Midterm Exam – Chanakya Gaur

Identify the following organizations and briefly describe their role in global cybersecurity: WSIS, ITU, ICANN, IETF, IGF.

World Summit on the Information Society (WSIS):

The World Summit on the Information Society (WSIS) was a two-phase United Nations-sponsored summit on information, communication and the information society that took place in 2003 in Geneva and in 2005 in Tunis. The conferences established 17 May as World Information Society Day. One of its chief aims of WSIS was to bridge the global digital divide separating rich countries from poor countries by spreading access to the Internet in the developing world. In the 1990’s, the new Information and Communication Technology (ICT) was implemented predominantly in developed countries which changed society leading to the digital revolution. In 2003 at Geneva, delegates from 175 countries took part in the first phase of WSIS where they adopted a Declaration of Principles which aims to achieve an information society which is accessible to all and is based on shared knowledge. A Plan of Action sets out a goal of bringing 50 percent of the world's population online by 2015. It does not spell out any specifics of how this might be achieved. The Geneva summit also left unresolved more controversial issues, including the question of Internet governance and funding.

International Telecommunication Union (ITU):

The International Telecommunication Union, previously known as International Telegraph Union, based in Geneva is a member of the United Nations Development Group, a specialized agency of the United Nations, that is responsible for issues that concern information and communication technologies. The role of ITU is to coordinate the shared global use of the radio spectrum, improve telecommunication infrastructure, promote international cooperation in assigning satellite orbits, improve telecommunication infrastructure in the developing world, and assists in the development and coordination of worldwide technical standards. ITU also organizes worldwide and regional exhibitions and forums which brings together representatives of government and the ICT industry to exchange ideas, knowledge and technology. The ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks.

The Internet Corporation for Assigned Names and Numbers (ICANN):

ICANN was created on September 18, 1998, and incorporated on September 30, 1998, in the U.S. state of California. It is headquartered in the Playa Vista neighborhood of Los Angeles. ICANN identifies itself as a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers. Through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet. ICANN carries out the actual work of central address pools and DNS root zone registries.

Much of its work has concerned the Internet's global Domain Name System (DNS), including policy development for internationalization of the DNS system, introduction of new generic top-level domains (TLDs), and the operation of root name servers. The numbering facilities ICANN manages include the Internet Protocol address spaces for IPv4 and IPv6, and assignment of address blocks to regional Internet registries. ICANN also maintains registries of Internet Protocol identifiers.

The Internet Engineering Task Force (IETF):

The Internet Engineering Task Force (IETF) is a large international community of network designers, operators, vendors and researchers who are concerned with the development and smooth operation of the internet. The IETF is an open community which allows any interested individual to participate. The IETF was initially started as an activity supported by the U.S. Government. However, since 1993, it has operated as an international membership-based non-profit organization concerned with standards development function under the Internet Society. The IETF develops and promotes Internet Standards, TCP/IP in particular. The technical work of IETF is done in working groups, which are organized by topic into several areas for example, routing, transport and security. These working groups are managed by Area Directors who are members of the Internet Engineering Steering Group (IESG). The Internet Architecture Board provides an oversight architectural oversight and also adjudicates appeals when there is a complaint against the IESG. The IETF meets 3 times a year.

Internet Governance Forum (IGF):

The Internet Governance Forum(IGF) was formally announced by the United Nations Secretary-General in July 2006. It was first convened in October–November 2006 and has held an annual meeting since then. The IGF is a multi-stakeholder forum for issues of internet governance. It involves all stakeholders such as governments, private sector and civil society to participate in the debate of internet governance. At their annual meeting, members discuss, exchange information and share good practices with each other. On December 16, 2015, the UN General Assembly extended the existing mandate of the IGF for another 10 years. The mandate of the Forum is to:

* Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet;
* Facilitate the exchange of information and best practices, and in this regard, make full use of the expertise of the academic, scientific and technical communities;
* Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world;
* Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries;
* Contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise;
* Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes;
* Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users;
* Publish its proceedings

Define and briefly discuss “attack surface” and “attack vector” in terms of cyber threats. Give examples of each.

