

ASK PC
MAGAZINE[®]

Free Periodical E-Publication

2010

**IS IT THE YEAR OF
INFORMATION WARFARE?**

The World Is Involved In Cyberwar!

E-WASTE DISPOSAL & THE MIDDLE EAST

TOP THREATS FOR 2011

MIDDLE EAST FRAGILE ICT INFRASTRUCTURE



WikiLeaks



تخصصات معتمدة عالميا في تكنولوجيا المعلومات...
شهادات معتمدة عالميا...

لكل من يبحث عن التميز في تكنولوجيا المعلومات والاتصالات



Your Career starts here!

Internationally recognized IT qualifications
Vocational & Academic Programs
eLearning & Instructor-led Training

ASK PC Academy

MENA Centers:
+20100040214

www.ask-pc.com
www.askpc.net
info@ask-pc.com



الفن والتكنولوجيا في الشرق الاوسط!

القراء الاعزاء،

ارحب بكم جميعا في مستهل هذا العدد الجديد من اعداد مجلة اكااديمية ASK PC والتي يشرفنا ان نطرحها لكم بشكل دوري لزيادة المعرفة لدى القاريء العربي المهتم بتكنولوجيا المعلومات.

في مستهل عام 2011 ونحن مازلنا في البداية يبدو اننا ذاهبون لما هو ابعد من افلام الخيال العلمي، والتي في رأيي كان مبتكروها واصحاب افكارها وما زالوا ملهمون للكثير من الافكار والتقنيات التي نستمتع بها في عالمنا المعاصر. لهذا تجد في الدول المتطورة الكثير من الاعمال الفنية التي تعتمد على التكنولوجيا وفي نفس الوقت تتطور وتقدم بدورها افكارا جديدة لهذه التقنيات او للعلماء في مجالات العلوم المختلفة. ربما لو عدنا إلى افلام الخيال العلمي وحرب النجوم على الاخص سنجد ان العلماء حاليا عاكفون على تطوير الكثير من الأفكار التي طرحت في هذه السلسلة من الافلام مثل [حالة البلازما](#) والكثير من التطبيقات الاخرى. لكن عند النظر إلى حال الفن في المنطقة العربية، نجد الكثير من الإسفاف والتلوث السمعي والبصري والاخلاقي ولا نجد ايا من المواد الإعلامية التي تحاول ان تتناول اقل القليل مما يحدث حولنا من تطور. وبما انني مؤمن بان الفن في الكثير من الاحوال هو الملهم للأفكار العبقريّة فأنني ارى الامر غريب في منطقتنا وهذا يفسر ما نحن فيه من تغير في كل شيء...فما هو السبب ؟ للحوار بقية ان شاء الله

المحتوى | Contents

4- The World at War!

6- Security News

7- Automation

8- Freedom Ship

10- Security News

12- E-Waste Disposal in MENA

14- Fragile ICT Infrastructure in MENA

ASK PC Magazine is an electronic magazine published by ASK PC to enhance the information technology knowledge in Arabic language for Arabic native speakers.

ASK PC is a leading IT training company based in the UK, USA, and MENA.

The opinions expressed herein are not necessarily those of ASK PC or the organizations employing the authors.
© 2011 ASK PC

ASK PC Magazine is registered at the Library of Congress.

Copying: Permission to copy for educational purposes only without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage; the ASK PC copyright notice and the title of the publication and its date appears; and notice is given that copying is by permission of ASK PC. To copy otherwise, or to republish, requires specific permission from ASK PC and may require a fee. All names, trademarks, brands or logos mentioned here are properties of their respective owners. Certain photos and artwork used here might have special rights for their own respective owners.

Tel-UK: +44-2033181972
Tel- USA: +1-678-919-2315

ASK PC UK:
Dalton House, 60 Windsor Avenue,
London SW19 2 RR
United Kingdom

www.ask-pc.com





العالم في حالة حرب – د. محمد الجندي

ان جاز لنا استخدام هذا التعبير الذي استخدم خلال اشتعال الحرب العالمية الثانية عندما دخل العالم وبشكل دقيق الدول العظمى وقتها في حرب دامية – فقد تعبر هذه العبارة عن حالة الحرب الافتراضية التي اندلعت على الإنترنت نهاية عام 2010 بسبب موقع...

بدأت القصة عندما تم بدأ موقع Wikileaks بنشر وثائق دبلوماسية سرية على الإنترنت والتي قيل انه تم تسريبها من قاعدة بيانات خاصة بوزارة الدفاع الامريكية. عندها بدأت الكثير من الرسائل السرية للسفارات الخاصة بالولايات المتحدة في دول العالم بالانتشار على الإنترنت وهي ما تسمى Embassy Cables لكونها من المفترض ان تكون سرية او لا يطلع عليها سوى الدبلوماسيون او

الاشخاص المعينون بالامر. موقع Wikileaks ليس جديدا بالمناسبة ولم تكن هذه التسريبات الاولى التي قد سربها اذ نشر من قبل آلاف الوثائق فيما يخص الحرب في كلا من افغانستان والعراق ولم يحرك العالم ساكنا في هذا الامر وهو امر مبهم إلا انه لا يخصنا في هذا المقام فسوف نحاول استعراض بعض الامور المتعلقة بتكنولوجيا المعلومات في هذا المضمار بعيدا عن الجانب السياسي الذي بالطبع يحتاج إلى دراسة وتحليل علمي من المتخصصين في بلادنا!!!

كيف حدثت عملية التسريب الكبيرة؟

الكثيرون بدأوا بالتساؤل عن كيفية حدوث هذا التسريب الكبير لعدد الوثائق السرية التي تم نشر بعضها منها حتى الآن. وهو سؤال منطقي ويحتاج إلى اجابة من المختصين في مجال امن المعلومات والامن القومي وهي الإجابة التي لم اجدها بشكل علمي في اطار ما كتب باللغة العربية. تحديدا في نوفمبر 2010 بدأت Wikileaks بنشر العديد من الوثائق السرية الخاصة بسفارات الولايات المتحدة في الدول المختلفة وقد بدأت هذه الوثائق ايضا بالظهور على عدد من الجرائد والمصادر الصحفية مثل Guardian, New York Times, El Pais, Le Monde و Der Spiegel الالمانية. وكان التسريب مقدارا ضئيلا من الكم الكبير الذي لم ينشر حتى هذه اللحظة وهو ما يقارب الربع مليون وثيقة تتناول الوثائق منذ عام 1966 حتى 2010.

