رئاسة مجلس الوزراء
المجلس الأعلى للأمن السيبراني

نحو استراتيجية وطنية للأمن السيبراني

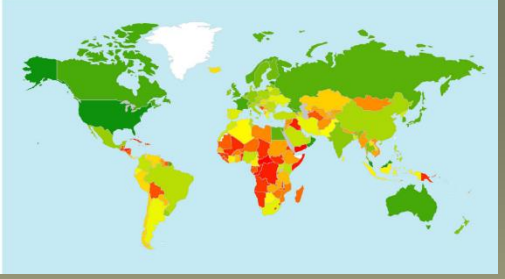
د. شريف هاشم
مستشار أول رئيس الجهاز القومي لتنظيم الاتصالات للأمن السيبراني
رئيس المكتب التنفيذي للمجلس الأعلى للأمن السيبراني – رئاسة مجلس الوزراء

أهم الاخطار السيبرانية

- **اختراق وتخريب البني التحتية للاتصالات وتكنولوجيا المعلومات**
- هجمات اعاقة أو تعطيل الخدمات
  Distributed Denial of Service Attacks (DDOS)
- انتهاك الخصوصية وسرقة البيانات والهوية الرقمية
- هجمات الفيروسات الخبيثة
- الاعلام والدعاية المغرضة

أمثلة من أبرز الهجمات السيبرانية

- شهد عام 2007 أول «حرب سيبرانية» تعرضت لها دولة إستونيا عن طريق هجمات اعاقة خدمات الاتصالات وتكنولوجيا المعلومات DDOS، وخاصة في القطاع الحكومي والمصرفي. استمرت الهجمات حوالي عشرة أيام.
- عام 2007، تعرضت شركة TJXلهجمات قراصنة حيث تمكنوا من سرقة بيانات البطاقات الائتمانية وحسابات البنوك وعناوين أكثر من 45 مليون عميل..
- عام 2009، أكدت وزارة الدفاع الامريكية تعرض قاعدة بيانات تصميمات الطائرة المقاتلة F35i - التي تكلف تطويرها أكثر من 300 مليار دولار أمريكي - للاختراق من قبل قراصنة تمكنوا من سرقة بيانات يقدر حجمها بعدة «ترا بايتس tera bytes»، مما قد يؤثر علي نظم تأمين الطائرة وحمايتها في المستقبل.
- عام 2010، تم اكتشاف فيروس «ستاكس نت Stuxnet» الذي تمكن من اختراق وتعطيل منظومة التحكم في المفاعلات النووية الايرانية في بوشاهر ونتاز. كما أعلن في نوفمبر 2013، أن الفيروس اخترق مفاعلا نوويا روسيا يستخدم في توليد الطاقة الكهربية.
- عام 2014 تعرضت شركة Sony لاختراقات نتج عنها سرقة أكثر بيانات يقدر حجمها بأكثر من (100 تيرا بايتس tera bytes) منها أفلام وبيانات الفنانين والموظفين.
- أعلنت أحدي شركات ادارة المستشفيات الامريكية Community Health Systems (CHS)عن تمكن القراصنة من اختراق أنظمة المستشفيات وسرقة بيانات أكثر من 4.5 مليون مريض (أغسطس 2014).



الاستعداد لمواجهة تحديات الأمن السيبراني

- جاءت مصر في **الترتيب الرابع عشر بين الدول ال193** في مؤشر الجاهزية للأمن السيبراني **Global Cybersecurity Index GCI** الصادر عن الاتحاد الدولي للاتصالات في يونيو 2017، حيث يقيس المؤشر الاستعدادات التي قامت بها الدول وفقا **لخمسة معايير** هي: **المعيار القانوني، المعيار التقني، المعيار التنظيمي، معيار بناء القدرات، ومعيار التعاون**، وهي المعايير التي سبق أن حددتها الاجندة العالمية للأمن السيبراني (Global Cybersecurity Agenda GCA) التي أطلقها الاتحاد الدولي للاتصالات عام 2008 والتي شاركت مصر في وضع أطارها ضمن الدول والمؤسسات الاعضاء في الاتحاد.
- وقد جاء ترتيب مصر المتقدم في المؤشر العالمي نتيجة لجهود ومبادرات عدة - في مجال الامن السيبراني، تعكس مشاركة فاعلة وناجحة بين الحكومة والقطاع الخاص ومؤسسات الاعمال في قطاع الاتصالات وتكنولوجيا المعلومات الصري.