The attack surface of a system is the different points from where an attacker could gain unauthorized access to the system and try to extract data. It is a good idea to keep the attack surface as small as possible.

Attack Surface of a system can possibly be:

* The path for data and commands in and out of the application
* the code that secures these paths
* all valuable data used in the application, including secrets and keys, intellectual property, critical business data, personal data and PII.

According to Skybox Security, there are three steps towards understanding and visualizing an attack surface:

Step 1: Visualize the system of an enterprise is the first step, by mapping out all the devices, paths and networks.

Step 2: Find Indicators of Exposures that correspond to each indicator of a vulnerability being potentially exposed to the visualized map in the last step.

Step 3: Find Indicators of Compromise to ensure that an attack has already succeeded.

Developers and attackers both use attack surface analysis to detect security vulnerabilities in a system. Attack surface analysis is assessing the exploitable vulnerabilities in any system. In fact, the first step of hackers is to scan the target’s attack surface so that possible vulnerabilities are detected and can be exploited. An attack surface can be divided into a few categories:

Software Attack Surface: This consists of all the functions in the code that can be accessed by an unauthenticated user.

Network Attack Surface: This consists of all the possible ways an unauthenticated user can access either or the hardware or the software of the system.

Physical Attack Surface: This consists of all the possible ways an attacker can gain physical access to the system

The attack surface can easily add up into the thousands or more. Some of which can be:

* Login/authentication entry points
* Admin interfaces
* Inquiries and search functions
* Data entry (CRUD) forms
* Business workflows
* Transactional interfaces/APIs
* Operational command and monitoring interfaces/APIs
* Interfaces with other applications/systems

An attack vector can be defined as the technique by which an attack surface can be exploited to compromise the system. An attacker can gain unauthorized access for assaulting or exploiting a network, computer or device. In most cases, programming is heavily involved and it is rare to see hardware means involved in an attack vector.

No protection method is totally secure. Human ignorance or weaknesses are also put to use for social engineering attack vectors. For example, in a case of deception, users are fooled into weakening the system or network defenses. Social engineering attacks can be carried out by mediums such as viruses, e-mail attachments, web pages, pop-up windows, instant messages, chat rooms, and deception.

To some extent, [firewall](http://searchsecurity.techtarget.com/definition/firewall)s and [anti-virus software](http://searchsecurity.techtarget.com/definition/antivirus-software) can block attack vectors. Anti-virus software and firewalls use measures like packet classification & marking, IP source trackers, traffic policing, TCP intercept, policy-based routing, firewalls, TCP intercept, network-based application recognition, committed access rate and layer-3 switches which could provide some defense or block attack vectors to some extent. However, a completely attack-proof technique is currently unavailable, as hackers are constantly upgrading and updating their attack vectors.

Here are some examples of attack vectors:

* Phishing
* SQL Injection
* Distributed Denial of Service Attacks (DDOS)
* Malware
* Botnets
* Cross-site scripting
* XML Poisoning

Describe and discuss three (3) key elements in any national cybersecurity strategy or program. [1]

Cyber security is important since modern life depends upon the timely, adequate and confidential performance of cyber space. Cyber security is now no longer a pure computer security problem but a National Policy matter since it could hamper economic, public health and national security activities. The elements that are considered the main features of a holistic, multi-stakeholder and strategized cybersecurity program are: Government Cybersecurity Accountability, National Cybersecurity Coordinator, National Cybersecurity Focal Point, Legal Measures, National Cybersecurity Framework, Computer Incident Response Team (CIRT), Cybersecurity Awareness and Education, Public-Private Sector Cybersecurity Partnership, Cybersecurity Skills and Training Program and International Cooperation.

