الرسائل في جميع أنحاء العالم.

3 تقوم مواقع الويب والاستضافة **للتصيد** الاحتيالي بتقليد أو انتحال صفة موقع الويب أو عناوين البريد الإلكتروني لكيانات جديرة بالثقة (مصارف على سبيل المثال) مع القصد الجنائي الرامي للحصول على معلومات حساسة مثل كلمات المرور، أو أسماء أو تفاصيل بطاقة ائتمان. إذ يمكن تثبيت برمجيات ضارة على الحاسوب الذي سيوجه المستخدم إلى موقع ويب للتصيد الاحتيالي بدلاً من الموقع المقصود الموثوق به. أو يمكن إرسال رسائل اقتحامية بعناوين منتَحلة تدعو المستخدم للنقر على وصلة إلى موقع تصيد احتيالي. وقد اكتشفت التقارير زهاء 55 000 موقع يستضيف التصيد الاحتيالي في عام 2008، بزيادة قدرها 66 في المائة مقارنة بعام 2007.

4 ويجري إنشاء الحواسيب المسيرة وشبكات الحواسيب المسيّرة باستخدام حواسيب العديد من المستخدمين دون علمهم. وهي إما تُستخدم مباشرةً أو "تُستأجر" من السوق السوداء للاستخدام الجنائي. وقد وجدت شركة سيمانتيك حوالي 75 000 حاسوب مصاب ببرمجية التسيير في اليوم الواحد، و15 197 أمر تسيير ومخدّم تحكم في التسيير متميز وجديد. وتوفر مخدمات الاقتصاد السري سوقاً سوداءَ تُتداول فيها معلومات مسروقة (عن بطاقات الائتمان، والهويات وغير ذلك) وتباع فيها أو تؤجَر البرمجيات الضارة أو شبكات الحواسيب المسيّرة.

ورغم ما يقال عموماً عن أن معظم مصادر الهجوم تقع في الولايات المتحدة تليها البرازيل والصين، فإن أي شخص يمكنه شن هجمات في أي وقت وحتى من مواقع نائية. وعلى الرغم من أن هجوم كونفيكر (Conficker)، القائم على نقطة ضعف اليوم صفر، ما زال حياً في ذاكرتنا، يمكن الاستنتاج بحذر أن عدد نقاط الضعف اليوم صفر الخطيرة آخذ في التناقص بسبب الاهتمام المتزايد بأمن أنظمة التشغيل والتطبيقات من جانب شركات البرمجيات الكبيرة.

وينصب تركيز النوايا الإجرامية على القطاع المالي الذي يستقطب أكثر من 70 في المائة من التصيد الاحتيالي، ويأتي مقدمو خدمات الإنترنت في المرتبة الثانية بنسبة 11 في المائة فقط.

إن *الكتاب الأبيض* الذي وضعه اتحاد FORWARD بعنوان *التهديدات الناشئة في تكنولوجيا المعلومات والاتصالات*[78] حاول أن يستكشف التهديدات الناشئة والمستقبلية بطريقة منهجية. فعرّف أربعة محاور للتطورات المستقبلية المرتقبة وللتطورات المتكشفة حالياً: *التكنولوجيات الجديدة والتطبيقات الجديدة ونماذج الأعمال الجديدة والدينامية الاجتماعية الجديدة*.

وحدد 28 تهديداً مصنفاً في ثماني فئات:

1 *الربط الشبكي*: التهديدات المتعلقة بإدخال ونشر تكنولوجيات الشبكة الجديدة وبخدمات البنية التحتية (التسيير، نظام أسماء الميادين (DNS)) على شبكة الإنترنت.

2 *العتاد والافتراضية*: التهديدات الناجمة عن التطورات الجديدة في العتاد والبرمجيات والمتصلة بالحوسبة الافتراضية والسحابية.

3 *الأجهزة الضعيفة*: التهديدات المتأتية من أجهزة الحوسبة الجديدة المحدودة من حيث الحوسبة والقيود المفروضة على القدرة على حد سواء.

4 *التعقيد*: التهديدات التي تنشأ بسبب تعقيد الأنظمة المستقبلية ونطاقها، والتي تؤدي إلى تفاعلات ترابطية غير متوقعة وغير مقصودة، وإلى مضاعفات أمنية.

5 *التلاعب بالبيانات*: التهديدات التي تنبع من واقع أن الناس (والأنظمة) تخزن المزيد من البيانات على الخط، وأن قيمة هذه البيانات وحساسيتها تتزايدان.

6 *البنى التحتية للهجوم*: التهديدات المتصلة بواقع أن الخصوم يعكفون على تطوير ونشر منصات الهجوم (مثل شبكات الحواسيب المسيرة). وأنهم لم يعودوا إلى الاكتفاء بتنفيذ هجمات الكر والفر، بل أسسوا لأنفسهم قواعد تشغيلية على شبكة الإنترنت لشن حملات خبيثة.

7 *العوامل البشرية*: تهديدات تعود إلى هجمات من الداخل، ولا سيما في سياق الاستعانة بمصادر خارجية؛ والتهديدات المتعلقة بهجمات على الهندسة الاجتماعية الجديدة.

8 *عدم كفاية المتطلبات الأمنية*: التهديدات المتعلقة بالأنظمة التجارية التقليدية والجاهزة التي لم تُزوَد بما يكفي من الحماية والتي تُستخدم الآن وتُنشر في سيناريوهات لا تفي فيه آليات حمايتها بالغرض.

ويسمح هذا التصنيف بتحديد أولويات ما يلزم من الجهود الإضافية (البحوث) لتخفيف التهديدات، مع مراعاة الشدة والاحتمالات المتوقعة والجهود القائمة. وخلص الكتاب الأبيض إلى أن الأولوية القصوى تتمثل في مواجهة التهديدات المتعلقة بما يلي: *التوازي، والنطاق، وهياكل دعم الاقتصاد السري، والبرمجيات الضارة التي تطال الأجهزة المتنقلة، والشبكات الاجتماعية*.

---

[78] "الكتاب الأبيض لاتحاد FORWARD عن التهديدات الناشئة لتكنولوجيا المعلومات والاتصالات"، www.ict-forward.eu/whitebook/.

ومن الواضح أن الحالة الراهنة للتهديدات تدعو إلى القلق وتستلزم إجراءات عاجلة منسقة على الصعيد العالمي من قبل خبراء في مختلف التخصصات، فضلاً عن السياسيين والدبلوماسيين. وفي حين أن بعض هذه التهديدات تتطلب في المقام الأول بذل جهود في سبيل تطوير أو تحسين لوائح الأمن أو معاييره أو تقنياته أو أدواته، فإن البعض الآخر منها بحاجة ماسة لجهود البحث العلمي الأساسية ولحلول تُنفَّذ عملياً.

الاستنتاجات

إن البحوث المستقبلية والمنتجات المطورة في تكنولوجيا المعلومات والاتصالات سوف تؤثر تأثيراً كبيراً على السلوك الفردي والاجتماعي والثقافي في جميع أنحاء العالم، في الحياة الخاصة والعامة. وقد أصبحت الثورة الجارية في الأنظمة الرقمية والإنترنت، وفي خدماتها وتطبيقاتها، موارد أساسية للحياة اليومية. ويوفر هذا العالم الرقمي الكثير من الفوائد والفرص للإنسانية وللتقدم التقني، فضلاً عن سبل جديدة للتغلب على بعض المشاكل العالمية مثل الطاقة أو الرعاية الصحية. ويتناول هذا الفصل الفرص والمزايا الأساسية لتكنولوجيات المعلومات والاتصالات وتطبيقاتها في المستقبل.

ورغم هذه الجوانب الإيجابية، تعالَج مشاكل أصعب وأحدث عهداً تتطلب المزيد من البحوث الأساسية الحثيثة والحلول المناسبة: إذ تطالعنا المشكلة الأساسية في الافتقار إلى طرائق التصميم والتحليل المثبتة علمياً في قدرتها على السيطرة على التعقيد الهائل للأنظمة الرقمية المستقبلية الموصولة بينياً، وخصوصاً فيما يتعلق بالسلامة والموثوقية والأداء الوظيفي والأمن (الخصوصية والأصالة ، وأمن البيانات). فوضع الحلول لهذه المشكلة الأساسية هو أحد أهم التحديات التي تواجه علم الحاسوب ودوائر بحوث علم الويب. ولعل من الخطوات المفيدة جداً في هذا الصدد، التوزيع العالمي "لقائمة المشاكل الصعبة"، كتلك التي أعدها الاتحاد العالمي للعلماء، مشفوعةً بتدابير مضادة ناجعة إن وجدت.

غير أن "فجوة السيطرة" هذه لا تتعلق بتقنيات التصميم والإنتاج الحالية فحسب. فلا مناص من الأخذ في الحسبان دوماً تبعات الأخطاء البشرية أو العيوب التقنية أو الأعطال أو إساءة الاستخدام والتلاعب، ووضع التدابير المضادة وتطبيقها إلى أقصى حد ممكن فيما يتعلق بقيود معينة.

وبالإضافة إلى ذلك، تغيب التدابير الكافية لتوعية المستخدمين والمستهلكين والمؤسسات بأهم المشاكل أو المخاطر أو حتى التهديدات لدى استخدام موارد تكنولوجيا المعلومات والاتصالات. فينبغي إشراك المهنيين في وضع مواد إعلامية بشأن قضايا أمن تكنولوجيا المعلومات تخاطب مجموعات مختلفة من الجمهور. وكما جاء في الفصل الثاني، فإن المجتمعات الحديثة تعتمد على تكنولوجيا المعلومات والاتصالات وشبكة الإنترنت الآخذة في التطور. ولذلك، فإن النتائج المترتبة على التطورات التكنولوجية في المستقبل نحو عالم مرقمن يتعين تحليلها بعناية والإخبار عنها من أجل بناء الثقة.

2.4 الرقابة الحكومية على الإنترنت: قمع سيبراني

بقلم هينينج فيجنر

إن حرية التعبير عن الرأي وحرية النفاذ إلى المعلومات هما في صميم مجتمع معلومات يؤدي مهامه وهما من العناصر الأساسية للاستقرار السيبراني والسلام السيبراني على النحو المحدد في الفصل السادس من كتاب "مفهوم السلام السيبراني" بقلم المؤلف نفسه. والتهديدات التي تطاول ممارستهما، تقوض الفوائد الرئيسية للإنترنت وتحرم الناس منها. ومن ثم، يتعين تصنيفها في عداد التهديدات الرئيسية الحالية في الفضاء السيبراني[79].

وقد كانت حرية الرأي وحرية الوصول إلى المعلومات على مر التاريخ عناصر أساسية في بناء المجتمعات المتحضرة. وهي جزء لا غنى عنه من حقوق الإنسان والحريات المدنية، وبالتالي فهي تكاد تكون في صلب الدساتير الحديثة كلها. والواقع أن حرية الفرد في الحصول على المعلومات وفي تبني آراء والإدلاء بها يمكن أن تكون مقياساً للتقدم البشري. ومن ناحية أخرى، فإن تعريف الحدود التي يجب أن تقيد هذه الحرية لأسباب تتعلق بالأمن العام والآداب العامة *والنظام العام* ظل دائماً جزءاً لا يتجزأ من النقاش السياسي الداخلي وجهداً دائماً وضرورياً في السعي للتوفيق بين الحرية الفردية والمصلحة العامة على السواء وترشيدهما.

والرقابة الحكومية من حيث تجاوز هذه الحدود بصورة منهجية وممارسة رقابة لصيقة على الرأي العام وتبادل وجهات النظر، ولا سيما فيما يتعلق بالمواد المطبوعة، هو جزء مؤلم ولكنه متكرر من التاريخ البشري، وقد أطلق، غير مرة، شرارة معارك حرية العقل.

وفي عصر الانترنت، لم تتغير هذه الكوكبة الأساسية، سوى أن أهميتها والشكل الذي تتخذه تغيّرا حقاً. فالتكنولوجيات الرقمية أطلقت العنان لفرص النفاذ إلى المعلومات ولفرص الاتصالات وأعطتها بعداً جديداً. وهذا هو جوهر مجتمع المعلومات الذي حل علينا الآن. وكحال كل جانب من الجوانب أخرى، فشبكة الإنترنت توسع الرحاب، وتفند المقاييس الكمية والنوعية، وتلغي المسافة والوقت، وتستحدث ظواهر جديدة متناقضة.

---

[79] سبق للاتحاد العالمي للعلماء أن تعامل مع هذه المشكلة في مساهمته المقدمة إلى القمة العالمية لمجتمع المعلومات في مرحلة تونس عام 2005 بعنوان :"أمن المعلومات في سياق الفجوة الرقمية"، وتحديداً في التوصية 5 الواردة في المساهمة بعنوان"منع النفاذ إلى معلومات من خلال اصطفاء الإنترنت"، الصفحة 12، والتعليقات التوضيحية في الصفحات 24-30، www.itu.int/wsis/docs.2/tunis/contributions/co1.pdf، وwww.unbiw.de/infosecur. انظر أيضاً، أسوةً بالفصل الحالي، "القمع السيبراني: تأطيرالمشكلة. تقييم حالة السجال والتفكير في استراتيجيات مضادة" بقلم هينينغ فيجنر في منشور بعنوان الحقوق والمسؤوليات في الفضاء السيبراني، موازنة الحاجة للأمن والحرية، 2010، معهد الشرق والغرب، والاتحاد العالمي للعلماء، www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty.

فالإنترنت لا تكتفي بزيادة المعلومات وتسهيل النفاذ إليها على نطاق هائل، بل تزيد أيضاً من إمكانية التدخل في العمليات التقنية الأساسية ومعالجة المحتويات الرقمية. وتتيح التكنولوجيا الرقمية برمجيات اصطفاء تستطيع سد أي مجال معلومات عبر شبكة الإنترنت بأسرها أو فيما يتعلق بمخدمات معينة فقط، فتسمح للحكومات بإدخال الرقابة الحكومية، بما في ذلك الرقابة على نطاق واسع. وبالتالي يجب النظر مجدداً في قضية حرية الرأي والمعلومات كحق من حقوق الإنسان: فالإنترنت تتحول سريعاً إلى معترك جديد في النضال من أجل حقوق الإنسان وحرية الرأي.

والتقنيات الرئيسية المتاحة للحكومات الممارسة للرقابة هي حظر بروتوكول الإنترنت واصطفاء نظام أسماء الميادين وإعادة التوجيه واصطفاء محدد موقع الموارد الموحد (URL) من خلال المسح بحثاً عن كلمات رئيسية مستهدفة أو اصطفاء الرزم التي تنهي إرسال رزم بروتوكول TCP حال الكشف عن كلمات رئيسية مثيرة للجدل. وتتميز برمجيات الاصطفاء الحالية بتفاعلها المكانيكي حصراً مع وقوع بعض الكلمات أو العبارات، وبالتالي كثيراً ما تفرط في استهداف الهدف ("الإفراط في الحجب").

وهناك حشد من الموردين الصناعيين لبرمجيات الاصطفاء التي تستخدم هذه التقنيات وغيرها. ومن بينهم معظم الأسماء الكبيرة في تكنولوجيا المعلومات، ولكن أيضاً شركات متخصصة. وتتعدد صفحات الويب المخصصة للتقييم المقارن لهذه البرمجيات وتصنيفها من حيث الكفاءة. في حين أن صفحات أخرى يديرها دعاة الحرية الكاملة في التعبير في الانترنت تنتقد مجرد ظهور هذه التكنولوجيا.

ويتعين النظر في تكنولوجيا الاصطفاء جنباً إلى جنب مع خيارات التحايل على الاصطفاء. فالحذق نفسه الذي اتسم به تطوير المراشيح يميز أيضاً التقنيات التي صممت لتجنب المراشيح أو التحايل عليها أو إعطابها. فمن الصعب جداً بل من المستحيل فرض رقابة كاملة على المعلومات في شبكة الإنترنت بسبب التكنولوجيا الأساسية الموزعة للشبكة. وبالتالي هناك عدد من الموارد والحلول التي تسمح للمستخدمين بتجاوز الرقابة على الإنترنت. ويعتمد جلّها على النفاذ إلى وصلة الإنترنت غير الخاضعة للاصطفاء، غالباً في ولاية قضائية مختلفة لا تخضع لقوانين الرقابة نفسها. والتحدي الواضح الذي يواجه ممارسي الرقابة الحكومية على الإنترنت هو إمكانية النفاذ إلى المادة المراقبة طالما أن هناك نظاماً واحداً غير خاضع للرقابة في العالم يمكن للعموم النفاذ إليه. والتقنيات المتاحة لهذا النفاذ المنسلّ تشمل استخدام مخدمات وكيلة وإنشاء الشبكات الخاصة الافتراضية وتحميل برمجيات المصدر المفتوح التي تتيح التصفح والدردشة ونقل الملفات مع إغفال الهوية (ومن الأمثلة على ذلك برمجيات Psiphon وI2P وTor).

ولا ريب أن اصطفاء المحتوى يؤدي وظيفة هامة في الحماية الاجتماعية. فحجب الصفحات التي تحوي الصور الإباحية للأطفال والتحريض على العنف والكراهية العنصرية والجريمة بصفة عامة يبدو أمراً مشروعاً لأي كان. ويصح الشيء نفسه على الاستخدام المتزايد للإنترنت من قبل الإرهاب على الصعيدين الوطني والدولي. فالمحتوى الذي يتعذر نشره قانونياً خارج الإنترنت يجب أن يخضع للعقوبات القانونية والمنع ضمن الشبكة أيضاً. وفي هذا الصدد، تلبي صناعة برمجيات الاصطفاء حاجة مشروعة.

ولكن ثمة فارق مهم تجب الإشارة إليه.

مهما كانت كفاءة المراشيح، وبالتالي أثر الرقابة، ومهما كانت المصالح التجارية المعنية، فالواقع الحاسم هو أنه في المجتمعات "الحرة"، أي في ما يسمى الديمقراطيات الغربية أساساً – وليس حصراً البتة – المتوافقة بدرجة عالية حول القيم، ، تنظم بوضوح القيود المفروضة على حرية التعبير والنفاذ إلى المعلومات من خلال القانون، ويخضع نطاقها لقاعدة الكفاية والتناسب، ويمكن تقييمها وفق إجراءات مراجعة قانونية في متناول الجمهور. فوجود إطار قانوني واضح وتوافر ضوابط قانونية مستقلة يشكلان في الواقع المعايير الحاسمة لتمييز التحكم المشروع في المحتوى عن الرقابة غير المشروعة. ويوفران أيضاً وسيلة لاستيعاب الاختلافات في القيم الثقافية وفي تعاريف الخصوصية. فالمحتوى المسيء للثقافة والدين والأخلاق وغيرها من المعتقدات الجماعية العميقة الجذور في بعض البلدان لا ينبغي أن يعفى من الرقابة تحت راية الحرية المطلقة للإنترنت، وينبغي لأولئك الذين يشجبون الرقابة الحكومية السياسية على وجه حق أن يتوخوا الحذر في الانحياز لهذا الجانب أو ذاك في مثل هذه القضايا.

وبما أن مسائل الاصطفاء الحكومي للإنترنت والحدود التي ينبغي مراعاتها في تقييد حرية التعبير والتوازنات التي يتعين إقامتها ودور صناعة تكنولوجيا المعلومات في توفير المرتكزات التقنية لمراقبة الإنترنت، تلامس جميعها موضوعات السيادة الوطنية الحساسة، فإن هذه المقالة تتحاشى إلقاء اللوم أو المسؤولية على أي حكومة بعينها. وفي الواقع، لا يُذكر أي بلد بالاسم. وبالمثل، لا يرد اسم أي عتاد أو برمجيات أو مقدم خدمات في تكنولوجيا المعلومات. والحال أن الغرض من هذه المقالة هو تأطير المشكلة وتقييم حالة النقاش الدائر، وليس التسرع في الاستنتاجات. وبالروح المنضبطة نفسها، ترد شواهد من صفحات الويب أو مقالات كمراجع فقط، وهي لا تعني أن هذه المقالة تقر محتوياتها أو تؤيدها.

ونظراً إلى طبيعة الإنترنت التي لا تحدها حدود، لا تكفي القواعد الوطنية لإدارة حرية الإنترنت. وهكذا، وضع الاتحاد الأوروبي نظاماً أولياً منذ عام 1999 على نطاق الاتحاد برمته لتنظيم الحريات المقبولة لمحتويات الإنترنت والإجراءات ذات الصلة ("برنامج إنترنت أكثر أماناً"). وهو يعتمد أساساً على مبدأ التنظيم الذاتي من جانب صناعة الإنترنت وعلى آلات البحث لاستبعاد المحتويات غير القانونية أو المضرة ولضمان توافقها مع التشريعات الوطنية. وفي بعض المجالات، يعمل التنظيم الذاتي بصورة مرضية، رغم ما يتطلبه أحياناً من تشريعات تكميلية.

وعلى الصعيد العالمي، تحدَد المعايير القانونية الدولية على وجه الخصوص بمعاهدتين عظيمتين من معاهدات حقوق الإنسان ترقيان إلى بواكير سنين الأمم المتحدة وهما: الإعلان العالمي لحقوق الإنسان *(1948)* و*العهد الدولي الخاص بالحقوق السياسية والمدنية* لعام 1966. وقد وقعت جميع الأمم عملياً وصادقت على هاتين المعاهدتين اللتين تعتبران الآن القانون الدولي العرفي مما يلزم الدول غير الموقعة بهما أيضاً. ويصادف في كلتا الوثيقتين أنه في المادة 19 يُعترف بمبدأ حرية التعبير والرأي الذي يتضمن حق أي شخص في تلقي ونقل المعلومات بجميع أنواعها ودونما اعتبار للحدود وبأي وسيلة يختارها. وما من شك في أن ذلك يشمل أيضاً تلقي المعلومات من خلال شبكة الإنترنت والحق في النفاذ إليها (بقدر حق الناس بمنع النفاذ إليهم). وبالتالي

فإن (القمة العالمية لمجتمع المعلومات لعامي 2003 و2005) أكدت هذه المبادئ رسمياً بوصفها ركناً أساسياً لا غنى عنه من أركان مجتمع المعلومات، وتحديداً في *إعلان مبادئ جنيف* (المبادئ 4 و5 و55). ومن الجدير بالذكر أن نص القمة يشدد على جانب الحرية، ويخفف من وقع التحذيرات المضافة في العهد الدولي الخاص.

والأمر الذي يتلخص في مشكلة – صعبة باعتراف الجميع – في المجتمعات "الحرة" بشأن التوازن السياسي الدائم بين الحرية وتدخل الدولة في إطار معايير قانونية واضحة، يصبح في العديد من الدول الأخرى مشكلة حقوق الإنسان ومشكلة جودة نظام المعلومات العالمي. فالرقابة الحكومية على الإنترنت عبر تقنيات الاصطفاء دون قيود قانونية وبعواقب وخيمة قطعية على الفرد الساعي لنقل المعلومات، تشكل انتهاكاً لحقوق الإنسان ذا بعد بالغ الأهمية. وعنصر الإشكالية في هذا التطور لا يكمن في أن شركات التكنولوجيا الغربية توفر تكنولوجيتها الاصطفائية للحكومات ذات النزعة الرقابية فحسب، بل تتعاون أيضاً في مجال استخدامها مؤسسةً بالتالي أنظمة رقابة تتميز بالفعالية والكفاءة. وهذه الظاهرة أمر أساسي لهذا التحليل الذي يهدف أيضاً إلى اقتراح سبل ممكنة للعمل الدولي لمكافحة هذه الممارسات. وعلى ما ذهب إليه جو غلانفيل، محرر منظمة "مؤشر الرقابة[80]": "الرقابة الآن، للمرة الأولى في تاريخها، هي مؤسسة تجارية"[81].

ويُكتب ذلك في وقت تلاحَظ فيه عملية نمو حرجة في عدد الحكومات التي تمارس الرقابة على الإنترنت، ومعظمها على حساب الحقوق السياسية والحريات، وفي إتقان أساليب الاصطفاء على حد سواء.

وتقوم العديد من المؤسسات الخاصة بمراقبة حالة الرقابة الحكومية على الإنترنت وتطورها. ومن هذه المؤسسات مبادرة الشبكة المفتوحة الطليعية، ومراسلون بلا حدود، وغالباً ما تستخدمان بيانات وتصنيفات متطابقة أو متشابهة، وتقرير الرقابة على الإنترنت[82].

وتُجمع هذه المصادر على أن عملية نمو الرقابة ذات أبعاد مذهلة. فاستناداً إلى قوائمهم وأرقامهم القطرية، يستنتجون أن 1,72 مليار شخص يتعرض للرقابة على الإنترنت، أي ما نسبته 25,3 في المائة من سكان العالم الحاليين.

---

[80] مؤشر الرقابة هي منظمة بريطانية مرموقة تدعو إلى حرية التعبير، http://www.indexoncensorship.org.

[81] جو غلانفيل، "مصلحة الأعمال الكبيرة في مراقبة الشبكة"، صحيفة الغارديان، 17 نوفمبر 2008. www.guardian.co.uk/commentisfree/2008/nov/17/censorship-internet

[82] مبادرة الشبكة المفتوحة، http://www.opennet.net. يستخدم المشروع شبكة دولية من المحققين لتحديد مدى وطبيعة برامج اصطفاء الإنترنت التي تديرها الحكومة. وتشمل المؤسسات الأكاديمية المشاركة مركز الدراسات الدولية في كلية مونك في جامعة تورنتو للشؤون العالمية، ومركز بيركمان للإنترنت والمجتمع في كلية الحقوق بجامعة هارفارد، ومعهد أوكسفورد للإنترنت في جامعة أكسفورد، ومجموعة SecDev التي تولت مهام مجموعة أبحاث الشبكة المتقدمة في برنامج أمن كامبريدج في جامعة كامبردج. انظر أيضاً www.chillingeffects.org للاطلاع على مجموعة أكبر من المؤسسات الأكاديمية الداعمة التي "ترصد المناخ القانوني لنشاط الإنترنت".

وتطول قائمة الدول التي تلجأ لهذه الممارسات. فلا أقل من 25 وربما أكثر من 30 من الحكومات تحرم مواطنيها جدياً من إمكانية النفاذ إلى مجموعة كاملة من المعلومات المتاحة على الإنترنت. وترد في الإنترنت عدة قوائم بالمنظمات التي تراقب هذه البلدان. وتصنف مبادرة الشبكة المفتوحة ممارسات الرقابة الحكومية ضمن الفئات المتفشية والكبيرة والاسمية وغير المباشرة، ولديها أيضاً فئة قائمة البلدان تحت المراقبة. أما منظمة مراسلون بلا حدود فلديها قائمة الثلاثة عشر من ألد "أعداء الإنترنت". ويتركز تدخل السواد الأعظم من البلدان المراقَبة على حظر المحتوى السياسي الذي لا يسمح به نظامها الحكومي، من ديمقراطية وانتخابات حرة وسبل الانتصاف القانونية وتقارير حول الأحداث السياسية الحساسة، ولكن العديد منها يذهب إلى أبعد من ذلك. فينصب تركيز بعض الحكومات على وضع ضوابط للمواضيع الأخلاقية وللنظام الأخلاقي والثقافي في موروثها. ويتفاوت التشدد والتدقيق في هذه الضوابط. فالرقيب في بعض البلدان يحجب صفحات ثم يحول النداء إلى صفحة توضيحية تتيح النفاذ إذا تبين وجود اهتمام خاص "مشروع" في المعلومات المحجوبة على نحو يقدم درجة معينة من الشفافية. وفي بلدان أخرى، تُمارس الرقابة بشكل متقطع وغير فعال ولا تطبَّق العقوبات في حالة انتهاك الحظر.

ولكن كقاعدة عامة، تمارَس الرقابة الحكومية دون حدود على شريحة واسعة من المعرفة الإنسانية دون أي تفسير أو تبرير منطقي، حتى من جانب بعض البلدان المحترمة تماماً، بخلاف ذلك. وكلما ابتعدنا عن البلدان الديمقراطية على النمط الغربي، ارتفع معدل الرقابة من خلال اصطفاء الإنترنت. فتغالي بعض الدول في الإشراف على سكانها إذ تشط في الرقابة على الإنترنت وتعاقب من يُضبط متلبساً بالنفاذ إلى صفحات محظورة من مستخدمي الانترنت، وفي بعض البلدان يلاحَق هؤلاء من قبل شرطة سيبرانية تحجمية. وعدد المستخدمين الذين أودعوا السجن، بقدر ما هو معروف، يبعث على القلق من أي وجهة نظر. ويتعين على بعض الشركات الدولية لتكنولوجيا المعلومات التي توفر البرمجيات أن تتعايش مع شبهة مساعدتها ودعمها لمثل تدابير الملاحقة القضائية هذه. فهي بالتالي تساهم في المعاناة البشرية الناجمة عن ذلك.

إن عواقب الرقابة الشاملة خطيرة، ولا يمكن المبالغة في تقديرها. فلا تُنتقص حقوق المواطنين بموجب القانون الدولي فحسب، بل إنهم يُحرمون من فوائد هامة في عصر المعلومات ويتلقون نظرة مشوهة للواقع العالمي وتتقلص مشاركتهم في إثراء عمليات الاتصال العالمية. فالاصطفاء واسع النطاق للإنترنت يمكن أن يغير الحالة الذهنية الجمعية لأمة. وعلى المرء أن يأخذ في الاعتبار أيضاً التأثير السلبي المزدوج لهذه الرقابة: حرمان المواطنين من معلومات ومن نظرة متبصرة إلى العالم، ولكن الرقابة هي أيضاً أداة للقمع السياسي والحد من حرية العمل.

إن هذا الوضع وسجل الرقابة على الإنترنت الذي يزداد سوءاً على سوء يستدعي إجراءات عاجلة. وقد أدرك الاتحاد الأوروبي ذلك من جانبه، واتخذ إجراءات. وهو يرفض أن تقوم شركات تكنولوجيا المعلومات بمساعدة الحكومات القمعية في ترسيخ طغيانها على العقول. ونحن مدينون أيضاً للاتحاد الأوروبي الذي صاغ مصطلحاً مناسباً جداً في وصف هذه الممارسات، ألا وهو "القمع السيبراني".

ولا ينفرد الاتحاد الأوروبي في ذلك، بل إن لوبي الإنترنت الدولي الذي يكافح من أجل حرية المعلومات وسلامة الانترنت في العالم نشيط ويقظ، حتى أكثر من العديد من المؤسسات البارزة التي سبق ذكرها والتي تراقب تطور القمع السيبراني وتندد به علناً.