وإذا بحثت عن كيفية تسريب هذه المعلومات او حصول الاشخاص عليها "وان صح القول" بان شخصا يدعى Bradley Manning وهو ضابط في احدى القواعد في العراق هو من قام بالحصول على هذه المعلومات عن طريق الدخول إلى قاعدة البيانات الخاصة بوزارة الدفاع وتحميل هذا العدد الكبير من الوثائق السرية على اسطوانة قابلة لاعادة الكتابة بعد ان غير غلافها إلى غلاف اسطوانة غنائية لكي لا يشك به زملاؤه. ثم بعد ذلك اعطاها إلى Julian Assange مؤسس Wikileaks وفي محادثة قيل انها سجلت وارسلت للـ FBI اعترف هذا الجندي بما فعله لزميله الهاكر المعروف Adrian Lamo الذي وشى به فيما بعد وتم القبض عليه!!! كما اشرنا سابقا "ان صح القول" حيث ان هذا ما نشر علنا في الصحافة وما تناقلته وكالات الأنباء وحتى ما رده خبراء الامن القومي والتقنية في بلادنا. لكن هل هناك سيناريو آخر (بعيدا عن نظرية المؤامرة)؟...

لكي نفهم الامر بشكل دقيق لابد ان نعرف ان هذه الوثائق تم الحصول عليها من نظام امني معقد وهو يسمى SIPERNet او Secure Internet Protocol Router Network للمزيد:

<http://www.fas.org/irp/program/disseminate/siprnet.htm>

وهو نظام يشبه إلى حد بعيد الإنترنت المفتوح للعام إلا انه مقصور على جهات خاصة فقط مثل وزارة الدفاع الامريكية والحكومة الامريكية وبعض الجهات الاخرى فيما لا يتعدى نصف مليون مستخدم معلومون جميعهم ولديهم احقية الدخول لهذه الشبكة ولا يخفي علي القاريء ان كل جزء من هذه الشبكة بالتاكيد له صلاحياته اي انه ليس من المفترض ان تكون مفتوحة امام الجميع بكل الصلاحيات وهذا امر بديهي في مؤسسة ناشئة وليس وزارة الدفاع الامريكية!

عدوة إلى ما يقال عن ان شخصا قام بالدخول إلى هذه الشبكة من قاعدة في العراق وقام بتحميل هذا العدد الهائل من المعلومات بالإضافة إلى ما نشرته الصحف من كونه حصل على دخول لهذه الشبكة لمدة 8 شهور، فهذا امر يستحق وقفة على الاقل من متخصصي امن المعلومات. كيف يحدث تسريب بهذا الحجم من شبكة بهذا الحجم في دولة بهذا الحجم بها كفاءات على الاقل نحن

متأكدون من وجودهم في مجالات التقنية وابتكارهم للكثير من هذه التقنيات الخاصة بالتأمين والتشفير وظهورها بالاساس في وزارة الدفاع الامريكية.. اليس امرا غريبا ان لا يصدر اي نوع من التحذير للقائمين على هذه الشبكة من خبراء في التقنية؟

لماذا لم يستطع اي شخص آخر غير هذا الجندي الصغير الدخول منذ ان تأسست هذه الشبكة؟

لماذا لم تدخل الصين على الاقل ونحن متأكدون من قدراتها في مجال الجيوش الافتراضية والإختراقات التقنية؟

مرة اخرى (نحن لا نرجح نظريات للمؤامرة) ولكن للأسف الشعوب العربية تساهم في ترسيخها...كيف تتأمر جهة على جهة اخرى هي بالاساس مستسلمة (ابن المؤامرة هنا...؟) ليس هذه قضيتنا كما اشرنا ولكن الجانب التقني لايمكنه باي شكل من الاشكال ان يغفل الجانب السياسي وبخاصة عندما تلتقي التكنولوجيا مع السياسة لفرض امور على ارض الواقع.

لم تعد الحروب تقاس بقدرة الجيوش العديدة من مدرعات وعتاد وجنود وانما اصبحت تقاس بقدر ما تمتلك هذه الجيوش من تقنيات وياتت الحروب تدار بالازرار بدلا من المدرعات ولهذا ظهرت "حروب المعلومات" Information Warfare فقد شهد العالم بالفعل في نهاية 2010 حرب معلوماتية من العيار الثقيل سواء اصابته نظرية المؤامرة او اخطات. فأصبح من السهولة تغيير الكثير من الاوضاع في ارض الواقع ببعض نقرات من جهاز الـ Mouse بدلا من خسارة بلايين الدولارات في حروب حقيقة، ليست هذه حروب بمفهومها الجديد والبعيد كل البعد عن اذهان الكثيرين من قاطني هذه المنطقة المليئة بالمشكلات من كل نوع؟

كيف يدخل العالم في حرب بسبب موقع على الإنترنت؟

بما ان الإنترنت هو بالاحرى مرآة لما يحدث في ارض الواقع وبمقدار معين اصبحت مواقع متأثرا بالإنترنت لهذا فرضت هذه التسريبات واقعا مختلفا على ارض الواقع حيث بدأ الإعلام يروج لهذه الوثائق وما بها من معلومات بغض النظر عن ما بها من معلومات قد تكون بالاساس ليست جديدة إلا انها اصبحت موثقة وهو الجزء المهم! فبدأت تظهر جماعات على الإنترنت مدافعة عن حرية التعبير ومدافعة عن حرية المعلومات وتدافع عن احقية الشعوب في معرفة ما يحدث وراء الكواليس السياسية ان صح التعبير. وظهر فريق آخر "ان صحت موافقة" معادي لهذه الظاهرة وهي ظاهرة Wikileaks وبدا باعلان الحرب على هذا الكيان على الإنترنت وتعرض الموقع للإغلاق وما بات ان تعرض للمنع في الكثير من الدول التي تناولتها الوثائق وبخاصة في الشرق الاوسط كما بدأت حرب اخرى على المواقع التي تنشر هذه الوثائق وتعرضها لهجمات من نوع الحرمان من الخدمة DDoS مما ادى إلى تضررها وعدم تمكن وزارها من دخولها لفترات كبيرة. وفجأة بدأت الكثير من المواقع على ارض الواقع والكثير من الجماعات المدافعة عن Wikileaks على الإنترنت وبدأت حرب اخرى مضادة استهدفت المؤسسات التي اعتبرت معادية لـ Wikileaks او التي تسببت باضرار لها مثل مواقع شركات PayPal, MasterCard, VISA والكثير وادت هذه الهجمات إلى خسائر كبيرة بالتأكيد إلا ان المواقع عادت للعمل ما ان هدأت عاصفة الهجوم. لكن نطاق الهجوم بدأ يتسع ليشمل جهات خارج الولايات المتحدة ايضا بل واستهدف ايضا مواقع لجهات في الشرق الاوسط مثل مواقع الحكومة التونسية التي مازالت لا تعمل حتى الآن منذ اكثر من شهر!!!