Legal Measures:

Gaps in national and regional legislation make cybercrime a low risk and lucrative undertaking. In keeping with the first GCA pillar, this priority aims to help devise strategies to govern the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures. Legal measure should elaborate strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures as well as consider a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas. It has been observed that national administrations are accountable for cybersecurity as cyber-attacks threaten national interests in economic, diplomatic and national security. Since the commercial sector owns the majority of the critical information infrastructure and global cooperation on cybercrime requires treaties on extradition and cross-border Internet searches, it is difficult to have a coherent legal policy. Therefore, the executive governance should structure a legal mandate that will provide the Head of Government the legal authority to create and fund a national cybersecurity program, define the legal basis for creating a national Computer Incident Response Team, grant powers to shut down a critical infrastructure asset if at risk of a cyber-attack provide the basis for promoting cybersecurity skills, training and awareness and define the legal and operational basis for an integrated and fully coordinated public-private sector partnership on cybersecurity. Nations should participate in efforts to develop and harmonize legal measures globally. The participation could be part of crosscutting international cooperation efforts. Countries may also consider incorporating legal measures into a cohesive international strategy for cyberspace. For example, the US strategy49 provides a roadmap for coordinating all the international cyberspace policy activities of the government, private sector, civil society and end-users. To build confidence in the use of cyberspace, the US aims to participate fully in international cybercrime policy development; improve cooperation through the harmonization of cybercrime law and Focus cybercrime laws on combating illicit use rather than restricting access. As ever, all nations have a sovereign right to choose the most efficacious approach.

Computer Incident Response Team:

The growing sophistication, frequency and gravity of cyber threats make it necessary for formal frameworks to watch, warn and respond to incidents. The national CIRT is responsible for:

* Providing incident response support to all relevant stakeholders via established, trusted, authorized and centrally coordinated initiatives at the national level;
* Dissemination of critical information such as early warnings and alert notifications, security advisory, and upholding security best practices;
* Acting as a single point of contact for cyber incident reporting and coordination;
* Analyzing and synthesizing incident and vulnerability information disseminated by others such as vendors to provide an assessment for interested stakeholders;
* Establishing trusted communications mechanisms and facilitating communications among stakeholders to share information and address cyber security issues;
* Developing mitigation and response strategies and coordinating incident response;
* Sharing data and information about the incident and corresponding responses;
* Determining trends and long-term remediation strategies;
* Publicizing best practices in incident response and prevention advice;
* Coordinating international cooperation on cyber incidents;
* Building capacity in all the above areas using advanced technology and techniques, establishing methods, and researching threat analyses and mitigations.

Cybersecurity Skills and Training Program:

Since cybersecurity has situation dependent needs, countries should adopt a framework which implements a training program. This framework should contain the following:

* Working Group: Participants should represent stakeholder groups in managerial, technical and information assurance areas. The business teams, represented under the heading “Government Ministry or Private Sector” in the Framework, provide the contextual factors for the skills i.e. assets protected and why. The technical teams should define the technical skills required to meet protection needs.
* Job Descriptions: The constituted Working Group should define a continuum of management, information assurance and technical job descriptions. The job descriptions help standardize the understanding of skills and training needs for a cybersecurity program.
* Certification: GCA strategic goal six calls for the development of a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how sharing. As such, this skills framework assumes that leaders of cybersecurity programs will consider sponsoring their staff to pursue commercial information security certifications. The logic is follows. The private sector designs most of the critical infrastructure around the world. Indeed, the private sector engineers the security enforcing functions in critical infrastructure such as firewalls, IDS, IPS and anti-virus software. Therefore, commercial certifications would facilitate global cybersecurity knowledge sharing on common issues. Besides, commercial certifications are most likely to keep pace with the increasingly sophisticated, frequent and severe cyber threats.
* Training Coordination: The skills framework assumes that, at least in the initial stages, some training should be coordinated centrally. Centralized training helps create common understanding of the cybersecurity challenge. This Guide assumes that a National Cybersecurity Agency or similar multi-agency organization should either deliver the training itself or coordinate courses provided on its behalf. The Agency should request stakeholder organizations to validate the courses and obtain commitment for funding from their local budgets.

[1] International Telecommunication Union (2011). National Cybersecurity Strategy Guide. International Telecommunication Union, pp.48-50 58-61.