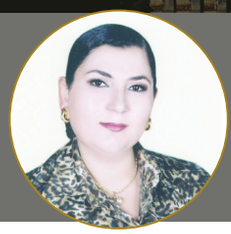
أمن البنية التحتية:
مشكلة تأمين البنية الأساسية ضد التهديدات الإرهابية



د.أمل صقر

منسق برنامج دراسة التحولات السياسية - مركز المستقبل للأبحاث والدراسات المتقدمة، أبوظبي

بات تعرض البنى التحتية، في كثير من الدول، إلى عمليات إرهابية من الأعمال الشائعة في السنوات الأخيرة، ولم يعد استهداف الجماعات الإرهابية لهذه البنى يتم بشكل عشوائي، كما كان في السابق، إذ تنحو هذه التنظيمات الآن إلى استهداف مدروس ومخطط لبنى تحتية لا تصيب الدولة فقط.

بات من الوارد استهداف البنى التحتية بأعمال إرهابية تؤثر على مجريات الحياة اليومية، مثل استهداف محطات الكهرباء الأساسية وخطوط السكك الحديدية، أو محاولة استهداف موانئ حيوية. وعلى الرغم من اختلاف شدة وتأثير هذه العمليات على سلامة البنى التحتية، وتفاوت تأثيراتها على المستوى القومي، فإن مثل هذه العمليات أشارت بقوة إلى خطر مهم يهدد أمن الدول واستقرارها.

وتعد البنى التحتية واستثماراتها أحد المعايير المهمة لقياس التقدم في دولة ما، وتعتمد عدداً من المؤشرات الدولية لقياس التقدم الاقتصادي في دولة ما وأفضليتها في جذب الاستثمارات على مؤشر جودة البنية التحتية، ومقدار الإنفاق على تطويرها. وتشير الإحصاءات إلى أن دول مجلس التعاون لدول الخليج العربية، وعلى رأسها دولة الإمارات، من أبرز الدول إنفاقاً على بنيتها التحتية، وقد احتلت دولة الإمارات المرتبة الثالثة عالمياً في مؤشر الاستثمار في البنية التحتية عام 2014[1]. وبلغت قيمة العقود المتوقع ترسيتها في مشاريع البنى التحتية في دول المجلس نهاية هذا العام 45 مليار دولار، وهي ضعف قيمة العقود المبرمة في القطاع عام 2012، والتي بلغت 22.6 مليار دولار، وتتجه أغلبها إلى مجالات السكك الحديدية والطرق والمطارات والموانئ[2]. ما سبق يؤكد أهمية البنى التحتية، والحاجة الماسة إلى تأمينها ضد أي أعمال إرهابية محتملة.

أولاً: مستويات تعريف البنية التحتية

مر مفهوم البنية التحتية بالعديد من التطورات، التي تزامنت مع التطور المجتمعي والصناعي والاقتصادي بصفة عامة، وفي هذا الصدد يمكن تحديد ثلاثة مستويات أساسية لتعريف البنية التحتية؛ المستوى الأول هو البنية التحتية التقليدية، والمستوى الثاني هو البنية التحتية الحرجة، والمستوى الثالث هو البنية التحتية الافتراضية الخاصة بمجال الفضاء الإلكتروني. ووفقاً للمكانة والدور والأهمية التي تلعبها منظومة محددة من منظومات البنية التحتية في استقرار واستمرارية وفاعلية نظام ما، يمكن تصنيفها باعتبارها بنية تحتية تقليدية أو حرجة[3].

1- البنية التحتية التقليدية

تتنوع تعريفات البنية التحتية، فهي: "منظومة المنشآت والتجهيزات والخدمات اللازمة من أجل أن تتمكن مؤسسة ما من أداء عملها"، ومن ناحية

أكثر شمولاً هي: "النظم الأساسية المادية وكل البنى التي تمد اقتصاد بلد ما بالقدرة على الإنتاج". وبذلك تتناسب القدرة الإنتاجية لأي بلد طردياً مع درجة تقدم وقوة ومتانة بنيتها التحتية وكفاءتها. وفي الأغلب تتولى الدولة تشييد تلك البنى، إلا في حالات استثنائية، عندما تصل درجة خصخصة الاقتصاد إلى درجات متقدمة كما هي الحال في الاقتصاد الأميركي[4].

وتحدد التعريفات الأكثر تفصيلاً عناصر هذه البنى التحتية بكونها "كل التجهيزات والمنظومات التي تمثل العمود الفقري والأساسي، والتي يتم تشييدها لكي تلبي الاحتياجات الحضرية والرفاهية للمواطنين، وتساعد الاقتصاد الوطني في العمل والإنتاج وتشمل: خدمات المرافق المختلفة، مثل شبكات المياه والصرف الصحي وتشييد منشآت التعليم والمستشفيات، وخدمات الأمن والدفاع المدني والترفيه، وشبكات المواصلات من طرق وسكك حديدية وجسور، وشبكات الاتصالات، وكذلك مرافق توليد الكهرباء وتوزيعها، والموانئ، والمطارات، والأنفاق، والسدود، ومصافي النفط، والمنشآت الحكومية المهمة[5].

وهناك اتجاهات توسع من دائرة تعريف البنية التحتية وتعتبرها مكونة من شقين، البنية الصلبة أو المادية، والتي تضم كل ما سبقت الإشارة إليه، بالإضافة إلى البنية المرنة التي تضم البنية الافتراضية، ومنها نظم تكنولوجيا المعلومات، وشبكات الإنترنت، بالإضافة إلى البنية التحتية "الناعمة"، والتي لها علاقة بالبرامج التنموية، التي تتبناها دولة ما، وكذا قدراتها التدريبية، ونظمها التعليمية، ومنظومة القوانين والتشريعات، التي تعتمدها، وحركة الأموال والاستثمار[6]. وعلى الرغم من أهمية الأبعاد المتعلقة بالقدرات الناعمة للدولة الواردة في هذا التعريف، فإنها لاتزال موضوعاً خلافياً فيما يتعلق بدمجها ضمن مقومات البنية التحتية من عدمه.

2- البنية التحتية الحرجة

المقصود بهذا المفهوم، مكونات البنية التحتية الجوهرية اللازمة لبقاء الخدمات الاجتماعية والاقتصادية الأساسية فاعلة، وهي بذلك أنظمة ومرافق وممتلكات إذا تعرضت للتدمير أو العطل فإن من شأن ذلك أن يؤثر سلباً على الأمن والاقتصاد والصحة والسلامة ورفاهة ورخاء وحياة السكان بدرجة قد تعتبر تهديداً للأمن القومي. وبذلك تعتبر البنية التحتية الحرجة من النظم والعمليات الأكثر حساسية وانكشافاً، نتيجة دورها الحيوي الذي تلعبه في بنية النظام وفاعليته واستقراره، بالإضافة إلى انعدام القدرة – في حال تعرضها للعطل أو التدمير – على استبدالها من دون تكلفة شديدة الارتفاع[7].

ومن أبرز عناصر البنى التحتية الحرجة: (السدود، والجسور الرئيسية الكبرى التي تصل الجزر بالكتلة الأساسية من الدولة، على سبيل المثال، جسر "جولدن جيت في نيويورك Golden Gate Bridge، ومولدات الطاقة الكهربائية والنووية، وموزعات الطاقة الكهربائية، والبنى التحتية للغاز والنفط، ووسائل الاتصال، ومنظومات المال والبنوك، ووسائل المواصلات، ومنظومات المياه والصرف الصحي، وقطاعات الطوارئ في المستشفيات الكبرى). ومن المهم ملاحظة أن البنية التحتية الحرجة أمر يختلف من دولة إلى أخرى وفقاً لدرجة تعقد وارتباط المنظومات المحركة لعمليات الإنتاج والمجتمع وارتباط بعضها ببعض. فالولايات المتحدة الأمريكية، على سبيل المثال، تعتبر أن لديها نحو 50 ألف منشأة بنية تحتية حرجة، تضم إلى جانب ما سبق ذكره قطاعات الصناعة العسكرية، وقطاعات صناعة الغذاء، بالإضافة إلى "الروابط nodes" المتعلقة بأدوات التوصيل والربط والمقصود مثلاً: (المطارات والموانئ، والأنفاق ومحطات الطاقة)[8].