الاستعداد لمواجهة تحديات الأمن السيبراني:
المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات EG-CERT

- أنشئ المركز في ابريل 2009، ويتبع الجهاز القومي لتنظيم الاتصالات
- يضم المركز 50 متخصصا في مجال الأمن السيبراني
- يقدم المركز الدعم لقطاع الاتصالات وتكنولوجيا المعلومات والقطاع الحكومي والقطاع المالي في مجال مواجهة الأخطار السيبرانية، وخاصة التصدي لهجمات اعاقة وتعطيل الخدمات (DDOS) ومكافحة اختراق قواعد البيانات ومواقع الانترنت
- يقدم المركز خدمات تحري الحوادث وتحليل الأدلة الرقمية وتحليل البرمجيات الخبيثة والكشف عن الثغرات ونقاط الضعف ومتطلبات مواجهتها والتغلب عليها في البني التحتية للاتصالات وتكنولوجيا المعلومات في قطاع الاتصالات فضلا علي القطاع الحكومي والقطاعات المالية والاقتصادية الهامة والمرافق العامة (الكهرباء، المياه، غيرها).
- يقدم المركز سنويا حوالي 250 تقريرا فنيا الي الجهات المعنية، فضلا عن تقديم الدعم التقني والميداني وأعمال الخبرة في مواجهة الهجمات السيبرانية، واعداد تقارير فنية الي جهات التحقيق والجهات القضائية، بالتنسيق مع الجهات الأمنية.

بناء القدرات وتطوير المهارات

- اطلق الجهاز القومي لتنظيم الاتصالات برنامجا وطنيا لتدريب 220 متخصص من 38 جهة حيوية للتدريب المكثف في مجال الأمن السيبراني

SANS

- يشارك مركز السيرت المصري في المناورات السنوية لدول جنوب شرق اسيا (APCERT) وللدول العربية (ITU/RCC) وللدول الإسلامية (OIC CERT) منذ عام 2012

ITU International Telecommunication Union

APCERT Asia Pacific Computer Emergency Response Team

OIC-CERT Computer Emergency Response Team

أبرز آليات التعاون الدولي

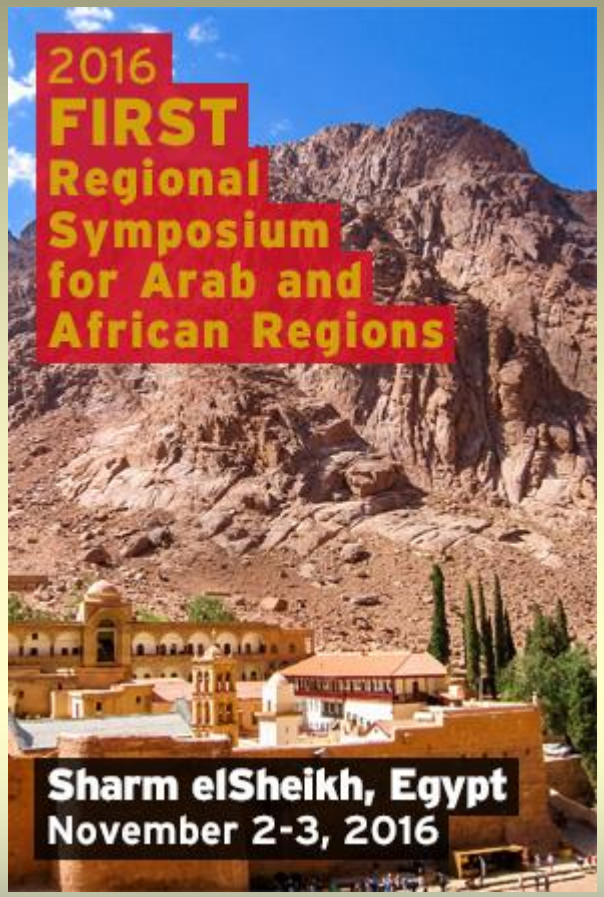
- شاركت مصر منذ عام 2012 في الفريق الدولي عالي المستوي للخبراء الحكوميين المعني بحماية الامن الدولي في اطار تطور الاتصالات وتقنيات المعلومات (UN GGE) on the Developments In The Field Of Information And Telecommunications In The Context Of International Security.
- قادت مصر الجهود التي أدت لإنشاء فريق مجلس الاتحاد الدولي لتنظيم الاتصالات المعني بحماية الأطفال والنشء علي الانترنت ITU's Council Working Group for Child Online Protection (CWG-COP) وترأست الفريق في الفترة من 2010-2017.
- تشارك مصر في شتي المحافل الدولية والتجمعات الإقليمية لدعم جهود الأمن السيبراني مثل UN, ITU, OECD, CRCC, AU, ESCWA, League of Arab States, OIC

أبرز آليات التعاون الدولي

لمركز السيرت المصري اتفاقيات تعاون مع العديد من المراكز النظيرة والهيئات الدولية ذات الصلة للتعاون في مجالات الامن السيبراني