وبما ان المعلومات التي توضع على الإنترنت يصبح من المستحيل محوها للأبد فقد ظهرت العديد من المواقع على الإنترنت التي تعتبر بمثابة Copy او نسخة طبق الاصل من Wikileaks والتي ابحت تعد بالآلاف الآن ولا يستطيع اي شخص ايقافها جميعا ناهيك عن الملفات التي ترسل او تشارك عبر شبكات Peer2Peer Sharing وهي الاصعب في التتبع والملاحقة!

إذا الامر بات مستحيلا ايقافه...بل والاهم هو ان المواقع بدأ يتأثر كثيرا بما يحدث في الفضاء الإلكتروني Cyberspace فبدأت المظاهرات تجتاح العديد من الدول ومنها الكثير في المنطقة العربية تأثرا بما نشر في بعض الوثائق. لكن ما يعيننا هنا هو ما يحدث على الإنترنت من هجمات وما سوف تؤول اليه الامور في المستقبل من تأثر البنى التحتية لدول باتت تعتمد على التكنولوجيا بشكل كبير كدول مستهلكة مثل الشرق الاوسط لكنها لا تمتلك التقنيات والكفاءات اللازمة للتعامل مع آليات هذه التقنيات الحديثة واطارها او ما قد تنطوي عليه هذه التقنيات ذاتها من ثغرات ومشاكل لا قبل لهذه الدول بها. في النهاية نود الإشارة إلى انه بمقدار اعتماد الدول على التكنولوجيا بمقدار ما سوف تكون متأثرة من حرب معلوماتية تلوح في الافق وتختلف النتائج والتبعات بمقدار ما تمتلكه الاطراف من عتاد في هذا المضمار كما ستحدد الخسارة بمقدار ضعف الاطراف الاخرى في امتلاك هذا العتاد او فقدان آلية التعامل معه!



12- يناير – 2011 – SC Magazine

تحقق السلطات حالياً في استراليا في حادثة اختراق للمعلومات في شركة Vodafone والتي ادى إلى اتاحة معلومات ملايين العملاء الخاصة والسرية متاحة مثل ارقام الهواتف والبيانات الخاصة وبطاقات الإئتمان والعناوين وتشير التقارير إلى ان مجموعة من الجهات التي ليس لها الحق في الحصول على هذه المعلومات مما يعرض الملايين من العملاء للكثير من الاخطار حيث عرضت مجموعة من المجرمين مبالغ طائلة للحصول على هذه المعلومات ايضاً!

نظام ويندوز 7 هو الأفضل | Windows 7 is the Best

9- ديسمبر – 2010 – Techradar.com – كتب محمد هشام

في ظل عالم من التقنية تجد عائلات ويندوز تتسع بأجزائها حتى ظهر ويندوز 7 أفضل نظام ويندوز حتى الان أطلقتى شركة ميكروسوفت فى 22 أكتوبر 2009



وبحسب إحصائيات statcounter فقد وصل نظام ويندوز 7 إلى نسبة 25% من إجمالي سوق أنظمة التشغيل بينما وصل نظام ويندوز إكس بي إلى 50% وهبوطه مازال مستمراً بسبب الاستحسان الذي لاقاه نظام ويندوز 7 الذي بلغت نسبة رضى المستخدمين عنه حوالي 93% بالإضافة إلى أن العديد من قطاعات الأعمال ستقوم بالانتقال إلى النظام بدايات العام 2011. مبيعات ويندوز 7 أيضاً مازالت قوية حيث يتوقع أن يتم بيع 300 مليون رخصة للنظام قبل نهاية العام الحالي.

فميكروسوفت بهذه المناسبة أعلنت عن بيع حوالي 240 مليون رخصة منذ صدور النظام مما يجعل النظام نسخة ويندوز الأكثر مبيعا في التاريخ، كما أن تبني النظام من قبل الشركات المصنعة ممتاز جداً فنسبة استخدام النظام في الأجهزة الجديد تمثل حوالي 97% ونسبة النظام في سوق أنظمة التشغيل العالمي وصلت إلى 17%.

كتب: محمد هشام

تخيلوا أن يأتي اليوم الذي تخرجون فيه من المنزل للعمل ثم تنجزون أعمالكم دون الاضطرار إلى التعامل مع أي إنسان فكل شيء آلي وعبر الكمبيوتر، وفي استراحة الغداء تدخلوا أحد المطاعم فتطلبوا الطعام عبر أيباد مثبت على الطاولة، وبعد أن تتناولوه تقوموا بدفع المبلغ إلكترونياً أيضاً.

بعد العودة إلى المنزل تحسوا بألم غريب في العين فتوجهوا لبرنامج حاسوبي وتجيّبوا عن أسئلة بنعم أو لا ومدة الأعراض وغيرها، فيعطيك البرنامج تشخيصاً للمرض والدواء بالجرعة، ثم تتذكروا الأشعة السينية التي أخذتموها بالأمس فتدخلوا نتائج الأشعة في الماسح الضوئي المنزلي scanner وبواسطة برنامج يقوم بمسح صورة الرأس، وتظهر نتيجة على الشاشة أمامك أنه لا وجود لأورام في دماغك.



التلفاز لا يعرض البرامج التي تعجبكم، لا بأس بإمكانكم التحكم في مواعيد العرض وتسجيل ما فاتكم عن طريق العبث بالإعدادات قليلاً لتناسب أولوياتكم.

لا تستغربوا فالتوجه الحديث الآن هو الأتمتة، ولفهم الفكرة أفضل فإن الأتمتة Automation طبقاً لتعريف ويكيبيديا: هو مصطلح مستحدث يُطلق على كل شيء يعمل ذاتياً (آلياً) دون تدخل بشري.

الجدير بالذكر أن بعض النماذج المذكورة سابقاً موجودة بالفعل، وبعضها لم تأخذ حيز انتشار واسع، ونماذج أخرى لا زالت في مرحلة الدراسات والتجارب، وهناك نماذج مستقبلية لحياة مترفة تعتمد على الحاسب الآلي وتطبيقاته كليا.

الأتمتة مصطلح عام يشمل عدة مجالات كالصناعة والتجارة والطب والإدارة وغيرها، لكنه يشترك في قاعدة أساسية كونه برنامج مكتوب بلغة برمجية معينة بناء على الغرض من إنشائه، ومجموعة البرامج التي تساعد في الأتمتة يُطلق عليها: نظم المعلومات Information systems، وهي استخدام تقنية المعلومات لتسهيل وتيسير العمل أياً كان نشاطه.

مع التوجه الحديث نحو الأتمتة إلا أن الثقة بالحاسب الآلي لا زالت منخفضة فيما يتعلق بالأتمتة الطبية مثلاً، أما بالنسبة للحالات الاستثنائية فنظم المعلومات غير قادرة على التعامل معها كون النظام يتكون من: مدخلات - عمليات - مخرجات، لذا لا يتعامل إلا مع المعطيات وليس مع المواقف غير العادية مثل أتمتة عملية مراقبة هبوط الطائرات والتنسيق بينها، فلو فرضنا أن أحد الطائرات تعرضت لخلل في عجلات الهبوط فالنظام لا يُساعد في شيء، وقد يتسبب في كارثة. هذه الحالة تستلزم إيقاف عمل البرنامج تماماً وتدخل الإنسان لإكمال العمل في ظل الخلل الحاصل.

مع معارضي الأتمتة ترى لديهم كثير من الخوف من أن تسرق نظم المعلومات وظائفهم ويصبحوا من دون فائدة، هذا الشيء لا يمكن أن يحصل لأن الصرافات الآلية هي أكبر دليل على أن الأتمتة، لا يمكن أن تسرق الوظائف كون كل فرع بنك يوجد فيه اثنان أو ثلاثة موظفين مختصين بالصرف لخدمة من تعذرت عليه الاستفادة من الصرافات الآلية.

بالإضافة إلى أن الأتمتة وإن ساعدت في تبسيط حياة البشرية بطريقة كبيرة إلا أن الحاسب الآلي في ذاته والبرامج التي تحقق عملية الأتمتة هي في الأصل من صنع البشر، أخطاء البشر يمكن تصحيحها مباشرة، وأخطاء الحاسب الآلي تحتاج إلى عملية أطول من ناحية الوقت. الأتمتة لم تلغى العنصر البشري ولكنها ساهمت في تغيير مسميات الوظائف. فوجود الإنسان ضروري جداً حول الآلة حتى لو كانت قائمة لكل العمل ولكن في رأيي الشخصي أنها أيضاً قد تساعد الإنسان على الخمول والكسل وخاصة الإنسان العربي.

كتب: محمد احمد عبد السلام



أنها رؤية لعالم مثالي لمجتمع مكون من مساحات شاسعة من الترفيهات والتسهيلات المتاحة . فلتتخيل مجتمع يعيش بدون أي ضرائب و لا رسوم جمركية . مجتمع يطوف حول العالم وهذه هي سفينة الحرية freedom ship ذات الإنشاء الضخم من 4,320 قدم طول و عرض 725 قدم و ارتفاع 340 قدم - انها المدينة المتحركة ذات خاصية المعيشة المرفهة وهي تمثل سوق عالمي تجارى مجاني .

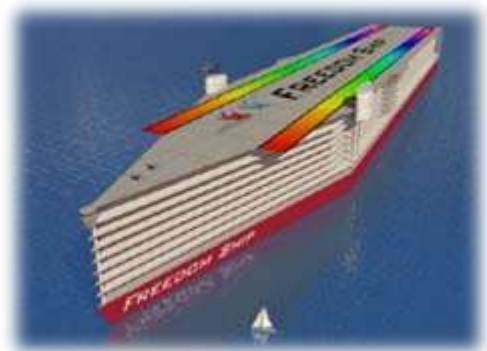
إن freedom ship ليست سفينة بحرية تطوف البحار للمتعة بل أنها مكان مثالي للعيش والعمل والاسترخاء وللإجازة والزيارة أيضاً.

تلك السفينة ستطوف العالم باستمرارية ، فمطارها سوف يخدم الطيران التجاري والخاص وسطحها سوف يحتوى على مكاتب مدارس, مستشفى من الدرجة الأولى, محال , بنوك, فنادق , مطاعم , منتدى للترفيه , مكاتب , مخازن , مشاريع مجلس النواب وإضاءة .بالإضافة إلى الأنشطة الرياضية مما يجعل freedom ship "مجتمع على الماء" .

أهداف freedom ship الأساسية :-

- تتيح مجتمع فريد ساكن رحال مازج المدينة الحديثة مع أرقى الأماكن في مظهر آمن وجذاب .
- تخلق مجتمع تجارى ملك المقاولين المتواجدين على ظهر السفينة مما يتيح لهم بيع منتجاتهم وخدماتهم حول العالم بدون أي ضرائب أو رسوم محلية .
- إنشاء اكبر سوق تجارى عالمي خالي من الرسوم وإتاحته لا سواق العالم.

صورة التصميم :-



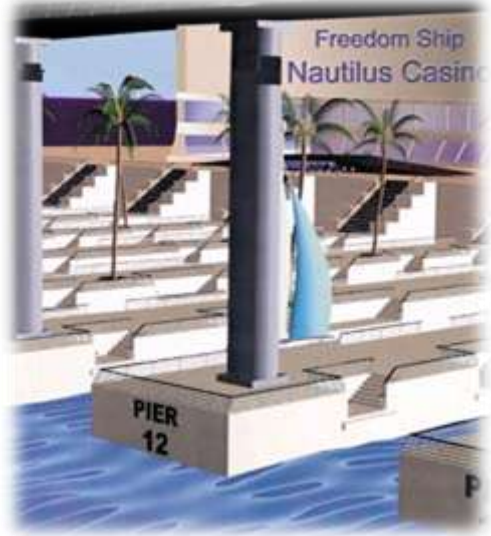
عمل فني جذاب و عمل معماري مبدع سيجعل من شكل السفينة. حدائق ومنتزهات شلالات وبرك ومناظر طبيعية واسعة. كما أن معظم المستويات سوف تتسم بأحواض كبيرة للأسماك. ويكون السوق التجارى الأكبر عالمياً فسيكون الأجل أيضاً وستهدى حصص لأهل القرى فيظهر ما يتسم به المعمارىون من ثقافة.

وستخصص 100 قدم من ظهر المركب كحوض لرسو السفن عند الصارم وأكثر من 200 فدان من الاراضى المفتوحة ستتاح للاسترخاء والابداع .

الراحة والأمان -

شكل منشأ السفينة الفريد مع حجمها الغير عادى سينتج نوعاً من الاستقرار و الأمان مما يتيح رحلة هادئة عبر أقاسي البحار .

وستكون السفينة مضادة للحريق كما سيقدم نظام للتهوية هواء معقم ونقى .



حركة السفينة و وسائل المواصلات-

عبر إبحارها حول العالم , ستقوم Freedom Ship بالعديد من الوقفات البعيدة عن الشاطئ تضم الجزر الاستوائية المتاحة فقط عبر البحر. تلك الوقفات ستتيح مستثمري ومقيمي السفينة بالعديد من الفرص المختلفة للعمل والسفر كما تأتى بنهر من الزوار الدائمين إلى السفينة لزيارة محلاتها ومطاعمها ووسائل ترفيهها. وسيقدم 40,000 سانج من مختلف أنحاء العالم. إن المدن والقرى ستدقق إلى السفينة كما أن السوق التجارى الخاص بالسفينة سيمثل المزارعين المحليين والصيادين و التجار .

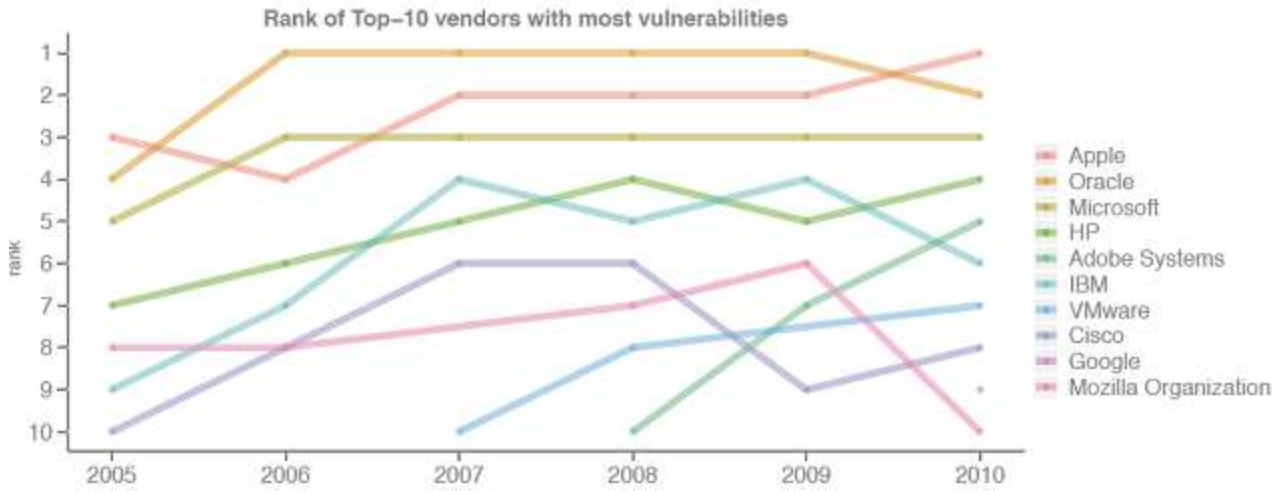
جدولة الوقوف ستعتمد على حجم العمل وشعبية السوق .

الزبائن والتجار ورجال الأعمال والمقيمين سوف يستخدموا سفينة الهواء و المغول المائى وخطوط الطيران التجارية المعاكسة لتأتى وتذهب على ظهر السفينة حتى ما بين توقفها.



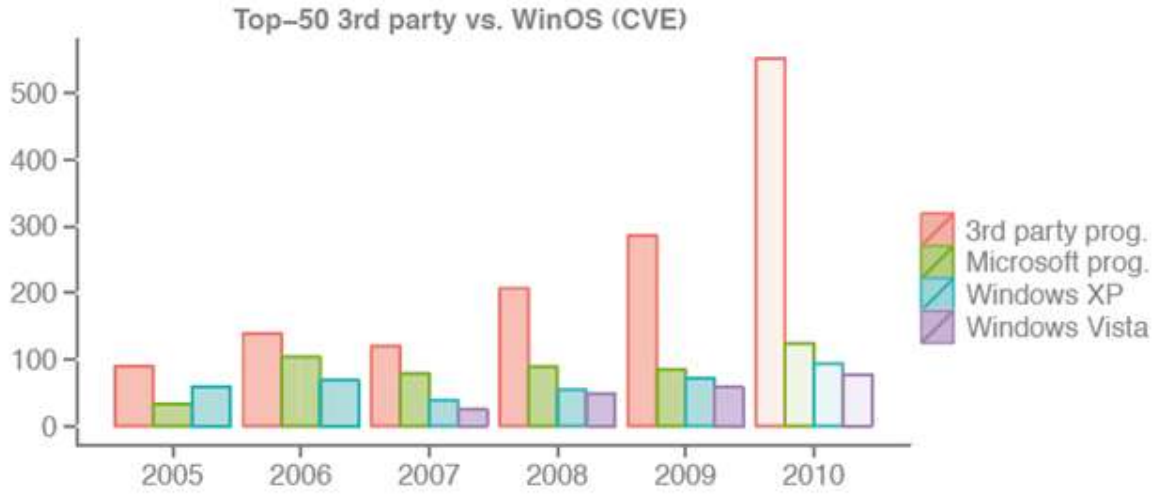
الشركة المتخصصة في مجال أمن المعلومات Secunia تعرض تقريرها النصف سنوي - كتب محمد هشام

عرضت الشركة المتخصصة في مجال أمن المعلومات Secunia تقريرها النصف سنوي والذي يحتوي على معلومات مهمة عن الثغرات الأمنية و ما يتعلق بها من إحصائيات وأرقام , ولقد أظهرت نتائج التقرير عن حصول شركة أبل على المركز الأول في وجود الثغرات الأمنية في تطبيقاتها , وحصلت شركة أوراكل على المركز الثاني ومن ثم تليها شركة مايكروسوفت ووصلت شركة أبل للمركز الأول لا يعني أن المشكلة من النظام , فالتقرير اعتمد على وجود الثغرات في النظام وأيضا في التطبيقات التابعة لكل شركة , فأبل لديها تطبيقات خاصة تعاني من بعض الثغرات مثل برنامج الكويك تايم ومتصفح السفاري, نفس الحال لدى شركة أوراكل وتطبيقات الجافا



رسم بياني لترتيب الشركات في التطبيقات الغير آمنة

وللتوضيح بتأثير البرامج التي تأتي من شركات الطرف الثالث على كثرة الثغرات , قامت الشركة بعرض إحصائيات لأكثر 50 ثغرة في نظام التشغيل الاكس بي ونظام التشغيل فيستا , وأظهرت الأرقام أن قبل خمس سنوات كانت الثغرات تأتي من النظام نفسه وأيضا من التطبيقات الخاصة به ولكن الحال تغير هذه الأيام , فالثغرات أصبحت تأتي من تطبيقات الطرف الثالث والسبب , وذكرت الشركة بأن احد أسباب تراجع الثغرات الأمنية في أنظمة مايكروسوفت هو التحديث السريع للثغرات من خلال التحديث التلقائي المتوفر مع أنظمة التشغيل , وهنا رسم بياني يوضح لأكثر 50 ثغرة من برامج الطرف الثالث والثغرات من نظام الاكس بي و نظام الفيستا وثغرات برامج مايكروسوفت خلال الخمس السنوات الأخيرة