3- البنية التحتية الافتراضية

مع التطور في البنية التقنية للمجتمع العالمي، والدور الذي تلعبه التكنولوجيا في عملية الإنتاج، ظهر ما يمكن تسميته البنية التحتية الافتراضية. وتتنوع التعريفات المختلفة التي تقدم لتحديد ماهية البنية التحتية الافتراضية، فتعرفها مصادر بأنها: "المنظومة المعلوماتية التي تضم أجهزة الكمبيوتر وقواعد المعلومات وشبكات الربط التي تصل هذه المنظومة، وشبكات الإنترنت، والبرامج والبرمجيات المستخدمة، والتي تستخدم جميعها لتسهيل عمل البنية التحتية التقليدية والحرجة في الدولة"[9]، أما اللجنة الوطنية لأمن البنية التحتية الحرجة في الولايات المتحدة الأمريكية فتعرف البنية التحتية الافتراضية باعتبارها كل التكنولوجيات التي تتعامل معها وسائل الاتصال والمواصلات ومولدات الطاقة الكهربية ومحطات إمدادات الغاز الطبيعي والمياه والصرف الصحي[10].

وتشير الدراسات إلى أن البنية التحتية الحرجة باتت أكثر الأمور اعتماداً على البنية التحتية الافتراضية، خاصة في اتصالها بشبكة الإنترنت، حيث توفر كثيراً في التكاليف، فلو تصورنا التكلفة اللازمة لإدارة منظومات كبرى لشبكات المياه أو الكهرباء في مدينة كبرى، والتحكم فيها من خلال أيد عاملة، مقارنة بتكلفة إدارة مثل هذه المنظومة من خلال شبكات الإنترنت، يمكن بالطبع اختيار بديل الإنترنت بسهولة[11]. ويمكن الإشارة إلى عدد من الأمور التي تتعلق بالبنية التحتية الافتراضية، ومنها ما يتعلق بعدم ارتباطها ببلد معين بالضرورة، ومنها ما يتعلق بالدور الذي يلعبه القطاع الخاص في مسؤولية تشييدها، وليس فقط الدولة[12].

ثانياً: أبرز التحديات الأمنية التي تواجه البنى التحتية بأنواعها

لقد أدت العولمة إلى تنامي التعقيد والاعتماد المتبادل بين قطاعات البنى التحتية المختلفة، ما زاد من درجة التهديدات المتوقعة لهذه البنى. ويمكن القول إن التحديات التي تواجه البنى التحتية من الناحية الأمنية ودرجة انكشافها يمكن أن تتوقف على عدد من الأمور، ومنها درجة تعقد وتشابك منظومات البنى التحتية بأنواعها واعتمادها على بعضها البعض، فكلما تعقد النظام وتشابك يزداد درجة انكشافه، فأي ضرر يتعرض له أحد أجزائه سوف تكون له تبعات على باقي الأجزاء[13]. وهناك العديد من الدول التي لا تدرك بوضوح درجة الترابط والتعقيد الذي تعمل من خلالها بناها التحتية الحرجة، وهو ما يزيد من خطوة تعرضها لأي مشكلة؛ لأنها في هذه الحالة لن تكون مستعدة لمواجهة مثل هذه الأخطار، ومن ثم فإن درجة انكشاف هذه النظم تتزايد[14].

من جانب آخر فإن البنية التحتية الحرجة وشبكاتها ومنها، على سبيل المثال، المواصلات وقطاع الطاقة والاتصالات يمكن أن

تكون عرضة للانكشاف، ليس فقط من قبل الفاعلين من الدول، بل أيضاً من قبل الفاعلين من دون الدول، والذين لا يمتلكون القدرات والإمكانيات التي تتوفر للدولة، بل يمكن لتنظيم إرهابي صغير أن يوجه ضربة كبيرة للبنية التحتية لدولة في حجم الولايات المتحدة ومن خارج أراضيها. ونتيجة الاعتماد الكبير للقطاعات الحيوية في الدولة على بعضها البعض، أصبح من السهل إحداث أضرار جسيمة فيها نتيجة تعرضها لعمل تخريبي أو حتى مجرد تعرضها لكارثة طبيعية مثل الأعاصير أو السيول أو الفيضانات[15].

