الاختراق الأمني للدولة الوطنية في عصر ثورة المعلومات

عبد الحفيظ ديب

أستاذ محاضر ونائب عميد لما بعد التدرج

والبحث العلمي والعلاقات الخارجية

كلية العلوم السياسية والإعلام

ـ جامعة الجزائر3ـ

إن التحدي الأمني الذي تواجهه البشرية اليوم، لا يتوقف على أمن الدول فقط، قد أصبح مصير المجتمعات بل مصير كل فرد منا معرضا للخطر، إذ لم يتمكن من الاكتساب العلمي لتقنيات هذا العصر وتحصين أمنه.

إننا نعيش زمن التغيير والنقلة النوعية أو الموجة الثالثة كما يسميها Toffler والذي يصطلح عليه بـ "مجتمع المعلومات" أو كما عبر عنها Péter Druker بـ "مجتمع المعرفة". وأن طبيعة التغيير يترتب عليه رد فعل إيجابي وسلبي حسب رؤية المرء لهذا التغيير، فالبعض لا يرى في هذا التغيير سوى الأخطار على مستقبله بينما يرى فيه الآخر فرص جديدة محفزة في تحقيق ازدهاره.

وقد شبه Laster Thurow هذا التغيير أو هذه التحولات بـ "... أن التحولات التي أحدثتها تقنية المعلومات والاتصالات بنفس حجم الثورة التي نجمت عن اكتشاف الكهرباء قبل قرن من الزمن. فقد انخفض سعر المصباح الكهربائي في عصره بالمقدار والسرعة نفسها التي تنخفض بها أسعار أجهزة الحاسوب الآن،

ومع انخفاض سعر المصباح الكهربائي فقد حول الليل إلى نهار وأصبحت الكهرباء وسيلة رئيسية في حياة البشرية، حيث عرفت إجراءات الأمن والسلامة العامة تطورا مذهلا، كتنظيم حركات المرور والتنقل واستمرار العمل ليلا"[1].

أما اليوم ونحن نعيش بداية الألفية الثالثة، قد أصبحت الوسائل الشائعة للاتصالات المحلية والدولية تتضمن الأجهزة المتطورة؛ مثل أجهزة المؤتمرات المرئية، وأجهزة الفاكس، والبريد الصوتي، والهاتف المتنقل، والبريد الإلكتروني، وخدمات الإنترنيت. ويعد هذا التقدم والتطور في مجال التقنيات بصفة عامة تقدما فائقا لم يقتصر على تطوير الأجهزة فحسب؛ وإنما شمل تطوير البرامج أيضا، وأن تطبيقاته المستقبلية سوف تكون مذهلة. إن التدفق السريع لهذه التقنيات أحدث تغييرا جذريا في سلوك مجتمعاتنا اليومية، حيث أن هذه التقنيات قد بلغت درجة عالية من الدقة والسرعة وهما عماد قوة تقنية المعلومات اليوم، وخاصة بعد ارتباطها بتقنيات الاتصال.

تتناول هذه الدراسة مزايا ثورة المعلومات ودورها في عملية التنمية المستدامة من جهة، والمعوقات الأساسية التي تمنع الدول النامية من استغلال هذه التقنية وجني فوائدها وجعلها عرضة للاختراقات الأمنية وأن حقيقة الحفاظ على السيادة الوطنية في عصر التقنية الجديدة هي لمن يمارس السيطرة على المعلومات حسب قول وزير الاتصالات الصيني ووجوشوان[2] Wu Juchan كما تشمل هذه الورقة ثلاثة محاور هي : المحور الأول : أهمية ودور المعلومات، مزاياها ومهدداتها لاختراقات الأمن الوطني. في حين يتناول المحور الثاني المخاطر الأمنية الجديدة والتهديدات المشتركة وخاصة في قطاع الاتصالات والمعلومات والأمن وفي المجال العسكري والمال والبنوك والخدمات الإنسانية. وأخيرا يتناول المحور الثالث البحث عن أثر التقنية الحديثة على الأمن الوطني والدولي.

I ـ أهمية المعلومات ودورها في تحقيق الأمن

للمعلومات دور رئيسي في الأمن على مر العصور، فحياة الإنسان القديمة، وصراعه مع قوى الطبيعة، حيث كان فيها الإنسان متعطشا للمعلومة لتفسير الظواهر المخيفة بالنسبة له في ذلك العصر، وشمل بحثه عن إجابات للعديد من الظواهر حوله والتي تتطلب البحث عن المعلومات حول ماذا يحدث ؟ لماذا يحدث ؟ متى يحدث ؟ وكيف يحدث ؟... ولم يتوقف ذلك عند الظواهر الطبيعية كالمطر والأعاصير والزلازل بل شمل ذلك خوفه من الحيوانات المفترسة كذلك، كما زادت هذه المخاوف في البحث المستمر عن المعلومات أثناء ظهور الصراعات البشرية، وقد مرت المجتمعات بثلاثة مراحل أساسية من تطور المعلومات مع تطور المجتمعات الإنسانية. ففي المجتمع الزراعي كانت فيه الأرض هي مصدر القوة، وكانت الوسائل التكنولوجية الاتصالية بسيطة، محدودة وبطيئة من خلال المشي على الأقدام، على الخيول وخاصة في الحروب.. ماذا لدى الخصم ؟ ماذا يعرف الخصم عني ؟ وماذا ينوي أن يفعل ؟ ماذا أفعل ؟ كيف لي أن أواجه تهديداته ؟ من ينتصر ؟.. إلخ. وقد استخدم الإنسان كافة الوسائل المتاحة لديه خدمة للحصول على المعلومة التي يمكن أن يوظفها في خدمة أمنه[3].

واستخدام الطيور في نقل المعلومات. وفي العصر الصناعي كانت الآلة هي محور الاقتصاد بدل من القوة العضلية للإنسان والحيوانات وكان مصدر القوة هو رأس المال، بينما في عصر المعلومات، اليوم، فإن القوة الذهنية هي أساس اقتصاد وأن البيانات والمعلومات هي مصدر القوة والثروة ولهذا يجب حمايتها وبقائها سرية لأن المعلومات كانت ولا تزال وستظل القوة الحقيقية لمن يمتلكها ويحافظ بحياته على سريتها.

كان الإنسان ولا يزال وسيظل مهتما بحفظ سر معلوماته على خصومه وعلى الطرف الآخر. فقبل أكثر من 5000 سنة، حمى إمبراطور الصين سر إنتاج الحرير، أودودة القز التي تنتج ألياف الحرير الطبيعي، وشجر التوت الذي يعد الغذاء الأساسي والمسكن المناسب لدودة القز، وقد هدد الإمبراطور من يبوح بسر صناعة الحرير بالقتل تعذيبا. وقد نفعهم هذا النظام الأمني الشديد لمدة وصلت حوالي3000 سنة، حيث نقل هذا السر من أميرة غادرت الصين لتتزوج أميرا في دولة بعيدة[4]. وكذلك، فإن تاريخ الكتابة بالشيفرة تعود إلى 500 سنة قبل الميلاد من قبل حاكم سبارطا الذي يعتبر الأول من استعمل نظام للكتابة العسكرية والمعروف بـ " الشيفرة "، حيث استعملوا وسيلة تدعى " حكاية الماء Sky tale "، وهي وسيلة في تاريخ العلوم العسكرية لنقل الكتابة السرية[5].

يحتدم الصراع بين الأمم منذ بداية التاريخ إلى عصرنا الحالي حول عناصر الثروة، والقوة، والمكانة التي يتنافس عليها كل فرد وكل دولة نظرا لمحدوديتها ونذرتها. ولقد تطورت مستلزمات هذه العناصر من السلاح والصناعة العسكرية الأساسية للطاقة والأسواق مما أصبح تهديد مباشر للأمن الوطني وللدولة والمجتمع معا.

وعلى الرغم كلفة المعلومات والمتمثلة في صعوبة الحصول عليها والمحفوفة بالسرية، إلا أن تقنية الاتصالات وفرت المعلومة بمقدار كبير، ويقول الأستاذ الدكتور ذياب البداينة "... أن الولايات المتحدة الأمريكية تنفق حوالي 5.6 مليار دولار سنويا على فرض السرية على المعلومات، ولديها حوالي 1.5 مليار صفحة حكومية عمرها أكثر من 25 سنة تحت أقفال السرية، وفي عام 1995 تم تصنيف 3.6 مليون وثيقة بأنها سرية منها 400 ألف وثيقة وصفت بأنها سرية للغاية، فإن الوثائق السرية وعلى الرغم من أهميتها، إلا أنها ليست جميعها تتصف بالموثقة وذات مصداقية... وقد عبر عن ذلك السيناتور الأمريكي إدوارد كينيدي بقوله : لا أعتقد أن هناك أكثر من مائة صفحة، أوبضع فئات من الصفحات

على الأكثر من بين آلاف الوثائق التي بحثنا فيها يكون من المهم الآن بقاؤها سرا."[6]

تشمل المعلومات، عادة، قوة مضادة وقيمة مضادة، وتزداد أهمية المعلومات في الأزمات والحروب بشكل كبير، وتوصيل المعلومات من خلال الوسائط المتعددة للنظم العسكرية (القيادة، السيطرة، الاتصالات والاستخبارات والتي تعرف بـ C4I)، عملية هامة تساعد على التوجيه الدقيق في إصابة الأهداف. أما القيمة المضادة للمعلومات فتصبح هي نفسها الهدف المرجو للخصم وعرضة للهجوم والتدمير من خلال التدمير لشامل لبناء القاعدة المعلوماتية.

II ـ المخاطر الجديدة على أمن الدولة الوطنية في مجتمع المعلومات

في مجتمع المعلومات، قد تحول العالم إلى شبكة العنكبوت Cowbeb Modal، موصول بطرق افتراضية وفضائية فائقة السرعة. عالم توحدت فيه البنى التحتية المعلوماتية على المستويات الوطنية والإقليمية والدولية لتصبح بنية معلوماتية كونية. عصر أصبح من الصعب التمييز فيه بين الواقع والخيال والافتراض. عصر تغيرت فيه قواعد الممارسة السياسية والأمنية والاقتصادية، عالم يعاد تشكيله من جديد وبسرعة، عصر حروبه بلا جدود، عصر استبدل فيه الرصاص بالبيانات. عصر تشكل المعلومات الأساس الأهم فيه للأعمال والأمن ولكل شيء[7].

حيث لم تعد الحكومات ولا الدول، في عصر المعلومات، تخشى من بعضها البعض بقدر خشيتها من المنظمات، والجماعات والأفراد. عصر أصبح فيه تصريح أو مقابلة تلفزيونية مع أسامة بن لادن أو حسن نصر الله يجعل من الولايات المتحدة وإسرائيل تعلن حالة التأهب في كثير من المناطق لتحصين مقراتها عبر العالم. وحيث، تستطيع مجموعة من الأفراد أن تغلق مكاتب الكونجرس الأمريكي بسبب مخاوف انتشار الرسائل الملوثة بالجمرة الخبيثة، وخير مثال على ذلك اختفاء الرئيس الأمريكي ونائبه في أحداث 2001/9/11 خوفا من استهدافهما. كما كلف

الولايات المتحدة الأمريكية ـ والتي تعتبر الدولة الأقوى في العالم ـ في نفقاتها على الدفاع أكثر من 9200 مليار دولار (9.2 تريليون) منذ أحداث 11سبتمبر2001 بحجة ما يسمى بـ (محاربة الإرهاب).

لقد أصبحت المعلومات في عصرنا الحالي مصدر قوة نادر وهام لمن يمتلكها، سلاح هجوم وسلاح دفاع، فمعرفة المعلومات عن الخصم ذات قيمة لا تقدر بثمن وخاصة في وقت الأزمات. تكمن قيمة أسلحة المعرفة أساسا في تقنية لمعلومات، حيث هذه التقنية الجديدة تساعد الأمم الصغيرة في إلحاق الأذى بالأمم الكبيرة إذا أتقنت استخدامها. وأصدق مثال على ذلك هو استعمال المجاهدين الأفغان لصاروخ ستينجر ضد الغزاة الروس. وستينجر واحد من أوائل الصواريخ الذكية والتي أثبتت فعاليتها بالحرب، حيث أظهر هذا الصاروخ وبشكل حاسم، بأن الذكاء الصناعي يمكنه أن يصنع سلاحا لا يكلف آلاف الدولارات، ويتوفر عند جماعات في حرب عصابات، يتفوق على طائرة تكلف عدة ملايين من الدولارات، لا تتوفر بأعاد كبيرة إلا للقوى العظمى[9].

وأما الجيل الجديد لسلاح المعلومات هو الأقل علنا، لكنه الأكثر تدميرا، فهو"فيروس البرامج" وتفكيك "الشيفرات" والدخول للمناطق السرية للغاية واختراقها. يقول Scott Borman وPaul Lever، عندما غزا برنامج مدمر على شبكة كمبيوتر وزارة الدفاع الأمريكية عام 1988بأنه : "... ومع وجود 80% من منظومة السلاح الأمريكي تحت التطوير في برامج الكمبيوتر، فإن الهجمات على تلك البرامج قد تكون أبسط الطرق وأرخصها وأكثرها فاعلية لتعطيل الدفاعات الأمريكية"[10]. فقد يكون هذا التخريب ضمن الإمكانات المالية والتقنية لدول صغيرة ومنظمات وجماعات إجرامية.

إن تحدي السيادة الوطنية أو الاختراق للأمن الوطني لأي دولة مهما كانت قوتها قد أصبح تحت التهديد الذي شكلته ثورة المعلومات في عامنا المعاصر. من

هذا المنظور، أن مصدر الثروة الحديث ليس مادة، وإنما معلومات، وموارد المعلومات ليست مقتصرة على منطقة جغرافية محددة أو تستطيع الحكومات أن تفرض عليها ضرائب وتتحكم في نقلها. فأي شخص يستطيع أن يكتب برنامجا معقدا للكمبيوتر يمكنه أن يمر عبر الشبكة الالكترونية دون أن تحس به استخبارات وجمارك العالم.

فالمعلومات كمصدر للثروة هي قيمة ناتجة عن سنوات بحث علمي متراكم مخزون في ذاكرة كمبيوتر استثمرت من خلال إستراتيجية يصطلح عليها بـ "الثروة البشرية" التي حولت القدرات البشرية إلى رأس مال فكري محمول إلكترونيا يصدر إلى العالم الذي هو في حاجة ماسة إلى خدماته. يقول"Walter B.Wriston" يوجد في الفلبين الكثيرون من خرجي الجامعات ولا يوجد لهم وظائف كافية. فكان عليهم أن يواجهوا خيارا صعبا : أن يهاجروا إلى مكان يستفيدون فيه من مهاراتهم أو أن يبقوا في بلادهم في أعمال وضيعة نسبيا ومنخفضة الأجر. أما اليوم، فإنهم يواجهون خيارا جديدا. البقاء في الوطن وتصدير أنتاجهم عبر البنية التحتية الالكترونية للاقتصاد العالمي. وأن العديد من فروع شركات المحاسبة الست الكبرى التي مقرها USA مثلا، تقدم الآن مراجعة حسابات عملائها الأمريكيين بمساعدة الكمبيوتر باستعمال برامج معدلة وفقا لطلب العملاء، يكتبها مبرمجون فليبيون وتشحن عائدة إلى USA عبر الأقمار الصناعية... وفي بعض المهام ترسل المعطيات المالية الخام إلى الفلبين حيث تراجع سجل الحسابات على بعد نصف محيط الكرة الأرضية من مقر تلك الشركات. ليست الفلبين فريدة في هذه المجال وحدها، فالمبرمجون الهنود يكتبون ملايين الأسطر من الرموز لشركات مثل American Express لاستعمالها في مراكز بياناتها، وكل هذا العمل يقوم به "عمال المعرفة" الذين لا تتاح لهم فرص عمل في أوطانهم أوتأشيرات الدخول إلى الدول المتقدمة"[11].

لم تعد، إذا، الجغرافيا حاجزا منيعا أو عائقا أمام عمال المعرفة مادامت الكرة الأرضية مرتبطة واقعيا بشبكة إلكترونية عنكبوتية تشمل الأقمار الصناعية وتقنية الاتصالات التي تنقل عن طريقها المعلومات والأخبار والأموال والصفقات التجارية من مكان إلى آخر بسهولة وسرعة فائقة. هذا الطريق الإلكتروني السريع E :High Way، أصبح المعبر الأساسي الذي تمر من خلاله الأموال والمعلومات ومصالح الدول والأفراد الاقتصادية، والسياسية والأمنية...الخ. كالعقود التجارية وقرارات الحرب وغيرها.

ليس من باب الصدفة أن إسرائيل استهدفت الخطوط التلفزيونية في لبنان، فضلا عن محطة تلفزيون المنار، وذلك بغرض فرض تعتيم إعلامي على ما ارتكبته القوات الإسرائيلية من جرائم في لبنان أثناء الحرب الأخيرة. ولكن، قد شاهدهم العالم، في ظل وجود تكنولوجية الاتصالات الحديثة، والشبكات الالكترونية، التي لا تستطيع أقوى الأسلحة تدميرها، وأيضا الهواتف المحمولة المزودة بكاميرات مصغرة، والتي تم عن طريقها نقل ما يحدث من انتهاكات وجرائم في حق الإنسانية من قبل قوات الاحتلال الأمريكية في أبو غريب وغيرها من المناطق. وأن الطريقة الغير حضارية في إعدام الشهيد البطل صدام حسين تثبت مصداقية قوة ونفوذ هذه التقنيات الحديثة[12].

III – التقنيات الحديثة وأثرها على أمن الدولة الوطنية

إن حرب المعلومات تتطلب منظومة متكاملة من الأجهزة والشبكات، بالإضافة إلى ثقافة الشعوب معلوماتيا، وهو ما يتوافر في مجتمعات الدول المتقدمة، ولكن هذه المنظومة نفسها تجعل هذه الدول بعينها هي الدول الأكثر هشاشة أمام وسائل وأسلحة حرب المعلومات.

فالاعتماد التام على المعلومات وتقنياتها يعني بالدرجة الأولى دول العالم المتقدم فهي الأقرب لشن هذه الحرب عليها، وأن التوافر التقني يغري أعداءها

بالإغارة عليها بوسائل حرب المعلومات، فما من داع للتدخل المباشر إذا كان محفوفا بالمخاطر، مادام الجلوس أمام شاشة كمبيوتر يكفي لإدارة العملية بدقة وإتقان، فما الداعي لزرع قنبلة في طائرة للضغط على نظام أو حكومة في عمل إرهابي، فيكفي التحكم الإلكتروني في برج المراقبة لمطار مثلا، لإلحاق أعداد كبيرة من الطائرات، لا طائرة واحدة، وبعيدا عن غياب المخاطرة ومن مناطق الخطر، فلا يحتاج لأكثر من كمبيوتر محمول في أي مكان بعيد عن البرج يقوم بوظيفته بنجاح باهر.

هذه المخاطر جعلت الهجوم على الولايات المتحدة الأمريكية مستهدفة في قواعدها الاتصالية، عوضا عن الهجوم عليها بالقنابل النووية أكثر احتمالا، وذلك بتعطيل اتصالاتها وإخراج مرافقها الحيوية من الخدمة، حيث كل شيء هناك يدار بالحاسب، وبالتالي شبكات الكهرباء والطاقة، والمؤسسات المالية، وقواعد البيانات الشخصية، والقانونية، والصحية، وحتى العسكرية وغيرها، صارت تدار الكترونيا، وبالتالي، تصبح هدفا ل hackers والإرهابيين، والبعض يئس وراح يجهز نفسه من قيامة يوم القيامة الرقمي أوما يسمى بـ (digital doom day)(DDD).

إذا كان البعض يتهكم على (www (world wide web) وينطقها Wide World Wait، فإن البعض الآخر ينظر إليها بمنتهى الجدية على أنها World Wide War باعتبارها ساحة المعركة القادمة، فالذي يدير العالم الآن هي الآحاد والأسفار، وعندما تندلع الحرب تدور رحاها لصالح من يتحكم في المعلومات؛ على ما نرى أوما نسمع أوما نعمل أوما نفكر فيه، وكلها حول المعلومات، إنها حرب معلومات التي طغت على أقوى ترسانات الأسلحة المتطورة عالميا[13].

إن مصطلح حرب المعلومات Cyber War ومترادفاته؛ C4I، WAR-I، IW يستخدم بكثافة في وسائل الإعلام المختلفة لهذا العصر وخاصة في المجال السكري، وغالبا ما يُساء فهمه على أنه يعني استخدام الأسلحة عالية التقنية في

الجيوش التقليدية، والصحيح أن في حرب المعلومات تتراجع فيه المدافع والصواريخ، وتتقدم فيه الحواسب لإدارتها[14].

فحرب المعلومات أو information warfare هي استخدام نظم المعلومات لاستغلال وتخريب وتدمير وتعطيل معلومات الخصم وعملياته المبنية على المعلومات ونظم معلوماته وشبكات الحاسب الآلي الخاصة به، وكذلك حماية ما لدي من كل ذلك من هجوم الخصم؛ لإحراز السبق، والتقدم على نظمه العسكرية والاقتصادية. وليس من الضروري أن تنشب تلك الحرب بسبب عداء تقليدي، بل قد تنشب مع منافس تجاري أو اقتصادي، أو خصم ثقافي قد يكون خصما أو صديقا.

لعل أحد الأسباب التي أدت لإساءة فهم معنى ومجال حرب المعلومات في وسائل الإعلام هو عدم وجود تعريف رسمي لحرب المعلومات Information Warfare أو (IW)، فهي ما زالت جديدة نسبيا، وبالمقارنة بالتعريف الوارد في مقدمة هذا المقال يحصر البعض النظر إلى حرب المعلومات بمنظار عسكري، فلا يمكن لوزارة الدفاع الأمريكية، مثلا، النظر إلى حرب المعلومات إلا على أنها الأعمال التي تتخذ لإحراز التفوق المعلوماتي بمساعدة الإستراتيجية القومية العسكرية للتأثير سلبا على معلومات العدو ونظم معلوماته، وحماية ما لدي من معلومات ونظم.

ومع ما سبق من تعريفات لحرب المعلومات واختلاف وجهات وزوايا النظر إليها، فإن الخبراء في مجال التقنيات يعرفون حرب المعلومات عن طريق فصلها إلى ثلاثة مستويات : شخصية، ومؤسسية، وعالمية. فنلخصها بإيجاز :[15]

حرب المعلومات الشخصية

يتم فيها الهجوم على خصوصية الأفراد في الفضاء المعلوماتي بالتصنت عليهم ومراقبة شؤونهم الإلكترونية عبر البريد الإلكتروني. ومكتب التحقيقات الفيدرالية الأمريكية له برنامج carnivore الشهير في التلصص على البرد

الإلكترونية. كذلك العبث بالسجلات الرقمية وتغيير مداخلاتها المخزونة في قواعد البيانات... وفيلم الشبكة The Net يعتبر مثالا دراميا يقرب الصورة لنتائج حرب المعلومات الشخصية، حيث لفق للشخصية الرئيسية فيه تهم القتل وتهريب المخدرات، بل وطمست شخصيتها الحقيقة واستبدلت هويتها بهوية جديدة.

حرب المعلومات بين الشركات والمؤسسات

وهي حرب تدور ضمن إطار المنافسة أكثر من العداء إلا أنها ليست بالشريفة بأي معيار، وتسودها قوانين الحرب التي قوامها استباحة كل شيء لتعطيل المنافس وتهديد أسواقه. فقد تقوم شركة باختراق النظام المعلوماتي لمنافسها، وتسرق نتائج وتفاصيل أبحاثه. ليس هذا فحسب بل قد تدمر البيانات الخاصة بمنافسها أو تستبدلها ببيانات زائفة في لمح البصر، وتستطيع بعد هذه الجولة من الحرب المعلوماتية أن تجعل الأمر يبدوكما لو كان حادثا أحدثه فيروس كمبيوتري.

حرب المعلومات العالمية

ينشب هذا النوع من الحرب المعلوماتية بين الدول وبعضها البعض، أوقد تشنه القوى الاقتصادية العالمية ضد بلدان بعينها، لسرقة أسرار الخصوم أو الأعداء وتوجيه تلك المعلومات ضده.. وهي حروب قائمة وجارية بالفعل، والجدل المثار حول نظام التجسس بين الدول الكبرى ـ بون استثناء ـ هو أبرز تجليات تلك الحرب. وأحدث وأكثر قضاياها سخونة على الساحة العالمية في هذه الألفية.

كما أن للأخطاء البشرية تعد السبب الرئيسي في الثغرات الأمنية وليست التكنولوجيا وحدها هي السبب وراء الثغرات الأمنية في تكنولوجيا المعلومات. وقال المسح المعنون «الالتزام بالقواعد الأمنية : تحليل أمن تكنولوجيا المعلومات الذي أعدته مؤسسة صناعة تقنيات الحاسب «C T I A» بـ «أن الأمر يتطلب مزيداً من التدريب والتأهيل إذا ما أراد العاملون في مجال تكنولوجيا المعلومات

وكذلك شركاتهم والهيئات الحكومية التعامل بصورة أفضل من معدلات اختراق النظم الأمنية المطبقة على أجهزة الحاسب الآلي الخاصة بهم. وأشار إلى أن أكثر من 63% من الاختراقات الأمنية ترجع في الأساس إلى أخطاء بشرية»[16].

خاتمة

نظرا لزيادة الاعتمادية على المعلومات في تسيير كافة النشاطات الإنسانية، فقد أصبحت المعلومات وسيلة وهدفا وقيمة عالية في تحقيق الأهداف الاجتماعية والسياسية والأمنية. ولأن الحصول عل المعلومة قد أصبح أسهل وغير مكلف، ولأنها ذات قيمة أمنية هامة، فقد أصبح الحصول عليها بالطرق المشروعة وغير المشروعة عملية في غاية الأهمية، نجم عنها التفكير بحمايتها والسعي لامتلاكها بأي ثمن وبأدوات ونظم تقنية عالية.

إن تدمير البنية المعلوماتية لأي طرف قد يؤدي حتما إلى وضع المجتمع في حالة من الفوضى الرهيبة، حيث لا ماء، ولا كهرباء، ولا طعام، ولا مواصلات، ولا اتصالات. بمعنى أدق، قد استبدلت المفاهيم الأمنية وحلت مفاهيم أمنية معلوماتية تتماشى مع البناء التحتي للبنية المعلوماتية، فظهر الإرهاب الإلكتروني أو الفضائي، وجرائم المعلومات، وزاد استخدام عمليات الاستخبارات الفضائية، وأصبح نقل المعلومة من مكان لآخر عملية في غاية السهولة واليسر.

كما أن نقل مئات المليارات من الدولارات يوميا، (2000 مليار دولار)، تتم عبر الفضاء دون الحاجة إلى دخول إلى خزينة البنوك. كل هذه التغيرات جعلت الأمن في مجتمع المعلومات مختلفا عنه في ما قبلها. فقد تلاشت الحدود السياسية بمعناها التقليدي، وتلاشت معها تأشيرات السفر، وأصبحت الاتصالات والمواصلات تربط الكون بشكل فعال. لقد أصبحت الثقافة والسلوك والجريمة والاقتصاد والسياسة...الخ، عابرة للحدود الوطنية. فهماك السفر الافتراضي،

يسافر فيه الأفراد بين المجتمعات ولكن الفرد لم يغادر منزله، وفيه تواصل مع الشعوب عن بعد، فيه جريمة عن بعد، فيه إدارة عن بعد. بمعنى آخر، فيه تأسيس مصالح عن بعد، وتنشأ علاقات صداقة عن بعد، وعداوة عن بعد، فقد أصبح الفضاء مشاع للجميع ومن يسيطر عليه يمتلك القوة والثروة ويمكنه من فرض إرادته على الآخرين.

جدول التطور

ينقسم تطور النوع البشري إلى أربع مراحل ؛ وهي :

الصيد والجمع : 3000000 سنة

الزراعة وتربية الحيوانات : 30000 سنة

الصناعة والتجارة : 300 سنة

الإبداع والاتصال : ؟ ؟

تفاصيل الجدول التطور

النشاط	الصيد والجمع	الزراعة/ تربية والحيوان	الصناعة والتجارة	الإبداع والاتصال
الأدوات	الأظافر والأسنان	الأذرع والأرجل	الحواس الداخلية	أعضاء الدماغ
القوة	الانسجام مع الطبيعة	ملكية الأرض	توافر الرأس المال	التمكن من البيانات الالكترونية
التبادل	المقايضة	العملات المعدنية	النقود الورقية	برامج الحاسوب التفاعلية
الاتصال	الشافهة	الكتابة والمخطوطات	وسائل الإعلام المسموعة والمرئية	شبكات متجاوبة
التنظيم	الأسطورة والقبيلة	النظام الملكي والملكة	الديمقراطية ودولة	ما بعد التاريخ
التاريخ	ما قبل التاريخ	التاريخ المقدس	التاريخ العلماني	

المراجع بالعربية

1- ندوة في كتاب : إشراف الأستاذ، جمال السويدي، "ثورة المعلومات والاتصالات وتأثيرها في الدولة والمجتمع بالعالم العربي"، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الإستراتيجية، أبوظبي، 1998.(1) ص. 19ـ20.

2ـ د/ذياب البداينة، "الأمن وحرب المعلومات"، دار الشروق للنشر والتوزيع، الإصدار الثاني، عمان، 2006. (2،3،4،5،6)، ص. ص. 57ـ104. 153ـ196.

3- د/ راشد بن سالم بن راشد البادي، "أثر التقنيات المعاصرة على الأمن"، دار العلوم العربية، بيروت، الطبعة الأولى، 2007. (7،8،9،10،11) ص ص 37ـ56. 168ـ181.

4- د/ عمار بوحوش، " نظريات الإدارة الحديثة في القرن الواحد والعشرين"، دار الغرب الإسلامي، بيروت، الطبعة الأولى، 2006. ص. 182.

5- مجموعة من المؤلفين، "الحرب السادسة : النصر المختطف"، مكتبة الشروق الدولية، الطبعة الأولى، بيروت، 2007. (14)، ص. 153.

English Bibiography :

6. Walter B. Wriston : "The Twilight of Sovereignty : How the Information Revolution is transforming our World", Macmillan Publishing Company, U.S.A., 1992. (12,13), pp. 142. 49.

7. D. Peter Huber : " Law and Disorder in Cyberspace", Oxford University Press, Oxford, England, 1997. (15, 16), pp 134.5.41.

8. Boorda, J.M. (1995). Leading the Revolution in C4I, Joint Forces Quarterly, Available (in PDF/ Adobe Acrobat format) via WWW at : http : / www. dtie.mil / doctrine / jel / jfq _ pubs / 0809. pdf.

9. Gillam, M. M. (1997), Information Warfare : Combating the Threat in the 21st Century, via WWW at : http : / www. au. af. Mil / au / database / projects / ay 1997 / acsc / 97, 0603C. pdf