ونظراً لقدرة مستخدمي الإنترنت المتمرسين على تجنب المراشيح أو التحايل عليها، انبرى العديد من المدافعين عن حرية الإنترنت الدولية في تزويد المواطنين في البلدان الخاضعة للرقابة ببرمجيات مضادة مقابلة كتلك المبينة أعلاه. فقد تطورت هذه التكنولوجيات المضادة للمرشاح لتصبح صناعة حقيقية تساعد على التقليل من فعالية الرقابة الحكومية دون أن تتمكن من التخلص منها تماماً. وتنشط مبادرة الشبكة المفتوحة، شأنها شأن المبادرات الأخرى، في هذا المجال فتورد أنظمة ذات فعالية معينة (مثل Psiphon) صممت للسماح للحاسوب المنزلي العادي بالعمل كمخدم وكيل شخصي مجفر وتخطي "الجدران النارية" الإلزامية التي وضعتها الحكومة للتنقل بحرية في الشبكة العالمية. ومع ذلك، فإن تطبيق هذا الجهاز وغيره من أجهزة أخرى مشابهة يحارَب بنشاط من قبل موردي مراشيح معينين. وهذا يدل مرة أخرى على الطبيعة الإشكالية للأنشطة التجارية للصناعات المتعددة الجنسيات التي تسهل القمع السيبراني في الواقع أو تساعده، عمداً أو كأضرار جانبية غير مرغوب فيها. ومن الواضح أنه يتعين إضافة الدول المتقدمة في التكنولوجيا الرقمية القادرة على تطوير مراشيح محلياً، والكثير منها يقوم بذلك بالفعل، مما ينأى بموردي البرمجيات الأجانب عن اللوم.

وكما جرى التأكيد آنفاً، لا يرمي هذا المقال لعرض تحليل مفصل عن كل بلد على حدة، لأن الانترنت توفر معلومات وافية بهذا الغرض. ولكن السؤال الذي يُطرح جراء الوصف الموجز الوارد هنا وبوادر المناقشة العلنية: كيف يمكن تلبية الحاجة الواضحة للعمل، وماذا يمكن للمجتمع الدولي القيام به لمواجهة القمع السيبراني باعتباره انتهاكاً مستمراً للقانون الدولي.

فالمشاكل القانونية والسياسية التي ينطوي عليها تحديد الحدود مقبولة دولياً لاصطفاء الإنترنت وللعقوبات المحتملة هي مشاكل واضحة وضخمة. ذلك أن مسائل الولاية والسيادة الوطنية وشبه استحالة وضع حدود فاصلة، تصلح على نطاق واسع، بين الحريات المدنية والمصالح العامة المرجَّحة، ومسائل اختيار القانون ووسائل الإنفاذ، والقضية الأوسع المتمثلة بإدارة الإنترنت، في جملة أمور، تجعل من محاولة وضع مدونة دولية في هذا الشأن غير ذات جدوى وعقيمة على الأرجح. وهناك أيضاً مسألة التنوع الثقافي واحترام الآخرين له. فلا يمكن توحيد تعريف *النظام العام* الثقافي والديني في جميع البلدان، رغم أنه يمكننا أن نفترض وجود تراث عالمي من القناعات الأساسية المشتركة ورغم أن الإعلان العالمي والعهدين يجب أن يُعتبروا ملزمين عالمياً. وكدأب القانون الدولي غالباً، لا توجد تعاريف سهلة ولا عقوبات تأتي أُكُلها على وجه السرعة.

إذن، لا بد من النظر إلى أي إصلاح لاصطفاء شبكة الإنترنت العالمية *بدلالة العملية الجارية والاستراتيجيات على مر الزمن*. وينبغي للمرء التفكير في الإجراءات التي تستنهض الضمير العالمي وتولد وعياً وضغطاً عاماً، وبالنسبة إلى حكومات البلدان المتضررة، تحدياً للرأي العام ودافعاً لتقديم مبررات تفصيلية.

وتقع مسؤولية مهمة على عاتق الحكومات الوطنية ودوائر الصناعة ومؤسسات المجتمع المدني بالنظر إلى قدراتها على تشكيل الآراء. إذ يمكن للحكومات أن تروج لتطوير وتوافر التكنولوجيات المضادة للمرشاح، وأن تُخضع صادرات تكنولوجيا المرشاح لضوابط التصدير المناسبة، وأن تستخدم الوسائل الدبلوماسية الوطنية لممارسة الضغط على الحكومات الممارسة للرقابة كي تكشف النقاب عن سياساتها التقييدية وتبررها توخياً للشفافية.

وتتحمل أوساط صناعة تكنولوجيا المعلومات – منتجي البرمجيات والشركات التي تقدم خدمات الإنترنت وجمعياتها – مسؤوليات واضحة، وينبغي أن نعتمد مدونات قواعد السلوك التي من شأنها أن تستبعد استخدام تكنولوجياتها من أجل الرقابة السياسية. وفيما تتعذر واقعياً مطالبة الشركات أن تنحي مصالح أرباحها جانباً بصورة تامة، وفي حين أنه من الحماقة إلقاء اللوم الرئيسي للرقابة الحكومية على الوسط الصناعي، فإن العمل الجماعي الطوعي من قبل الشركات يصب في خانة السمعة وسيعزز صوراً إيجابية. وقد أعطت سياسة التنظيم الذاتي، التي توفر معايير مشتركة واضحة، نتائج جيدة في الاتحاد الأوروبي، ويمكنها أيضاً تعزيز قوة مقاومة فرادى الشركات لتصمد في وجه الضغط من الحكومات ذات النزعة الرقابية الحريصة على القيام بأعمال تجارية معها. ومثال ذلك، مبادرة الشبكة العالمية وهي جهد طوعي من قبل الشركات التكنولوجية في الولايات المتحدة الأمريكية ينص على هذه المعايير ("ميثاق الإدارة") ويتفاعل مع طلبات الحكومة بشأن الرقابة ويدعو لحرية الإنترنت[83].

والمؤسسات الأكاديمية ومنظمات حقوق الإنسان التي تشجب القمع السيبراني بلا كلل – وقد وردت أسماء العديد منها أعلاه، تحظى الآن بتشجيع ودعم متزايد من الحكومات التي تتبنى قضيتها. ولكن نظراً للطبيعة الدولية العابرة للحدود للإنترنت، ولصلة القمع السيبراني بحقوق الإنسان العالمية، لعل المهمة الأهم تتمثل في وضع هذه المسألة على جدول أعمال المنظمات الدولية بطريقة جديدة وكبيرة.

وقد تخطى الخطوة الأولى في التوصل إلى تفاهم دولي أوسع بشأن التنمية والمرتكز التقني للاصطفاء الحالي للإنترنت، وفي إنشاء آلية مراقبة دولية.

وفي الخطوة الثانية، يمكن التفكير في إدخال إجراء لتقديم شكوى دولية، على أن يكون إجراءً متاحاً على نطاق واسع لجميع الأطراف المعنية ويتبع عدداً من معايير التقارير الملخصة.

فأي منظمة أو هيئة دولية يمكن أن تُسخَّر لخدمة هذا النضال؟

في المقام الأول، يمكن للمرء التفكير في منتدى إدارة الإنترنت الذي أنشئ عام 2006 تنفيذاً لمقررات القمة العالمية لمجتمع المعلومات ("جدول أعمال تونس"). فالقيود المفروضة على أداء الشبكة وإدارتها من جانب الرقابة السياسية على الإنترنت تتصل جلياً بالمهمة المنوطة بالمنتدى ويمكن أن تندرج بسهولة في إطار ولايته

---

[83] مبادرة الشبكة العالمية، www.globalnetworkinitiative.org.

(المادة 72 أ) وب) وهـ) وك) من برنامج عمل تونس)، حتى وإن لم يرد ذكر مشكلة القمع السيبراني حرفياً في هذه النصوص. ويؤسف أن منتدى إدارة الإنترنت في السنوات الخمس من وجوده، اقتصر على إجراء مناقشات غنية ومفيدة على نحو لا يمكن إنكاره، بما في ذلك بشأن حرية الإنترنت، ولكن لم تبدأ الأنشطة التنفيذية. فمن الوارد والمستحسن وضع إجراء مراقبة يمكن بموجبه متابعة ممارسات المرشاح وتحليلها وتقييمها نقدياً في إطار اختصاصات المنتدى إذا ما وُسعت ولايته كما يبدو مرجحاً[84]. (وعلى النقيض من ذلك، فإن المنتدى السنوي للقمة العالمية لمجتمع المعلومات هو منتدى للنقاش المفتوح بدون تكليف تنفيذي ولن يكون مناسباً بالقدر نفسه لهذا الغرض) .

وتفاخر اليونسكو في الإعلان عن نفسها وصياً دولياً فريداً على حرية المعلومات بموجب قانونها التأسيسي، وقد عهدت إليها القمة العالمية لمجتمع المعلومات بمهام واضحة تحت عناوين "النفاذ إلى المعلومات والمعرفة" و"البعد الأخلاقي للإنترنت". وقد اعتمدت اليونسكو إعلانات وتوصيات تلزم الدول الأعضاء والمنظمات الدولية بحرية النفاذ إلى شبكة الإنترنت دون عراقيل[85]، و لايكف مديرها العام عن التنديد علناً بالانتهاكات التي تنال من حرية الإعلام والصحافة. وليس هناك ما هو منطقي أكثر من الشروع في تنفيذ هذه المهام وبالحوار، ونتيجةً لذلك، القيام بفحص دوري لممارسات الرقابة.

وإذ نتعامل مع حقوق الإنسان والعهدين الدوليين الأساسيين اللذين يحددان التزامات الدول بموجبهما، فإن المضمار الرئيسي للعمل الدولي ينبغي أن يكون لدى المنظمات المختصة بحقوق الإنسان في إطار الأمم المتحدة ومجلس حقوق الإنسان المؤسس عام 2006 والهيئة الخاصة المكلفة بالتعامل مع انتهاكات *العهد الدولي الخاص بالحقوق السياسية والحقوق المدنية*. ويحق لمجلس حقوق الإنسان بولايته الواسعة أو يضع إجراءً رسمياً للشكاوى متاحاً لجميع الحكومات الأعضاء في الأمم المتحدة. فتتمثل إحدى الإمكانيات في إدراج موضوع حرية الإنترنت والرقابة على نحو إلزامي في عملية المراجعة الدورية الشاملة لحقوق الإنسان حيث

---

[84] على الأقل، أظهر منتدى إدارة الإنترنت أن قضية الرقابة ليست غريبة عن نطاق عمله. فأثناء السجال الحالي بشأن استمرار عمل المنتدى والتوسع الممكن في ولايته، قُدمت مقترحات لإجراء مزيد من الحوار بشأن حرية التعبير، وإيلاء المزيد من الاهتمام إلى البعد التنموي وذلك المتعلق بحقوق الإنسان في الإدارة الدولية. انظر وثيقة الجمعية العامة للأمم المتحدة A/65/78 (E/2010/68) بتاريخ 7 مايو 2020.

[85] "إعلان بشأن المبادئ الأساسية الخاصة بمساهمة وسائل الإعلام الجماهيري في دعم السلام والتفاهم الدولي وفي تعزيز حقوق الإنسان وفي مناهضة العنصرية والفصل العنصري والتحريض على الحرب" منظمة الأمم المتحدة للتربية والعلم والثقافة، 28 نوفمبر 1078. http://portal.unesco.org/en/ev.php-URL_ID=13176&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html؛
"توصيات بشأن تعزيز التعدد اللغوي ونفاذ الجميع إلى الفضاء السيبراني"، منظمة الأمم المتحدة للتربية والعلم والثقافة، 15 أكتوبر 2003،
http://portal.unesco.org/ci/en/ev.php-URL_ID=13475&URL_DO=DO_TOPIC&URL_SECTION=201.html
(الدعوة لنفاذ الجميع إلى الإنترنت كأداة لتعزيز إحقاق حقوق الإنسان على النحو المحدد في المادتين 19 و17 من الإعلان العالمي لحقوق الإنسان").

تخضع السجلات القطرية لمراجعة النظراء. وأيما كان الشكل الإجرائي الذي يقع عليه الاختيار، فإن تسليط الضوء الجماعي على انتهاكات حقوق الإنسان في هذا المجال يمكن أن يولد ما يلقى الترحاب من ضغط ومستلزمات جدلية على الحكومات التي يُشتبه بمخالفتها للقوانين. ويمكن من خلال إجراء الشكوى إلقاء ما يكفي من الضوء على الدور المريب لصناعة تكنولوجيا المعلومات الدولية الانترنت في تزويد القمع السيبراني بأدواته. وكما هو الحال في لجنة حقوق الإنسان، يمكن للاستعراض الدوري القطري في لجنة الأمم المتحدة لحقوق الإنسان أن يشمل أيضاً حرية الإنترنت.

ومهما بلغ قصور هذه الوسائل الإجرائية البحتة، فإن نظاماً ماثلاً للعيان يقضي بالالتزام أو التفسير، ويؤدي في نهاية المطاف إلى ضغط الرأي العام وازدراء العامة، يمكنه أن يمهد السبيل بالفعل لمزيد من الوعي العالمي بهذه المشكلة ولترشيد السلوك في العالم الرقمي في المآل الأخير.

5 النزاع السيبراني والاستقرار الجيوسيبراني

1.5 النزاع السيبراني

بقلم جانكارلو أ. باراليتا،[86] ووليام أ. باراليتا،[87] وفيتالي تسيجيشكو[88]

مقدمة: طبيعة التحدي

إن الحروب المعلوماتية قديمة قدم النزاع البشري. وظلت الدوافع الكامنة وراء هذه الحروب على حالها عموما. وتشمل هذه الدوافع السعي لتقويض ثقة الخصم، وتعطيل خطوط اتصالاته وإرباكها، وخلق الأوهام في نفسه بشأن طبيعة النزاع ومسرحه. و لم تزل مثل هذه الدوافع قائمة في عالم اليوم. أما ما استجد في القرن الحادي والعشرين الذي تشيع فيه البنى التحتية المعلوماتية الإلكترونية بصلاتها الرقمية ذات النطاق العريض السريع والمتوسعة أكثر فأكثر فهو الآتي: أ) شراسة الهجمات المعلوماتية التي يمكن أن تمزق النسيج الاجتماعي للبلد المستهدف وتكررها؛ ب) القدرة البالغة على إلحاق أضرار مادية واسعة؛ ج) الطاقات والقدرات الوبائية للهجمات المعلوماتية المتواصلة والمتاحة للجهات الفاعلة غير الحكومية بل والخاصة القادرة الآن على المشاركة في الحروب غير المتناظرة؛ د) نشوء حالة كامنة متفشية من النزاع الدائم منخفض المستوى، وهو ما يمكن أن يُطلق عليه اسم الحرب الباردة السيبرانية. وأدى الاستخدام المكثف لتكنولوجيا المعلومات الجديدة إلى تعزيز القدرات القتالية للأسلحة التقليدية والتكنولوجيات العسكرية الأخرى. ولهذا السبب فإن العسكريين ينظرون إلى تكنولوجيا المعلومات والاتصالات على أنها سلاح وهدف في آن معاً كما يعتبرون الفضاء السيبراني ميداناً لخوض الحروب مثله مثل الجو، والفضاء، والبر، والبحر.[89]

وعلى مدى العقدين الماضيين قامت البلدان الصناعية بنشر شبكات واسعة من الأصول الاقتصادية، والمادية، والاجتماعية الهامة المربوطة عبر تكنولوجيا المعلومات والاتصالات للنهوض بمستوياتها المعيشية، ورخائها الاقتصادي، وتأثيرها، وقوتها على المستوى الدولي. وبالمثل فإن البلدان النامية تنظر إلى تكنولوجيا المعلومات على أنها مسار اقتصادي سريع نحو المشاركة الكاملة في الاقتصاد العالمي. وثمة كم هائل من الأجهزة الذكية

---

[86] Global Cyber Risk, LLC; Washington, DC, USA.

[87] Massachusetts Institute of Technology, Cambridge, MA, USA.

[88] Institute for Systems Analysis, Russian Academy of Sciences, Moscow, Russia

[89] على سبيل المثال فإن "مهمة القوات الجوية للولايات المتحدة هي توفير خيارات سيادية للدفاع عن الولايات المتحدة الأمريكية ومصالحها العالمية – وأن تحلق، وتقاتل، وتنتصر في الجو، والفضاء، والفضاء السيبراني". "Air Force Strategy: Sovereign Options for Securing Global Stability and Prosperity," 26 Mar. 2008, Office of the Secretary of the Air Force, www.stormingmedia.us/98/9868/A986884.html. وثمة شرح أوسع لمنظور الولايات المتحدة في *Information Operations, Electronic Warfare and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service (CRS) Report, RL31787, 14 Sept. 2006, www.fas.org/irp/crs/RL31787.pdf. (المشار إليه فيما بعد باسم "تقرير هيئة بحوث الكونغرس").

الصناعية (والمحتوية على المحاسيس والمعالجات الصغرية)، وكذلك الأجهزة الاستهلاكية ذات المعالجات الصغرية والقدرات اللاسلكية (أو الخلوية) مثل الهواتف الخلوية، والمساعِدات الرقمية الشخصية، والمفكرات الإلكترونية. وتتيح شبكات الاتصالات الواسعة الاستخدام المكثف لموارد المعلومات لتيسير التجارة، وتوفير الخدمات، ورصد البيئة، ومعالجة المشكلات الاجتماعية الشائكة. وتشهد كل هذه الأجهزة تطوراً سريعاً مع قدرة على الاتصال بالأجهزة الأخرى في أي مكان في العالم.

وكما يشير جنرال أمريكي سابق فقد قامت الهيئات العسكرية والحركات شبه العسكرية باعتماد تكنولوجيات المعلومات والاتصالات ذاتها التي تربط الأصول الاقتصادية والمادية والاجتماعية البارزة وتكييفها، مما أسهم في إحداث ثورة في الشؤون العسكرية تعمل على تغيير سبل تخطيط الحروب، وتنظيمها، وإدارتها. وتشتمل هذه "الثورة" على تطورات في القدرة على تنفيذ مهام جمع المعلومات وتحليلها، والمراقبة، والاستطلاع؛ وقيادة القوات والعمليات والتحكم فيها؛ والنهوض بالتحركات اللوجستية؛ وإتاحة الملاحة الدقيقة واستخدام الأسلحة "الذكية". ومن المهم للغاية أن هذه التكنولوجيات تتيح استخدام "الشبكة" كوسيط يمكن، انطلاقاً منه، وعبره، وفيه، تنفيذ العمليات العسكرية.[90]

وتتطلب تكنولوجيا المعلومات وتيسر علاقات سببية جديدة على امتداد المجتمعات بقدرة طبيعية على تدعيم النمو الاقتصادي، والدفاع عن حقوق الإنسان، وفضح القمع الحكومي. وتستمتع سلطات القيادة الوطنية كثيراً بالقدرة الميسرة للغاية على التواصل من القمة إلى القاعدة، غير أن الأهم من ذلك، بالنسبة إلى توسيع حقوق الإنسان والرخاء الاقتصادي، أن دفقات المعلومات الأفقية والمتجهة من القاعدة إلى القمة قد توسعت لتصبح أنهاراً عظيمة. وتعزز مجتمعات المعلومات الحديثة باستمرار عُقد المعلومات (حيث يتم توليد المعلومات واستهلاكها) من حيث الأعداد والخواص، وكذلك عدد وعرض الوصلات. وبالإضافة إلى ذلك فإن هناك نسبة متزايدة من العُقد والوصلات على حد سواء مجهزة بمحاسيس آلية تُظهر حالتها التشغيلية.

ومثل هذه التوصيلة ذات السمة غير الخطية الشديدة تزيد في آن معاً من قدرة شبكة المعلومات على الصمود في وجه المخاطر والعواقب الناجمة عن الهجمات المنهكة على العقد والوصلات الجذعية، وكذلك من المصاعب المتعلقة بتوقع تبعات الأعطال الشبكية. وبمقدور التطور السريع لتكنولوجيا المعلومات والاتصالات والارتقاء اللاحق لمجتمع المعلومات العالمي أن ينتجا طائفة واسعة من الآثار الجيوسياسية السلبية المتمثلة بما يلي: استقطاب عالمي أسرع بين البلدان الغنية والفقيرة، واتساع الفجوة التكنولوجية بين البلدان الصناعية للغاية والبلدان النامية، بما يعني تخلف عدد متزايد من البلدان المهمشة اقتصادياً عن ركب التطور الحضاري، وهو ما يشكل بؤرة رئيسية لنشوء النزاعات والقلاقل السياسية. ومن ثم، ومع تطور تعقيد شبكات المعلومات عضوياً، فإن احتمالات اندلاع الحروب المعلوماتية تنحو بصورة متزايدة إلى تعريض قيم اجتماعية متزايدة الضخامة للخطر.

---

[90] Gen. John Casciano, "Threat Considerations and the Law of Armed Conflict," Aug. 2005 (on file with WFS Information Security PMP).

التحريم العام للهجمات السيبرانية مقابل الحروب السيبرانية التي تقودها الحكومات

أدت الهجمات على الشبكات، والنظم، والبيانات الرقمية الحاسوبية إلى سن قوانين ضد الجرائم السيبرانية في العديد من البلدان. ورغم أن لمعظم البلدان الصناعية نوع ما من أنواع قوانين مكافحة هذه الجرائم فإن هناك تغايرات واسعة في تحديد ماهية الجريمة السيبرانية، وفي كشف وتحديد السلوك الإجرامي في الفضاء السيبراني، وفي الأحكام الأساسية والإجرائية مما أعاق كثيراً التعاون الدولي في توفير المساعدة في التحقيقات المتعلقة بالجرائم السيبرانية. وقد تم إعداد اتفاقية مجلس أوربا بشأن الجريمة السيبرانية كاتفاق متعدد الأطراف يهدف إلى الشروع في تنسيق القوانين العالمية للجريمة السيبرانية. على أن الواقع قصَّر كثيراً عن التطلعات؛ و لم يزد عدد البلدان وقت الاتفاقية المذكورة عن 26 بلداً بحلول منتصف عام 2010، أي بعد نحو تسع سنوات من فتح بابها للتوقيع. وأعد الاتحاد الدولي للاتصالات كتيباً إرشادياً بشأن التشريعات المتعلقة بالجريمة السيبرانية كمسار بديل متسم بقسط أوفر من المرونة؛ ويعرض الكتيب عينة للغة التشريعية المنسجمة مع اتفاقية مجلس أوربا بشأن الجريمة السيبرانية وقوانين الجرائم السيبرانية في البلدان الصناعية، ويمكن أن تستعين بهذا الكتيب البلدان في مختلف أرجاء العالم عند صياغة أو تعديل قوانينها المتصلة بالجريمة السيبرانية.

وتشمل القوانين الأخرى المتعلقة ببعض أنواع الأنشطة السيبرانية القوانين التي تحمي الأنظمة والمعدات المادية لموردي الاتصالات، والتشريعات التي تحظر أعمال الجاسوسية الاقتصادية، وقوانين الملكية الفكرية، وما إلى ذلك. وبصورة إجمالية فإن هذه القوانين تهدف إلى فرض حظر قانوني على مختلف أنواع الهجمات السيبرانية الموجهة إلى كل أصناف البنى التحتية، والأنظمة، والبيانات.

وتتوسع الطائفة العريضة من الاحتمالات يومياً مع طرح تكنولوجيات للمعلومات أشد قوة وانتشاراً. ولا عجب في أن للبلدان حافزاً قوياً لقوننة السلوك في الفضاء السيبراني بغض النظر عن مسلكها هي إزاء البلدان الأخرى. وبما أن بمقدور تكنولوجيا المعلومات أن تقفز بسهولة عبر الحدود الدولية فلا حاجة للمجرمين على الإطلاق إلى دخول أراضي الدولة التي يقيم فيها ضحاياهم. وبالتالي فإن حوافز التعاون بين الدول القومية ينبغي أن تكون كثيرة، ولا سيما وأن موارد المعلومات الحكومية تشكل هدفاً جذاباً للسلوك الإجرامي. وفي الحقيقة فإن ضم الصفوف لترويج التعاون المثمر في شبكات المعلومات ومن خلالها وفي منع، أو على الأقل ردع، سوء السلوك في الفضاء السيبراني قد غدا شاغلاً من شواغل الهيئات الدولية ذات الطابع الدولي المتأصل مثل الاتحاد الدولي للاتصالات.

وبالنظر إلى اعتماد الحكومات المتزايد على الإنترنت لتسهيل توزيع المعلومات والخدمات على مواطنيها، فإن مجتمع المعلومات يقدم هدفاً مغرياً للأشرار، سواء أكانوا من المجرمين، أم المجموعات الإرهابية دون الوطنية، أم الدول القومية المعادية. وبرهن الهجوم[91] على البنية التحتية للمعلومات في إستونيا في أبريل عام 2007

---

[91] غطت الصحافة الدولية أنباء هذا الهجوم بشكل واسع. وذلك مثلاً في مقال Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian,* 17 May 2007, www.guardian.co.uk/world/2007/may/17/topstories3.russia.

بوضوح الهشاشة المتوقعة للحكومة الإلكترونية والافتقار إلى العوامل اللازمة لردع المهاجم. ويدعي الكثير من الخبراء أن التعقيد التقني للهجوم يفوق ما شهدته الحوادث المعروفة السابقة. وفي حين أن البعض منهم يصل إلى درجة القول بأن الأمر ما كان ليحدث دون معرفة أو تواطؤ من كيان وطني، فإن عدداً من الخبراء الأمريكيين قد قللوا من قيمة مثل هذه التكهنات. على أنه تجدر الإشارة إلى أن الحادثة الإستونية لم تترافق مع مطالب سياسية أو نقدية أو بيانات صادرة عن القادة المزعومين للهجوم،[92] مما يعني أن من المتعذر استبعاد أن يكون الأمر عملاً إجرامياً دون دوافع سياسية. ويعتبر هجوما غوستنت[93] وأورورا عام 2009 من بين الأمثلة الأخرى على الهجمات السيبرانية الأكثر استمراراً واتساعاً. وقد تركز جانب من الهجمات على مخدمات غوغل كجزء من جهد تجسسي سياسي ومؤسسي مدبر كما يبدو، وهذا الجهد " استغل ثغرات أمنية في ضمائم البريد الإلكتروني للتسلل إلى شبكات الشركات المالية، والدفاعية، والتكنولوجية، ومؤسسات البحوث البارزة في الولايات المتحدة".[94]

وكما يتضح من المثال الإستوني فإن الهجمات السيبرانية الكثيفة والمتواصلة يمكن أن تشكل فعلياً اعتداء مباشراً وواسعاً على الكيانات المدنية والحكومية على مستوى يتجاوز السلوك الإجرامي المجرد. وقد تشمل سمات مثل هذه الهجمات ما يلي: أ) أضرار مادية بالغة تلحق بالمرافق الحيوية؛ ب) إصابات أو خسائر واسعة في الأرواح؛ ج) انتشار الفوضى في المؤسسات المالية؛ د) تعطل وظائف البنى التحتية الحيوية. ومن المرجح أن يسفر تنسيق هذه الهجمات أو استمرارها لفترات مطولة عن تفاقم العواقب. وفي مثل هذه الحالات، وسواء

---

92 بحلول أوائل يونيو أعلن أحد قادة مجموعة الشباب الروسية الموالية لبوتين المسؤولية عن الهجوم. www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/15646 94.html على أنه لا يمكن التأكد من صدقية هذا الزعم.

93 *Tracking GhostNet: Investigation of a Cyber Espionage Network,* Information Warfare Monitor, 1 Sept. 2009, http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/. "كشف التحقيق في نهاية المطاف عن شبكة مؤلفة من أكثر من مركزاً موبوءاً في 103 بلدان. وتعتبر المراكز الموبوءة أهدافاً عالية القيمة وتشمل حواسيب في وزارات الخارجية، والسفارات، والمنظمات الدولية، ووسائل الإعلام، والمنظمات غير الحكومية. وبالنسبة للنظم الحاسوبية في التيبت التي تفحصناها يدوياً، والتي انطلق منها تحقيقنا، فقد لحق بها ضرر بالغ بفعل حالات عدوى متعددة أتاحت للمهاجمين نفاذاً غير مسبوق إلى معلومات حساسة محتملة.... على أن عزو كل البرامج الخبيثة إلى عمليات متعمدة أو موجهة تقوم بها الدولة الصينية لجمع المعلومات هو أمر خاطئ ومضلل. وبمقدور الأرقام أن تروي قصة مختلفة. إذ تضم الصين حالياً أضخم مجموعة سكانية من مجموعات الإنترنت في العالم. والعدد الصرف للمواطنين الرقميين الشبان المستخدمين للشبكة يمكن أن يفسر ويزيد تزايد البرامج الخبيثة الصينية. ومع تصاعد عدد الأشخاص المبدعين المستخدمين للحواسيب، فإن من المنتظر أن يزداد نصيب الصين (والأفراد الصينيين) من الجرائم السيبرانية".

94 Ariana Eunjung Cha and Ellen Nakashima, "Google China cyberattack part of vast espionage campaign, experts say," *The Washington Post*, 14 Jan. 2010,. www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

أكانت هوية المهاجم أم دوافعه مكشوفة، فإن الدول القومية قد تنظر[95] إلى هجوم سيبراني واسع على أنه عمل إرهابي أو أنه يكافئ وظيفياً هجوماً مسلحاً يبرر دراسة خاصة ومعاملة خاصة لمعالجة الأمر.

وفي الحدود الدنيا فإن الاحتمالات المثبتة للتعطيل واسع النطاق لمجتمع المعلومات تتطلب ثقافة من التعاون المشترك عابرة للحدود الوطنية. وفي المثال الإستوني فإن الموجة الأولى من تعطيل المواقع الحكومية قد أدت إلى إطلاق خطط احترازية للتصدي لموجة من الهجمات على الخدمات المالية مثل الخدمات المصرفية الشبكية. وفي الحقيقة، وخلال بضعة أيام، فقد " استُهدفت الخدمات المصرفية للقطاع الخاص والوسائل الإعلامية الشبكية بشكل كثيف وأدت الهجمات إلى الإضرار بعمل بقية البنية التحتية الشبكية في إستونيا".[96] وخلال الفترة ذاتها فإن التدابير المضادة، التي اتُخذت بالتعاون مع موردي خدمات الإنترنت في مختلف أنحاء العالم، عملت على توسيع حظر الحركة الواردة من مجموعات معنية من عناوين موردي خدمات الإنترنت وعلى عزل النظام المصرفي الإستوني عن كل الحركة الدولية. وتجدر الإشارة إلى أن حجم شبكة الموارد المطلوبة للتخفيف من آثار الهجمات السيبرانية قد فاق بالتأكيد، وبأضعاف مضاعفة، حجم الموارد المستخدمة في شن الهجمات.

وليست ظاهرة اللاتناظر الواسع بين الهجوم والدفاع في الفضاء السيبراني بالأمر الخافي. وبدون الحاجة إلى مثل هذه الهجمات واسعة النطاق فإن الوكالات العسكرية والاستخبارية للولايات المتحدة والدول القومية الأخرى (روسيا، الصين، الهند، باكستان، إيران) تنفذ بالفعل "عمليات الاستطلاع والجس لتحديد شبكة (شبكات) رقمية صالحة للاستغلال بسبب أوجه ضعفها في صفوف الخصوم المحتملين". ويعمل واضعو القرارات في هذه البلدان كما لو أن عصر الصراع السيبراني قد حل بالفعل. وفي الواقع فإن بلداناً مثل الولايات المتحدة هي التي تمتلك قدرات وطاقات لا متناظرة لشن أو رعاية الهجمات السيبرانية (وخصوصاً على شكل عمليات سرية) على البلدان الأقل قدرة على الرد بالمثل. وبالإضافة إلى ذلك فإن السلطات في هذه البلدان وغيرها تدرك حق الإدراك أن اللاتناظر الواسع بين الهجوم والدفاع حينما يترافق مع الهوية الخفية تقريباً للمهاجم المصمم يطرح احتمال الاستعانة بصورة مباشرة أو غير مباشرة بـــ "جيوش" من المرتزقة السيبرانيين أو "المقاتلين غير الشرعيين" الذين يزودون السلطات الوطنية بالقدرة على الإنكار المعقول.

وعلى الصعيد العملي، فإن الأضرار المحتملة لهجوم ما يمكن أن تتباين تبايناً واسعاً وفقاً لدرجة استعداد المجتمع والقدرة الأمنية المتأصلة في البنية التحتية المتعرضة للهجوم. ومن زاوية واضعي القرارات العسكريين أو

---

[95] قام مايك ماكونيل المدير السابق للمخابرات الوطنية في الولايات المتحدة عام 2009 بتصنيف الأسلحة السيبرانية على أنها من أسلحة الدمار الشامل (أو أنها يمكن أن تكون كذلك). CRS Report at 3.

[96] "ENISA commenting on massive cyber attacks in Estonia," ENISA press release, 24 May 2007, www.enisa.europa.eu/act/cert/contact/press-releases/enisa-commenting-on-massive-cyber-attacks-in-estonia.

السياسيين فإن "المسألة المهمة المتعلقة بالتصدي لأي شكل من أشكال الهجمات السيبرانية تتمثل في تبين نوع الهجوم وهوية الخصم بسرعة ثم الرد بالشكل المناسب. وفي الوقت الراهن فإن تتبع عمليات الاقتحام الحاسوبية هو وظيفة من وظائف تطبيق القوانين ... ومن المحظور على الهيئات العسكرية التي تخوض الحروب التقليدية تنفيذ مهمتها محلياً ... [ولذلك] فإن للتدابير المحلية لإنفاذ القوانين دوراً حاسماً في الأمن والدفاع الوطنيين".[97] وعلى هذا فإن الدول القومية تحتاج سواء أفي وكالاتها العسكرية أم وكالات إنفاذ القوانين إلى أدوات تحقيق رقمية قوية، وهيكل قانوني مناسب لاستخدامها، ونُهج معقولة للحفاظ على منعة الأدلة وفرض عقوبات ذات قيمة ردعية حقيقية على المخالفين. وبما أن هذه الأدوات تتمتع بقدرة كامنة قوية لـــ "الاستخدام المزدوج"، فإن البلدان التي تتطلب أقوى القدرات الدفاعية والتحقيقية وأشدها مرونة، ستمتلك بالتالي قدرات هجومية وتجسسية سيبرانية بالغة. وفي حين أن احتمالات الاستخدام المزدوج وأوجه اللاتناظر الهجومي الدفاعي قائمة أيضاً في عالم الأسلحة المادية، فإن احتمال شن هجمات حركية قيد القمع (وإن لم يكن مستبعداً تماماً) بفعل مفاهيم الردع وبسبب السهولة النسبية لتحديد مصدر الهجوم.

التفاعل بين النزاع المعلوماتي والحركي

يؤدي الاستخدام المكثف لتكنولوجيات المعلومات الجديدة إلى تعزيز قدرات الأسلحة التقليدية والتكنولوجيا العسكرية وزيادتها على حد سواء. وتتيح تكنولوجيا المعلومات إدخال تغييرات نوعية في ميادين الشؤون العسكرية، والاستطلاع، والاتصالات. كما أنها تزيد كثيراً من سرعة معالجة مجموعات هائلة من البيانات واتخاذ قرارات تشغيلية معقدة، ومن ثم فإنها تمكّن من التحول بسرعة إلى طرق جديدة جذرياً للتحكم بالقوات والأسلحة على مختلف المستويات الاستراتيجية منها والتكتيكية. وتزيد تكنولوجيا المعلومات الجديدة بشدة من القدرات القتالية لمرافق الحرب الإلكترونية وتخلق نوعاً جديداً من الأسلحة ولا سيما الأسلحة المعلوماتية المصممة لإتلاف البنية التحتية المعلوماتية العسكرية والمدنية للخصم عبر اختراق شبكاته الحاسوبية.

وبالنسبة إلى الجهات العسكرية فإن ثورة المعلومات والتكنولوجيا تزيد بشدة من القدرات القتالية للقوات، لا بتبديل أشكال وطرق المستويات المختلفة للحروب فحسب، بل وبتغيير النموذج التقليدي أيضاً للصراع العسكري وتصعيد النزاع. ووفقاً للخبراء الأمريكيين فإن التسليط الانتقائي للأسلحة المعلوماتية على البيئة التحتية المعلوماتية العسكرية والمدنية الحيوية يمكن أن ينهي النزاع قبل بدء العمليات القتالية الحركية للأطراف، إذ إن تصعيد الهجوم المعلوماتي سيسفر عن كارثة. ويتيح امتلاك أسلحة المعلومات مزية ساحقة للبلدان التي تفتقر إليها. وستتجاوز المتغايرات المعلوماتية والسياسية للمجابهة بين القوى من حيث أهميتها المتغايرات النووية إن لم يكن اليوم ففي المستقبل القريب. وعلى النقيض من ذلك فإن كل البلدان، ولا سيما

---

[97] Bonnie N. Adkins, "The Spectrum Of Cyber Conflict: From Hacking to Information Warfare: What Is Law Enforcement's Role?" Air Command and Staff College, Maxwell Air Force Base, AU/ACSC/003/2001-04, Apr. 2001, .http://stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA406949

المتقدمة منها للغاية، معرضة لهجمات الأسلحة المعلوماتية. وبالمستطاع استخدام هذه الأسلحة، وعلى غرار الأسلحة الذرية، كعامل للضغط السياسي وللردع.

وليست الحرب المعلوماتية مجرد حقيقة افتراضية من حقائق الألعاب الحاسوبية، بل إنها أداة محسوسة لإحراز النصر في نزاع عسكري أو سياسي. ومما لاشك فيه أن الأسلحة المعلوماتية تغدو يوماً بعد يوم عنصراً بارزاً في القدرات العسكرية للبلدان، وأن الكثير من هذه البلدان، ولا سيما الولايات المتحدة الأمريكية والصين، تستعد بنشاط وإصرار لشن حروب المعلومات.

طبيعة الأسلحة المعلوماتية

يعتبر تعريف وتحديد "الأسلحة المعلوماتية" من بين المشكلات المفاهيمية المطروحة عند صياغة نموذج للأمن المعلوماتي. فما السمات المميزة للأسلحة المعلوماتية؟ وما مستوى النزاع السيبراني (إن وجد) الذي ينبغي أن يُعامل على أنه نزاع مسلح؟ إن الافتقار إلى أي توافق دولي بشأن هذه الأسئلة يعرقل إطلاق مفاوضات بناءة بشأن الأمن المعلوماتي العالمي. ويستند أحد النُهج المستخدمة في تعريف "الأسلحة المعلوماتية" إلى قدرتها على الإضرار بالبنية التحتية المعلوماتية العسكرية والمدنية.[98] ومن مثالب هذا النهج أن بالمستطاع بالتالي إطلاق اسم سلاح معلوماتي على أي نوع من أنواع الأسلحة، بما في ذلك التقليدية منها، القادرة على إلحاق الضرر بالبنية التحتية المعلوماتية. وعلى سبيل المثال، هل هناك من أهمية لنوع الجهاز الذي يُستخدم في تعطيل نظام التحكم بالاقتصاد البلدي، سواء أكان هذا الجهاز شفرة برنامجية، أم نبضة إلكترونية شديدة، أم ضربة مباشرة من متفجرة تقليدية؟ وثمة نهج آخر يمكن بمقتضاه اعتبار الأسلحة المعلوماتية على أنها كل وسائل التدمير التي تستخدم تكنولوجيا المعلومات والاتصالات.

وما ينبغي تفاديه عند التصدي لمسألة النزاع السيبراني هو خفض الحاجز القائم في وجه الحرب عبر اعتماد تعاريف تشمل أنشطة تمارس بكثرة خلال فترات السلم. فما السمات المميزة للأسلحة المعلوماتية؟ وما مستوى النزاع السيبراني الذي يجب أن يُعامل على أنه نزاع مسلح؟ إن من الحمق ومن الخطير على الاستقرار الدولي أن تتم معاملة النزاعات التي لا تشتمل على تهديدات واضحة للأرواح البشرية أو الحرية الاجتماعية على أنها "نزاع مسلح". وفضلاً عن ذلك، وبالنظر إلى أن كل أنظمة السلاح المتطورة عملياً تستخدم تكنولوجيا المعلومات والاتصالات، فإن من العسير للغاية، إن لم يكن من المستحيل، أن نعزل الأسلحة المعلوماتية عن الطائفة الكاملة للأسلحة. وبما أن الحرب المعلوماتية هي ظاهرة مستمرة في تاريخ النزاع البشري، فإن من الصعب على وجه الخصوص تقديم تعريف قاطع بالنظر إلى المستويات المتعددة

---

[98] على سبيل المثال، "أي قدرة، أو جهاز، أو مجموعة من القدرات والتقنيات الذي يؤدي على الأرجح، في حال استخدامه للغاية المزمعة منه، إلى الإضرار بمنعة أو توافر المعلومات، أو ببرنامج، أو معلومات في حاسوب أو نظام لمعالجة المعلومات".
Graham H. Todd, "Armed Attack In Cyberspace: Deterring Asymmetric Warfare With An Asymmetric Definition," *Air Force Law Review,* Vol. 64, 2009 at 65 – 102, http://lawlib.wlu.edu/CLJC/index.aspx?mainid=418&issuedate=2010-03-23&homepage=no.

للتعقيد المفاهيمي. فكيف لنا مثلاً أن نصنف عملية التزويد المتعمد بالمعلومات الخاطئة؟ وماذا عن التجسس، أو اعتراض تدفقات المعلومات؟ إن المنظور الذي يعتمده الفرد إزاء مثل هذه الأنشطة يتأثر بشدة بما إذا كانت تُنفذ خلال حرب حركية.

والسمات التشغيلية الهامة للأسلحة المعلوماتية هي: 1) تكلفتها المنخفضة نسبياً وسهولة الحصول عليها؛ 2) إمكانية تطويرها، ومراكمتها، ونشرها بشكل سري؛ 3) اتسامها بصورة متأصلة بأثر يتجاوز حدود الإقليم ولا يمكن تحديد مصدره. وتتيح هذه السمات الانتشار العشوائي للأسلحة المعلوماتية ويجعل من حيازة الأنظمة العدوانية لها مسألة عالمية خطيرة. ويستدعي الخطر اللاحق على السلام والاستقرار الدوليين أن يبادر المجتمع العالمي إلى مجابهة التهديد الموجه إلى البنى التحتية الوطنية والعالمية للأمن المعلوماتي من خلال اتخاذ خطوات عملية لتحييد التهديدات السيبرانية. وبما أن تكنولوجيا المعلومات والاتصالات تشكل جزءاً من البنية التحتية للمجتمع الحديث فإنها تندرج ضمن مجموعة الأدوات المتاحة لبلد ما في حربه ضد أعدائه.

وتتخذ العديد من البلدان إجراءات لمجابهة التهديدات الموجهة إلى الأمن المعلوماتي؛ ومع ذلك فإن طابع هذا التهديد العابر للبلدان والهوية المغفلة للمعتدين تقلل من كفاءة حتى أشد هذه الإجراءات صرامة. وفي مثل هذه الظروف فليس بمقدور أي بلد أن يتمتع بالسلامة إذا ما حاول التصدي بمفرده للتهديدات المعلوماتية. ولا يمكن الحد من انتشار الأسلحة المعلوماتية وتقليل خطر نشوب حروب معلوماتية، وعمليات إرهابية معلوماتية، وجرائم سيبرانية، إلا بإرساء نظام دولي للأمن المعلوماتي يبذل المشاركون فيه جهوداً دؤوبة في هذا الصدد.

وفي الحد الأدنى فإن بالإمكان اعتبار البرمجيات المصممة خصيصاً لتدمير البنية التحتية المعلوماتية (الفيروسات المختلفة، وعلامات التأشير، وما إلى ذلك) على أنها بدون أدنى شك أسلحة معلوماتية. غير أن الغالبية العظمى من الوسائل المتطورة للصراع المسلح التي تستخدم تكنولوجيا المعلومات والاتصالات هي ذات استخدامات متعددة، أي أنها ليست مصممة فحسب لتدمير البنى التحتية المعلوماتية بل لمهام قتالية أخرى أيضا. وتتمتع البلدان التي تمتلك أنظمة أسلحة متطورة، ووسائل استطلاع، واتصال، وملاحة، وتحكم مستندة إلى الاستخدام الواسع لتكنولوجيا المعلومات والاتصالات بتفوق عسكري حاسم؛ ومن ثم فإن من المشكوك فيه أن تنضم هذه الدول إلى اتفاقيات تحد من مزاياها الاستراتيجية.

وعلى هذا فإن المسألة ذاتها المتعلقة بحظر إنتاج، وانتشار، واستخدم الأسلحة المعلوماتية أو الحد من ذلك ستقتصر على الأرجح على الأسلحة ذات الغرض الواحد المصممة فحسب لضرب عناصر البنية التحتية المعلوماتية، مثل الأسلحة المرتكزة على الشفرات البرامجية أي الفيروسات المختلفة ووسائل تسليمها. ومن سوء الطالع أن الغالبية الساحقة من التكنولوجيات الحديثة للمعلومات والاتصالات التي يمكن أن تُستخدم لأغراض عسكرية، وإرهابية، وإجرامية هي من إنتاج الصناعات المدنية؛ ومن ثم فإن التحكم بتطويرها وانتشارها سيكون عسيراً جداً.

والتهديد الذي تطرحه أدوات النزاع السيبراني والحرب المعلوماتية هو تهديد حقيقي بالنسبة إلى الجميع، ولا سيما البلدان المتقدمة حيث تتحكم البنية التحتية المعلوماتية المعقدة بكل أنشطتها الحيوية.[99] ولا يمكن على الأرجح التخفيف من حدة التهديد بالاستخدام المؤذي لتكنولوجيا المعلومات إلا من خلال الجهود الدؤوبة للمجتمع الدولي من أجل حماية البنى التحتية المعلوماتية الوطنية الهامة. وسيتيح توافق الآراء بشأن هذا الصنف من نظم المعلومات توفير ردع فعال وإجراءات وقائية كفوءة، بما في ذلك الحق في لجوء البلدان إلى إجراءات ثأرية في حال تنفيذ عمليات معلوماتية ضدها تلحق بها آثاراً مباشرة خطيرة وغير مقبولة. وحتى في هذا الجانب فإن من الواجب توخي الحذر الشديد. فمن غير المبرر الشروع في حرب حركية نتيجة عمل ما مهما كان نوعه من الأعمال المعلوماتية العدوانية؛ ومن الحماقة منح الحكومات الحجج اللازمة لكي تبت في الأمر بنفسها.

الحد من النزاع السيبراني

يؤدي اللاتناظر الهائل المحتمل بين التكنولوجيات المعلوماتية الهجومية والدفاعية إلى وضع يستطيع فيه المستخدمون الفعليون شن "حروب سيبرانية" شخصية ضد البنية التحتية المعلوماتية المهمة للمجتمع وذلك بالقوة ذاتها تقريباً التي يمكن أن تستخدمها الدول القومية. وبالتالي فإن النظام القانوني والسياسي لردع النزاع السيبراني والحد منه بين الدول سيرتبط بحكم الواقع بالأطر القانونية والإجرائية المتعلقة بردع الإرهاب السيبراني والجريمة السيبرانية والتعامل معهما.

وفي ميدان مجتمع المعلومات فإن مفهوم الردع عبر العقوبات المدنية والجنائية قد يكون قابلاً للتطبيق على مستوى الإجرام أو "التقرصن"[100] إذا ما أمكن إرساء شبكة مناسبة من التماثل الدولي في القوانين الجنائية. ولسوء الحظ، وعلى مستوى الهجمات السيبرانية التي تشنها الدول القومية، فقد لا يكون لمفاهيم الردع التي استُحدثت خلال الحرب الباردة من قيمة تُذكر، إذ إن شن هجوم مضاد من النوع ذاته قد يلحق الضرر بالتوصيلة الاجتماعية والمادية الدولية على مستوى غير مقبول للأطراف الثالثة وللقائمين بالهجوم المضاد على حد سواء. وفي الفضاء السيبراني فإن الضرر المصاحب يمكن أن يكون على مستوى العالم، وهو ما ظهر مراراً أثناء العدوى السريعة بالشفرات الخبيثة مثل الفيروسات الحاسوبية. وفي الحالة المتوسطة من الإرهاب

---

[99] إن قرار السلطات العسكرية الأمريكية بعدم شن هجوم سيبراني على النظم المالية العراقية هو موضوع بحث تقرير *Warfare and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service, RL31787, 19 July 2004 at 5-6, www.fas.org/irp/crs/RL31787.pdf. كما أن تقرير هيئة بحوث الكونغرس هذا يرسي إطار السلطات العسكرية الأمريكية المتعلق بالتصدي للحروب السيبرانية ويوضح موقع هذه الحروب ضمن استراتيجية هذه السلطات وبرامجها طويلة الأجل المتصلة بالحروب المعلوماتية.

[100] يشير "التقرصن" إلى كتابة أو استخدام شفرة حاسوبية "قرصنة" لمهاجمة شبكة المعلومات والاتصالات التابعة للمستهدف بغرض ترويج أيديولوجيا سياسية أو هدف اجتماعي. وكثيراً ما يدافع المتقرصنون عن أفعالهم على أنها أعمال احتجاج وعصيان مدني. للإطلاع على مثال عن ذلك انظر http://thehacktivist.com/hacktivism.php.

السيبراني، فإن السلوك الأخير للولايات المتحدة إزاء " المقاتلين غير الشرعيين" في "حربها ضد الإرهاب" يشير إلى أن نموذج الردع على مستوى العقوبات المدنية والجنائية يمنى بالفشل هنا أيضاً.

وفي حين أن مصاعب الردع قد تشجع على التماس الدفاع التكنولوجي الأكمل ضد الهجمات السيبرانية فإن تاريخ كل نوع آخر من أنواع الأسلحة يؤكد أن معالجة ما هو في جوهره مشكلة سياسية اجتماعية ينبغي أن تتم في نهاية المطاف على مستوى سياسي اجتماعي. ومن الناحية السياسية فإن الاحتمالات الخطيرة للنزاع الدولي السيبراني تستدعي اهتماماً فورياً. وتستبعد الطبيعة مزدوجة الاستخدام للتكنولوجيا إمكانية اللجوء إلى نوع من أنظمة الرقابة الدولية مماثل لما تم استخدامه لتنظيم التكنولوجيا الذرية. وكل ما يمكن أن نأمله (ونسعى إليه) هو إنشاء إطار قانوني عابر للدول يرسي القواعد والعقوبات المتعلقة بالنزاع السيبراني في مجموعة من الاتفاقيات الملزمة المنظمة والناتجة عن مفاوضات دولية. ومن الواجب أن تحدد مثل هذه القواعد التزامات البلدان الموقعة فيما يتعلق بضبط المنظمات أو الشبكات غير الحكومية التي تعمل فعلياً ضمن حدودها.

وفي حين أن الولاية القضائية عن الهجمات الإرهابية السيبرانية أو التجسس السيبراني يمكن أن تُدرج عموماً ضمن القوانين الجنائية المدنية العامة والاعتبارات المصاحبة لهذه الولاية، فإن بعض سماتها قد تدعو إلى اعتماد قوانين خاصة تثير بحد ذاتها اعتبارات تتعلق بالولاية القضائية. وقد تشمل هذه السمات ما يلي: 1) أذى واسع مترافق مع معان سياسية؛ 2) تزايد صعوبة تحديد المرتكبين، والقبض عليهم، ومحاكمتهم؛ 3) الحضور القوي للدوافع السياسية الهادفة إلى الزعزعة المجتمعية بما ينتهك الأفكار المقبولة عموماً للقوانين الجنائية وقوانين النزاع المسلح على حد سواء. وثمة حجة إضافية لإخضاع الإرهاب السيبراني لمعاملة خاصة. "إذ إن بالمستطاع تبرير رد خاص عادة حينما ينبع الإرهاب من مجموعة ذات قدرة على التنظيم الجماعي وعلى أساس مستمر، وأن تنخرط في خطط وعمليات معقدة، وأن تعمل بصورة مستقلة عن الحياة العادية، أو أن تكون قادرة على تخويف المجتمع العادي بحيث يقبل بوجودها".[101] وقد يتطلب النزاع السيبراني المطول المنفذ لأغراض إرهابية أو عسكرية أو يحفِّز عملاً منسقاً دولياً للحد من استخدام القوة أو ضبطه.

كما ينبغي أن يعمل نظام الرقابة الفعال على قوننة التدابير التي يمكن اتخاذها ضد المهاجمين من غير الدول إذا كان بالمستطاع فعلاً تحديدهم. وفي حالة عمل إرهابي نابع من البلد المتعرض للهجوم، فإن بالإمكان اتخاذ التدابير بحق المهاجم في سياق القانون الجزائي الوطني، بما في ذلك تشريعات مكافحة الإرهاب. أما بالنسبة إلى الهجمات المنطلقة من دول محايدة أو متعاونة فإن هناك خيارات متعددة هي: 1) تسليم الفاعل إلى الدولة التي تعرضت للهجوم؛ أو 2) المحاكمة المحلية في البلد المحايد الذي انطلق منه الهجوم؛ أو 3) تسليم الفاعل إلى طرف ثالث يدَّعي ولاية قضائية عالمية ويلتزم عموماً بالحدود المناسبة للإجراءات. أما ما هو الخيار الذي

---

101 Clive Walker, "Cyber-Terrorism: Legal Principle and the Law in the United Kingdom," *Penn State Law Review*, Vol. 110, 2006 at 625-65, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1109113#%23.

ينبغي اعتماده فهو مسألة تتعلق بالموازنة بين اعتبارات مشاركة دولة المنشأ، ومظهر تطبيق العدالة، ودعم عدم التسامح الدولي إزاء الطرق الإرهابية.

وفي حال انطلاق الهجمات السيبرانية من دول مارقة أو غير متعاونة فإن ذلك يؤدي إلى استبعاد توافر القنوات العادية للتعاون في التحقيقات المتعلقة بالهجمات، واعتقال الفاعلين ومحاكمتهم، أو تسليمهم إذا كان ذلك مناسبا. والمسألة في نهاية المطاف هي ما إذا كان المهاجم أو المهاجمون سيحاكمون في الدول التي تعرضت للهجمات، أو في دولة طرف ثالث محايدة، أو في المحكمة الجنائية الدولية. وبالتالي فإن مثل هذه الحالات تتحول بالطبع إلى مسائل للتدخل بالقوة أو عبر العقوبات الدولية. وتوازي هذه المسائل تلك المتعلقة بالإرهاب بالوسائل الحركية. والخيارات المفتوحة أمام البلد الذي تعرض للهجوم هي التالية:

1 رد ثأري ضد البلد المعني؛

2 دخول بدون تفويض واعتقال[102] المذنبين المشتبه بهم؛ و

3 الاحترام اللائق للسيادة من خلال إشراك دولة طرف ثالث كوسيط.

وفي حال تصور نظام يتم فيه حظر بعض أنواع الإجراءات في الفضاء السيبراني بالتوازي مع اتفاقيات جنيف المتعلقة بالحرب الحركية، فإن بالإمكان تصور حالة من الولاية القضائية العالمية تدخل فيها مجموعة دولية. ويثير هذا الاحتمال حججاً مضللة بشأن حالة التمرد العامة (وقمعها) على الإنترنت. وتجدر الإشارة هنا إلى أن اتفاقية مجلس أوربا بشأن الجريمة السيبرانية لا تحدد، وبالتالي لا تجيز، أي أسباب للعمليات العابرة للحدود بحثاً عن الأدلة في الشبكات الحاسوبية، حتى لو كان ذلك في سياق المطاردة الحثيثة.

ملاحظات ختامية

إن الحقائق المقبولة هي التالية: (1) تعتمد معظم أعمال البلدان، والحكومات، والمرافق العامة اعتماداً شديداً على الحواسيب وشبكة الإنترنت؛ (2) ورغم أن الإنترنت تتسم بصورة أصيلة بالمتانة فيما يتعلق بالتوصيلية، فإن الحواسيب المربوطة بها أكثر هشاشة بكثير أمام الهجمات؛ (3) يتطلب اكتساب قدرات هجومية قوية إلى حد ما مستويات منخفضة نسبياً من الاستثمار؛ (4) إن من الصعب تحديد مصدر أي هجوم بشكل قاطع.

وفيما يتعلق بقوانين الحروب، فإن معظم البلدان قد توافق على بعض المبادئ العامة كأساس لنظام متسق للفضاء السيبراني.

1 إن الهجمات السيبرانية على البنية التحتية الحيوية ليست أسلحة هجومية مشروعة حتى أثناء الحروب الحركية. (على غرار الأسلحة البيولوجية والكيميائية).

---

[102] بمقتضى القانون الأمريكي فإن وسيلة جلب المشتبه فيه إلى الولاية القضائية الإقليمية لا تشكل حجة دفاعية تتعلق بالولاية و تحول دون إجراء المحاكمة.

2 إن التجسس الإنترنتي المتفشي الممول من الحكومات يجعل من الصعب تحديد الخروقات والقلاقل الناجمة عن الجريمة المنظمة، والمنظمات دون الوطنية، والقراصنة، كما أن ذلك يعرقل المحاكمة الجنائية لهذه المجموعات بموجب قوانين الجريمة الحاسوبية.

3 إن التجسس الحاسوبي منخفض المستوى الذي تقوم به الحكومات قد يكون محتملاً، غير أن التخريب غير مسموح به. ويؤدي "التنافس" الحكومي ذو المستوى المنخفض إلى حفز التقدم التكنولوجي. وفضلاً عن ذلك فإن لكل بلد مصلحة في أن يعرف بأن أمن النظم العسكرية الأجنبية محمي من الأشرار المحتملين.

4 يخلّف التجسس الحكومي على الشركات الخاصة أثراً غير واضح في العالم الحقيقي ولكنه صغير على الأرجح. غير أن ذلك يثير أحاسيس قومية محمومة وغير صحية في نفوس المواطنين، ويبعث برسائل سيئة إلى الصناعة، وإذا ما كان هذا التجسس يتم لحساب الصناعة الخاصة للبلد القائم بالتجسس فإنه ينحو إلى خلق قوة اقتصادية دون منافسة.

5 بما أن من العسير للغاية تحديد مصدر الهجوم وما إذا كان ممولاً من الحكومة، فإن بمقدور الكيانات غير الحكومية إثارة نزاع وطني.

وبالنظر إلى أن الاتفاقيات الرسمية قد لا تكون قابلة للتثبت منها فقد يتمثل الهدف الأولي للحوار الدولي في إرساء قواعد الأدلة اللازمة لإنفاذ قواعد الامتثال للقوانين. ومن هذا المنظور فإن التأكيدات المتعلقة بالمزايا الاقتصادية أو الديناميات السياسية الأساسية توحي كما يبدو بدينامية من نوع الحرب الباردة التي يمكن أن تقوض الأهداف ذاتها التي ستسعى اتفاقية دولية[103] إلى تحقيقها. والأهم من ذلك فإنه إذا كانت تأكيدات المزايا صحيحة فلن تستطيع أي اتفاقية للأمم المتحدة إيقاف هذه العملية.

وعند طرح هدف التخفيف من حدة النزاع السيبراني، فإن إجراء المزيد من التحقيقات الفكرية في المجالات الواردة أدناه سيكفل تنوير مناقشات السياسات الجارية في المحافل الدولية:

1 الديناميات الهجومية/الدفاعية النظرية للأمن الحاسوبي،

2 الديناميات الهجومية/الدفاعية لتطوير الأمن الحاسوبي كمسألة تتعلق بعائد الاستثمار،

3 الإعاقة التي تخلفها النظم الأمنية المتينة على العمليات (المعالجة الحاسوبية، وتخزين البيانات، وإدارة النظم، ووقت الواجهة البينية البشرية)،

4 الحوافز الإجرامية والردع في الجريمة العابرة للحدود،

5 أثر التجسس الحاسوبي على القطاعين العام والخاص.

---

[103] انظر المقال المعنون "مفهوم السلام السيبراني" بقلم هننغ فيغنر في هذا الكتاب.

2.5 دعوة إلى الاستقرار الجيوسيبراني

بقلم جودي ر. وستبي

من المتعذر تحمل وتيرة تصاعد الجريمة السيبرانية. فالجهات الفاعلة المارقة التي تستخدم الشبكات المستعبَدة الاختراقية بصورة معتادة لاستخلاص المعلومات السرية والخاضعة لحقوق الملكية وشن هجمات توزيعية تعطِّل الخدمات التي توفرها نظم الحكومات والشركات. ووفقاً لتقديرات تقرير شركة مكافي *لعام 2009 المعنون "النظم الاقتصادية غير المحمية: حماية المعلومات الحيوية"* فقد أضاعت الجهات التي ردت على استبيان الشركة ما مجموعه 4,6 مليار دولار أمريكي من حقوق الملكية الفكرية وأنفقت زهاء 600 مليون دولار أمريكي لإصلاح الأضرار الناجمة عن خروقات البيانات. وبناء على هذه الأرقام فقد توقعت شركة مكافي أن تكون قيمة الخسائر التي تكبدتها الشركات حول العالم عام 2008 أكثر من تريليون دولار أمريكي. وتثقل أعباء التحديث المتواصل للبرمجيات التشغيلية وبرامج الحماية من الفيروسات كاهل الأفراد، علماً بأن العديد من نظمهم موبوءة ومستخدمة في الهجمات.

وتدرك البلدان أن نظمها التابعة للحكومة وقطاع الأعمال قيِّمة وأن أمنها الوطني والاقتصادي معرض للخطر. وعلى هذا فقد شرعت في تطوير استراتيجيات للحرب السيبرانية وإرساء مراكز قيادة سيبرانية ذات قدرات هجومية ودفاعية. وفي حين أن مثل هذه التدابير مناسبة ومنتظرة، فإن هناك خواء ملحوظاً فيما يتصل بالحوار المتعلق بالسلام السيبراني، بل وحتى بشأن الحفاظ على مستوى مقبول من الاستقرار الجيوسيبراني. وكما جرت الإشارة في المقدمة فإن المؤلف يعرِّف "الجيوسيبرانية" على أنها العلاقة بين شبكة الإنترنت والجغرافيا، والديموغرافيا، والاقتصاد، والسياسة لبلد ما وسياسته الخارجية. أما تعريف "الاستقرار الجيوسيبراني" فهو قدرة كل البلدان على استخدام الإنترنت لاستخلاص منافع اقتصادية، وسياسية، وديموغرافية مع الإحجام عن القيام بأنشطة قد تؤدي إلى أنماط من المعاناة والتدمير لا داعي لها.[104]

وقد يرجع تردد البلدان في الانخراط في مداولات بشأن "الاتصالات الأساسية الدنيا" الضرورية للحفاظ على الوظائف المجتمعية الحيوية ومنع المعاناة والتدمير غير الضروريين الناجمين عن الهجمات السيبرانية، في جانب منه، إلى عدم اليقين العام بشأن سبل مقاربة مثل هذا الموضوع ضمن الإطار القانوني الدولي الراهن.