اللافت أن الدرجة التي يمكن بها أن تصبح الأعمال والتنظيمات الإرهابية مصدراً لتهديد البنية التحتية في الدول كانت قضية محل نقاش في فترة من الفترات، خاصة في أعقاب أحداث الحادي عشر من سبتمبر، فقد قللت بعض الآراء من الخطر الذي تمثله التنظيمات الإرهابية في إمكانية أن تستهدف البنى التحتية الحرجة في الدول، كون هذه البنى تتسم بدرجة عالية من المرونة تمكنها من التعامل مع التهديدات الإرهابية بسهولة، وبذلك فإن قدرة أي عمل إرهابي على إصابة هذه البنى بإصابات حقيقية ومهددة للأمن القومي محل شك[16]. في مقابل هذه الرؤية تعتبر دراسات أخرى أن شبكات البنية التحتية الحرجة هي من الأهداف الجذابة لأي أعمال إرهابية وتخريبية من قبل التنظيمات الإرهابية مثل تنظيم القاعدة[17]. من جانب آخر تعبر دراسات أخرى عن أنه من غير الواضح إلى الآن إجابة السؤال التالي: هل يمكن أن تؤدي ضربة قوية ناجحة للبنية التحتية الحرجة – كقطاع الكهرباء على سبيل المثال – للتأثير سلباً في المجتمع بصورة كبيرة، أم أن توجيه الضربة الإرهابية إلى استهداف الأرواح البشرية ورموز معنوية هي الأكثر تأثيراً؟ الأغلب أن رد الفعل في كل حالة أمر نسبي، لأن حالة الهلع من انقطاع الكهرباء عن مدينة بالكامل، على سبيل المثال، يمكن أن توازي ما حدث في الحادي عشر من سبتمبر مثلاً[18].

وتشير الخبرات المعاصرة إلى تعرض البنية التحتية لقطاع الطاقة في دول عدة منها مصر والسعودية، على سبيل المثال، إلى هجمات إرهابية استهدفت هذا القطاع، كونه من القطاعات شديدة التأثير في الاقتصاد من جانب، وانكشافه بدرجة ما من جانب آخر ما يعني قدراً من السهولة في استهدافه[19]، إلى جانب التهديدات الإرهابية، تتعرض البنى التحتية لحوادث فجائية أو كوارث طبيعية، مثل الأعاصير والزلازل والفيضانات. ومن الأمور الخطيرة في تهديد البنية التحتية الحرجة أنها في بعض الحالات يؤدي تعرضها للأضرار أو التدمير إلى آثار عابرة للحدود الوطنية، كما في حال تعرض مفاعل نووي للأضرار وحدوث تسريبات إشعاعية[20].

ومع تنامي اعتماد المجتمعات على البنية التحتية الافتراضية وتنامي دورها في إدارة منظومة البنى التحتية كاملة، وبصفة خاصة البنية التحتية الحرجة، فقد تنامى خطر التهديدات الافتراضية، وباتت التنظيمات الإرهابية حالياً تهتم بصورة كبيرة بتجنيد عناصر من الخبراء في مجال حروب الفضاء الإلكتروني من أجل التمكن من توجيه ضربات حقيقية للبنى التحتية الافتراضية[21].

وكلما ارتبطت البنى التحتية بشبكة الإنترنت، زادت التهديدات التي يمكن أن تتعرض لها هذه البنى، وقد عبّر المستشار السابق لشؤون الإرهاب في الإدارة الأمريكية ريتشارد كلارك، عن أن الولايات المتحدة من الممكن أن تتعرض لما أسماه "بيرل هاربر رقمية" باعتبار أن البنية التحتية الافتراضية من الممكن استهدافها من قبل أعداء الولايات المتحدة[22]، وإن كانت الدراسات ترى أن تعرض البنية التحتية الحرجة لهجمة افتراضية تتطلب وقتاً ومجهوداً وخبراءً، لكنها أمر ممكن. ومن أحد الأمثلة البارزة على تعرض البنية التحتية لهجمات إلكترونية من قبل مخترقين ما قامت به جماعة من القراصنة الإلكترونيين لمحطة كهرباء في كاليفورنيا في إبريل 2001، ومن الأمثلة الأخرى تعرض إسرائيل لهجمات قرصنة إلكترونية من قبل حزب الله في سوريا في عام 2000، استهدفت بنك إسرائيل وكذلك بورصة تل أبيب، ووقتها كانت إسرائيل أكثر ارتباطاً في بنيتها التحتية من دول الجوار. وعلى خلفية التوترات بين إسرائيل وغزة، عام 2006 تمكن بعض القراصنة الفلسطينيين من اختراق عدد من المواقع الإسرائيلية المهمة منها بنوك ووكالات سيارات في إسرائيل[23].