ولمزيد من المعلومات يمكن تحميل التقرير من هنا

Top Security Threats for 2011

يتوقع الخبراء ان لا يكون العام 2011 افضل من سابقه فيما يخص تهديدات امن المعلومات والتقنية بشكل عام فهناك تكهنات بوجود المزيد من الإختراقات مع ظهور العديد من التقنيات الجديدة في الإختراق والتي قد تسعى إلى التدمير أكثر من جني المال استنادا على حاجة الدول وبعض المنظمات إلى الدخول في حروب البكترونية ولعل ابلغ مثال على ذلك هو دودة [Stuxnet](#) كما يتوقع الخبراء ايضا زيادة الإنتهاكات والخروقات لامن المعلومات من داخل المؤسسات التي تعتمد على التقنية لعدم وجود تدريب كافي داخل المؤسسات لتأمين المعلومات، كما ان اختراقات تطبيقات الإنترنت سوف تشهد زيادة كبيرة في العام 2011 نظرا لما وصلت اليه من انتشار في الأونة الاخيرة مع اعتماد المؤسسات والشركات على هذه التقنيات بشكل كبير، ومن أكثر التهديدات التي سوف تزداد ايضا هي تهديدات الإختراقات المتعلقة بالمستخدمين على الشبكات الإجتماعية **Social Networks** وهو ما سوف يعرض المستخدم والمنظومة التي يعمل بها ايضا للمزيد من الإختراقات. ومن اهم الأشياء التي لا بد ان توضح في الحسبان في العام 2011 هو زيادة وشعبية تقنيات **Cloud Computing** والتي بدورها سوف تتعرض لمزيد من الهجمات لان تأمينها مازال امرا ليس هينا في ظل التعقيدات التقنية التي تتمتع بها هذه الاخيرة. وسوف تتنامى ايضا الإختراقات التي تتعلق بالاجهزة المتنقلة والمحمولة نظرا لانتشارها بين المستخدمين وازدياد عدد مستخدميها حول العالم مع اختلاف توجهاتهم وهو ما سوف يؤدي إلى المزيد من الإختراقات في هذا الجانب. واخيرا نود الإشارة إلى ان الحروب الإليكترونية سوف تشهد طفرة كبيرة في العام 2011 وابلغ دليل على هذا ما يحدث حاليا بسبب **Wikileaks** والمناهضين والتعصبين له مع ظهور نوع جديد من الحروب بين النشطاء على الإنترنت وبين الحكومات التي تعاني مشكلات مع شعوبها مما يندّر بالكثير من الخسائر لكون معظم البلدان العربية على سبيل المثال لانها ليست مستعدة للخوض في مثل هذه الأشياء او حتى التعامل معها بشكل تقني والتخلي عن مفهوم التعامل مع الامور بالمنظور الامني البحث وليس توصيفه بما يستحق والتعامل معها بأليات تتناسب والحقيقة التي نعيشها من توغل للتقنية في جميع مناحي الحياة وهو ما سيجعلها بلا شك مؤثر كبير في ارض الواقع... إلا انها مسألة وقت!

النفايات الإلكترونية في دول الشرق الأوسط وشمال أفريقيا - د. محمد الجندي

ربما يكون مصطلح النفايات الإلكترونية جديدا بعض الشيء في المنطقة العربية وربما أيضا يكون المصطلح الخاص بدفن أو التخلص من النفايات الإلكترونية ليس جديدا باعتبارها نفايات ولكن للأسف لم تعر الدول العربية والمنطقة باكملها اي اهتمام لفرض قوانين صارمة فيما يتعلق بالتخلص من هذه النفايات الإلكترونية بشكل آمن وبدلا من ذلك فتحت الابواب على مصراعها لتجارة اخرى ونوع آخر من السماسرة الذين بدورهم يربحون الملايين وفي نفس الوقت يتسببون بكارث من الصعب معالجتها فيما بعد مثلها مثل الكثير من المشكلات التي تفاقمت في المنطقة عند استخدام التقنية ليس لعيب في التقنية ولكن



لعدم الوعي عند التعامل مع التقنية أو بالأحرى عدم الإستعداد...

مامعنى النفايات الإلكترونية؟

النفايات الإلكترونية E-Waste هو مصطلح يعبر عن جميع الاجهزة الإلكترونية من كمبيوتر ومشتملاته وتلفاز وهواتف نقالة واجهزة اليكترونية قد تحوي اجزاءا عالية الإشعاع او تسبب مشكلات ببنية وصحية عند التخلص منها. ومشكلة النفايات الإلكترونية تكمن في ان اعادة تدويرها تحتاج إلى تكاليف باهظة قد تفوق تكلفة انتاجها! وهو ما يضع المشكلة في بعدين: البعد الاول وهو سهولة ارسالها للدول النامية عن طريق سماسرة في الدول المتطورة وسماسرة آخرون في الدول النامية وهو ما يعرف بعملية E-Waste Trafficking مثلها مثل الإتجار في المخدرات والبشر! ومن ثم يتم تداولها في الدول النامية لفترة قصيرة لما لها بالاساس من عمر قصير في الإستخدام ثم تبدأ الكارثة في الظهور عند الحاجة إلى التخلص من هذه النفايات!

البعد الثاني وهو النهم الكبير لاستخدام كل ما هو تقني وبخاصة في البلدان العربية التي تعتبر من البلدان الغنية مثل دول الخليج يليها البلدان ذات الكثافة السكانية العالية مثل مصر والتي تستهلك سنويا اعداد هائلة من الهواتف النقالة على سبيل المثال، تبدأ المشكلة في التفاقم عندما يقرر الاشخاص استبدال اجهزتهم القديمة باجهزة احدث فيتم بيع الاجهزة القديمة عن طريق شبكة من التجار أو الأفراد على حد سواء وبالتالي تذهب هذه الاجهزة ايا كانت إلى ايدي مجموعة اخرى سوف تقرر التخلص منها في فترة قصيرة لما اشرنا اليه من قصر عمر هذه الأجهزة وهو ما يسمى (دورة العمر) ثم تصبح نفايات في فترة قصيرة عندها تظهر المشكلة الكبرى في كيفية التخلص من هذه النفايات. فإن كانت الدول الكبرى لا تريد صرف اموال طائلة لإعادة التدوير فما باننا بالدول النامية التي ان امتلكت المال لتصرفه لن تملك التقنية لإعادة التدوير!!

من المعلوم ان اتفاقية بازل لحظر تداول المواد الخطرة والتخلص منها هي الاتفاقية العالمية المختصة بهذا الشأن كون الأجهزة الإلكترونية تعتبر من النفايات الخطرة لما لها من اضرار ببنية وايضا على صحة الإنسان والحيوان عند التخلص منها. بالنظر إلى الدول الموقعة على الاتفاقية سوف تجد الكثير من الدول العربية لم توقع ولكن لديها تحفظات وملاحظات وان صح التعبير "مهاترات" نعتقد ان الغرض منها اشياء اخرى غير معلنة لاسباب ترجع إلى هذه الحكومات في عدم التعاون وهو امر يطول شرحه ويخرج عن اطار هذا المقال.

هناك العديد من المبادرات التي تهتم بهذا الشأن في المنطقة العربية في الإمارات والسعودية ومصر وقطر على سبيل المثال مع بعض المبادرات الاخرى من القطاع الخاص لا نستطيع انكارها إلا انها جهود "ضئيلة جدا" مقارنة بحجم المشكلة الرئيسي وفي غياب كامل لقوانين محلية او على مستوى المنطقة تتعامل مع هذه المشكلة المتفاقمة والتي لا تلوح في الافق اية مبادرات جادة للتعامل معها وتقنينها للحد من التخلص من هذه النفايات على اراضي هذه الدول او حتى كيفية التعامل مع الاجهزة التي يتم انتهاء فترة عملها في هذه الدول فالعمر القصير لهذه الاجهزة يجعل المشكلة تتفاقم سريعا...

ولعل الصورة التالية توضح مدى انتشار هذا الامر في دول افريقيا بشكل كبير حيث تبدأ المنابع من الولايات المتحدة وغرب أوروبا ثم إلى شرق أوروبا ومنها إلى الصين ثم الشرق الأوسط وأفريقيا في رحلة تحكمها معاملات مادية كبيرة!

Export of e-waste



وجدير بالذكر ان الدول الغربية هي اول من يبدأ بكسر الحظر على تداول هذه النفايات الاكثر خطرا على البيئة وصحة الإنسان عن طريق التعامل مع شبكات لها مصالح خاصة في مناطق مختلفة من دول العالم الثالث والدول النامية مما يجعل السيطرة على الامور اكثر صعوبة لوجود شبكات مهربين وسماسرة وفساد في دول كثيرة يتسبب في عبور هذه النفايات إلى داخل الدول النامية ووجود مصالح مشتركة بين جميع الاطراف يحتاج إلى وقفة حازمة من الحكومات والاجهزة المعنية والتي لا نرى امل في ظهور مثل هذه الجهود في الافق او في المدى القريب لانها متعلقة بمنظومة من القوانين والإجراءات التي لا توجد فكيف ستطبق!

ولكي تفهم خطورة هذه النفايات سوف نأخذ مثلا واحدا فقط من هذه النفايات وهو هاتف نقال:

يحتوي الهاتف النقال الذي سيتحول إلى نفايات على أكثر من 45 عنصرا من المواد منها الخطر جدا وقد يسبب الموت ومنها المشع ومنها ما يحمل اضرارا للإنسان والبيئة والحيوان عند حرقها او التخلص منها في باطن الأرض او بشكل غير سليم.

من هذه المواد:

- اللوحات الإلكترونية تحوي مواد سامة مثل الرصاص والنيكل والبريليوم وكلها معادن سامة تسبب امراض خطيرة
- تحوي الشاشات مادة الزئبق
- تحوي البطاريات النيكل والكادميوم
- البلاستيك بالطبع في جميع هذه الاجهزة وهو ما يتسبب في



تسميم البيئة عند حرقه كما انه ايضا يعلق في الهواء وفي المنازل وقد يؤثر على سلسلة الغذاء وتم العثور على آثار له في بعض الاسماك في البحيرات والانهيار القريبة من اماكن التخلص من هذه المواد.

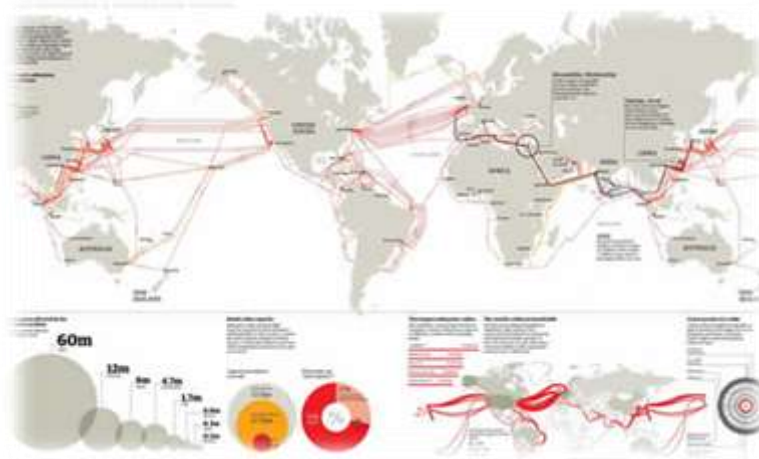
يكفي ان نخبر القاريء إلى ان الهاتف المحمول هو الاقصر عمرا في الاجهزة الإلكترونية حيث يتراوح عمره من سنة ونصف سنتين مقارنة ثلاث سنوات او 4 للكمبيوتر مثلا. كما ان أكثر من 65 الف طن من النفايات الإلكترونية تأتي من الهواتف النقالة فقط. شاهد هذا الفيديو واحكم بنفسك:

http://www.youtube.com/watch?v=Ukbpil9UsY8&feature=player_embedded

مما لاشك فيه ان بعض الاجهزة الإلكترونية التي يراد التخلص منها قد تستخدم كهبات او منح لبعض الدول الفقيرة لتشجيع التعامل مع التقنية او حتى الحصول على كمبيوتر من قبل اشخاص غير قادرين على توفير اعباء جهاز كمبيوتر حديث وهذا امر جيد في شكله العام إلا ان مشكلة قصر العمر لهذه الاجهزة تجعل المشكلة ذات جوانب اخرى كثيرة فمازلت اكرر وسوف اظل اكرر هذا الامر دوما ان التقنية في حد ذاتها شيء مطلوب ومفيد لكن تبقى المشكلة الكبرى هي كيفية تمكين هذه التقنية ومدى استعداد المستقبل لها فليس معنى ان الهاتف النقال لا غنى عنه لرجال الاعمال فهذا ليس معناه انه مبرر لان تقوم بالقاء نفاياتك من الهواتف النقالة في ايدي اطفال العالم الثالث والدول الفقيرة مثل غانا او غيرها..!

نتمنى ان نجد مبادرات قيمة في بلادنا للتعامل مع هذه المشكلة بجدية او حتى وجود مواقع توعوية لتوعية المستخدمين لهذه الاجهزة (الذين مازلت اضعهم في خاثة المستهلكين) فهناك الكثير من الامور البسيطة التي يمكن لاي مستخدم لهذه التقنيات او يقوم بها للحفاظ على البيئة او الحفاظ على صحة اقرانه وذويه مثل الإحتفاظ بهاتفك النقال لاطول فترة ممكنة مع المحافظة على بطاريته فليس هناك داعي لان تقوم بشراء هاتف جديد كل عدة شهور والتخلص من القديم في النفايات ربما يمكنك استخدامه في شيء آخر فالافكار كثيرة، ولنا عودة ان شاء الله في هذا الموضوع الهام.