---

[104] طُرح هذا التعريف لأول مرة في مؤتمر معهد آنسر للأمن الوطني، "Homeland Security 2005: Charting the Path Ahead", University of Maryland, Presentation by Jody Westby, "A Shift in Geo-Cyber Stability and Security", 6–7 May 2002.

قوانين النزاع المسلح

على امتداد التاريخ الحديث تم تحديث القوانين الدولية للنزاع المسلح استجابة لفظائع الحروب وللطرائق الجديدة لخوضها. وثمة حاجة ملحة للقيام بذلك مجدداً لمواءمتها مع القدرات السيبرانية لأن أعمال الحرب السيبرانية ستسفر على الأرجح عن خرق أحكام عديدة في القوانين الحالية المسلحة أو أنها ستكون خارج نطاق هذه القوانين تماماً.

والأطر القانونية الأساسية التي تحكم النزاع المسلحة واسعة وتم وضعها في القرن الماضي عموماً. وتشمل الوثائق الأساسية ذات الصلة بالنزاع السيبراني ما يلي:

- ميثاق الأمم المتحدة[105]
- معاهدة حلف شمال الأطلسي[106]
- اتفاقيات جنيف لعام 1949[107]
- البروتوكول الإضافي لاتفاقيات جنيف الصادر في 12 أغسطس عام 1949 والمتعلق بحماية ضحايا المنازعات الدولية المسلحة (البروتوكول الأول)[108]
- اتفاقيات لاهاي (1899 و1907)[109]
- اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر.[110]

وبالمستطاع تبسيط المقدمات المنطقية الأساسية لهذه الوثائق. فقوانين النزاع المسلح تنظّم تنفيذ الأعمال العدائية المسلحة، وعلى الجهات العسكرية أن تخطط وتنفذ عملياتها ضمن هذه القوانين. وتنطبق القوانين المذكورة على العمليات العسكرية والأنشطة المتصلة بها، وهي تهدف إلى منع المعاناة والدمار غير الضروريين في الحرب. وتتكلف أحكام خاصة بحماية المدنيين، والسجناء، والجرحى، والمرضى، والناجين من حالات غرق السفن.

---

[105] ميثاق الأمم المتحدة، www.un.org/en/documents/charter/index.shtml..

[106] معاهدة حلف شمال الأطلسي، www.nato.int/cps/en/natolive/official_texts_17120.htm..

[107] اتفاقيات جنيف لعام 1949، www.icrc.org/web/eng/siteeng0.nsf/html/genevaconventions.

[108] البروتوكول الإضافي لاتفاقيات جنيف الصادر في 12 أغسطس عام 1949 والمتعلق بحماية ضحايا المنازعات الدولية المسلحة (البروتوكول الأول)، 8 يونيو، 1977، www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 (المشار إليه فيما بعد باسم البروتوكول الأول).

[109] الاتفاقية المتعلقة بقوانين وأعراف الحرب البرية (اتفاقية لاهاي الثانية)، 29 يوليو 1899، http://avalon.law.yale.edu/19th_century/hague02.asp؛ قوانين وأعراف الحرب البرية (اتفاقية لاهاي الرابعة)، 18 أكتوبر 1907، http://avalon.law.yale.edu/20th_century/hague04.asp.

[110] اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر، 28 نوفمبر 2003، www.icrc.org/web/eng/siteeng0.nsf/html/p0811 (المشار إليها فيما بعد باسم "اتفاقية الأسلحة مفرطة الضرر").

كيف تُنفذ الأعمال العسكرية

هناك ثلاثة مبادئ أساسية تتحكم *بالكيفية* التي يمكن بها تنفيذ الأعمال العسكرية وهي: الضرورة، والتمييز، والتناسبية.

الضرورة: يفرض مبدأ الضرورة على القوات المقاتلة الانخراط في تلك الأعمال الضرورية فحسب لإنجاز الأهداف العسكرية المشروعة. ويمكن استهداف المرافق، والمعدات، والقوات العسكرية إذا ما كان ذلك سيقود إلى استسلام العدو بشكل جزئي أو كامل.

التمييز: يتطلب مبدأ التمييز من العسكريين التمييز بين الأهداف المشروعة وغير المشروعة، مثل المدنيين، والممتلكات المدنية، والجرحى. ومن الواجب فصل الأهداف المدنية عن الأهداف العسكرية إلى أقصى درجة ممكنة. أما الهجمات العشوائية فهي تلك التي تضرب الأهداف العسكرية والمدنية/المدنيين على حد سواء.

التناسبية: يحظُر مبدأ التناسبية استخدام القوة التي تتجاوز ما هو ضروري لإنجاز الأهداف العسكرية. ويقارن المبدأ بين المزايا العسكرية المحققة من الهجوم والأذى اللاحق، ويتطلب الموازنة بين المزايا العسكرية المباشرة المنتظرة والإصابات أو الأضرار المدنية.

من الذي يستطيع أن ينخرط في النزاع المسلح

بمقدور *المقاتلين الشرعيين* فقط الانخراط في النزاع المسلح. والمقاتلون الشرعيون هم أشخاص مفوضون من جانب سلطة حكومية للانخراط في الأعمال العدائية. وقد يكون هؤلاء قوة غير نظامية غير أن من الواجب أن يخضعوا لقيادة شخص مسؤول عن المرؤوسين، وأن يرتدوا شعارات مميزة بحيث يمكن تمييزهم عن بعد (مثل البزة أو اللون)، وأن يحملوا أسلحتهم بصورة مكشوفة، وأن ينفذوا العمليات وفقاً للقوانين الدولية للنزاع المسلح.

المقاتلون غير الشرعيين هم أولئك الذين يشاركون مباشرة في الأعمال العدائية دون أن يكون ذلك بترخيص من سلطة حكومية أو ضمن القانون الدولي. ومن الأمثلة على المقاتلين غير الشرعيين المدنيون الذين يهاجمون القوات، والقراصنة، والإرهابيون.

غير المقاتلين هم الأشخاص غير المفوضين من جانب سلطة حكومية بالانخراط في الأعمال العدائية، ولكن لهم علاقة بها. وتشمل هذه المجموعة أشخاصاً مثل رجال الدين، والموظفين المدنيين المرافقين للعسكريين، والطواقم الطبية. ومن غير الجائز أن يكون غير المقاتلين هدفاً لهجوم مباشر، غير أنهم قد يُقتلون كحادث من حوادث الهجوم المباشر.

وإذا لم يكن وضع المقاتل معروفاً تُطبَّق اتفاقيات جنيف حتى البت في وضعه.

ما الذي يمكن استهدافه

إن *الأهداف العسكرية* هي الأهداف التي تسهم، بحكم طبيعتها أو موقعها أو غرضها أو استخدامها، إسهاماً فعالاً في قدرة العدو العسكرية، والتي يؤدي تدميرها أو تحييدها بصورة كاملة أو جزئية وقت الهجوم إلى دعم الغايات العسكرية الشرعية.

أما *الأهداف المحمية* فهي الأهداف التي تحميها اتفاقيات جنيف، مثل المستشفيات، ووسائل نقل الجرحى أو المرضى، والمواقع الدينية أو الثقافية، ومناطق السلامة. غير أنه في حال استخدام أي من هذه المواقع لأغراض عسكرية فإن من الجائز مهاجمتها. وعلى سبيل المثال فإذا ما استخدمت الهيئات العسكرية كنيسة كقاعدة للعمليات، فإنها يمكن أن تصبح هدفاً عسكرياً مشروعاً.[111]

وضمن السياق السيبراني فإن هذه المبادئ تثير بعض المسائل المعلقة وهي:

- ما الذي يشكل نزاعاً سيبرانياً مسلحاً؟
- هل يمكن استهداف البنية التحتية الحيوية؟
- وإذا ما كانت البنية التحتية الحيوية تدعم أهدافاً تحميها اتفاقيات جنيف، فهل يمكن استهداف هذه الشبكات؟
- هل تعتبر الهجمات على البنية التحتية الحيوية ضرورية لتحقيق الغايات العسكرية؟
- كيف يمكن للمشاركين في أعمال العداء التفريق بين الأهداف العسكرية والأهداف المحمية؟
- هل يتناسب التلف اللاحق بالبنية الأساسية الحيوية مع الغايات العسكرية؟
- ما القوة المفرطة في الفضاء السيبراني؟
- ما العلامات المميزة للجنود السيبرانيين؟
- كيف يمكن تقرير أن أطرافاً ثالثة تعمل لصالح دولة قومية؟

وليس هناك من جواب واضح على هذه الأسئلة في ظل القانون الحالي. وعلى سبيل المثال هل تعتبر شبكات اتصالات القطاع الخاص الأمريكي هدفاً عسكرياً مشروعاً وضمن الضرورة العسكرية بالنظر إلى أن نسبة 90 في المائة من اتصالات الحكومة الأمريكية تستخدم الشبكات المدنية، بما في ذلك الإنترنت، والمهاتفة، والهواتف الخلوية، والسواتل؟[112] وبالتأكيد فإن الشركات وحملة الأسهم الذين يملكونها سيحاجون

---

[111] انظر Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace,* Aegis Research Corp., Falls Church, VA, 2000; *The Law of Armed Conflict: Basic Knowledge,* International Committee of the Red Cross, June 2002, http://www.icrc.org.

[112] *The Insider Threat to U.S. Government Information Systems*, National Security Telecommunications and Information Systems Security Committee, NSTISSAM INFOSEC/1-99, www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf.

ضد مثل هذا المنطق. وهو ما ستفعله المستشفيات التي تعتمد اعتماداً كلياً على الشبكات المذكورة؛ وستنظر على الأرجح إلى هذه الهجمات على أنها ضد هدف محمي.

وإذا ما كانت القوانين الدولية للنزاع المسلح تسمح باستخدام القوات غير النظامية، فهل تستطيع الحكومات التعاقد مع مديري الشبكات المستعبَدة الاختراقية واستخدام شبكاتهم كمقاتلين شرعيين في النزاعات السيبرانية؟ ومن الجائز تخويل القوات غير النظامية المشاركة في الأعمال العدائية، ولكن الشبكات المستعبَدة الاختراقية ليست مميزة كما أن أسلحتها غير ظاهرة للعيان.

ولا تحمل العناصر الحاسوبية المنخرطة في شبكة مستعبَدة شعاراً أو علامة مميزة بالتأكيد. بل ربما يتعذر تعقب الأمر وصولاً إلى الحواسيب الفردية لأن الشركات المستعبَدة الاختراقية تنشر برامجها الخبيثة عبر الصفحات الشبكية، وشبكات الاتصال بين الأقران، والوصلات الخبيثة، ومواقع الربط الشبكي الاجتماعي، والرسائل الدعائية المتطفلة. وقد يكون الحاسوب الشخصي العامل كعنصر حاسوبي مستعبَد في هجوم يُشن بأمر من دولة قومية مملوكاً لمدني بريء غير مدرك بأن حاسوبه قد تم اختراقه. وفي حال القبض على مدراء الشبكات المستعبَدة الاختراقية فهل يمكن محاكمتهم كمجرمي حرب؟ وماذا عن مالكي الحواسيب؟

وتحدد اتفاقيتا لاهاي الخامسة والثالثة عشرة حقوق وواجبات البلدان المحايدة فيما يتعلق بالحرب في البر والبحر، لكنها لا تشير إلى الفضاء السيبراني. ولا يجوز لبلد ما تحريك أو نقل قواته عبر إقليم دولة محايدة أو ارتكاب أي عمل من الأعمال العدائية في المياه الإقليمية لبلد محايد، ولكن ماذا عن عبور شبكات البلدان المحايدة؟ وهي ينبغي على البلدان أن تطلب الإذن من البلدان المحايدة لشن هجوم سيبراني عبر شبكاتها؟ ومع تبديل الرزم كيف يمكن للبلدان أن تعرف حتى ما هي الشبكات التي ستُستخدم؟ وهل يمكن لبلد ما استخدام شبكة مستعبَدة اختراقية كقوة غير نظامية إذا ما كانت تشتمل على حواسيب في بلد محايد؟

إن ميثاق الأمم المتحدة، واتفاقيات جنيف ولاهاي، ومعاهدة حلف شمال الأطلسي لا تتناول النزاع السيبراني. ويستخدم ميثاق الأمم المتحدة ومعاهدة حلف شمال الأطلسي على حد سواء مصطلحات من قبيل "السلامة الإقليمية"، و"استخدام القوة المسلحة"، و"عمل من جانب القوات الجوية أو البرية أو البحرية" و"هجوم مسلح"، وهي مصطلحات لا تنسجم مع التصورات السيبرانية مما يضعها ظاهرياً خارج نطاق القانون الدولي. ويوضح النزاعان الإستواني والجورجي بصورة مثيرة عواقب النزاع السيبراني والتشويش المحيط بجهود الرد الناجم عن عدم اليقين بشأن قواعد القانون.[113]

[113] للاطلاع على مناقشة مستفيضة عن النزاعين الإستوني والجورجي والردود والمسائل القانونية انظر Jody R. Westby, "The Path to Cyber Stability," *Rights and Responsibiliites in Cyberspace: Balancing the Need for Security and Liberty",* EastWest Institute and World Federation of Scientists, 2010 at 1, www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty.

دفاعاً عن الاستقرار الجيوسيبراني

تناقش الفقرات الواردة أعلاه بضعة جوانب فحسب من جوانب الالتباس القانونية فيما يتعلق بالنزاع السيبراني. ويكشف استعراض القوانين الدولية للنزاع المسلح عن استعداد تاريخي لتحديث هذه الوثائق بحيث تغطي التكنولوجيات الجديدة، مثل الأسلحة البحرية والطائرات.[114] وهكذا فإن بالمستطاع تعديل هذه الصكوك ذاتها لاستيعاب النزاع السيبراني.

على أن السؤال المهم الأول هو ما هي درجة النشاط التي ينبغي السماح بها؟ ويرى المؤلف أن من الواجب تطبيق أربعة مبادئ في ظروف النزاع السيبراني وهي:

1 *ينبغي حماية قدر معين من البنية التحتية الحيوية لمنع أوجه التدمير، والأذى، والمعاناة غير الضرورية وضمان الحد الأدنى من الاتصالات الأساسية.*

إن البنى التحتية الحيوية المحمية ستشمل البنى التي تدعم المستشفيات، والمرافق الطبية، ومراكز إقامة العجائز، والنظم المالية، ونظم دعم الحياة والأجهزة الطبية الهامة، وسلاسل الإمداد، ووسائل النقل، ومرافق الأخبار، ودور العبادة والمراكز الدينية، والمرافق التعليمية، والمسعفين، وأجهزة إنفاذ القانون. وليس المقصود بالقائمة المعروضة آنفاً أن تكون كاملة، بل أن تقدم أمثلة على أنواع النظم التي تساند المدنيين الأبرياء، بما في ذلك صغار الأطفال، والعجزة، والجرحى، والعجائز. ومن المفروض أن تساعد مساهمات الجهات المعنية الدبلوماسيين في رسم الحدود المقدسة للبنية التحتية الحيوية.

الأساس المنطقي: تدعم القوانين الدولية الحالية للنزاع المسلح هذا المفهوم. *وكما تلاحظ القواعد الأساسية لاتفاقيات جنيف وبروتوكوليها الإضافيين* فإنه:

> في أي نزاع فإن حق أطراف النزاع في اختيار طرق أو وسائل الحرب ليس بالحق اللامحدود. وتنشأ قاعدتان أساسيتان من هذا المبدأ. الأولى تحظر استخدام الأسلحة، والقذائف، ومواد وطرق الحرب التي تتسبب في إصابات غير ضرورية. والثانية تلزم أطراف النزاع، وبغية ضمان احترام وحماية السكان المدنيين والممتلكات المدنية، بالتمييز على الدوام بين السكان

---

[114] انظر مثلاً "حماية الأشخاص المدنيين والسكان في وقت الحرب" المقتطف من القواعد الأساسية لاتفاقيات جنيف وبروتوكوليها الإضافيين، اللجنة الدولية للصليب الأحمر، 31 ديسمبر 1988، www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV (المشار إليها فيما بعد باسم "حماية الأشخاص المدنيين"). ("استدعت التطورات الاستثنائية في الحرب الجوية تطوير القانون الحالي للنزاع المسلح وجعله أكثر تحديدا. وهذا هو موضوع الجزء الرابع أو البروتوكول الأول المضاف إلى الاتفاقية")؛ وأضيفت اتفاقية جنيف الثانية لاستيعاب مسألة استخدام القوات البحرية في البحر والعناية بأمر معالجة الجرحى، والمرضى، وغرقى القوات المسلحة في البحر.

المدنيين والمقاتلين، وكذلك بين الممتلكات المدنية والأهداف العسكرية، وبأن توجه عملياتها نحو الأهداف العسكرية فحسب.[115]

إن الأذى والضرر الناجمين عن تدمير أو تعطيل نظم البنية التحتية الحيوية غير ضروريين وسيتسببان في معاناة ومصاعب جسيمة من النوع الذي هدفت قوانين النزاع المسلح إلى منعه. وفضلاً عن ذلك، ولأن هذه الشبكات تخدم أعداداً ضخمة من السكان، فإن الأذى والضرر المتأتيين من مثل هذا الهجوم سيكونان على نطاق واسع وغير متناسبين مع المزايا العسكرية المستخلصة.

وتساند العديد من أحكام اتفاقية جنيف الرابعة هذا المبدأ المقترح. وتتناول الاتفاقية بشكل محدد مسألة حماية السكان المدنيين ولا سيما حماية الجرحى، والمرضى، والعجزة، والحوامل (المادة 16). وخلال الأعمال العدائية، يجوز لأي طرف في النزاع، أن يقترح إنشاء مناطق محيدة في الأقاليم التي يجري فيها القتال بقصد حماية الجرحى والمرضى من المقاتلين وغير المقاتلين، والأشخاص المدنيين الذين لا يشتركون في الأعمال العدائية ولا يقومون بأي عمل له طابع عسكري (المادة 15). ولا يجوز بأي حال الهجوم علي المستشفيات المدنية المنظمة لتقديم الرعاية للجرحى والمرضي والعجزة والنساء النفاس (المادة 18). ومن الواجب تيسير إعالة الأطفال دون الخامسة عشر من العمر الذين تيتموا أو افترقوا عن عائلاتهم بسبب الحرب، وممارسة دينهم وتعليمهم في جميع الأحوال (المادة 24). ويحظر أن تدمر أي ممتلكات خاصة ثابتة أو منقولة تتعلق بأفراد أو جماعات، أو بالدولة أو السلطات العامة، أو المنظمات الاجتماعية أو التعاونية (المادة 53).

ويستكمل البروتوكول الأول من اتفاقية جنيف الاتفاقية الرابعة ويوسِّع نطاق حماية الأشخاص المدنيين في وقت الحرب. وتتسم المواد 48-59 من هذا البروتوكول بأهمية خاصة. فالمدني هو أي شخص لا ينتمي إلى القوات المسلحة. ويتمتع المدنيون بحماية عامة ضد الأخطار الناجمة عن العمليات العسكرية، ولا يجوز أن يكونوا محلاً للهجوم أو أن يتعرضوا لأعمال تستهدف بث الذعر أو لهجمات العشوائية غير موجهة إلى هدف عسكري محدد (تعتبر الهجمات التي ينتظر أن تتسبب في خسائر عرضية في الأرواح البشرية، أو إصابات، أو إتلاف للأعيان المدنية بشكل يفرط في تجاوز الأهداف العسكرية هجمات عشوائية) (المادة 51). ولا تكون الأعيان المدنية محلاً للهجوم أو لعمليات الثأر؛ وإذا ثار الشك حول عين ما فيجب اعتبارها مدنية (المادة 52). ويحظر ارتكاب أي من الأعمال العدائية الموجهة ضد الآثار التاريخية أو الأعمال الفنية أو أماكن العبادة (المادة 53). ومن المحظور مهاجمة الأعيان التي لا غنى عنها لبقاء السكان المدنيين (مثل المواد الغذائية، والمناطق الزراعية، والمحاصيل، والماشية، ومرافق مياه الشرب وشبكاتها، وأشغال الري (المادة 54). ولا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة، ألا وهي السدود والجسور والمحطات النووية، محلاً

---

[115] "حماية الأشخاص المدنيين والسكان في وقت الحرب" المقتطف من القواعد الأساسية لاتفاقيات جنيف وبروتكوليها، اللجنة الدولية للصليب الأحمر، 31 ديسمبر 1988، www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV

للهجوم، حتى ولو كانت أهدافاً عسكرية مشروعة، إذا كان من شأن مثل هذا الهجوم أن يتسبب في انطلاق "قوى خطرة ترتب خسائر فادحة بين السكان المدنيين" (المادة 56). وتبذل رعاية متواصلة من أجل تفادي السكان المدنيين (المادة 57). وعلى المخطط لهجوم أن يبذل ما في طاقته عملياً للتحقق من أن الأهداف المقرر مهاجمتها ليست أشخاصاً مدنيين أو أعياناً مدنية وأنها غير مشمولة بحماية خاصة، وأن يتخذ جميع الاحتياطات المستطاعة عند تخير وسائل وأساليب الهجوم من أجل تجنب إحداث خسائر عرضية في أرواح المدنيين (المادة 57). ويحظر على أطراف النزاع أن تهاجم بأية وسيلة كانت المواقع المجردة من وسائل الدفاع (ليس فيها عمليات أو قوات عسكرية) (المادة 59).

وبالإضافة إلى ذلك فإن القوانين الدولية للنزاع المسلح تتضمن أحكاماً عديدة أضيفت على مر السنين لحظر استخدام التكنولوجيات مفرطة الأذى أو ذات الآثار العشوائية. ومنذ عهد بعيد يرجع إلى عام 1899 تم اعتماد إعلانات في إطار اتفاقية لاهاي تحظر إطلاق القذائف والمتفجرات من المناطيد أو غيرها من الوسائل الجديدة المماثلة، [116] واستخدام القذائف التي تشتمل على نشر الغازات الخانقة أو المؤذية، [117]، واستخدام الطلقات المتمددة أو المتسطحة.[118] وفي عام 2001 تم اعتماد اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر، وحظرت هذه الاتفاقية طائفة واسعة من الأسلحة الخطرة والمؤذية للغاية، بما في ذلك الأسلحة المشار إليها أعلاه والتي يرجع عهدها إلى عام 1899، وكذلك الألغام، والشراك، والأسلحة الحارقة، وأسلحة الليزر المسببة للعمى، والمتفجرات من مخلفات الحرب.[119] وبالإمكان تعديل هذه الاتفاقية لتشمل الهجمات السيبرانية ضد البنى التحتية الحيوية المحددة.

2 *ينبغي حظر استخدام الشبكات المستعَبدة الاقتحامية والقوات السيبرانية الأخرى غير النظامية.*

الأساس المنطقي: بالنسبة للضحية، وفي مستهل الهجوم، فإنه لا يمكن تمييز هؤلاء المقاتلين عن غيرهم من المهاجمين؛ فالضحية لا يعرف ما إذا كان الشخص الذي يهاجم نظامه هو عنصر داخلي، أو قرصان منفرد، أو جهة فاعلة خبيثة، أو مجرم منظم متطور، أو إرهابي، أو دولة قومية. ومن الصعب تتبع واقتفاء أثر أنشطة الجريمة السيبرانية، ومن المتعذر أحياناً تحديد الجهة الفاعلة، حتى مع الاستعانة

---

[116] إعلان حول منع إطلاق القذائف والمتفجرات من المناطيد (اتفاقية لاهاي الرابعة)؛ 29 يوليو عام 1899، http://avalon.law.yale.edu/19th_century/dec99-03.asp.

[117] Declaration on the Use of Projectiles the Object of Which is the Diffusion of Asphyxiating or Deleterious Gases, The Hague Conference of 1899, 29 July 1899, http://avalon.law.yale.edu/19th_century/dec99-02.asp.

[118] Declaration on the Use of Bullets Which Expand or Flatten Easily in the Human Body, The Hague Conference, 29 July 1899, http://avalon.law.yale.edu/19th_century/dec99-03.asp.

[119] اتفاقية بشأن الأسلحة مفرطة الضرر.

بالمحققين والباحثين المهرة العاملين على القضية. وبالإضافة إلى ذلك فإن من المستحيل تمييز الجنود السيبرانيين التابعين لطرف ثالث لأنهم لا يستطيعون حمل إشارة مميزة، كما أنه لا يمكن تمييزهم بكل تأكيد عن بُعد. وهكذا فإن القوات السيبرانية غير النظامية تخرق إحدى القواعد الأساسية للنزاع المسلح.

3 *على البلدان أن تحترم حياد البلدان الأخرى وألا تنقل أي نوع من الهجمات عبر بناها التحتية الحيوية* (اتفاقيتا لاهاي الخامسة والثالثة عشرة).

يتسق هذا مع اتفاقيات لاهاي التي تقيد نقل القوات أو قوافل الإمدادات أو الذخائر عبر الأقاليم أو المياه المحايدة. وبالمستطاع تدمير العديد من البنى التحتية الحيوية، مثل الشبكات الكهربائية، من خلال فرط تحميل النظام. وهكذا فإن السماح للبلدان بشن الهجمات السيبرانية التي يمكن أن تعبر من خلال العديد من شبكات البلدان الأخرى دون علمها لا يتسق ببساطة مع تاريخ القوانين الدولية للنزاع المسلح والغاية منها. وسيتطلب هذا المبدأ المقترح الحصول على إذن من البلدان الأخرى قبل شن هجوم سيبراني، وبالتالي العمل كرادع ضد شن نزاع سيبراني.

4 *ينبغي أن تساعد البلدان بعضها في التحقيقات المتعلقة بأنشطة الجريمة السيبرانية.*

يعتبر تعاون مزودي خدمات الإنترنت والحكومات الأخرى في التحقيقات المتصلة بأنشطة الجريمة السيبرانية عاملاً حاسماً في ضمان قسط من الاستقرار الجيوسيبراني. وفي حين يبدو من المفارقة أن يُطلب من بلد محايد المساعدة في تحقيق ما، حتى في أوقات الحرب، فإن كل الهجمات السيبرانية تبدو متماثلة في البداية. ولا يمكن للضحية أن يستخلص فكرة عن هوية المهاجم إلا من خلال التحقيقات. وكمبدأ أساسي فإن من الواجب أن تلتزم البلدان التي ترغب في أن ترتبط بالإنترنت، وكذلك مزودو الخدمات العاملون على أراضيها، بتقديم المساعدة في تحقيقات الجرائم السيبرانية. وإذا سُمح للبلدان بالامتناع عن تقديم مثل هذه المساعدة بحجة الحياد، فسيتمتع كل المجرمين السيبرانيين بوقت عظيم في نهبهم للبلدان المنخرطة في الأعمال العدائية. وبمعنى معاكس فإن رفض البلدان المحايدة لتقديم المساعدة سيعني فعلياً أنها تساند وتتواطأ مع المجرمين أو مع البلد المهاجِم. ووفقاً لتصورات الهجمات السيبرانية فإنه لا يمكن لبلد ما أن يظل محايداً إلا من خلال توفير المساعَدة.

تحقيق الاستقرار الجيوسيبراني

خلقت شبكة الإنترنت كوكباً سيبرانياً لا يعترف بالحدود التقليدية ويعمل عموماً خارج سيطرة الحكومات. ويمثل ذلك شكلاً جديداً من أشكال الأسلحة التي تعرض المدنيين، ولا سيما منهم صغار الأطفال، والعجائز، والمرضى، والضعفاء، والمعوقين، لأخطار لم يسبق لها مثيل. كما أنه يقلب قوانين النزاع المسلح رأساً على عقب لأن الأهداف في أي نزاع سيبراني ستكون في غالبها على الأرجح مدنية لا عسكرية وستؤثر على السكان المدنيين لا على القوات العسكرية. وفي معظم البلدان يمتلك القطاع الخاص البنى التحتية الحيوية ويتولى تشغيلها. ولذلك فإن الهجمات على البنى التحتية الحيوية ستكون مكافئة للهجمات

على السكان المدنيين وعلى الشبكات ذاتها التي تساند حياتهم وموارد رزقهم. ولا يمكن التغافل عن إلحاح الحاجة إلى تحديث قوانين النزاع المسلح بما يراعي الأخطار الجديدة لأن *الافتقار* إلى إطار قانوني يمكن أن يُفسر بسهولة على أنها موافقة قانونية على شن الهجمات.

ويدعو بعض الخبراء القانونيين والأمنيين إلى وضع قانون شامل أو إبرام معاهدة بشأن الفضاء السيبراني. وهذا لغط لا طائل من ورائه. وعلى مدى التطورات التي شهدتها الأساطيل البحرية والجوية والتكنولوجيات الأخرى، تمكنت القوانين الدولية للنزاع المسلح من أن تتكيف مع هذه التطورات وظلت تشكل مجموعة متسقة، وإن متطورة، من القوانين. وبالإضافة إلى ذلك فإن هناك اعتبارات عملية. فالمعاهدات محفوفة بالمشكلات؛ إذ إنها تتطلب مداولات مطولة متعددة الأطراف في مرحلة الصياغة، لتفتح بعدها للتوقيع. وبعد هذا يتعين على الأطراف الموقعة المصادقة على المعاهدة قبل أن تدخل حيز التنفيذ، بل وحتى عقب ذلك فإنها لن تكون سارية المفعول إلا بالنسبة إلى تلك البلدان التي صادقت عليها وطبقتها. وكل هذا يحتاج إلى وقت طويل، وهو ما سيكون في صالح الجهات الفاعلة الشريرة والمجرمين السيبرانيين.

ولكن الصكوك القائمة، مثل ميثاق الأمم المتحدة ومعاهدة حلف شمال الأطلسي واتفاقية جنيف واتفاقية لاهاي، تتمتع جميعاً بقابلية التعديل، *كما* أنها تتميز بأنها قد جرت المصادقة عليها وتطبيقها فعلاً كجزء من القوانين الوطنية.

وفي الفضاء السيبراني، الذي تتسم كل دقيقة تمضي فيه بالأهمية، فإن الحل الواضح هو الحل الأمثل. ومن الواجب أن تضم البلدان القومية صفوفها، بمساهمة من الجهات المعنية، لإدخال التعديلات التالية على القوانين الدولية القائمة للنزاع المسلح:

1 ينبغي تعديل ميثاق الأمم المتحدة لاستيعاب النزاع السيبراني وإيضاح أن "السلامة الإقليمية" تشمل البنى التحتية الحيوية، والإتاحة والمنعة والسرية السيبرانية. وعلى وجه الخصوص فإن من الواجب تعديل المادة 42 بما يسمح لمجلس الأمن باتخاذ التدابير اللازمة من خلال الوسائل السيبرانية.

2 ينبغي تعديل ميثاق حلف شمال الأطلسي لإتاحة الدفاع الجماعي بموجب المادة 5. ومن الواجب توسيع نطاق مصطلح "الهجوم المسلح" الوارد في المادة 6(1) بحيث يتجاوز "الأقاليم" و"القوات، والسفن والطائرات" ليشمل الهجمات السيبرانية.

3 ينبغي تعديل اتفاقيات لاهاي بغرض تحريم استخدام القوات غير النظامية في القتال السيبراني وحظر نقل الهجمات السيبرانية عبر شبكات البلدان المحايدة.

4 ينبغي تعديل اتفاقيات جنيف بغرض تحريم الهجمات على البنية التحتية الحيوية التي يمكن أن تعطل الاتصالات الأساسية الدنيا وتعرض السكان المدنيين للخطر.

وثمة مجال واحد يحتاج إلى اتفاقية جديدة. إذ إن من الواجب أن توافق البلدان بصورة منفصلة على التعاون وتقديم المساعدة إلى التحقيقات المتعلقة بالأنشطة السيبرانية التي يُعتقد أنها مرت عبر شبكاتها. وبالنسبة إلى البلدان التي تحجم عن توقيع هذه الاتفاقية فإن من الواجب أن تفقد حق التظلم بموجب القانون الدولي إذا ما قامت البلدان الأخرى بوقف الاتصالات الصادرة عنها.

وستمكّن التدابير آنفة الذكر الدول القومية والناس من منح الثقة لتكنولوجيا المعلومات والاتصالات ومواصلة دمجها بحياتهم ومجتمعاتهم دون خشية من تحولهم إلى أهداف في الصراعات السيبرانية. كما أنها ستكفل البدء بحوار بناءٍ بين البلدان تأتي إليه وهي تحمل، وللمرة الأولى، موقفاً مشتركاً.

6 السلام السيبراني
مفهوم بشأن السلام السيبراني

من إعداد هينين ويجنر

أعِد هذا الكتاب في سياق السلام السيبراني في تناقض مقصود مع الظواهر السلبية المتمثلة في الحرب السيبرانية والإرهاب السيبراني والجريمة السيبرانية. وإن اختيار الجانب الإيجابي من النقيضين "الحرب والسلام" ينطوي على تغيير مهم في منظور ومستوى الأولويات، إذ يوجه الأذهان نحو منافع مجتمع المعلومات وإمكاناته الإيجابية، ثم يحدد هدفاً بعد ذلك من خلال تعزيز الدلالة السلبية للحرب السيبرانية والمصطلحات والمشاكل المتصلة بها، ويثير حركة حيوية في اتجاه ثقافة أمن سيبراني عالمية.

وإن هذه المحاولة الرامية إلى إبراز عدم شرعية الحرب السيبرانية من خلال عكس المنظور، واعية تماماً بأن البنى التحتية الرقمية منتشرة في كل مكان الآن، وبأنها لا محالة سوف تُستخدم أيضاً لأغراض عدوانية وغير سلمية. وبالتالي، فإن الهدف الأهم هو كبح مثل هذه الاستخدامات وفرض أشد قيود ممكنة على أية تطبيقات عدوانية لتكنولوجيا المعلومات والاتصالات. وبما أن مصطلح "الحرب السيبرانية" في حد ذاته يؤدي إلى تحفيز أنماط التفكير العسكري، وتصور الدفاع السيبراني لا سيما من منظور الإجراءات والتقنيات العسكرية ("الإجراءات الانتقامية")، فإن هذا الفصل سيحاول مكافحة هذه التلقائية الذهنية وبلورة التماس من أجل سلوك سلمي في الفضاء السيبراني. لكنه لا يعدو أن يكون أكثر من ملخص للأساس النظري للسلام السيبراني، في حاجة إلى الإثراء مع مرور الوقت. وتساهم بالفعل عدة أقسام أخرى من هذا الكتاب في مهمة التعريف هذه.

وخلال عدد من السنوات، وضع اتحاد العلماء العالمي مفهوم السلام السيبراني في صميم عمله،[120] وساهم مؤخراً الاتحاد الدولي للاتصالات، عن طريق أمينه العام بالتحديد، في زيادة توضيح المفهوم،[121] لكن بالطبع استُخدم المصطلح من قبل، وإن لم يكن على النحو الشامل نفسه. وكان أبرز استخدام للمصطلح، وإن كان استخداماً خاصاً ومحدداً، وهو خاص بالأطفال في هذه الحالة، في سنة 2007 في مصر من أجل الترويج لبرنامج مبادرة للسلام السيبراني في إطار حركة سوزان مبارك الدولية للمرأة من أجل السلام،[122] مع الإحالة إلى إعلان وبرنامج عمل الأمم المتحدة بشأن ثقافة السلام. وتتمثل مهمة المبادرة في تمكين شباب أية أمة،

---

[120] انظر المراجع المختلفة تحت عنواني "منشورات" و"أنشطة" على الموقع www.unibw.de/infosecur، وتحت العنوان الثاني، يوجد تسجيل مؤتمر عُقد في ديسمبر 2008، بعنوان "أزمة الإنترنت العالمية: السعي إلى السلام السيبراني".

[121] مقال "UN Chief proposes int'l accord to prevent cyber war"، الذي نشر في 31 يناير 2010، على الموقع www.thepoc.net/breaking-news/world/3930-un-chief-proposes-intl-a.

[122] حركة سوزان مبارك الدولية للمرأة من أجل السلام، المبادرة الإلكترونية للسلام، على الموقع التالي: http://smwipm.cyber peaceinitiative.org/.

عن طريق بناء القدرات في مجال تكنولوجيا المعلومات والاتصالات، لتحقيق الأمان على الإنترنت وتشجيع الابتكار. كما يرد مصطلح السلام السيبراني أحياناً وبشكل غير منتظم وغير محدد في أنشطة أوساط البحث بشأن السلام.

وفي السياق الحالي، يُفهم السلام السيبراني على نحو أوسع من المفهوم الذي استخدمته حركة سوزان مبارك الدولية للمرأة من أجل السلام، ويقصد منه أن يكون مبدأ أساسياً في إقامة "نظام عالمي للفضاء السيبراني". وإذا كان استخدام المصطلح أقرب إلى السياسة والتركيز السياسي، مع توجيه الذهن نحو الاختيارات الصحيحة، فإن هذا يستتبع أيضاً أنه يجب أن يبقى غير مقيد إلى حد ما. ولا يمكن أن يكون التعريف جامداً، بل يجب أن يكون بديهياً، ومتنامياً في قائمة العناصر التي يشملها.

ومع ذلك، لا بد من تعريف أساسي. ويجب أن تكون نقطة البداية بالنسبة لأية محاولة تعريف كهذه هي المفهوم العام للسلام كحالة هدوء نافعة، وغياب الفوضى أو الاضطراب والعنف- وليس المقصود فقط غياب العنف "المباشر" أو استخدام القوة، بل أيضاً غياب القيود غير المباشرة. ويعني السلم سيادة المبادئ القانونية والأخلاقية العامة، وإمكانيات وإجراءات تسوية النزاعات والاستدامة والاستقرار.

ونحن ممتنون للجمعية العامة للأمم المتحدة لمحاولتها الشاملة لتحديد معنى ذي مغزى لمفهوم السلام - ومفهوم ثقافة السلام. ويقدم الإعلان وبرنامج العمل بشأن ثقافة السلام الصادر عن الجمعية العامة للأمم المتحدة في أكتوبر 1999[123] قائمة من العناصر والشروط الأولية للسلام ويرسمان الطريق لتحقيقه وحفظه من خلال ثقافة للسلام. ويصف القرار هذه العناصر وصفاً مستفيضا، مذكراً بالميثاق التأسيسي لمنظمة الأمم المتحدة للتربية والعلم والثقافة، الذي ينص على ما يلي: "لما كانت الحروب تتولد في عقول البشر، ففي عقولهم يجب أن تُبنى حصون السلام"، وبعد ذلك يحدد القرار نقاط العمل بالنسبة للعقد حتى عام 2010.

ولا تقتصر الجوانب المهمة للسلام وثقافة السلام على عدم استخدام القوة، وتعزيز وممارسة عدم العنف، بل تشمل مجموعة مشتركة من قيم وأساليب سلوكية ونظام دولي ومشروعية وإجراءات تشاركية حيوية وإيجابية وحقوق الإنسان (ومنها التمسك بمبادئ الحرية والعدالة والديمقراطية والتسامح والتضامن والتعاون والتعددية والتنوع الثقافي والحوار والتفاهم وتعزيز تسوية النزاعات). وفضلاً عن العناصر الأخلاقية للسلام التي تحظى بكثير من التركيز، من المهم بشكل خاص في السياق السيبراني أن تشمل قائمة الشروط الأولية للسلام احترام وتعزيز حق كل شخص في حرية التعبير والرأي والإعلام والحصول على المعلومات. وتبقى هذه الإحالات بالطبع مجرد إحالات استرشادية، إذ يمكن قراءة القرار بكامله بعناية. وقد صاغ الاتحاد مؤخراً خمسة مبادئ للسلام السيبراني، تحدد أيضاً إجراءات والتزامات معينة من شأنها أن تضمن السلام والاستقرار في الفضاء السيبراني. ويُنصح القارئ بالرجوع إلى هذه القائمة لأهميتها الحيوية.

---

[123] "إعلان بشأن ثقافة السلام"، اليونسكو، A/Res/53/243، على الموقع التالي: www.unesco.org/cpp/uk/declarations/2000.htm.

وقام اتحاد العلماء العالمي، من جانبه بترجمة المبادئ العامة التي يتضمنها القرار، وغيرها من المبادئ العامة التي أقرتها الأمم المتحدة والتي يمكن تطبيقها في البيئة السيبرانية بمزيد من التفصيل، في "إعلان إيريس بشأن مبادئ الاستقرار السيبراني والسلام السيبراني" في أغسطس 2009.[124] ويبين هذا الإعلان أن تحقيق الاستقرار السيبراني وتحقيق السلام السيبراني أمران متداخلان تداخلاً وثيقاً. ويتسم الإعلان بالإيجاز ويركز على العناصر التشغيلية الأساسية للسلام السيبراني. وهي كالتالي:

1 ينبغي لجميع الحكومات الاعتراف بأن القانون الدولي يضمن للأفراد التدفق الحر للمعلومات والأفكار؛ وتنطبق هذه الضمانات أيضاً على الفضاء السيبراني. وينبغي عدم فرض القيود إلا عند الاقتضاء، على أن تخضع لعملية مراجعة قانونية.

2 ينبغي لجميع البلدان العمل معاً لوضع مدونة مشتركة للسلوك السيبراني وإطار قانوني عالمي منسق، بما في ذلك أحكام إجرائية تتعلق بالمساعدة في التحقيق والتعاون بما يكفل احترام الخصوصية وحقوق الإنسان. وينبغي لجميع الحكومات وموفري الخدمات والمستعملين دعم الجهود المبذولة في سبيل إنفاذ القانون الدولي ضد مرتكبي الجرائم السيبرانية.

3 وينبغي لجميع المستعملين وموفري الخدمات والحكومات العمل معاً لضمان ألا يستخدم الفضاء السيبراني بأي شكل من شأنه أن يفضي إلى استغلال المستعملين، لا سيما الشباب والمستضعفين منهم، من خلال العنف أو الإذلال.

4 ينبغي للحكومات والمنظمات والقطاع الخاص بما في ذلك الأفراد، تنفيذ برامج شاملة للأمن وتحديثها بناءً على أفضل الممارسات والمعايير المقبولة دولياً واستعمال تكنولوجيات حماية الخصوصية والأمن.

5 ينبغي لمطوري البرمجيات والمعدات السعي إلى تطوير تكنولوجيات آمنة تعزز القدرة على التصدي وتقاوم نقاط الضعف.

6 ينبغي للحكومات أن تشارك بفعالية في جهود الأمم المتحدة الرامية إلى النهوض بالأمن السيبراني والسلام السيبراني في العالم وأن تتفادى استعمال الفضاء السيبراني من أجل النزاعات.

ويمكن أن يستشف المرء وراء هذه المبادئ، ولا سيما المبدأ السادس، الإرادة الصارمة من أجل كبح إمكانية النزاعات في الفضاء السيبراني. وفي الواقع لا بد، في إطار السعي إلى السلام السيبراني، وفي ضوء الزيادة المهولة لقدرات "الحرب السيبرانية" العدوانية، من التركيز بشكل خاص على الجانب الحربي للأنشطة في الفضاء السيبراني التي تقوم بها الحكومات وجهات فاعلة غير حكومية على حد سواء.

وتعالَج هذه المشاكل بالتفصيل في أجزاء أخرى من هذا الكتاب. ومع ذلك ترد بعض البيانات المبدئية في هذا السياق توضيحاً للسلام السيبراني. وما زال الفضاء السيبراني، إلى حد كبير جدا، فضاءً بدون قوانين،

---

[124] "إعلان إيريس بشأن مبادئ الاستقرار السيبراني والسلام السيبراني"، اتحاد العلماء العالمي، أغسطس 2009، على الموقع التالي: www.ewi.info/system/files/**Erice**.pdf.

يسمح لأي شخص بفعل ما يشاء بدون مبادئ توجيهية أو عقوبات، مما يجعله يبدو وكأنه يرخص اقتراف أفعال خارجة عن القانون. ومن هنا يأتي النداء إلى وضع قواعد مشتركة للسلوك السيبراني في جميع مجالات النشاط الرقمي. وقد دعا الاتحاد العالمي للعلماء منذ سنة 2001 إلى العمل من أجل وضع قانون عالمي للفضاء السيبراني، من الأفضل أن يكون تحت رعاية الأمم المتحدة.[125] وسيكون ذلك أنفع ما يكون في مجال الاستخدامات العدوانية والعسكرية للفضاء السيبراني.

ولا يخفى على أحد الطابع المعقد لهذه المهمة والحواجز القانونية، وربما قبل كل شيء- الحواجز السياسية التي تعترض هذا الطريق. ومثلما ذُكر في مكان آخر في هذا الكتاب، فإن القوانين التقليدية للحرب والنزاع المسلح مبهمة أو ذات فائدة جد محدودة بالأحرى، كما أن التعاريف غير موجودة. وإن الإحالات إلى الحدود التقليدية للنزاع في النصوص الأساسية للقانون الدولي، مثل ميثاق الأمم المتحدة أو معاهدة الناتو، إحالات عديمة الفائدة إلى حد كبير في هذه الحالة. ويمكن القيام في أفضل الأحوال بقياسات ومقارنات بسيطة وغير تامة[126] انطلاقاً من نصوص اتفاقيات جنيف وبعض قرارات واتفاقيات الجمعية العامة للأمم المتحدة، المتعلقة مثلاً بمجال الجريمة المنظمة عبر الوطنية أو الإرهاب أو السلوك في الفضاء الخارجي. وليس بالأمر الواضح "الحد من السلاح" أو تعيين الحدود بين الاستخدام الشرعي وغير الشرعي لتكنولوجياالمعلومات والاتصالات أو بين الاعتداء والدفاع، بما أن التكنولوجيات متماثلة، وبما أن مشكلة "الاستخدام المزدوج" التي تعرقل مساعي الحد من السلاح في جوانب عديدة جداً هنا أصبحت مستوطنة. وإلى جانب هذا، فإن مأزق التتبع والتعقب- نَسب الأعمال إلى أصحابها بشكل موثوق وفي أطر زمنية مناسبة- الذي يجعل من ملاحقة جريمة سيبرانية "بسيطة" مشكلة عويصة، يتفاقم في الميدان العسكري بسبب احتمال أن يزيد المهاجم المعتدي إلى أقصى حد من تقنيات التهرب والتمويه المتطورة. ومن المستحيل تقريباً القيام بالتحقق الذي يشكل مكوناً أساساً من مكونات الحد من السلاح. ولا يمكن تطبيق الردع بمعناه التقليدي عندما تكون شروطه الأساسية (النسب، وتحديد موقع المصدر، ومستوى الاستجابة) غير متوفرة. وبالتالي، من المنطقي أن أصوات قوية في مؤلفات عديدة تأييداً للمراهنة على الدفاع السيبراني (بما فيه الدفاع

---

[125] انظر "*Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwa*"، تقرير وتوصيات، فريق الرصد الدائم المعني بمجتمع المعلومات والتابع لاتحاد العلماء العالمي، 19 نوفمبر 2003، تقرير مقدم إلى القمة العالمية لمجتمع المعلومات، www.itu.int/dms_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf.

[126] بسيطة لكنها لا تعني غير مهمة بالمرة.

انظر Sergei Komov, Sergei Korotkov, Igor Dylewski, "Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law," *ICTs and International Security*، معهد الأمم المتحدة لبحوث نزع السلاح. 2007، على الموقع التالي:
www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?fecvnodeid=128420&dom=1&groupot593=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&fecvid=21&ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&v21=128420&lng=en&id=47166 .

السيبراني "الموسع" ليشمل الحلفاء) بدلاً من المراهنة على الردع السيبراني في حد ذاته، باعتبارها الخيار الأنسب.[127]

بيد أنه، إذا أُخذ مفهوم السلام السيبراني مأخذ الجد، فإن من الضروري وجود إطار قانوني لتعريف ما الذي يشكل خرقاً للسلام، وينبغي ألا تتخاذل الدول بسبب العيوب المتأصلة في مثل هذا الإطار. وقد اقترح الأمين العام للاتحاد الدولي للاتصالات، في مفهومه الذي ينطلق من المبادئ الخمسة للاتحاد، أنه ينبغي للأمم أن تتعهد في هذا الإطار بألا تبدأ بالعدوان السيبراني ضد أمة أخرى ("عدم المبادأة")، وينبغي أن تلتزم بعدم حماية الإرهابيين السيبرانيين والمهاجمين في بلدانها دون أن تعاقبهم.[128] ويمكن أيضاً تشجيع الأمم على إبرام مواثيق ثنائية أو متعددة الأطراف بشأن عدم الاعتداء السيبراني. ويمكن أن تكون هناك التزامات متبادلة بعدم مهاجمة الهياكل الأساسية الوطنية الحساسة (لا سيما تلك التي لها أهداف إنسانية أو التي تلبي احتياجات الناس الأساسية، والتي يكفل القانون الدولي الحالي حمايتها نوعاً ما) ويمكن تأكيد ضرورة عدم الإضرار بشبكات البيانات العابرة للحدود. وستكون إحدى الخطوات العظيمة والشجاعة هي التأكيد في صك دولي على عدم شرعية الأسلحة السيبرانية المؤذية والاستراتيجيات العدوانية لاستخدامها.

وعلى أرض الواقع، من المرجح ألا تستطيع هذه الاستراتيجيات والمبادئ المصممة لتعزيز السلام السيبراني الاعتماد على الدعم التلقائي للعديد من البلدان التي استثمرت بالفعل وما زالت تستثمر بشكل كبير تحسباً لإمكانية نشوب حرب سيبرانية، مستغلة الفراغ القانوني الحالي في مجال الفضاء السيبراني. وفي الحقيقة، فإن التقارير الحالية بشأن "التسليح" المنتظم للفضاء السيبراني، واستحداث قيادات سيبرانية ووضع استراتيجيات سيبرانية عدوانية، وغير ذلك، لا تبشر بالخير بأي شكل من الأشكال. كما لا ينبغي التقليل من شأن الانعكاسات الأخلاقية وللإجراءات المضادة متعددة الأطراف. وإن الشرعية لأداة مهمة من أدوات فن الحكم لأي دولة، ومن شأن مجرد رسم الخطوط الحدودية للعمل ووضع المعايير والاتفاق عليها أن يولّد مع مرور الوقت الزخم والحافز. ولا بد للسلم السيبراني من إجراءات تنفيذ محددة لكي يساهم في الاستقرار السيبراني والحقوق الأساسية.

ويمكن الاستشهاد بمنطق قوي تأييداً لهذه الغاية. فسير عمل هيكل الشبكة العالمية المترابطة واستقرارها والثقة الموضوعة فيها من المنافع العامة المشتركة. ومن الصعب التحكم في الهجمات السيبرانية الضخمة حتى وإن كانت في جزء فقط من النظام، وقد يكون من غير الممكن إحصاء عواقبها؛ وهناك نزعة طبيعية لإطلاق

---

[127] انظر على سبيل المثال، Martin C. Libicki “Cyber deterrence and Cyberwar”, Santa Monica, 2009, p. 158 et. seq.

[128] انظر الفصل "سابعاً".

العنان لسلسلة ردود الأفعال حتى عندما يتعلق الأمر بحوادث بسيطة.[129] وقد تؤدي ردود الأفعال هذه بشكل حاسم إلى قلب موازين القوة وزعزعة الاستقرار الجغرافي للبيئة الرقمية الكاملة التي يعتمد عليها المجتمع، مما قد يتعدى إلى حد كبير مجرد أطراف النزاع. والانشغال بالحفاظ على الشبكات وهياكل المعلومات العابرة للحدود انشغال مشترك بين جميع الجهات الفاعلة الدولية.

ولا حاجة إلى حجج على أن الأعمال السيبرانية العدوانية غير المستحثة، وأية هجمة سيبرانية في الواقع، هي أعمال لا تتماشى مع مبادئ السلام السيبراني.

لكن المفهوم يجتاز اختباره الحاسم عندما يتعلق الأمر بتعريف وتقييم *رد الفعل* تجاه هجمات سيبرانية متوقعة أو حقيقية، في حالة *وقوع* نزاع سيبراني. وبالنسبة لما إذا كان يُفهم- أو عندما يُفهم- الهجوم السيبراني على أنه هجوم مسلح أو لا: هناك اتفاق عام على أن المبدأ السائد في القانون الدولي والمتعلق بالحق في الدفاع عن النفس *بمعناه العام* المتمثل في شرعية حماية النفس وتفادي الاعتداء، مبدأ قائم. ومثلما ذُكر مراراً وتكراراً في هذا الكتاب، لا بد من تعريف العمل العدواني باعتباره "هجوماً مسلحا"، بالمعنى الوارد في ميثاق الأمم المتحدة ومعاهدة الناتو والقانون الدولي العام، للتمكين من الدفاع الفردي والجماعي المشروع *بواسطة الوسائل العسكرية*. ويمكن القول بالتأكيد إن هجوماً سيبرانياً على دولة أخرى أو ذا عواقب في دولة أخرى هو بمثابة "هجوم مسلح" أو معادل له، على الأقل عندما يستتبع دماراً كبيراً أو خسائر في الأرواح البشرية.[130]

ويمكن أن يوفر هذا الأساس القانوني للعمل الجماعي، بما في ذلك عن طريق الوسائل العسكرية. لكن تعريف وفرصة العمل الانتقامي العسكري في سياق تكنولوجي رقمي يستدعي تفكيراً متزناً وجديداً كما يستدعي، في التحليل الأخير، سياسة لضبط النفس بشكل متعمد.

وإن الاختلافات بين النزاع السيبراني و"الحرب" التقليدية الحركية مذهلة وتتعدى الاختلاف الواضح في "الأسلحة" المستخدمة. وتلخيصاً للحجج المقدمة في عدة أقسام أخرى من هذا الكتاب، وفي هذا الفصل بالذات، هناك في المقام الأول الارتياب في نسب الهجمات السيبرانية، ومستويات نسبها، مما يؤدي إلى عدم اليقين بشأن الهدف الذي ينبغي أن توجه إليه أية تدابير مضادة أو إجراءات انتقامية- أي ضد من ستُوجّه

---

[129] "لا بد أن يكون المجتمع الدولي على وعي بأن مناوشة سيبرانية صغيرة قد تكون خطوة أولى نحو نزاع سيبراني كبير من شأنه أن يؤجج شرارة اشتباك حركي إقليمي تكون له عواقب دولية." نص مقتبس عن جون بومغارنر، رئيس قسم التكنولوجيا، وحدة النتائج السيبرانية في الولايات المتحدة، مجلة "*Jane's Defence Weekly*"، 29 سبتمبر 2010 على الموقع التالي: www.jdw.janes.com (المشار إليها فيما بعد "Jane's").

[130] في وقت كتابة هذا النص، كانت الأمم الأعضاء في الناتو بصدد التفكير في قرارات جماعية بشأن التهديدات الجديدة، بما فيها الهجمات السيبرانية، في سياق التحضير لاجتماع قمة للدول الأطراف في معاهدة واشنطن (20 نوفمبر 2010). وفي حالة ما أدرجت هذه الهجمات على قائمة الأعمال التي تدفع إلى الدفاع الجماعي، سوف تطبق المادة 4 (المشاورات المشتركة) والمادة 5 (المساعدة المتبادلة باتخاذ أي إجراء "يعتبر لازماً، بما في ذلك استخدام القوة المسلحة").

بطريقة قانونية؟ ومن جهة ثانية، ونظراً لانتشار الشبكات والنظم الرقمية في كل مكان وترابطها، لا يمكن التنبؤ بعواقب التدابير المضادة الرقمية ومن ثم يصعب تقدير الأثر التصاعدي لأية تدابير مضادة. وثالثا، قد يندلع النزاع السيبراني في شكل هجوم منسق كبير ومعوّق بالتالي، أو قد يأخذ شكل حالة هادئة وإن كانت سائدة من التهديدات الضعيفة والمتواصلة (التجسس السيبراني أو استحداث برامج تسلل غير معترف بها أو غير ذلك) مع درجات متفاوتة من إمكانية تطورها إلى تدمير بعيد المدى للبنى التحتية. وفي سياق نزاع بين دولتين، هناك عنصر جديد وهو أن عدد الجهات الفاعلة الممكنة لا حصر له؛ ولا يمكن ببساطة نقل دروس الحرب الباردة التي شهدها النصف الثاني من القرن الماضي، وتحقيق التوازن العسكري النووي بين قوتين مع مزيجه الفريد من الردع وضبط النفس، إلى سيناريو عدواني تتعدد فيه الجهات الفاعلة. وأخيرا، ومثلما أُكد مسبقاً، هناك مصلحة مشتركة للجميع في الحفاظ على سير عمل البنى التحتية العالمية للمعلومات.

ويجب أن تُبلور هذه الاختلافات وغيرها من الاختلافات التي يمكن ذكرها، تفكيرنا بشأن التصدي للهجوم. وفي إطار مفهوم السلام السيبراني، يجب أن تُمنح الأولوية للحفاظ على بيئة سالمة ومستقرة أو إحلالها بشكل مبكر. ويشدد هذا بوضوح على الدفاع.

وإن الدفاع الوقائي عن النفس هو الأساس نحو ردود أفعال متناسبة مع السلام. وفي إطار هذا المفهوم، ينبغي الإقرار بوجود مسؤولية مشتركة بين جميع أصحاب المصالح الرقمية فيما يخص تجهيز أنفسهم بشبكات ونظم آمنة، وهذا شرط أيضاً من الشروط التي نص عليها إعلان إيريتشي. ويكتسي التعاون بين الشركات والحكومات الأهمية نفسها التي يكتسيها التعاون الدولي. والمصطلح الجوهري هو القدرة على التصدي: ولا يقتصر هذا على جودة النظم فقط، بل يجب أن تساهم إدارة النظم أيضاً في صمودها وثباتها أمام الهجوم. وينبغي لأصحاب المصالح إذكاء الوعي على نحو أمثل بحالة شبكاتهم، وتحديد نقاط قوتها عالية القيمة ومعالجة نقاط ضعفها (رصد الشبكة بكاملها في الوقت الفعلي، وتطبيق المناطق الآمنة، وتجزئة الشبكة، وضمان أمن الطاقة). ونتيجة لذلك، ينبغي أن تُتاح على نطاق واسع نظم وبرامج حاسوبية متينة تتقيد بشدة البروتوكولات والمعايير الأمنية الصادرة عن الاتحاد الدولي للاتصالات وعلى المستوى الوطني. فالبنى التحتية المتينة لتكنولوجيا الاتصالات تحبط الهجمات، وتساهم في إرساء بيئة آمنة. ويمثل الدفاع المحكم مكوناً من المكونات الأساسية للاستقرار السيبراني؛ حيث أن عمليات الدفاع المحكم تردع الهجمات كما أنها تساهم في تحقيق الثقة وتمكن المشغلين من الشعور بالراحة.

وتشمل القدرة على التصدي، من حيث تعريفها العام، عدة عناصر منها قدرة الأنظمة على التعافي ذاتياً وتوافر أنظمة الإنذار وقدرات الدعم الاحتياطي المدمجة، كما تشمل أنماطاً سلوكية مدربة مثل استكشاف مجالات التعاون داخل مجتمع أصحاب المصلحة كجزء من بيئة سالمة، وزيادة تقاسم المعلومات، وبشكل مختصر، وينبغي التشديد على الإجراءات الإيجابية والتشجيع الضروري لممارستها. ويمكن أيضاً للدول التي تفكر وترغب في التصدي لسيناريوهات نزاع سيبراني ممكن، أن تفكر في أنشطة تنظيمية رفيعة المستوى، مثل مذكرات تفاهم بشأن عدم الاعتداء السيبراني وترتيبات الشفافية فيما يخص نشر صور العدو ومراقبة الأعمال العدائية وتقاسم المعلومات مما يسمح بنسب الأعمال إلى مرتكبيها في حالة النزاع. وقد أُدرج

العديد من هذه المقترحات أيضاً في المقترح السالف الذكر الذي تقدم به الأمين العام للاتحاد الدولي للاتصالات. وتكتسي الآلية العالمية الحديثة للإنذار المبكر (مركز الاستجابة العالمي (GRC) أو برنامج نظام الإنذار المبكر للشبكات (NEWS) أو برنامج المنصات الإلكترونية الآمنة لتطبيقات الخبراء التعاونية (ESCAPE)) أهمية واضحة في السماح باستجابات غير عنيفة. وينبغي لأطر التعاون الدولي أن تستخدم شبكات أفرقة التصدي للطوارئ الحاسوبية (CERT) الآخذة في التوسع.

وعلى الرغم من هذا، ينبغي التحسب لسيناريوهات النزاع السيبراني الجسيم التي لا يكفي فيها مجرد موقف دفاع سلبي، ويجب الاستشهاد على نحو فعال بالحق في الدفاع عن النفس الذي ينص عليه القانون الدولي. ومن منظور للسلام السيبراني، ستكون هنا أيضا المقارنات مع القانون التقليدي للنزاعات المسلحة غير مناسبة. فهي تنطوي على احتمالات أن يؤدي الإطار الذهني المستحدث إلى سيناريوهات حرب عسكرية انتقامية والمنطق العسكري المتمثل في تدمير ممتلكات العدو بأقصى حد. وقد يؤدي الالتجاء إلى قواعد الاشتباك المتأصلة إلى نتائج خطيرة. ولا يتطلب السلام السيبراني التخلي تماماً عن التدابير المضادة العدائية والانتقامية، ولكنه يؤثر نوعاً ما في السيناريوهات التي يمكن تطبيقها بشكل رئيسي.

وهنا سيكون المصطلح الجوهري في رسم الاستجابات هو *ضبط النفس*. وستشمل عناصره تحليلاً قوياً ومستمراً للتهديدات والأخطار للحيلولة دون وقوع نتائج لا يمكن التحكم فيها فيما يخص إعاقة الشبكات السيبرانية الشاملة؛ والتركيز على الاستجابات المختارة بحكمة وغير التصعيدية؛ والصبر والتوقيت الملائم في الاستجابة من أجل السماح بتحسين إمكانية نسب الهجوم إلى صاحبه وتفعيل قدرات الدعم الاحتياطي وتحالفات الدفاع مع النظراء؛ والعناية الفائقة في تطبيق مبادئ التناسب والضرورة اللازمة في الترخيص بالدفاع عن النفس؛ والحماية الدقيقة للبنى التحتية الأساسية ذات الطابع الإنساني أو الاجتماعي الضروري.

وفي حين قد يكون من قبيل المبالغة القول إن الدفاع في إطار التصدي للهجمات السيبرانية هو *دائماً* الاعتداء الأفضل، يبدو أن السلام السيبراني في هذا التحليل يتطلب إلى جانب وضع حدود صارمة للانتقام، مبدأ منح الأولوية للدفاع الكامل عن النفس على الاعتداء.[131] ويبدو هذا المبدأ متوافقاً مع النداء إلى نزع التشديد باستمرار على عدم شرعية "الأسلحة" السيبرانية والاستراتيجيات السيبرانية العدائية على مستوى الدول مثلما نُوقش أعلاه.

[131] "لم يكن بإمكان كلوسويتز التنبؤ بأن الاعتداء الأفضل في القرن الواحد والعشرين سيكون دفاعاً سيبرانياً قوياً". من مجلة Jane's.

7 الاستجابة الدولية للحرب السيبرانية

بقلم الدكتور حمدون إ. توريه

1.7 السياسات والنهج الوطنية

تستجيب بلدان العالم للتهديد الجديد المتمثل في الحرب السيبرانية بشتى الطرق. وعلى الرغم من أن بعض الدول بدأت لتوها بمعالجة قضية الأمن السيبراني[132]، فإن معظم الحكومات على أقل تقدير، تعترف بضرورة إعادة توزيع الموارد وإصلاح استراتيجيات الأمن الوطنية على بعض المستويات. وتبادر كثير من البلدان إلى زيادة التمويل وبحث الموارد التكتيكية والدبلوماسية لتعزيز أمنها السيبراني.[133] وتلجأ بعض البلدان إلى استخدام "الثغرات الجوية" – محاولة عزل شبكات محددة من خلال عدم ربطها بأنظمة أخرى – لحماية الهياكل والأنظمة الحيوية للمعلومات من التعرض للهجمات.[134] وتعرض الفقرات التالية النهج المختلفة التي تبنتها مختلف الدول.

أ) دمج القدرات السيبرانية في استراتيجية الحرب التقليدية

تقوم بعض البلدان باستكشاف إمكانية اتباع نهج حربي تقليدي عندما يتعلق الأمر بمناورات سيبرانية، مما يجعلها تصمم أسلحة سيبرانية هجومية وقدرات دفاعية أيضاً. وهي تعتبر الأسلحة السيبرانية بمثابة "مضاعِفات القوة" التي ينبغي استعمالها في المقام الأول بالاقتران مع الأعمال العسكرية الأكثر تقليدية من أجل تعزيز قدراتها الحربية بشكل كبير.[135] وأصبحت الإنترنت على مدى السنوات الأخيرة من الوسائط الهامة لتبادل المعلومات والأنشطة الدعائية أثناء النزاعات المسلحة. وبهذا الصدد، فإن العديد من البلدان تعتبر إتلاف المعلومات على الإنترنت شكلاً من أشكال الاعتداء العسكري ضد معنويات الجمهور ومن ثم تكون

---

[132] مثلاً أعلنت جنوب إفريقيا مؤخراً (فبراير 2010) عن نيتها بدء صياغة سياسة وطنية منسقة للأمن السيبراني. "Notice of Intention to Make South African Cybersecurity Policy,"، جمهورية جنوب إفريقيا، الجريدة الرسمية رقم 32963 بتاريخ 19 فبراير 2010، www.pmg.org.za/files/docs/100219cybersecurity.pdf.

[133] "Cyberwar: Sabotaging the System – 60 Minutes – CBS News,"، 8 نوفمبر 2009، www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml (تقرير يفيد أن الولايات المتحدة خصصت 17 مليار دولار أمريكي للمبادرات الهجومية والدفاعية).

[134] David Eshel, "Israel Adds Cyber-Attack to IDF," *Military.com,* 10 فبراير 2010، www.military.com/features/0,15240,210486,00.html (hereinafter "Eshel").

[135] Kevin Coleman, "Russia's Cyber Forces,"، *DefenseTech*، 27 مايو 2008، http://defensetech.org/2008/05/27/russias-cyber-forces/.

مستعدة للتصدي للتهديدات السيبرانية باستخدام القوة العسكرية.[136] وتبين الأحداث التي وقعت مؤخراً المتعلقة بتسرب وثائق عسكرية سرية من الأسباب التي تجعل الدول قلقة بشأن العواقب المحتملة لأوجه الضعف السيبراني بالنسبة إلى الدعم المعنوي والعام.[137] وقد أشار بعض موظفي الدولة في الماضي إلى أنهم يعتبرون مناورات حرب المعلومات أعمالاً عسكرية سواء أسفرت عن خسائر أم لا، وبناءً على ذلك، فإن الاستجابة العسكرية قد يكون لها ما يبررها.[138]

ب) اعتماد النُهج السيبرانية كمورد وطني

من خلال إعادة توزيع الموارد والتمويل والتخطيط الاستراتيجي، تتعامل عدة بلدان مع بنيتها الرقمية وتكنولوجيا المعلومات والاتصالات باعتبارها مورداً وطنياً أو قيمة استراتيجية. وقد أعربت بعض البلدان عن ذلك بوضوح كسياسة وطنية جديدة.[139] وحولت البلدان بعض موارد الميزانية إلى مبادرات الفضاء السيبراني، حيث وضعت جانباً مبالغ كبيرة خصصتها للبحث وتطوير قدرات الحرب السيبرانية.[140] وقد أعلنت حكومات عديدة عن خطط وطنية متكاملة وبدأت تنفيذها للتصدي للتهديدات السيبرانية الجديدة، وتعبئة

---

[136] "Gregory Asmolov, "Russia: New Military Doctrine and Information Security، Global Voices، 23 فبراير 2010، http://globalvoicesonline.org/2010/02/23/russian-military-doctrine/ (يصف المبدأ العسكري الحديث لروسيا، الذي يصنف حرب المعلومات باعتبارها شكلاً من أشكال الاعتداء العسكري).

[137] انظر مثلاً، "Jo Biddle, "AFP: Huge leak of secret files sows new Afghan war doubts، 27 يوليو 2010، www.google.com/hostednews/afp/article/ALeqM5gZkjOIqwM0xJDr0u5fPrc5rxdEQg.

[138] Congressional Research Service, *Cyberwarfare*، RL30735، جرى تحديثه في 19 يونيو 2001، www.fas.org/irp/**crs**/RL30735.pdf. (يورد على سبيل المثال استبعاد مسؤول عسكري روسي إمكانية تصنيف حرب المعلومات كعمل غير عسكري)، (فيما بعد "CRS Cyberwarfare"). انظر ايضاً Peter Beaumont, "US appoints first cyberwarfare general،" *Guardian.co.uk*، 23 مايو 2010، www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general/. أشارت الولايات المتحدة أيضاً إلى أنها يمكن أن تنظر في استخدام النهج العسكري التقليدي للاستجابة للهجمات السيبرانية) (فيما بعد، "Cyber General").

[139] الرئيس باراك أوباما، "Remarks by the President on Securing Our Nation's Cyber Infrastructure،" البيت الأبيض، 29 مايو 2009، www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (تصريح بأن البنية التحتية الرقمية للبلد يُمكن أن يُنظر إليها الآن باعتبارها "مورداً وطنياً استراتيجياً" وأنها حمايتها تمثل "أولوية من أولويات الأمن الوطني").

[140] إيران (تقدر الميزانية المعتمدة للحرب السيبرانية في إيران بحوالي 76 مليون دولار أمريكي).

قطاعات متعددة وتحويل الموارد والاستراتيجية تحويلاً تاماً.[141] ويمكن أن يشمل هذا النوع من التحويل تدريب الموظفين العسكريين (أو إعادة تدريبهم) ، وتحديث خدمات الاستخبارات للتركيز على جمع المعلومات العلمية والتكنولوجية ذات الصلة وإجراء عمليات محاكاة للحرب السيبرانية والمناورات العسكرية مع إيلاء اهتمام خاص لتطبيقات تكنولوجيا المعلومات والاتصالات.[142] وقد بادرت بلدان عديدة إلى إجراء مسابقات وطنية لتحديد أفضل الأذهان السيبرانية من بين سكانها المدنيين وتعيينهم.[143] وتُشجَّع الاقتصادات المحلية على تطوير قدرات تكنولوجية معززة لدعم الاستراتيجية العسكرية الجديدة. وتعكف بعض الحكومات أيضاً على إقامة مجموعة من القراصنة المدنيين من القطاع الخاص الذين يمكن اللجوء إليهم عند الحاجة.[144] ويمكن أن تكون هذه "الجهات الناشطة في مجال القرصنة" أفراداً متخصصين في مجال التكنولوجيا أو حتى قراصنة سابقين غير شرعيين تم تعيينهم وتدريبهم لاستخدام مهاراتهم لأغراض الأمن الوطني.[145] وقد تلجأ بعض البلدان إلى الاستعانة بوكلاء وقراصنة ومتخصصين من بلدان أخرى يعملون بالنيابة عنها.[146] وتبين هذه التغيرات كلها التحول عن استراتيجيات رد الفعل إزاء التهديدات السيبرانية وإعادة توجيه نحو تطوير نُهج استباقية لحرب المعلومات للعمل بفعالية في ظروف التكنولوجيا العالية.[147]

---

[141] Gurmeet Kanwal, "China's Emerging Cyber War Doctrine," at 20, Journal of Defense Studies, 2009، متاح في: www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf (يناقش حرب المعلومات في الصين وسياسة العلاج). [فيما بعد، "Kanwal"].

[142] الحرب السيبرانية: تحليل الوسائل والدوافع لدول مختارة،
Dartmouth College, Institute for Security, Technology, and Society, Nov. 2004 at 2, www.ists.dartmouth.edu/docs/execsum.pdf، (فيما بعد، "Selected Nations").

[143] انظر مثلاً، Richard Westcott, "UK Seeks Next Generation of Cybersecurity Specialists," *BBC News*, 26 يوليو 2010 www.bbc.co.uk/news/technology-10742588 .

[144] Kanwal at 20

[145] Gordon Corera, "Cyber-security strategy launched," *BBC News,* 25 June 2009, http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm?ad=1 (hereinafter "Corera"); Tom Gjelten, "Cyberwarrior Shortage Threatens U.S. Security," National Public Radio, 19 July 2010, www.npr.org/templates/story/story.php?storyId=128574055.

[146] Eshel

[147] Kanwal at 20

ج) إقامة العُدة العسكرية السيبرانية

استجابت بلدان عديدة للتهديد الجديد للحرب السيبرانية من خلال تكليف عدد كبير من الأفراد العسكريين بمهمة القتال الافتراضي.[148] ويمكن أن يشمل هذا التحول السياسي إنشاء فرق حربية للإنترنت تكون مكرسة لتحقيق الأمن السيبراني، ويمكن دمجها في وكالات استخبارات أخرى،[149] أو حتى إنشاء قطاعات جديدة تماماً ضمن الهيكل العسكري المكرس للنشاط السيبراني.[150] وتقام هذه العدة العسكرية الجديدة لدمج وإعداد الموارد العسكرية من أجل جميع أنواع عمليات الفضاء السيبراني.[151] ويمكن أن تكون أيضاً مسؤولة عن تأمين الشبكات الخاصة التي تشغّل جزءاً كبيراً من العمليات العسكرية، وإن كان تركيزها في المقام الأول على حماية الشبكات العسكرية وتسيير العمليات العسكرية في الفضاء السيبراني.[152]

د) استعمال النُهج السيبرانية لإتاحة فرص متكافئة

تأمل بعض البلدان، من خلال تحسين المعلومات والنُهج الحربية الإلكترونية، أن تكون على قدم المساواة مع البلدان التي تعتمد على البرمجيات وأنظمة الحاسوب لتعبئة قواتها المسلحة التقليدية. ويقتضي هذا التحول الاستثمار في أنظمة تحكم جديدة مؤتمتة، تشمل معدات مثل كبلات الألياف البصرية والسواتل وأنظمة راديوية رقمية عالية التردد، إلى جانب زيادة التركيز على أنظمة المراقبة الفضائية وتلك المقامة جواً وبحراً وبراً.[153] وتستعمل بعض الحكومات بالفعل تكنولوجيا المعلومات والاتصالات بالاقتران مع موظفين عسكريين متخصصين في التكنولوجيا لمراقبة الحدود الوطنية.[154] وقد تعتمد الاستراتيجيات الموجهة نحو المجال السيبراني اعتماداً أكبر على هذه الموارد والأنظمة المؤتمتة المصاحبة لها، لتأمين الحدود. ويمكن أن تشمل النُهج

---

[148] كشفت بعض البلدان عن تحولات مكثفة في ملاك الموظفين. انظر Cyber General (يشير إلى أن الولايات المتحدة أعلنت عن إعادة توزيع 30 000 مجموعة للدفاع السيبراني). غير أن المعلومات المتعلقة بالاستراتيجيات المعتمدة في كثير من البلدان ليست متاحة بسهولة. انظر Robert McMillan, "Black Hat Talk on China's 'Cyber Army' Pulled After Pressure", *InfoWorld,* 15 July 2010, http://www.infoworld.com/print/130362.

[149] Eshel

[150] أعلنت الولايات المتحدة على سبيل المثال، إنشاء وحدة جديدة للشؤون العسكرية السيبرانية في 2009. Cyber General. وأعلنت المملكة المتحدة مؤخراً إنشاء مركز لعمليات الأمن السيبراني كجزء من استراتيجيتها للأمن السيبراني. Corera.

[151] انظر "U.S. Cyber Command Fact Sheet,"، وزارة الدفاع الأمريكية، 25 مايو 2010، www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf

[152] Siobhan Gorman, "U.S. Backs Talks on Cyberwarfare"', *The Wall Street Journal*، 4 يونيو 2010، http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html (مشيراً إلى أن 90 بالمائة من القوة العسكرية يوفرها القطاع الخاص، وفقاً لمسؤولين عسكريين في الولايات المتحدة) (فيما بعد، "Gorman").

[153] Kanwal at 16

[154] Kanwal at 14

الأخرى عمليات التحكم والمراقبة التي تركز على تعطيل تدفق معلومات العدو واستهداف البنى التحتية لتكنولوجيا المعلومات والاتصالات المعادية لإتلاف أو تدمير الأجهزة الوظيفية والشبكات والبيانات الحيوية.[155] وتركز هذه التغييرات على شن هجمات على نقاط الضعف المحتملة للخصوم — أي اعتمادهم على الفضاء السيبراني والتكنولوجيات الجديدة. وقد تكون البلدان التي تملك أقوى قدرات الحرب السيبرانية والتقليدية أشد ضعفاً في الواقع بسبب التكنولوجيا التي تقوّيها والتي تكون عرضة لأنواع جديدة من الهجوم مثل البرمجيات الخبيثة والقرصنة[156]. وتأمل البلدان في إضعاف القدرات العسكرية لخصومها من خلال الاستفادة من الاختلاف المحتمل في الأعمال في الفضاء السيبراني.[157]

هـ) تثقيف المواطنين وإذكاء الوعي بمشاكل الأمن السيبراني

تعترف حكومات عديدة بأن التعليم العام وتوعية الجمهور من الأساليب القوية للدفاع السيبراني.[158] وتساعد قواعد بيانات المعلومات وبرامج التوعية الوطنية التي تنفذها الحكومة أو الكيانات الخاصة على تعزيز الوعي على مستوى القاعدة الجماهيرية.[159] وتركز هذه البرامج في الغالب على تعليم فرادى المستعملين والشركات الصغرى كيفية حماية معلوماتها وأنظمتها من الجرائم السيبرانية مثل انتحال الشخصية والقرصنة. وفي معظم الحالات، يكون النفاذ غير الشرعي لأنظمة الحاسوب مجرد خطوة أولى حيوية، ويمكن أن تكون قرصنة الحواسيب أو الأنظمة الفردية تمهيداً لارتكاب المزيد من الجرائم التي تؤثر على الأمن الوطني مثل هجمات التجسس للحصول على البيانات أو هجمات منع الخدمة. وعندما ترتكب هذه "الجرائم" ضد موارد وطنية حيوية أو هيئات حكومية، يمكن وصفها كهجمات أو حروب سيبرانية. ويحاول القراصنة بالفعل التسرب إلى الحكومات والأعمال التجارية الخاصة وأنظمة الدفاع الوطنية على أساس منتظم مع تحقيق نجاح

---

[155] Kanwal at 18

[156] تغيير جذري ("Because the United States is the most Internet-dependent and automated . . . it's also the most vulnerable to cyberattack.")

[157] Kanwal at 18؛ CRS Cyberwarfare at 11.

[158] انظر مثلاً، Selected Nations at 5 (يوصي ببذل جهود منتظمة ومستدامة لتغيير الطريقة التي ينظر بها الجمهور الأمريكي إلى أمن الشبكات من أجل تحسين الأمن السيبراني الوطني).

[159] على سبيل المثال، تشرف لجنة الحاسوب الوطني في موريشيوس، تحت ولاية وزارة تكنولوجيا المعلومات والاتصالات، على بوابة لإذكاء الوعي بالأمن السيبراني، متاحة في العنوان التالي: www.gov.mu/portal/sites/ncbnew/main.jsp، وتنظم الولايات المتحدة شهراً لإذكاء الوعي بالأمن السيبراني الوطني في أكتوبر من كل سنة. كما أن الشراكات بين القطاعين العام والخاص، مثل التحالف الأمريكي للأمن السيبراني الوطني، تعلّم المستعملين والمديرين للبنية التحتية الرقمية كيفية إقامة أنظمة مرنة وآليات وقائية. انظر "About Us,"، التحالف الأمريكي للأمن السيبراني الوطني، www.staysafeonline.org/content/about-us.

ملموس.[160] ويمكن القيام بالتجسس للحصول على بيانات أو النفاذ إلى معلومات حساسة بواسطة استعمال وسائل تقنية فضلاً عن "الهندسة الاجتماعية" التي هي عبارة عن أسلوب يعتمد على التفاعل البشري لخداع الناس بجعلهم يوفرون النفاذ إلى أنظمة آمنة عموماً.[161] وبالتالي، فإن تثقيف الجمهور بشأن استعمال كل من الهندسة الاجتماعية والأساليب التقنية مثل عدم استعمال مفاتيح الذاكرة المصابة بفيروس في الأماكن العامة، يمكن أن يساعد على حماية الموارد الوطنية.[162]

و) البلدان قليلة التوصيل والبلدان النامية

على الرغم من أن العديد من البلدان تعتمد اعتماداً كبيراً على تكنولوجيا المعلومات والاتصالات والإنترنت من أجل البنية التحتية والخدمات الحيوية، لا تعتمد شعوب أخرى على هذه التكنولوجيات أو ليست موصلة بها، وبدلاً من ذلك، تستعمل شبكات الإنترانت الوطنية أو موارد أخرى غير موارد تكنولوجيا المعلومات والاتصالات برمتها. ومع ذلك، يبدو أن حتى هذه البلدان تقوم بزيادة قدراتها على الخط، وإن كان هذا التقدم يقتصر على الاستخدامات العسكرية والحكومية.[163] والبلدان التي دخلت مؤخراً العالم السيبراني قد تواجه مشاكل أقل من حيث تعرضها للهجمات السيبرانية، وذلك لأن أنظمتها الحكومية بصورة عامة لديها توصيلات أقل بباقي الفضاء السيبراني.[164] ولكن حتى البلدان النامية التي لا تملك بعد البنية التحتية اللازمة للاستفادة من الفوائد الكاملة التي يمكن تحقيقها بفضل تكنولوجيا المعلومات والاتصالات، ما زالت تعتمد على الإنترنت وتكنولوجيات أخرى للاتصالات المتنقلة والرقمية لتلبية بعض احتياجاتها الأساسية.[165] وبناءً على ذلك، لديها مصلحة أيضاً في مستقبل الأمن السيبراني.

---

[160] *انظر مثلاً*، Understanding at 20 (يسرد الأهداف الشهيرة لهجمات القرصنة، بما في ذلك وزارة الدفاع الأمريكية، والحكومة الألمانية، وGoogle وEbay وإدارة الولايات المتحدة الوطنية للملاحة الجوية والفضاء (ناسا)).

[161] انظر المرجع نفسه في الفقرات 23-24

[162] على سبيل المثال، تم التسلل إلى القيادة المركزية الأمريكية بواسطة مفتاح ذاكرة مصاب بفيروس في 2008. انظر "Fifth Domain".

[163] Martyn Williams، "North Korea Moves Quietly Onto the Internet," *Computerworld*، 10 يونيو 2010، www.computerworld.com/s/article/9177968/North_Korea_moves_quietly_onto_the_Internet

[164] Corera.

[165] انظر مثلاً الوثيقة "Economic and Social Council Opens General Segment of 2010 Session," ECOSOC/6444, 3، 16 يوليو 2010، www.un.org/News/Press/docs/2010/ecosoc6444.doc.htm (التي تناقش مسألة "الأوراق المالية الرقمية" أو النظام النقدي الرقمي المستخدم في البلدان الإفريقية) (فيما بعد "ECOSOC 2010").

2.7 الاستجابات الدولية الأخيرة

هناك اليوم جهود دولية أقل بكثير من الاستراتيجيات الوطنية للتصدي لتهديدات الحرب السيبرانية، على الرغم من بعض المحاولات التي جرت في إطار المبادرات متعددة الأطراف. كما وضِعت نهج ثنائية الأطراف إلا أنها كانت أبعد ما يكون عن استراتيجية شاملة لتحسين الأمن السيبراني وضمان السلام السيبراني علماً أنها تشمل فقط جزءاً صغيراً جداً من الأطراف ذات الصلة في معادلة السلام السيبراني. وقد دعت بعض البلدان إلى وضع معاهدة للحد من استعمال الأسلحة السيبرانية في حين أصر آخرون على أن هذه المعاهدة غير ضرورية أو سابقة لأوانها.[166] وعلى الرغم من أن هذه الاقتراحات قد تدل على خطوة نحو التعاون الدولي، فإنها أيضاً أبعد ما يكون عن نهج شامل فعلاً واستراتيجية واضحة للمضي قدماً، أي استراتيجية تشمل جميع أصحاب المصلحة المعنيين. وتعرض الفقرة التالية بعض الاستجابات الدولية الأخيرة وإن كانت لا تمثل قائمة شاملة.

أ) مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) – مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية (UNCPCJ)

قامت لجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية في أبريل 2010 في دورتها الثانية عشرة بصياغة مجموعة من الإعلانات التي تشمل حكماً يدعو إلى إنشاء فريق خبراء حكومي دولي لبحث مشكلة الجريمة السيبرانية والاستجابات الدولية لها.[167] ووفقاً لذلك، أعدت الدول الأعضاء في اللجنة المعنية بمنع الجريمة والعدالة الجنائية أثناء دورتها التاسعة عشرة، التوصية ذات الصلة التي تطلب من اللجنة إنشاء فريق خبراء حكومي دولي مفتوح العضوية لتنفيذ الحكم الصادر عن هذه اللجنة.[168] وعلى الرغم من أن المؤتمر لم يتوصل إلى توافق في الآراء بشأن إعداد معاهدة جديدة للجريمة السيبرانية، أدت إلى إبرام اتفاقات بشأن المساعدة التقنية وبناء القدرات التي تشكل أساساً جيداً لمناقشة المزيد من الإجراءات.[169]

---

[166] Gorman.

[167] "Draft Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention andCriminal Justice Systems and Their Development in a Changing World،" الإعلان 42، مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، 18 أبريل 2010، www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6_Rev.2/V10529031A_CONF213_L6_REV2_E.pdf.

[168] تقرير مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، UNODC، سلفادور، البرازيل، 12-19 أبريل 2010، www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf

[169] ملخص النتائج المتعلقة بالجريمة السيبرانية: مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، مشروع عن الجريمة السيبرانية، 26 أبريل 2010، http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/2079_UNCC_cyberoutcome.pdf

ب) المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة (ECOSOC)

افتتح المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة دورته لعام 2010 بجلسة إعلامية عن التحديات التي يطرحها الأمن السيبراني، فضلاً عن التهديدات والفرص التي يتيحها استخدام الإنترنت الآخذ في الاتساع. وقد شدد المجلس من بين عدة أمور على الحاجة إلى اتخاذ مبادرات دولية تكفل تبادل المعلومات وأفضل الممارسات والتدريب والبحث. وإضافة إلى ذلك، أعلن المشاركون في المناقشة أنه يتعين على الأمم المتحدة أن "توحد أداءها" بشأن هذه القضية، مما سيؤدي حتماً إلى زيادة التعاون بين البلدان بل وبين الدول والقطاع الخاص أيضاً لضمان الأمن السيبراني.[170] وحذّروا من أن النطاق الدولي لحرب سيبرانية فعلية وعواقبها الوخيمة سوف تقضي استجابة منسقة؛ ولا تكفي الآن استراتيجيات اعتماد حلول على أساس مخصص وتقوية الدفاع.[171]

ج) منظمة حلف شمال الأطلسي (الناتو)

نفذت الناتو السياسة الخاصة بها في مجال الدفاع السيبراني في 2008 من أجل حماية مواردها التكنولوجية وتلك الخاصة ببلدانها الأعضاء.[172] وكجزء من هذه السياسة، أنشأ الحلف هيئة معنية بإدارة الدفاع السيبراني، وفريقاً للاستجابة للحوادث الحاسوبية يكفل إرسال فرق الدعم السريع إلى فرادى البلدان الأعضاء، ومركزاً للتميز من أجل الدفاع السيبراني التعاوني.[173] ويضم هذا المركز الذي يوجد مقره في إستونيا خبراء يضطلعون بالبحث والتدريب في مجال الأمن السيبراني. وتضم البلدان التي ترعى هذا المركز: إستونيا ولاتفيا وليتوانيا وألمانيا وإيطاليا والجمهورية السلوفاكية وإسبانيا.[174]

وإضافة إلى ذلك، قدمت الناتو تمارين في مجال الدفاع السيبراني حيث تقوم فرق من الدول الأعضاء بمحاولة الدفاع عن الشبكات الحاسوبية الافتراضية من الهجوم السيبراني. ويُقصد بهذه التمارين زيادة فهم البيئة السيبرانية الدولية وتعزيز التعاون الدولي لمعالجة الحوادث التقنية.[175] ووقعت الناتو أيضاً مذكرة تفاهم بشأن الأمن السيبراني مع إستونيا والولايات المتحدة والمملكة المتحدة وتركيا وسلوفاكيا.[176]

---

[170] ECOSOC 2010.

[171] *المرجع نفسه* (مناقشة "الأوراق المالية الرقمية" أو النظام النقدي الرقمي المستخدم في البلدان الإفريقية).

[172] " الدفاع ضد الهجمات السيبرانية"، الناتو، www.nato.int/cps/en/natolive/topics_49193.htm

[173] "NATO 2020", www.nato.int/cps/en/natolive/official_texts_63654.htm?selectedLocale=en.

[174] مركز التميز للدفاع السيبراني التعاوني، www.ccdcoe.org/

[175] "Defence exercise to boost skills for countering cyber attacks", NATO-News، 10 مايو 2010، www.nato.int/cps/en/SID-012B6A76-D60B9579/natolive/news_63177.htm.

[176] أبرمت الناتو وإستونيا اتفاقاً بشأن الدفاع السيبراني، NATO-News، 23 أبريل 2010، www.nato.int/cps/en/natolive/news_62894.htm

د) المجلس الأوروبي – اتفاقية بودابست بشأن الجرائم السيبرانية

تعالج اتفاقية المجلس الأوروبي بشأن الجرائم السيبرانية[177] بعض الجرائم السيبرانية من خلال توفير أحكام قانونية نموذجية يمكن أن تعتمدها البلدان وتكيفها مع احتياجاتها الخاصة. وعلى الرغم من أن الاتفاقية تقدم بعض الحلول القانونية للجرائم من قبيل النفاذ غير القانوني (القرصنة) واعتراض الاتصالات، فإنها لا تعالج بعض أنواع عمليات الهجوم السيبراني الأكثر تهديداً مثل التجسس للحصول على البيانات وأعمال التخريب. وعلى الرغم من أن الاتفاقية تساعد على تعزيز التعاون الدولي من خلال تجريم التهديدات السيبرانية الأساسية، فإن قوتها الإلزامية محدودة بسبب محاولة الجهة التي قامت بصياغتها عدم مخالفة تشريعات وطنية أخرى يحتمل أن تتعارض معها. وتؤدي الاختلافات الثقافية والقانونية الكبيرة إلى جعل إصدار قانون موحد أمراً بطيئاً إن لم يكن مستحيلاً تماماً في إطار هذا النهج.[178] وقد صدّق ثلاثون بلداً فقط على هذه المعاهدة منذ فتح باب التوقيع في نوفمبر 2001، مع بلد واحد منها من خارج أوروبا.[179]

تشكل الأحكام القانونية مثل تلك المنصوص عليها في الاتفاقية طريقة واحدة لمعالجة بعض التهديدات التي يتعرض لها الأمن السيبراني الوطني والدولي. غير أن الأحكام الواردة في الاتفاقية لا تتناول مسألة الحرب السيبيرانية بين البلدان بشكل مباشر. وعلى الرغم من أن التهديد بفرض عقوبات قد يؤدي إلى ردع بعض المجرمين الذين يزمعون ارتكاب جرائم سيبرانية، فإن هذا النوع من التشريع قد لا يفي بالغرض بشكل كافٍ لردع المهاجمين الذين هم واثقون من قدرتهم على التهرب من الكشف أو تعرّف هويتهم أو مقاضاتهم.