تقترح الدراسات أن على متخذي قرار تأمين شبكات البنية التحتية بصفة عامة الإجابة عن أسئلة رئيسية: إلى أي مدى تعتمد البنية التحتية الحرجة على تكنولوجيا المعلومات وعلى البنية التحتية الافتراضية؟ وإلى أي مدى تعتمد تكنولوجيا المعلومات على شبكة الإنترنت؟

ثالثاً: حالات تطبيقية للتعامل مع أمن البنية التحتية

تقدم الولايات المتحدة أمثلة شديدة الأهمية في القدرة على التعامل مع التهديدات التي تستهدف بنيتها التحتية بأشكالها كافة، وتعتبر من أول دول العالم في الاهتمام بأمن البنية التحتية الحرجة، وتعتمد في هذا الصدد على إنشاء كيانات ومؤسسات هدفها حماية البنية التحتية. وتتعامل الولايات المتحدة بمنطق تبني معايير محددة منها: تأمين المعلومات، والقدرة على ضمان البقاء، والتحسب للايقين، كمفاتيح مهمة في صياغة استراتيجية التأمين والحماية لبنيتها التحتية. وقد أنشأت منذ عام 1997 مؤسسة أمن البنية التحتية، والتي تهدف إلى توقّع وردع وتقييم والحد من استخدام تكنولوجيا المعلومات في تهديد أمن البنى التحتية الحرجة. يشار إلى أن الولايات المتحدة قد صاغت من خلال مؤسساتها الاتحادية، خاصة وزارة الأمن الوطني في 2006، ما يعرف بخطة أمن البنية التحتية الوطنية (National Infrastructure Protection Plan)، وحددت فيها الأدوار التي تلبيها الدولة وكذلك القطاع الخاص والأفراد في حماية البنى التحتية[24].

كما تبدي الولايات المتحدة وغيرها من الدول، التي تمتلك محطات طاقة نووية أهمية كبيرة بتأمين هذه البنى، من منطلق أن تعرضها لأي عمل هجومي يعد من الأمور التي تحمل أبعاداً كارثية على الأمن القومي والبيئي ليس فقط في حدود الدولة، بل إن تأثيراتها تمتد إلى دول الجوار، كما أن هناك خطراً يكمن في أن تعرض هذه البنية للتخريب المتعمد بهدف الاستلاء على المواد النووية التي تمكن من تصنيع أسلحة نووية أمر ذو مردود خطير على الأمن القومي. لذلك قامت الولايات المتحدة بعد أحداث

الحادي عشر من سبتمبر بتأمين هذه المنشآت بوحدات من الجيش الأمريكي[25].

وتقترح الدراسات أن على متخذي قرار تأمين شبكات البنية التحتية بصفة عامة الإجابة عن أسئلة رئيسية: إلى أي مدى تعتمد البنية التحتية الحرجة على تكنولوجيا المعلومات وعلى البنية التحتية الافتراضية؟ وإلى أي مدى تعتمد تكنولوجيا المعلومات على شبكة الإنترنت؟ ونظرياً كيف يمكن أن تكون أكثر الضربات في الفضاء الإلكتروني تأثيراً وفاعلية ضد البنية التحتية؟ وإلى أي مدى يمكن أن تهدد هذه الضربة ركائز أساسية في الأمن القومي؟[26].

من جانب آخر تعتبر الدراسات أن التمكن من تطوير خطط حماية وتأمين البنية التحتية، خاصة الحرجة، يتطلب أمرين على درجة عالية من الأهمية وهما: تحديد دقيق لما يمكن اعتباره منظومات ومكونات البنية التحتية الحرجة، وتحديد مدى ودرجة تشابكها وتعقيدها واعتمادها المتبادل على بعضها البعض[27].

وأشارت تقارير في عام 2012 إلى اعتماد دول منطقة الشرق الأوسط، خاصة دول مجلس التعاون لدول الخليج العربية، على البنية التحتية الافتراضية بصورة كبيرة، وحذرت من أن أغلب دول المجلس غير مستعدة بصورة ملائمة لمواجهة أخطار يمكن أن تتعرض لها هذه البنى، وأن 54% من الشركات في دول مجلس التعاون الخليجي لا تدرك أهمية تبني حلول أمنية للبنى التحتية الافتراضية. ويبدو أن هذا التقرير حمل رسائل تحذيرية مهمة دفعت دول المجلس إلى تبني إجراءات أكثر تركيزاً على تأمين هذه البنى، حيث أجمع 42% من صانعي القرار في شركات تعمل في البنى التحتية الافتراضية في دول المجلس على أن أمن هذه البنى بات محركاً رئيسياً وشاغلاً شديد الأهمية لهم[28].