Middle East Fragile ICT Infrastructure



بنية المعلومات المهلهلة في الشرق الأوسط: د. محمد الجندي

منذ ان دخل الإنترنت المنطقة العربية وبدأ عدد المستخدمين للتكنولوجيا والكمبيوتر بشكل عام في تزايد كبير اضافة إلى ذلك بدأت تظهر العديد من المشروعات والاعمال والخدمات التي تعتمد على الإنترنت بشكل اساسي واصبحت الإنترنت هي القناة الرئيسية للعديد من الاعمال حتى خدمات الحكومة الإلكترونية دخلت هذا المضمار وبدأت تتشعب الخدمات بدءاً من حجز تذاكر الطيران حتى البورصة والاعمال التجارية والاتصالات إلى آخره. وهذا الانتشار للتقنية لها محاسنها الكبيرة إذا وظفت بشكل صحيح وإذا استخدمت في هدف اكبر وهو التطوير وليس الربح المادي فقط، كما ان استعداد البلدان واستعداد البنى التحتية للمعلومات بها إلى تطبيق هذه الخدمات يعد من اهم الاشياء التي اعتقد انها لم توضع في الحسبان عند تعميم هذه التقنيات ونشرها في هذه البلدان.

وتعد مشكلة استعداد البنى التحتية للمعلومات لتطبيقات وخدمات تكنولوجيا المعلومات هي من اهم الاشياء التي لا بد من وضعها في الحسبان عند تطبيق اية تقنيات جديدة وقد [اصدرت الامم المتحدة في تقرير لها عن هذا الامر](#) الكثير من المعلومات عن

الإستعداد للبنى التحتية المعلوماتية والاطار ايضا التي تواجه هذه البنى التحتية من كونها اكثر عرضة من غيرها لعدم الصمود امام الإختراقات والتهديدات Threats الخاصة بالمعلومات. وإذا معنا النظر في استعداد البنى التحتية لتبنى تطبيقات جديدة فستجد ان هذا الامر ينذر بكارث كثيرة في المستقبل القريب لان دول المنطقة للأسف الشديد لا تضع في حساباتها الخطط المستقبلية والزيادة الكبيرة في هذه التطبيقات وتطوراتها وعدد المستخدمين المتضاعف سنويا. ناهيك عن ان البنى التحتية المعلوماتية للأسف الشديد لا تستطيع الصمود امام اختراقات المعلومات فليس هناك تامين كافي لهذه البنى التحتية او حتى الاعمال والخدمات التي تعتمد عليها وهذا لقلّة الوعي المعلوماتي والتفكير في الربح اولا وعدم الإهتمام بامن المعلومات كجزء هام من هذه المنظومة ناهيك عن غياب القوانين المتعلقة بجرام المعلومات إلا ماندر في بعض الدول العربية!

وبما اننا نتحدث عن تهديدات فلا بد ان نذكر ان المفوضية البريطانية الامريكية قد ذكرت في تقرير لها ان الدول التي تعتمد على التقنية دون وعي او تقنين هي الاكثر عرضة للأخطار المتعلقة باختراقات المعلومات والامن، فالأخطار تزداد بزيادة اعتماد هذه الدول والحكومات على التقنية بلا وعي او تخطيط. ولعل ابلغ دليل على ذلك عدد المواقع العربية الخاصة بالحكومات في هذه الدول وخدماتها والتي تتعرض لإختراقات بشكل مكثف من عناصر داخلية وخارجية دون ان تتمكن الجهات المختصة من القبض عليهم او حتى تقفي اثرهم لغياب القانون والكفاءات وعدم انضمام هذه الدول لاتفاقيات دولية تنظم هذا الامر مثل اتفاقية بودابست الخاصة بالجريمة الإلكترونية.

ومن الأحداث الاخيرة التي تدل على ان البنى التحتية المعلوماتية في المنطقة العربية مهلهلة بدرجة كبيرة هو الهجوم المتواصل على البنى التحتية المعلوماتية في تونس منذ اواخر 2010 وحتى هذه اللحظة ومن المؤسف ان تجد اغلب المواقع الحكومية التونسية لا تعمل على الإطلاق ولا تستطيع الوصول اليها وهو نتاج هجوم سمي "العملية: تونس"

اين التقنية التي يتحدثون عنها في بلادنا؟ اين تذهب الاموال التي تنفق في تكنولوجيا المعلومات؟ ما هي نتيجة المؤتمرات الدولية التي تستضيفها بلادنا العربية فيما يتعلق بتكنولوجيا المعلومات والجرام المعلوماتية؟

هذه اسئلة وغيرها الكثير يحتاج إلى اجابات على الرغم من اننا نعلم الإجابة سلفا..!

نحن لا ننكر ابدا ان هناك اختراقات كبيرة جدا على الصعيد العالمي في تكنولوجيا المعلومات وفي بلدان متطورة وتتكبد من جرائمها الحكومات والشركات والمؤسسات ملايين الدولارات بل بلايين في بعض الاحيان. لكن الامر مختلف فالبنى التحتية للمعلومات لديهم ليس كالبنى التحتية لدينا وهذا امر والكفاءات في هذه الدول وفي هذه التخصصات تحديدا ليست كمثيلتها لدينا بدون تقليل من شأن خبراءنا- لكن النسب كبيرة والهوة تزداد اتساعا...

لايمكن باي حال من الاحوال ان تظل دولة باكملها غير موجودة على الإنترنت بسبب هجوم مجموعة من Hackers او حتى Hacktivists او مناهضين لفكرة معينة، بالطبع هذه حرية في التعبير لكن القانون يعاقب على الإختراق في الدول المتقدمة...

نظرة او لمحة سريعة على اختراقات البنى التحتية للمعلومات في منطقتنا عبر هذا الموقع كفيلة بوضع المشكلة نصب اعيننا بشكل اكثر وضوحا

<http://www.zone-h.com/archive>

نحن ذاهبون إلى ما هو ابعد من اختراق موقع لكن الامور ذاهبة إلى الحروب الإلكترونية لا محالة..فماذا نحن فاعلون؟



Information Systems Security Association
The Global Voice of the Information Security Profession

منظمة امن نظم المعلومات
الآن في مصر...

Training Tomorrow's Security Professionals...

The largest organization for IS Security Professionals
More than 140 chapter in 35 countries
Now in Egypt!

امن المعلومات يبدأ بالتوعية والتدريب
دورات متخصصة ومعتمدة عالميا
شهادات معتمدة من اعرق المؤسسات العالمية



ASK PC

Founding Sponsor & Course Provider

BRITISH INSTITUTE
FOR LEARNING &
DEVELOPMENT
ORGANISATIONAL
MEMBER

BCS
REGISTERED
COURSE PROVIDER

IEEE

ISSA in Egypt:

+20 100040214

www.issa-eg.org