ه) الاتفاقات الثنائية بشأن الأمن السيبراني

تحاول فرادى الدول أيضاً إقامة علاقات مع بلدان أخرى فيما يتعلق بالأمن السيبراني. فعلى سبيل المثال، أقامت وزارة تكنولوجيا المعلومات والاتصالات التابعة لحكومة الهند علاقات تعاون في شكل مذكرات تفاهم أو أشكال أخرى من مساعي التطوير وتقاسم المعلومات مع بلدان مختلفة. فعلى سبيل المثال، وقّعت الهند وكوريا الجنوبية بياناً مشتركاً من أجل التعاون الثنائي في مجال تكنولوجيا المعلومات في 2004 كما أن فريق الاستجابة لحالات الطوارئ الحاسوبية في الهند وقع مذكرة تفاهم مع مركز الأمن السيبراني الوطني في

---

[177] Convention on Cybercrime CETS no.: 185، المجلس الأوروبي، http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (آخر زيارة في 10 أغسطس، 2010 (فيما بعد "Convention").

[178] "National Security Threats in Cyberspace," نقابة المحامين الأمريكيين، اللجنة الدائمة المعنية بالشؤون القانونية والأمن الوطني ومنتدى الاستراتيجية الوطنية، 13 سبتمبر 2009 في: www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf (فيما بعد "Workshop").

[179] اتفاقية "Convention".

كوريا من أجل التعاون الرسمي في مجال الأمن السيبراني من بين مجالات أخرى.[180] كما أن الهند لديها عدد من مذكرات التفاهم الثنائية فيما يتعلق بتكنولوجيا المعلومات بصورة عامة وقليل منها يركز على الأمن السيبراني والجريمة السيبرانية بوجه خاص.[181] ووقع المغرب وماليزيا كذلك مذكرة تفاهم بشأن الأمن السيبراني أثناء المؤتمر الإقليمي للأمن السيبراني الذي عقد في المغرب في وقت سابق هذا العام.[182] وأقيمت بموجب هذه المذكرة علاقة تعاونية بين وزارتي الأمن السيبراني لهذين البلدين، تغطي مجالات تشمل حماية البنية التحتية الحيوية للمعلومات وتطوير أطر الأمن السيبراني وبناء القدرات والتدريب وإذكاء الوعي. وعلى الرغم من أن هذه الأنواع من التعاون قد تعزز الأمن السيبراني في بلد ما، فإنها غير كافية لحماية أي بلد واحد من الحرب السيبرانية العالمية. وبالتالي، هناك حاجة لوضع هيكل عالمي أكثر شمولاً يتعلق بالأمن السيبراني لتأمين السلام لجميع الدول.

و) الاتحاد الدولي للاتصالات (لجنة الدراسات 17 التابعة لقطاع تقييس الاتصالات) – المعايير الدولية

بغية معالجة مسألة الأمن السيبراني المتنامية فيما يتعلق بالشبكات الذكية تحديداً، قام الاتحاد الدولي للاتصالات بإنشاء فريق متخصص معني بالشبكات الذكية من أجل جمع وتوثيق المعلومات والمفاهيم التي ستكون مفيدة من أجل إعداد توصيات لدعم الشبكات الذكية من منظور الاتصالات.[183] والأفرقة المتخصصة هي أداة من أدوات الاتحاد التي تعزز برنامج عمل لجان الدراسات من خلال توفير بيئة عمل بديلة لتطوير المواصفات بسرعة في مجالات عملها.[184] وقد أصبحت الأفرقة المتخصصة تستعمل اليوم استعمالاً واسعاً لتلبية احتياجات الصناعة فور ظهورها، مما يجعلها مثالية للتكنولوجيات المتغيرة والمتطورة بسرعة مثل الشبكات الذكية. ويتألف الفريق المتخصص المعني بالشبكة الذكية من ممثلين من مختلف الدول الأعضاء وسيقوم بالتعاون مع مجتمعات الشبكة الذكية في جميع أنحاء العالم (مثل معاهد البحوث والمنتديات والأوساط الأكاديمية). وسيقوم الفريق المتخصص لدى إنجاز أهدافه المتمثلة في توفير توصيات من أجل معايير الشبكة الذكية، بالاحتفاظ بقائمة محدثة بالهيئات المعنية بوضع المعايير المتعلقة بالشبكات الذكية، وجمع الرؤى وتقييم الاقتراحات بشأن الشبكات الذكية وتوفير المصطلحات والتصنيف اللازم لدعم الشبكات

---

[180] "Bilateral Cooperation: Asia"، دائرة تكنولوجيا المعلومات والاتصالات في الهند، حكومة وزارة الاتصالات وتكنولوجيا المعلومات في الهند، www.mit.gov.in/content/bilateral-cooperation (فيما بعد، "Cooperation").

[181] على سبيل المثال، يركز تعاون الهند مع بروني وماليزيا وفرنسا وأستراليا بوجه خاص على أمن المعلومات و/أو الجريمة السيبرانية في حين أن العلاقات تركز على تنمية الموارد والمرافق. Corporation.

[182] ماليزيا والمغرب شريكان جديدان في مجال الأمن السيبراني، CyberSecurity Malaysia، CyberSecurity Malaysia، 24 يناير 2010، www.cybersecurity.my/data/content_files/44/632.pdf?.diff=1265036362.

[183] لمزيد من المعلومات بشأن الفريق المتخصص، يرجى زيارة الموقع: www.itu.int/ITU-T/focusgroups/smart/

[184] الأفرقة المتخصصة التابعة لقطاع تقييس الاتصالات: www.itu.int/ITU-T/focusgroups/.

الذكية، وجمع أفكار جديدة ذات صلة وتحديد مجالات الدراسة المحتملة لدعم الشبكات الذكية، وتحديد الآثار المحتملة لتطوير المعايير فيما يتعلق ببعض المجالات المتعلقة بمواضيع محددة مثل الأمن والخصوصية وقابلية التشغيل البيني.[185] وستوفر هذه الأنشطة جميعها نهجاً شاملاً ومتعدد الجوانب لتحديات الأمن السيبراني سريعة التطور والمتزايدة فيما يتعلق بالشبكات الذكية.

وعلاوة على ذلك، فإن الفريق المتخصص، من خلال تواصله مع قطاع تقييس الاتصالات بالاتحاد (ITU-T)، الذي هو من أهم المنظمات المعترف بها في مجال وضع معايير الاتصالات، سيكون بإمكانه العمل بصفته مصدراً موحِّداً وموثوقاً للمعلومات والإرشاد تدعمه سمعة تشهد بجودة المعايير المعتمدة بالتوافق. كما أن العلاقة مع قطاع تقييس الاتصالات توفر بيئة تسمح بتقدم نتائج أعمال الفريق المتخصص من خلال لجنة الدراسات في شكل توصيات لقطاع تقييس الاتصالات أو إضافات أو كتيبات وما إلى ذلك. وسيكون بإمكان الفريق المتخصص، بصفته جزءاً من قطاع تقييس الاتصالات، الحصول على قبول أكبر لمواصفاته في العديد من الأسواق في العالم، لا سيما في البلدان النامية وفي مناطق غير تلك التي تشارك مشاركة أكثر فعالية في هذا المنتدى.

3.7 الحاجة إلى وضع إطار دولي

أ) عدم جدوى الردع

تظهر تحديات جديدة مع كل ميدان جديد. ويخلق الفضاء السيبراني عقبات ومآزق جديدة مثلما أثارت التهديدات المتعلقة بالبر والبحر والجو والفضاء مشاكل تتعلق بالتوزيع وكفاءة الاستعمال وتسوية النزاعات في الماضي وما زالت قائمة اليوم. وكل شخص موصل بالإنترنت يتأثر بالأمن السيبراني، ونظراً للاعتماد المتنامي على تكنولوجيا المعلومات والاتصالات من أجل البنية التحتية المجتمعية الأساسية، فتأثيرها الآن يطال حتى غير الموصلين. والهجوم ضد البنية التحتية للمعلومات وخدمات الإنترنت لديه القدرة الآن على إلحاق الضرر بالمجتمع بطرق جديدة وحرجة. ونظراً للخصائص والتحديات الفريدة التي تطرحها الحرب السيبرانية، فإن استراتيجيات حفظ السلام الفعلية التي جُربت في الماضي قد لا تكون فعالة الآن.

كانت عملية الردع منذ فترة طويلة نهجاً مفضلاً لحفظ السلام والأمن بين الدول في مواجهة الأسلحة التي يمكن أن تتسبب في الدمار الشامل. غير أن كفاءة الردع تتوقف على بعض الظروف والافتراضات التي لا ينطبق معظمها على الفضاء السيبراني.[186] ويتطلب الردع بصورة عامة أربعة عناصر رئيسية: العزو (معرفة

---

[185] تتاح اختصاصات الفريق المتخصص المعني بالشبكات الذكية والتابع لقطاع تقييس الاتصالات في العنوان التالي: www.itu.int/ITU-T/focusgroups/smart/tor.html

[186] تغيير جذري (نقلاً عن مستشار الأمن الأمريكي ريتشارد كلارك، "القوة التي منعت الحرب النووية – أي الردع – لا تعمل بشكل جيد في الحرب السيبرانية").

من المهاجم)؛ والموقع (معرفة مصدر الهجوم)؛ والاستجابة (القدرة على الاستجابة حتى وإن تعرضت للهجوم أولاً)؛ والشفافية (إدراك العدو لقدراتك ونيَّتك للاستجابة بقوة كبيرة).[187] ويثير الفضاء السيبراني والحرب السيبرانية مشاكل جديدة تقوض الافتراض الأساسي بوجود هذه العناصر الأربعة عند إعداد البلدان لقواعدها الدفاعية العسكرية. وتكنولوجيا المعلومات والاتصالات تسمح بزيادة عدد الطرق التي يمكن بها للمهاجم إخفاء هويته وموقعه؛ ويمكن للمهاجم استعمال وكلاء أو خدمات مثل أجهزة الإنترنت العمومية والشبكات اللاسلكية والخدمات المتنقلة مسبقة الدفع التي لا تتطلب الاستيقان من المستعمل. ويمكن أيضاً استخدام تكنولوجيا التشفير التي تعتبر من الحلول التكنولوجية الرئيسية لضمان السرية والسلامة والتيسر، لإخفاء الهوية أو على الأقل إبطاء تقدم البحث في مصدر الهجوم السيبراني. ويمكن للعمليات التقنية والسياسات التي تحد من احتجاز البيانات المتوفرة عبر حركة الإنترنت أن تساهم أيضاً في هذه المشكلة المتعلقة بالعزو والموقع.

وإن خطر الانتقام بإصابة الهدف الخاطئ والغموض الذي يكتنف الأضرار الناجمة عن أي هجوم سيبراني مضاد – الذي يمكن أن يؤدي بسهولة إلى إلحاق الضرر بحليف أو طرف محايد، يزيد من إفشال قدرة الدول على الرد على الهجوم.[188] وإذا كان المهاجم يعتقد أن عدم كشفه ممكن أو يعتقد أن ضحاياه لن يردوا بقوة عسكرية خوفاً من مخالفة المعايير الدولية، يكون تأثير التهديد الانتقامي ضئيلاً للغاية. ومن خلال الاستجابة بقوة لهجوم سيبراني لا يستخدم قوة عسكرية تقليدية ويهدف إلى الاستغلال أكثر منه إلى التدمير، تتعرّض الضحية المنتقمة لخطر تفسير المجتمع الدولي لعملها على أنه عمل عدواني وغير مبرَّر.[189] كما أن الاعتماد على استراتيجية الردع يشجع البلدان على اتخاذ مواقف عدائية فيما بينها واستحداث تهديدات انتقامية جديدة عبر مختلف الميادين تأهباً لسيناريوهات مختلفة محتملة مما يؤدي إلى إحباط فوائد زيادة الاندماج وتصعيد التوتر بين البلدان.[190] وفي جميع هذه الطرق، تقوض الخصائص الأساسية للفضاء السيبراني فعالية الردع بوصفه نهجاً للسلم السيبراني.

وقد يصبح الإطار ذاته للنهج القانونية الحالية غير مناسب لإدارة المخاطر المتصلة بالأمن السيبراني. فعلى سبيل المثال، في ظل القانون الدولي الحالي على النحو المحدد في المادة 51 من ميثاق الأمم المتحدة، يجوز لدولة أن تتصرف بصورة شرعية للدفاع عن نفسها عندما تواجه هجوماً مسلحاً. أما في سياق الحرب السيبرانية،

---

[187] Tang Lan and Zhang Xin، "Can Cyber Deterrence Work?" *في الردع السيبراني العالمي: وجهات نظر من الصين والولايات المتحدة وروسيا والهند والنرويج*، EastWest Institute، أبريل 2010 في 1، www.ewi.info/system/files/CyberDeterrenceWeb.pdf.

[188] James A Lewis، "Cross-Domain Deterrence and Credible Threats,"، مركز الدراسات الاستراتيجية والدولية، يوليو 2010، http://csis.org/files/publication/100701_Cross_Domain_Deterrence.pdf.

[189] *المرجع نفسه.*

[190] *المرجع نفسه.*

تطرح هذه المسألة المنطقية المزيد من الأسئلة بشأن متى يمكن اعتبار هجوم سيبراني معادلاً لهجوم مسلح ومن ثم ما إذا كان من الممكن أن يُعزى الهجوم إلى دولة ما.[191] ويبدو أن نظرية "مسؤولية الدولة" تسلط بعض الضوء على التساؤل الأخير؛ فهي تنطوي على اقتراح أن كل دولة يتعين عليها أن تتصرف بحيث تمنع استعمال أراضيها لشن هجوم على دول أخرى، وإذا رفضت اتخاذ إجراءات وقائية، يمكن أن تُعزى مسؤولية هذه الهجمات إليها. ولكن، كما رأينا في تقييماتنا الأولية للهجوم السيبراني، يصعب كثيراً الرد على هذا التساؤل العملي في إطار الفضاء السيبراني – نظراً لأن بعض الهجمات ليس لها مصدر جغرافي (كما هو الحال بالنسبة للبرمجيات الروبوتية الخبيثة)، بحيث يمكن أن تنتشر عبر حدود متعددة، وتصدر من تحالفات تقع ضمن ولايات قضائية متعددة أو ينفذها وكيل يعمل بالنيابة عن مرتكبها الحقيقي. وفي بعض الأحيان تكون الدول نفسها غير قادرة على كشف الأطراف التي تتصرف داخل أراضيها أو التحقق منها. وحتى إذا تمكنت دولة معينة من تحديد هوية الطرف الذي يتصرف داخل منطقتها الجغرافية، فإن الطبيعة ذاتها للمجال السيبراني تجعل من المستحيل لأي كيان واحد التحكم على نحو شامل بهذا الصدد.[192] وهكذا، فإن الغموض لا يقتصر على مسألة المصدر فقط وإنما يشمل أيضاً مسألة التحكم بصورة لا يمكن تفاديها.

ب) ضرورة وضع إطار دولي

نظراً لأن المعايير والصكوك القانونية الدولية الحالية غير مجهزة تجهيزاً كاملاً للتعامل مع التحديات الجديدة التي يطرحها الأمن السيبراني، يعتبر الحوار العالمي والتعاون من الأمور الضرورية بهذا الشأن. والطبيعة المتغيرة للتكنولوجيا ذاتها – مع تداخلات متزايدة بين السلطات القضائية الوطنية وتكنولوجيا المعلومات والاتصالات المرتبطة بها، والموارد والأنظمة على الخط – تجعل اعتماد استراتيجيات جديدة والتعاون الدولي يتسمان بأهمية أكثر لضمان السلام السيبراني.[193]

ويمكن أن تصدر الهجمات السيبرانية وتضرب من أي مكان من جميع أنحاء المعمورة، مما يجعل هذه التهديدات دولية بطبيعتها وتتطلب التعاون الدولي، والمساعدة في التحقيق والأحكام الإجرائية والموضوعية المشتركة لمعالجتها على نحو ملائم. وإضافة إلى ذلك، من المعترف به على نطاق واسع أن التعاون الدولي يمثل أحد المتطلبات الرئيسية لضمان الأمن السيبراني على الصعيد العالمي. وفي 2003 و2005، اتفقت الدول في القمة العالمية لمجتمع المعلومات (WSIS) على ضرورة وضع أدوات تتسم بالفعالية والكفاءة على المستويين الوطني والدولي للنهوض بالتعاون الدولي بشأن الأمن السيبراني.[194] وينبغي أن يكون هذا التعاون الدولي،

---

[191] Workshop at 14.

[192] *المرجع نفسه*.

[193] *المرجع نفسه*.

[194] "القمة العالمية لمجتمع المعلومات: برنامج عمل تونس بشأن مجتمع المعلومات"، الفقرة 40، القمة العالمية لمجتمع المعلومات، WSIS-05/TUNIS/DOC/6(Rev.1)-E، 18 نوفمبر 2005، www.itu.int/wsis/docs2/tunis/off/6rev1.html (فيما بعد، "Tunis Agenda").

ليس فقط بدافع الرغبة المشتركة في السلام، وإنما بدافع المصلحة الفردية المستنيرة لكل بلد. وأصبح كل بلد الآن يعتمد على التكنولوجيا من أجل خدمات التجارة والشؤون المالية والرعاية الصحية والطوارئ وتوزيع الأغذية وأكثر من ذلك. ومن شأن إتلاف الشبكات الحيوية أن يشل حركة أي بلد بسرعة – وما من أحد منا في مأمن من الهجوم السيبراني. ومن ثم تؤدي تكنولوجيا المعلومات والاتصالات والترابط بين التكنولوجيات التي يجري تطويرها إلى تشكيل نظام عالمي جديد، نظام يدعو إلى التعاون بشأن القضايا الجديدة لضمان الاستقرار.

ومن الضروري أن تعمل البلدان على تنسيق أطرها القانونية لمكافحة الجرائم السيبرانية وتيسير التعاون الدولي الدينامي متعدد الجوانب. ويتعين على الدول أن تعمل في سبيل وضع إطار قانوني وتنظيمي مشترك، وإقامة نظام لتحديث هذه القوانين على أساس منتظم لمعالجة الطبيعة المتغيرة للتهديدات التي يتعرض لها الأمن. وقد دعت بعض المجموعات بالفعل إلى إصدار معايير دولية وقواعد سيبرانية كوسيلة لتحسين الأمن السيبراني على الصعيد الدولي.[195] وفي أي حال من الأحوال، ينبغي أن تكون كل استراتيجية فعالة للسلام السيبراني مرنة وقابلة للتكيف بشكل كافٍ لتتسنى إدارة تقدم التكنولوجيا السريع ونمو تكنولوجيا المعلومات والاتصالات وتحديات الأمن المرتبطة بها والاستجابة لها. كما يتعين على البلدان أن تتفق بشأن إجراءات ونهج لتحديد مصدر الهجمات وهوياتها من أجل التصدي للهجمات السيبرانية المجهولة الهوية والاشتباكات الدولية التي تهدد بنشوبها. وتحاول مقترحات لإبرام اتفاق دولي يقضي بأن ينظم كل بلد الفضاء السيبراني الخاص به، معالجة مشكلة عزو الهجوم؛ وإن ربط المسؤولية بالمصدر الجغرافي قد يؤدي إلى تفادي العملية المعقدة لتحديد هوية مرتكب الهجوم السيبراني تحديداً دقيقاً.[196] غير أن هذه المقترحات لا تحل المشاكل المتعلقة بتحديد هوية الوكلاء وتتبع الهجوم إلى أن يتم تحديد المصدر الجغرافي – أي الموقع الصحيح. ونظراً لأوجه القصور في النهج التقليدية والحالية المتبعة في مجال الأمن الدولي، من الواضح أن المجتمع العالمي بحاجة إلى تبني استراتيجية جديدة للتصدي لتحديات الأمن السيبراني وضمان تحقيق سلام سيبراني دائم.

4.7 مقترحات لإصدار مبادئ دولية في مجال الفضاء السيبراني

يتعين علينا لدى إصدار مبادئ توجيهية لتحقيق السلام السيبراني، النظر في الخصائص المميزة للفضاء السيبراني وأبرز التحديات التي تطرحها هذه السمات. ومع ذلك يمكننا الاستفادة من إنجازات أخرى ترمي إلى مكافحة تهديدات شبيهة عبر وطنية، مثل اتفاقية مكافحة الجريمة المنظمة عبر الوطنية، لإثراء منهجنا.

---

[195] اعتزم المشاركون في ورشة العمل بمن فيهم أعضاء من نقابة المحامين الأمريكيين، واللجنة الدائمة المعنية بالشؤون القانونية والأمن الوطني ومنتدى الاستراتيجية الوطنية، مؤسسة McCormick ومنتدى الاستراتيجية الوطنية، إنشاء فريق مهام يعنى بالأمن السيبراني الدولي لوضع المعايير والقواعد السيبرانية من أجل تحسين الأمن السيبراني. Workshop at 26.

[196] Robert Mullins، "'Pearl Harbor' post struck a nerve،" *NetworkWorld*، 11 مارس 2010، www.networkworld.com/community/node/58450 (نقلاً عن مستشار الأمن الرئاسي الأمريكي السابق ريتشار كلارك في حلقة مناقشة بشأن الأمن السيبراني).

وعلى غرار الجريمة المنظمة عبر الوطنية، تمتد الهجمات السيبرانية عبر الحدود الوطنية وتعمل من خلال شبكات معقدة تضاهي الأنظمة السلمية والمنتِجة أو تتعداها. وتقدم هذه الاتفاقية فهماً مشتركاً يفيد أن هذه المشاكل المتفشية العابرة للحدود الوطنية يلزم معالجتها بواسطة التعاون الدولي الوثيق وأنها تقتضي اعتماد أطر جديدة والمساعدة القانونية والإنمائية المتبادلة وتبادل المعلومات والتعاون في مجال إنفاذ القانون.[197]

وتدعم المبادئ القانونية الراسخة والمعايير التي أقرت دولياً بعض العناصر الضرورية لوضع خطة للسلام السيبراني. وتنص المادة 19 بالتحديد من الإعلان العالمي لحقوق الإنسان على الحق في حرية الرأي والتعبير الذي يشمل حرية استقاء المعلومات والأفكار وتلقيها ونقلها عبر أي وسيلة كانت دون التقيد بالحدود الجغرافية.[198] وأكدت القمة العالمية لمجتمع المعلومات من جديد في إعلان المبادئ الصادر عنها في جنيف، 2003، مفهوم حرية الاتصال باعتبارها قاعدة أساسية لمجتمع المعلومات. ويسلط الإعلان الضوء أيضاً على دور الاتصالات بوصفها عملية اجتماعية أساسية وحاجة إنسانية أساسية تشكل دعامة أساسية لكل تنظيم اجتماعي. ولذا ينبغي تأمين نفاذ الجميع على قدم المساواة إلى تكنولوجيا المعلومات والاتصالات[199]. وأعلنت الأمم المتحدة عن التزامها بضمان هذا النفاذ للجميع وتسخير إمكانات الثورة الرقمية تسخيراً كاملاً لتحقيق هذه الغاية.[200]

وعلى الرغم من تعدد أوجه الاختلاف بين المواد النووية وتكنولوجيا المعلومات والاتصالات، هناك أوجه تشابه رئيسية متعددة تجعل أنشطة التعاون الدولي اللازمة لضمان السلام النووي مفيدة لوضع استراتيجية من أجل الأمن السيبراني. وعلى غرار السلام السيبراني وتكنولوجيا المعلومات والاتصالات، فإن الطاقة والتكنولوجيا النووية يمكن استخدامهما في عدد من الأعمال السلمية والعسكرية، إذ يمكنهما إحداث أضرار مدمرة عند استخدامهما في هجوم، ويمكن لجميع البلدان أن تشعر بأثر هذا الهجوم حتى وإن كان ضد بلد واحد.[201] وإدراكاً للطبيعة العالمية الملازمة لتهديد الهجمات النووية، سعى المجتمع الدولي إلى وضع استراتيجية تعاونية متعددة الأطراف تشمل استحداث نهج مشترك والتزام مشترك إزاء الأمن النووي.[202] وتقدم

---

[197] اتفاقية منع الجريمة المنظمة العابرة للحدود، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2004، www.unodc.org/unodc/en/treaties/CTOC/index.html.

[198] الإعلان العالمي لحقوق الإنسان، المادة 19، U.N. G.A., Res. 217A (III)، U.N. GAOR, U.N. Doc. A/810, 1948، www.un.org/en/documents/udhr/index.shtml#a19.

[199] إعلان المبادئ الصادر عن القمة في جنيف، الفقرة 4 القمة العالمية لمجتمع المعلومات، 2003؛ www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

[200] "Ban urges greater use of digital technology to improve living conditions,"، مركز أخبار الأمم المتحدة، 17 مايو 2010، www.un.org/apps/news/story.asp?NewsID=34716

[201] البيان الوطني للولايات المتحدة، قمة الأمن النووي لعام 2010، 13 أبريل 2010، www.whitehouse.gov/the-press-office/nuclear-security-summit-national-statement-united-states، (فيما بعد "البيان الوطني للولايات المتحدة").

[202] *المرجع نفسه.*

المعاهدات مثل معاهدة عدم انتشار الأسلحة النووية (NPT) مثالاً عن نهج فعال للتحدي المتمثل في الحفاظ على استخدامات سلمية للمواد المدمرة القادرة على عبور الحدود الوطنية. وتحدد هذه المعاهدة المسؤولية عن المواد استناداً إلى الولاية الإقليمية أو الأنشطة "التي تجري تحت سيطرة [دولة ما] في أي مكان."[203] وتأكيداً لهذا النهج، جدّد سبعة وأربعون بلداً في قمة الأمن النووي لعام 2010، الالتزام بتأمين المواد النووية التي توجد تحت سيطرتها والاستمرار في تعزيز الأمن وفقاً للظروف المتغيرة وتبادل أفضل الممارسات والحلول العملية المتعلقة بالأمن.[204]

وتؤكد معاهدة عدم انتشار الأسلحة النووية أيضاً على فوائد التطبيقات السلمية للتكنولوجيا النووية وأهمية إتاحة هذه الفوائد لجميع الدول، بما فيها البلدان النامية.[205] وتشدد المعاهدة على أهمية التعاون الدولي بين جميع الدول بما في ذلك تبادل المعلومات والمواد للمساهمة في زيادة تطوير التطبيقات السلمية للطاقة الذرية.[206] وعلاوة على ذلك، تلزم المادة 3 الموقعين ببعض الضمانات التي يقصد بها منع تحول الطاقة النووية من الاستخدامات السلمية نحو الأسلحة النووية أو غيرها من الاستخدامات المدمرة.[207] وإن الوكالة الدولية للطاقة الذرية المشهود لها بخبرتها وتجربتها وقدرتها على تسهيل المناقشة في منتدى محايد، مكلّفة بالإشراف عن التفاوض وإبرام اتفاق بين الدول التي ستقيم نظام ضمانات كهذا.[208]

وتشمل أنشطة التعاون الأخرى لضمان السلام النووي المبادرة العالمية لمكافحة الإرهاب النووي، وهي شراكة دولية للبلدان الملتزمة بالعمل على نحو فردي وجماعي لتنفيذ مجموعة مبادئ مشتركة للأمن النووي.[209] وتشمل هذه المبادئ: تطوير المحاسبة وتحسينها وتدابير المراقبة والأمن المتعلقة بالمواد النووية والمرافق النووية المدنية، وتعزيز قدرات الدول الأعضاء المتعلقة بالكشف والمراقبة، ومنع توفير الملاذ الآمن للإرهابيين، وتعزيز قدرات الدول الأعضاء في مجال الاستجابة في حالة الهجوم والتخفيف من وطأته والبحث والنهوض بتبادل المعلومات.[210]

---

[203] معاهدة عدم انتشار الأسلحة النووية (NPT)، المادة 3، 1970، www.un.org/disarmament/WMD/Nuclear/pdf/NPTEnglish_Text.pdf (فيما بعد "NTP").

[204] البيان الوطني للولايات المتحدة

[205] معاهدة عدم انتشار الأسلحة النووية، في الديباجة والمادة 5.

[206] *المرجع نفسه* في الديباجة.

[207] *المرجع نفسه* في المادة 3.

[208] *المرجع نفسه*.

[209] "المبادرة العالمية لمكافحة الإرهاب النووي"، وزارة الدفاع الأمريكية، www.state.gov/t/isn/c18406.htm.

[210] إعلان المبادئ، المبادرة العالمية لمكافحة الإرهاب النووي، وزارة الدفاع الأمريكية، www.state.gov/documents/organization/141995.pdf.

كما أن الجهود الدولية المبذولة لضمان السلام في مجالات جديدة أخرى لا حدود لها تشجع بقوة التعاون الدولي الواسع. فعلى سبيل المثال، يشمل إعلان المبادئ القانونية التي تحكم أنشطة الدول في مجال استكشاف الفضاء الخارجي واستخدامه، من بين مبادئه التوجيهية، الاقتراح الذي يقضي بأن تسعى جميع الدول الأعضاء إلى التعاون والمساعدة المتبادلة في مجال استكشاف الفضاء الخارجي واستخدامه.[211]

ويقترح الأمين العام للاتحاد الدولي للاتصالات، إذ يدرك الخطر المتنامي لهجوم سيبراني يمكن أن يصدر من أي مكان وأن يؤثر على كل بلد، خمسة مبادئ توجيهية لإحلال السلام وحفظه في العالم السيبراني الناشئ. وتشمل هذه المبادئ قيم الاتحاد وثقافته وترتقي بها وهي موضحة عبر تاريخه العريق من خلال الدور الريادي الذي يضطلع به في مجال وضع المعايير والتنظيم على المستوى الدولي. وتشكل لوائح الاتصالات الدولية (ITR) المرجعية الصادرة عن الاتحاد مثالاً واحداً فقط على هذا التقليد القائم على تعزيز التنمية المتسقة وكفاءة التشغيل والنفاذ الشامل في مجال الاتصالات الدولية والتكنولوجيا. وقد أعدت لوائح الاتصالات الدولية كإطار تنظيمي جديد لمعالجة القضايا الناشئة والتحديات التي تصاحب عالم الاتصالات الجديد الذي تجسد في أواخر ثمانينات القرن الماضي.[212] وقد صيغت هذه اللوائح لتعزيز الكفاءة والتنمية في إطار التعاضد والتعاون والنفاذ العادل مما يجعلها تجسد تقاليد الاتحاد. كما أنها تبرز تركيز الاتحاد على حماية الحق في الاتصال وفي الوقت نفسه تفادي إلحاق الضرر بالمرافق.

وعلى غرار ذلك، تتضمن المبادئ الخمسة التي اقترحها الأمين العام للاتحاد الدولي للاتصالات فيما يتعلق بالسلام السيبراني هذه القيم الجوهرية مع تحديد إجراءات والتزامات محددة من شأنها أن تضمن السلام والاستقرار في الفضاء السيبراني. وتنص هذه المبادئ على ما يلي:

1 أن تلتزم كل حكومة بإتاحة نفاذ شعبها إلى الاتصالات.

2 أن تلتزم كل حكومة بتأمين الحماية لشعبها في الفضاء السيبراني.

3 أن يلتزم كل بلد بعدم إيواء الإرهابيين/المجرمين في أراضيه.

4 أن يلتزم كل بلد بألا يكون الطرف الذي يبدأ بشن هجوم سيبراني على غيره من البلدان.

5 أن يلتزم كل بلد بالتعاون مع غيره ضمن إطار دولي للتعاون لضمان السلام في الفضاء السيبراني.

---

[211] علان المبادئ القانونية التي تحكم أنشطة الدول في مجال استكشاف الفضاء الخارجي (الفضاء الخارجي)، المبدأ 6، 1967، www.oosa.unvienna.org/oosa/SpaceLaw/lpos.html..

[212] لوائح الاتصالات الدولية: الوثائق الختامية للمؤتمر الإداري العالمي للبرق والهاتف، الاتحاد الدولي للاتصالات، 1989، http://www.itu.int/osg/spu/intset/itu-t/mel88/mel-88-e.pdf.

8 برنامج الأمن السيبراني العالمي للاتحاد الدولي للاتصالات

بقلم الدكتور حمدون إ. توريه

يمثل الاتحاد الدولي للاتصالات محفلاً عالمياً فريداً لمناقشة مسألة الأمن السيبراني. وأدى الاتحاد دوراً كبيراً في مجال الاتصالات وأمن المعلومات ووضع المعايير بصفات مختلفة منذ تأسيسه في 1865، أي منذ 145 سنة مضت. ويدرك الاتحاد أن نطاق التحدي الذي يطرحه الأمن السيبراني وطبيعته يقتضيان توحيد جهود أصحاب المصلحة المتعددين وتنسيقها ومن ثم فهو يعمل في سبيل تحقيق هذا الهدف. ويقوم الاتحاد حالياً بتعزيز الأمن السيبراني من خلال الاضطلاع بمجموعة أنشطة تتصل بالتوحيد القياسي وتقديم المساعدة للبلدان النامية مع مراعاة احتياجاتها الخاصة. واعترافاً بخبرة الاتحاد الطويلة وقدرته وتجربته، فقد عيّنه قادة العالم والحكومات بصفته الجهة الميسرة الوحيدة لخط العمل جيم5 المنبثق عن القمة العالمية لمجتمع المعلومات، بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.[213] ومن ثم، فإن رؤساء الدول وغيرهم من زعماء العالم المشاركين في القمة فضلاً عن الدول الأعضاء في الاتحاد، قد عهدوا إلى الاتحاد بتولي زمام الأمور من خلال اتخاذ خطوات ملموسة لكبح التهديدات وأوجه عدم الأمن فيما يتعلق بمجتمع المعلومات. كما أن مؤتمر المندوبين المفوضين للاتحاد كلّف الأمين العام للاتحاد، بموجب القرار 140 (المراجع في أنطاليا، 2006) الذي يتناول دور الاتحاد في تنفيذ نواتج القمة العالمية لمجتمع المعلومات، بأن يتخذ جميع التدابير اللازمة للوفاء بولاية الاتحاد.

وهكذا، أطلق الأمين العام في مايو 2007 برنامج الأمن السيبراني العالمي (GCA) لتوفير إطار يمكن من خلاله لجميع أصحاب المصلحة تنسيق استجابة دولية للتحديات المتنامية التي يطرحها الأمن السيبراني. ويقوم برنامج الأمن السيبراني العالمي على التعاون الدولي ويرمي إلى إشراك جميع أصحاب المصلحة المعنيين في جهود متضافرة لبناء الثقة والأمن في مجتمع المعلومات. وقبل وقت قصير، أكدت الدول الأعضاء عمل الاتحاد في هذا المجال في مؤتمر المندوبين المفوضين لعام 2010، من خلال إعادة التأكيد على برنامج الأمن السيبراني العالمي باعتباره إطاراً للتعاون الدولي في القرار 130 (المراجع في غوادالاخارا، 2010). ويكلف القرار الأمين العام بمواصلة استعراض التقدم المحرز في نطاق اختصاصه وتعزيزه. وبالتحديد، لاحظت الدول الأعضاء تعزيز دور الاتحاد في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات إلى جانب المبادرة العالمية للاتحاد بالتعاون مع الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبراني (IMPACT) ومنتدى فرق التصدي للحوادث والأمن (FIRST). ويقرر هذا القرار أيضاً الاستمرار في إعطاء أولوية عالية داخل الاتحاد لأعماله المتعلقة بأمن شبكات المعلومات والاتصالات.

---

[213] جدول أعمال تونس.

يرمي برنامج الأمن السيبراني العالمي إلى تحقيق سبعة أهداف استراتيجية رئيسية هي:

أ) وضع استراتيجيات لاستحداث تشريع نموذجي لمكافحة الجريمة السيبرانية يمكن تطبيقه عالمياً وقابل للاستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي.

ب) وضع استراتيجيات عالمية لإيجاد الهياكل التنظيمية والسياسات العامة الملائمة على الصعيدين الوطني والإقليمي بشأن الجريمة السيبرانية.

ج) وضع استراتيجية لصوغ معايير أمنية دنيا وخطط اعتماد للأجهزة الحاسوبية ولتطبيقات البرمجيات والأنظمة تكون مقبولة عالمياً.

د) وضع استراتيجيات لإيجاد إطار عالمي للرصد والإنذار والاستجابة للحوادث لضمان التنسيق عبر الحدود بين المبادرات الجديدة والقائمة.

ه) وضع استراتيجيات عالمية لإنشاء وإقرار نظام هوية رقمي عام عالمي، والهياكل التنظيمية اللازمة لضمان الاعتراف بوثائق التفويض الرقمية عبر الحدود الجغرافية.

و) وضع استراتيجية عالمية لتيسير بناء القدرات البشرية والمؤسسية من أجل تعزيز المعارف والمهارات عبر القطاعات وفي المجالات الآنفة الذكر.

ز) وضع مقترحات بشأن إطار لاستراتيجية عالمية لأصحاب المصلحة المتعددين لتحقيق التعاون والحوار والتنسيق على الصعيد الدولي في جميع المجالات الآنفة الذكر.

وبغية تحقيق هذه الأهداف، يركز برنامج الأمن السيبراني العالمي على خمس ركائز لتوجيه مجالات أنشطته. وهذه الركائز هي كالآتي:

1 التدابير القانونية

ارتفع عدد الجرائم السيبرانية المنظمة نظراً لأن شبكة الإنترنت أثبتت أنها من مجالات التجارة المربحة منخفضة المخاطر. ويعزى ذلك إلى استمرار وجود ثغرات في التشريعات الوطنية والإقليمية مما يجعل من الصعب ملاحقة المجرمين. والهدف من هذه الركيزة، في إطار هيكل برنامج الأمن السيبراني العالمي، وضع استراتيجيات من أجل تطوير نموذج للتشريعات المتعلقة بالجرائم السيبرانية يكون قابلاً للتطبيق والتنفيذ على الصعيد العالمي. ويقوم الاتحاد حالياً بمساعدة الدول الأعضاء في فهم الجوانب القانونية للأمن السيبراني من أجل تنسيق أطرها القانونية لا سيما من خلال موارده المختلفة الخاصة بالتشريعات المتعلقة بالجرائم السيبرانية.

2 التدابير التقنية والإجرائية

تركز هذه الدعامة على تدابير لمعالجة مواطن الضعف في المنتجات البرمجية التي ترمي إلى استحداث خطط الاعتماد والبروتوكولات والمعايير المقبولة عالمياً. ويحتل الاتحاد الدولي للاتصالات ولا سيما قطاع تقييس الاتصالات (ITU-T) وقطاع الاتصالات الراديوية (ITU-R) مكانة فريدة في أعمال التقييس المتعلقة بتكنولوجيا المعلومات والاتصالات كما أنه يؤدي دوراً حيوياً في معالجة أوجه الضعف المتعلقة بالأمن في البروتوكولات. وبغية تحديد التهديدات السيبرانية والتدابير الوقائية للحد من المخاطر، يعمل الاتحاد بشأن توفير خدمات الاتصالات الآمنة وإعادة النظر في إدخال تحسينات على مواصفات الأمن فيما يتعلق باتصالات البيانات المتنقلة من طرف إلى طرف والنظر في متطلبات الأمن فيما يتعلق بخدمات الويب وبروتوكولات التطبيقات. وتوفر الأفرقة المتخصصة ولجان الدراسات التابعة للاتحاد مثل الفريق المتخصص المعني بالشبكات الذكية الذي أنشئ مؤخراً آليات فعالة لتحقيق هذه الأهداف.

3 الهياكل التنظيمية

أدرك العالم أن أنظمة الرصد والإنذار والتصدي للحوادث ضرورية للتصدي للهجمات السيبرانية مثلها مثل التدفق الحر للمعلومات والتعاضد والتعاون بين الهياكل التنظيمية الوطنية وداخلها. وبالتالي فإن هذه الركيزة ترمي إلى إقامة هياكل واستراتيجيات تنظيمية للمساعدة في منع شن هجمات ضد البنى التحتية الحيوية للمعلومات وكشفها والاستجابة لها. وفي هذا السياق، يتعاون الاتحاد مع الدول الأعضاء لتحديد احتياجاتها الخاصة في مجال الأمن السيبراني ومساعدتها في إنشاء أفرقة وطنية للاستجابة للحوادث الحاسوبية (CIRT). كما أن مركز الاستجابة العالمية يؤدي دوراً محورياً في تحقيق أهداف برنامج الأمن السيبراني العالمي، وذلك في إطار التعاون بين الاتحاد والشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبراني (IMPACT).

وأبرم الاتحاد ومؤسسة إمباكت مذكرة تفاهم أصبح من خلالها المقر الرئيسي المتطور لمؤسسة إمباكت في سيبرجايا، ماليزيا، المقر الفعلي لبرنامج الأمن السيبراني العالمي. ويوفر هذا التعاون للدول الأعضاء للاتحاد البالغ عددها 192 دولة عضواً الخبرة والمرافق والموارد اللازمة للتصدي بفعالية لأخطر التهديدات السيبرانية في العالم. وهذا التآزر الوثيق بين مجالات العمل الخمسة لبرنامج الأمن السيبراني العالمي والخدمات والبنية التحتية التي توفرها مؤسسة إمباكت، يجعل هذه الشراكة بمثابة خطوة منطقية في إطار التصدي العالمي للتهديدات السيبرانية. وقد انضم ما يقرب من ستين بلداً لهذا التعاون.[214]

[214] "الشراكة الدولية المتعددة الأطراف لمكافحة التهديدات السيبرانية"، الاتحاد الدولي للاتصالات، www.itu.int/ITU-D/cyb/cybersecurity/impact.html.

وتوفر مؤسسة إمباكت موارد الاستجابة للطوارئ لتسهيل تعرف هوية التهديدات السيبرانية وتبادل الموارد لمساعدة الدول الأعضاء.[215] ومركز الاستجابة العالمية مجهز بغرفة لإدارة الأزمات، وأحدث تكنولوجيا المعلومات وأجهزة اتصالات ومركز لعمليات الأمن يعمل بصورة دائمة وبكل طاقاته، ومركز بيانات آمن مع وجود بيانات احتياطية كاملة، ومرافق للعاملين في نوبات ومركز للإذاعة في الموقع وصالة عرض خاصة بكبار الشخصيات. وهكذا، يؤدي مركز الاستجابة العالمية دوراً محورياً في تحقيق هدف برنامج الأمن السيبراني العالمي المتمثل في وضع تدابير تقنية لمكافحة التهديدات السيبرانية الجديدة والناشئة. وأبرز البرامج الرئيسية لمركز الاستجابة العالمية هما NEWS (نظام الإنذار المبكر للشبكات) وESCAPE (منصة تطبيقات التعاون الآمن إلكترونياً من أجل الخبراء). ويساعد برنامج NEWS الدول الأعضاء على تحديد التهديدات السيبرانية بشكل مبكر ويوفر التوجيه الحاسم بشأن التدابير الواجب اتخاذها للتخفيف من وطأتها. وبرنامج ESCAPE هو من الأدوات والأنظمة المتخصصة التي سيتاح للدول الأعضاء النفاذ إليها. وبرنامج ESCAPE هو أداة إلكترونية تمكّن الخبراء السيبرانيين المخولين من بلدان مختلفة من تجميع الموارد والتعاون فيما بينهم عن بعد، وذلك في ظل بيئة آمنة وموثوقة. ومن خلال تجميع الموارد والخبرة من بلدان مختلفة كثيرة في غضون فترة قصيرة، سيمكّن برنامج ESCAPE فرادى الدول والمجتمع العالمي من التصدي للتهديدات السيبرانية على الفور لا سيما أثناء حالات الأزمات.

إن الأهداف والموارد التي يوفرها هذا التعاون لا تتماشى فحسب مع الركائز الخمس لبرنامج الأمن السيبراني العالمي، وإنما تتوافق أيضاً بشكل وثيق مع مبادئ السلام السيبراني المقترحة. وسوف تساعد الموارد المتاحة للدول الأعضاء من خلال مؤسسة إمباكت كل حكومة في حماية شعبها من الهجوم السيبراني، مما يضمن استمرار نفاذ الجمهور إلى الاتصالات عبر الإنترنت وغيرها من تكنولوجيات المعلومات والاتصالات. ومن خلال الانضمام إلى مؤسسة إمباكت والمشاركة في تبادل الموارد والمناقشات مع دول أعضاء أخرى، ستكون كل دولة قد امتثلت للمبدأ الخامس بصورة فعالة – ألا وهو الالتزام بالتعاون ضمن إطار دولي بما يكفل السلام السيبراني. وعلاوة على ذلك، تقدم مؤسسة إمباكت أيضاً منحاً دراسية للدول الأعضاء من البلدان النامية المؤهلة لذلك لحضور دورات تدريبية تركز على إيجاد مجموعة من الموارد والمعارف المكتسبة التي يمكن للمتدربين تقاسمها مع الآخرين لبناء القدرات والخبرة الوطنية في مجال الأمن السيبراني. ومن شأن هذه المنح الدراسية تحسين قدرة كل بلد على تأمين موارده في مجال تكنولوجيا المعلومات والاتصالات وضمان نفاذ شعبه إلى هذه التكنولوجيات.

---

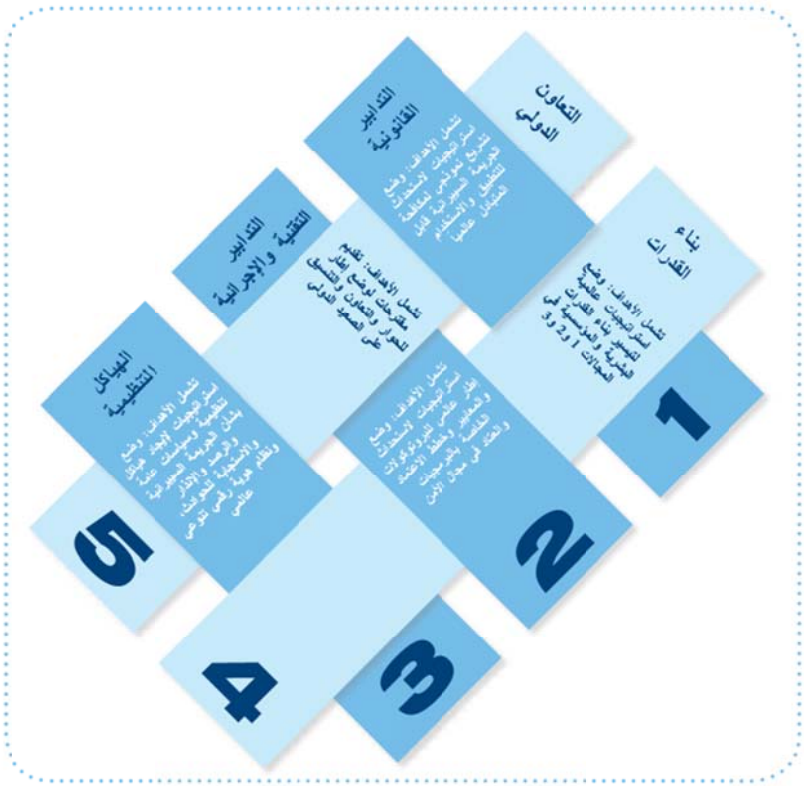
[215] رسالة معلومات موجهة من الاتحاد الدولي للاتصالات إلى جميع الدول الأعضاء بشأن "تنمية القدرات في مجال الأمن السيبراني – مركز الاستجابة العالمية التابع لمؤسسة إمباكت"،
www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT-information-letter- sent-to-member-states-2009.pdf

4 بناء القدرات

تسعى هذه الركيزة في إطار برنامج الأمن السيبراني العالمي إلى تطوير استراتيجيات لتعزيز المعرفة والخبرة لرفع مكانة الأمن السيبراني في جدول أعمال السياسات الوطنية. وهناك حاجة إلى تشجيع بناء القدرات لاستحداث ثقافة مستدامة واستباقية بشأن الأمن السيبراني. وإدراك المخاطر المحتملة في الفضاء السيبراني وفهمها من الأمور الحاسمة لاستفادة المستعمل النهائي من تكنولوجيا المعلومات والاتصالات بصورة آمنة. ويعمل الاتحاد جاهداً في إطار ولايته المتمثلة في مساعدة الدول الأعضاء على تطوير قدراتها في مجال الأمن السيبراني من أجل تسهيل تنفيذ قدرات الأمن السيبراني وتبنيها، مثل دليل الأمن السيبراني الوطني للاتحاد، وموارد الاتحاد المتعلقة بالجريمة السيبرانية، ومجموعة أدوات الاتحاد للحد من البرمجيات الروبوتية الخبيثة.

5 التعاون الدولي

الأمن السيبراني ذو طابع عالمي وبعيد المدى مثله مثل الإنترنت. ولذا، فإن الركيزة الخامسة تؤكد على وضع استراتيجيات من أجل التعاون الدولي والحوار والتنسيق. ويمثل التعاون في إطار مؤسسة إمباكت تقدماً كبيراً في هذا الاتجاه، إذ يوفر محفلاً للدول الأعضاء والأطراف الثالثة لمناقشة السياسة العامة وتبادل المعلومات. وهذا العمل يعزز بصورة مباشرة ولاية الاتحاد أناطتها به طائفة واسعة من الدول الأعضاء بموجب خط العمل جيم5 المنبثق عن القمة العالمية لمجتمع المعلومات. وينص إعلان المبادئ الصادر عن القمة العالمية لمجتمع المعلومات على أن تعزيز إطار الثقة بما في ذلك أمن المعلومات والشبكات، والاستيقان، والخصوصية، وحماية المستهلك، من الشروط المسبقة لتطوير مجتمع المعلومات وبناء الثقة بين مستعملي تكنولوجيا المعلومات والاتصالات. وبغية تحقيق ذلك، هناك حاجة إلى تشجيع ثقافة عالمية بشأن الأمن السيبراني وتطويرها وتنفيذها على نحو فعال بالتعاون مع جميع أصحاب المصلحة والهيئات الدولية المتخصصة. وبالإضافة إلى لوائح الاتصالات الدولية للاتحاد والأفرقة المتخصصة، فإن التعاون في إطار مؤسسة إمباكت يعزز من إطار الثقة، ويعمل في سبيل تحقيق هذه الأهداف باستعمال نهج شامل وتوفير مكان يلتقي فيه جميع أعضاء المجتمع العالمي.



برنامج الأمن السيبراني العالمي: الركائز الاستراتيجية الخمس

الخلاصة

على الرغم من أن التهديدات التي تصاحب التطور السيبراني وزيادة الاعتماد على تكنولوجيا المعلومات والاتصالات تتسم بالخطورة، تظل الفوائد المحتملة أهم بكثير. وعلى الرغم من أننا شهدنا فعلاً بعض مخاطر الحرب السيبرانية، فقد جنيْنا أيضاً فوائد الفضاء السيبراني – كما أن إمكانية تحقيق فوائد في المستقبل لا حدود لها. ويتعين علينا، ونحن نمضي قدماً، أن نعالج بصورة استباقية مسألة كيفية الاستمرار في زيادة الاعتماد على الفضاء السيبراني وتطويره وتكامله فضلاً عن كيفية حماية الموارد وتهيئة بيئة مستقرة لاستمرار ازدهار البنية التحتية والتكنولوجيات الجديدة وكفالة سلام دائم. وعلى الرغم من أن العديد من النهج الحالية تمثل خطوات إيجابية، فإنها لا ترتقي إلى التوقعات وقد لا يوفر كثير منها أكثر الحلول كفاءة. ولكن هناك إمكانية كبيرة تقوم على مبدأ يفيد أن العمل معاً يمكّن من تحقيق هذه الأهداف وتجنب الظروف العصيبة للنـــزاع السيبراني. ويعمل الاتحاد بفعالية في سبيل تحقيق هذا الهدف بشتى الطرق ويسخر الموارد والعوامل المؤثرة اللازمة لتعزيز ما يلزم من دعم ومشاركة متعددة الأطراف.

9 إعلان إريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني

بقلم الاتحاد العالمي للعلماء

إعلان إريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني

إنه إنجاز علمي غير مسبوق أن يصبح بحوزة البشرية الآن الوسائل اللازمة لبسط الموارد الاقتصادية لتشمل جميع البلدان وتعزيز القدرات الفكرية لمواطنيها، وتطوير ثقافتهم وبناء ثقتهم في مجتمعات أخرى، وذلك بفضل استعمال تكنولوجيا المعلومات والاتصالات الحديثة. وتتميز الإنترنت، مثلها مثل سائر العلوم، بطبيعتها العابرة للحدود والمتاحة في كل مكان. وتمثل الإنترنت وأدواتها المرتبطة بها القناة الأساسية للخطاب العلمي على الصعيدين الدولي والوطني إذ توفر للجميع فوائد العلوم المتاحة للجميع بدون سرية وبدون حدود.

وفي القرن الحادي والعشرين، أصبحت الإنترنت والشبكات الأخرى الموصلة بينياً (الفضاء السيبراني) حاسمة لتحقيق رفاه الإنسان والاستقلال السياسي والسلامة الإقليمية للدول.

ويتمثل *الخطر* في أن العالم أصبح على درجة عالية من التوصيل البيني وأصبحت المخاطر والتهديدات معقدة ومتفشية إذ تضاعفت بالمقارنة مع القدرة المتاحة للتصدي لها. وبإمكان الدول أو الأطراف المارقة الآن أن تعطّل بشكل كبير الحياة والمجتمع في جميع البلدان؛ فالجريمة السيبرانية وما ينتج عنها من نزاعات سيبرانية، تهدد التعايش السلمي للبشرية والاستخدام المفيد للفضاء السيبراني.

وتدعم أنظمة وشبكات المعلومات والاتصالات الأمن الوطني والاقتصادي لجميع البلدان وتشكل الجهاز العصبي المركزي لقدرات الاستجابة، والعمليات التجارية والحكومية والخدمات البشرية والصحة العامة والإثراء الشخصي.

وقد أصبحت البنى التحتية للمعلومات وأنظمتها بالغة الأهمية للصحة البشرية والسلامة والرفاهية لا سيما للمسنين والمعوقين والعجزة وصغار السن. ويمكن أن يؤدي تعطل بالغ في الفضاء السيبراني إلى معاناة ودمار لا ضرورة لهما.

وتدعم تكنولوجيا المعلومات والاتصالات مبادئ حقوق الإنسان التي يكفلها القانون الدولي، بما في ذلك *الإعلان العالمي لحقوق الإنسان* (المواد 12 و18 و19) *والعهد الدولي للحقوق المدنية والسياسية* (المواد 12 و18 و19). واضطراب الفضاء السيبراني (أ) يضعف حق الفرد في الخصوصية والأسرة والمأوى والتواصل بدون تدخل أو هجمات، و(ب) يتعارض مع الحق في حرية الفكر والوجدان والدين، و(ج) ينتقص من الحق في حرية الرأي والتعبير، و(د) يحد من الحق في تلقي المعلومات والأفكار ونقلها عبر أي وسيلة كانت دون التقيد بالحدود الجغرافية.

ويمكن أن تكون تكنولوجيا المعلومات وسيلة لجلب الخير أو الضرر ومن ثم فهي أيضاً أداة للسلام أو للنزاع. ويتطلب جني فوائد عصر المعلومات أن تكون شبكات المعلومات وأنظمتها ثابتة وموثوقة ومتيسرة ويمكن التعويل عليها. وتتطلب سلامة الفضاء السيبراني وأمنه واستقراره تضافر الجهود الدولية بصورة عامة.

وبناءً على ذلك، فإننا نؤيد المبادئ التالية لتحقيق الاستقرار والسلام السيبراني وحفظهما:

1 ينبغي لجميع الحكومات الاعتراف بأن القانون الدولي يضمن للأفراد التدفق الحر للمعلومات والأفكار؛ وتنطبق هذه الضمانات أيضاً على الفضاء السيبراني. وينبغي عدم فرض القيود إلا عند الاقتضاء، على أن تخضع لعملية مراجعة قانونية.

2 ينبغي لجميع البلدان العمل معاً لوضع مدونة مشتركة للسلوك السيبراني وإطار قانوني عالمي منسق، بما في ذلك أحكام إجرائية تتعلق بالمساعدة في التحقيق والتعاون بما يكفل احترام الخصوصية وحقوق الإنسان. وينبغي لجميع الحكومات وموفري الخدمات والمستعملين دعم الجهود المبذولة في سبيل إنفاذ القانون الدولي ضد مرتكبي الجرائم السيبرانية.

3 وينبغي لجميع المستعملين وموفري الخدمات والحكومات العمل معاً لضمان ألا يستخدم الفضاء السيبراني بأي شكل من شأنه أن يفضي إلى استغلال المستعملين، لا سيما الشباب والمستضعفين منهم، من خلال العنف أو الإذلال.

4 ينبغي للحكومات والمنظمات والقطاع الخاص بما في ذلك الأفراد، تنفيذ برامج شاملة للأمن وتحديثها بناءً على أفضل الممارسات والمعايير المقبولة دولياً واستعمال تكنولوجيات حماية الخصوصية والأمن.

5 ينبغي لمطوري البرمجيات والمعدات السعي إلى تطوير تكنولوجيات آمنة تعزز القدرة على التصدي وتقاوم نقاط الضعف.

6 ينبغي للحكومات أن تشارك بفعالية في جهود الأمم المتحدة الرامية إلى النهوض بالأمن السيبراني والسلام السيبراني في العالم وأن تتفادى استعمال الفضاء السيبراني من أجل النزاعات.

أعد إعلان إريشتي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء (WFS)، جنيف، واعتمدته الجلسة العامة للاتحاد العالمي للعلماء في الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ العالمية، في إريتشي (صقلية) في 20 أغسطس 2009.

10 خلاصة

بقلم ر. جودي ويستباي

كان السعي إلى إحلال السلام السيبراني حتى الآن هادئاً بشكل يثير القلق. وقد طرح فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء مفهوم السلم السيبراني في إطار برنامج حيوي عرضه في الأكاديمية البابوية للعلوم التابعة للفاتيكان في ديسمبر 2008. ومن ثم، أعد فريق الرصد الدائم "إعلان إريتشيه بشأن مبادئ الاستقرار السيبراني والسلام السيبراني" في 2009، الذي اعتمده الاتحاد العالمي للعلماء وجرى تعميمه على كل عضو من أعضاء الأمم المتحدة. وتبرز المفاهيم والمبادئ المطروحة في هذا المنشور التقييم المتوازن للفريق الذي يفيد أن العالم يميل نحو الفوضى السيبرانية، إلا أن الطريق نحو الأمن السيبراني سينتج عنه استقرار عالمي أكبر.

وتبين الإحصاءات والسيناريوهات المقدمة بهذا الصدد ضرورة احتواء الجرائم السيبرانية والنزاع السيبراني. فشبكة الإنترنت أتاحت ارتكاب عدد من الجرائم نظراً لأن إسناد الجريمة إلى مرتكبها عملية صعبة ونادراً ما يتم القبض على المجرمين ومقاضاتهم. ونخشى أن تصبح الإنترنت أيضاً السلاح المفضل لارتكاب الجرائم. ومع سهولة النفاذ إلى أكثر البيانات حساسية لدولة ما وعمليات البنية التحتية الحاسمة، يمكن لأصغر البلدان أن تتحدى البلدان التي لها أكبر ميزانيات الدفاع. وقد أظهرت البلدان النامية للبلدان المتقدمة كيفية إنشاء بنية تحتية لتكنولوجيا المعلومات والاتصالات بطريقة غير مباشرة من خلال استعمال السواتل والتكنولوجيا اللاسلكية. وعلى غرار ذلك، تدرك البلدان أن الإنجازات السيبرانية تقدم خياراً جذاباً غير مباشر لتعزيز مصالح الأمن الوطني والاقتصادي.

لم لا يكون الاحتواء السيبراني أو السلام السيبراني شعار اليوم؟ وعوضاً عن ذلك، يعلن القادة العسكريون في العالم عن إقامة قيادات سيبرانية وخطط لتعزيز القدرات لشن الهجمات على الشبكات والدفاع عنها واستغلالها. وعندما كانت البلدان تواجه الأسلحة النووية بدأت تطالب باحتوائها ومنع انتشارها. وتكاتفت بلدان العالم حول قضية مشتركة تتمثل في وقف خطر عالمي يهدد البشرية جمعاء. وكما بينت الهجمات على إستونيا وجورجيا، عندما يواجه بلد مهاجَم إطاراً قانونياً دولياً ضعيفاً، وغموضاً دبلوماسياً وقيوداً تقنية وعدم القدرة على تتبع الاتصالات وتسلسلها، يصبح مفهوم السلام السيبراني في الواقع أكثر أهمية.

وعلى الرغم من أن العديد من المنظمات متعددة الجنسيات تعمل حالياً بشأن جوانب مختلفة للجريمة السيبرانية و/أو النزاع السيبراني، فإن الاتحاد هو الوحيد الذي أحاط بنظرة شاملة بهذا الشأن وعرض برنامجاً من أجل معالجة المجالات الرئيسية للمشكلة، مع الاستفادة في الوقت نفسه من الجهود التي تبذلها منظمات

أخرى. ويستحق الأمين العام كل التقدير لقيادته ورؤيته وشجاعته في معالجة مثل هذه المشكلة الضخمة بصورة حاسمة. ونأمل بإخلاص أن تبادر منظمات أخرى إلى تأييد هذا النهج والاقتداء به وأن يخطو القادة خطوة إلى الأمام لوضع مدونة سلوك بشأن الفضاء السيبراني وإطار دولي يدعم استقرار الفضاء الجيوسيبراني ويعمل على تحسينه.

إننا نقترب من حافة هاوية خطيرة في الوقت الذي يلقي فيه الجانب الأسود للإنترنت بظلاله لحجب الفوائد الهائلة لتكنولوجيا المعلومات والاتصالات وزعزعة النظام العالمي. لقد حان الوقت الآن لإحلال السلام السيبراني.

لمزيد من المعلومات:

شعبة الاستراتيجية المؤسسية
الاتحاد الدولي للاتصالات
Place des Nations – 1211 Geneva 20
Switzerland

بريد إلكتروني: strategy@itu.int
www.itu.int/cybersecurity

طبع في سويسرا
جنيف، مارس 2011

03/2011