من جانب آخر تهتم دول المجلس بحماية وتأمين بنيتها التحتية من جوانبها كافة، ولذلك أنشأت أجهزة مختلفة لحماية المنشآت الحيوية. ولايزال على دول المنطقة العمل على بناء منظومات تعاونية لتأمين البنى التحتية، خاصة فيما يتعلق بالبنى التحتية الافتراضية، والعمل على اتخاذ الخطوات المناسبة لتحويل منطقة الخليج إلى "منطقة فضاء إلكتروني آمن" من جانب، والاستثمار البشري والمادي المناسب في اتجاه تأمين البنى التحتية الحرجة بالأساس من خلال تحديد مكوناتها، والسيناريوهات المختلفة للتهديدات التي يمكن أن تواجهها، والطرق المثلى للتعامل معها.

1- الإمارات الثالثة عالمياً في مؤشر استثمارات البنية التحتية 2014، **صحيفة البيان**، 21 سبتمبر 2014، http://goo.gl/4DpSKr

2- إنفاق 300 مليار دولار على المطارات في 5 سنوات، **صحيفة الرؤية**، 16 أكتوبر 2014، http://goo.gl/0o2W2U

3- Mihai Marcel NEAG, Critical Infrastructure Protection-The Foundation Of National Security, (**Buletin Ştiinţific,** Nr. 1 , 37, 2014), p. 57

4-**Ibid.**, p. 56

5- Alexander E Farrell, Hisham Zerriffi, Hadi Dowlatabadi, Energy Infrastructure And Security, (**Annual Review of Environment and Resources**; 2004); p.439

6- Douglas Warfield, Critical Infrastructures: IT Security and Threats from Private Sector Ownership, (**Information Security Journal: A Global Perspective**, Vol. 21, No.3, May 2012), p.128

7- Mihai Marcel NEAG, **Op.cit**, p. 57-59

8- Douglas Warfield, **Op.cit**, p 128

9- Kenneth Geers, The Cyber Threat to National Critical Infrastructures: Beyond Theory, (**Information Security Journal: A Global Perspective**, Vol 18, No.1, Feb 2009), p.1

10- Richard L. Baskerville, A Possibility Theory Framework for Security Evaluation in National Infrastructure Protection, (**Journal of Database Management**, Volume 14, Issue 2. 2003), p.2

11- Kenneth Geers, **Op.cit**, p.3

12-Silvia-Alexandra Zaharia, NATO AND EU: POLICIES, STRATEGIES, ACTIONS, "Critical Infrastructure": Concept's Evolution And Prospects Within The Euro-Atlantic Framework, (**STRATEGIC IMPACT**, No.4, 2012), p.59

13- Douglas Warfield, **Op.cit**, p. 128

14- **Ibid**, p.127

15- Silvia-Alexandra Zaharia, **Op.cit**, p. 62

16- Richard Matthew, And George Shambaugh, The Limits of Terrorism: A Network Perspective, (**International Studies Review**, No. 7, 2005), p. 619

17- Sir David Omand GCBCambridge, Ethical Guidelines in Using Secret Intelligence for Public Security, (**Review of International Affairs**, Vol. 19, No. 4, December 2006), p.614

18- Alexander E Farrell, **Op.cit**, p.423

19- Martin Rudner, Protecting Canada's Critical National Infrastructure From Terrorism- Mapping A Proactive Strategy For Energy Security, (**International Journal**, Summer 2009), p.778

20- Alexander E. Farrell, **Op.cit**, p. 421

21- Richard L. Baskerville, **Op.cit**, p.4

22- Kenneth Geers, **Op.cit**, p.1-2, and Alexander E Farrell, p. 433

23-**Ibid**, p. 4

24- Silvia-Alexandra Zaharia, **Op.cit**, p. 62

25- Alexander E Farrell, **Op.cit**,p. 452

26- Richard L. Baskerville, **Op.cit**, p.6

27- Alexander E Farrell, **Op.cit**, p.422

28- 2014 IT Security Risks for Virtualization summary report, http://me.kaspersky.com/news?id=9100