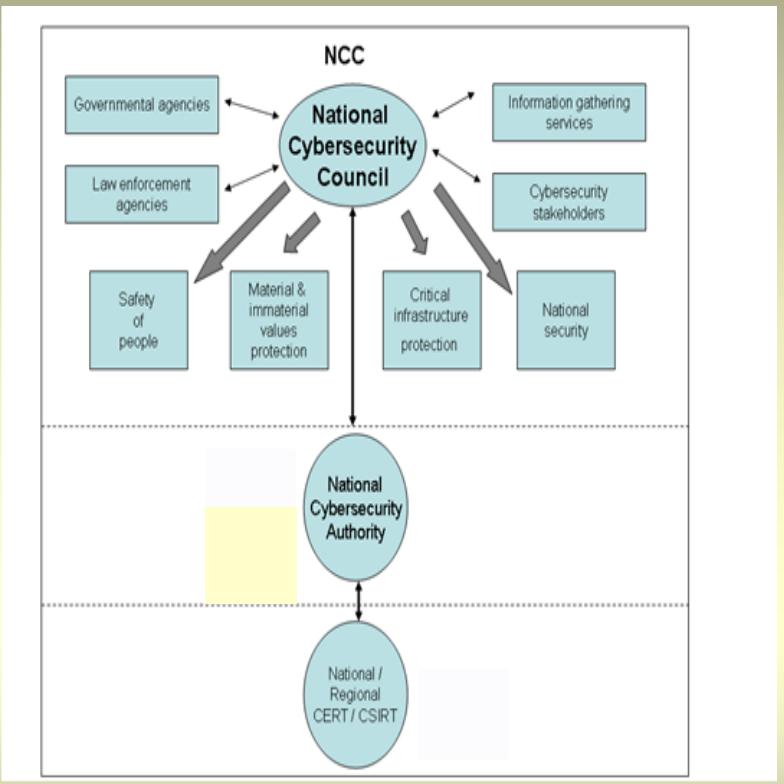
- مركز السيرت المصري عضوا كاملا في منظمة FIRST.
- مركز السيرت المصري عضوا مؤسسا في
- OIC-CERT و Africa CERT.
- مركز السيرت المصري له اتفاقيات تعاون مشترك وعلاقات مهنية وثيقة مع Cybersecurity Malaysia, South Korean CERT, US-CERT, Uganda, Tanzania, Team Cymru, IMPACT, and Indian CERT ومع العديد من المركز النظيرة علي المستوي العربي والافريقي والدولي

Recent Two Regional Cybersecurity Conferences in Sharm elSheikh



Egypt hosted the ITU ARCC Regional Cybersecurity Summit (Oct 30 - Nov 1) and the FIRST Regional Cybersecurity Symposium for the Arab and African Region (Nov 2-3), For more information visit: http://www.rcssummit.com/module.php?module=registration & http://www.first.org/events/symposium/egypt2016

رئاسة مجلس الوزراء
المجلس الأعلى للأمن السيبراني



تم تشكيل مجلس أعلي مسئول عن اعداد استراتيجية وسياسات وبرامج وخطط تأمين البني التحتية للاتصالات والمعلومات الحرجة لكافة قطاعات الدولة (المجلس الأعلى للأمن السيبراني) يتبع مجلس الوزراء يرأسه وزير الاتصالات وتكنولوجيا المعلومات، ويضم ممثلي الاطراف المعنيين بالأمن الوطني (وزارة الدفاع ووزارة الخارجية ووزارة الداخلية والمخابرات العامة) وممثلي إدارة وتشغيل البني التحتية في القطاعات الحيوية والمرافق العامة والحكومة الالكترونية. و يتولى المجلس وضع وتفعيل استراتيجية وطنية للأمن السيبراني ولمواجهة الهجمات السيبرانية، كما يتولى الاشراف علي تنفيذ تلك الاستراتيجية، مع ضرورة تحديثها تمشيا مع التطورات التقنية المتلاحقة.

الاستراتيجية الوطنية للأمن السيبرانى (2017-2021)

"أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذى ينظمه القانون"

مادة (31) من الدستور المصري (يناير 2014)

ركائز التوجه الاستراتيجي لمواجهة الاخطار السيبرانية

أهم البرامج الاستراتيجية في المرحلة الحالية (2017-2021)

1. برنامج لتطوير الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية
2. برنامج لتطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبراني وتأمين البني التحتية الحيوية
3. برنامج لحماية الهوية الرقمية (برنامج المواطنة الرقمية)، وتفعيل البني التحتية اللازمة لدعم الثقة في التعاملات الالكترونية بوجه عام وفي الخدمات الحكومية الالكترونية بوجه خاص

أهم البرامج الاستراتيجية في المرحلة الحالية (2017-2021)

4. برنامج لإعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات
5. برنامج لدعم البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني
6. برنامج للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية للأفراد والمؤسسات والجهات الحكومية، وبأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها