Christos Beretas, MSc

http://www.christosberetas.com

chr.beretas@gmail.com

(+30) 693-890-9477

Greece

U.S CYBER STRATEGY OF 2020

Short Bio

I am holder of Bachelor and Master of Science degree in the field of Computer Systems from City University of Seattle, USA, also I am holding various certificates from other universities. My research areas are: **Cyber Security**, **Networks**, **Privacy**, **Software Development**, and **Social Media**. Also, I am active in the field of IT, telecommunications, and social media campaigns. I am involved in various research and other projects globally both in public and private sector, I am designed and developed various kind of software applications which are available globally and divided in 3 categories, (**1**) some of them are freeware, (**2**) some of them are for commercial purposes (organizations globally asked me to create that custom applications), and (**3**) some of my software applications are "honeypot" applications for different purposes.

Abstract

The principles of **confidentiality**, **integrity** and **availability** of information processing and storing should remain intact. The establishment of a secure electronic environment for the protection of privacy with actions for the protection of critical information infrastructure seems more than necessary. The USA is not prepared as it should have against an cyber attack, the reason for this failure is that there is not a unique and official national cyber security policy nor a unique organization which has

the sole responsibility and power to achieve that. In cyber security sector, federal agencies do not cooperate sufficiently with each other. This situation in the cyber security field is no longer acceptable as stake most numerous and important.

Cyber Policy

The need to protect critical information infrastructure is necessary to minimize the negative effects and disastrous consequences of possible malicious actions. These critical infrastructures should be identified and assessed on the basis of predetermined criteria. The most effective way to achieve a satisfactory level of safety in all critical information infrastructure is to establish a **National Cyber security Framework**. This framework could be divided into the following eight (8) categories.

- Risk Management
- Vulnerability Assessment
- Penetration Testing
- Software Management (Including software for example: Easter Eggs with hidden code, vulnerable encryption systems that will be used from the enemies and they will believe they are safe, etc.)
- Monitoring
- Contingency Plan
- Honeypot Systems
- Cyber Exercises

None technological system or set of measures can not protect 100% critical information infrastructures. That's why a **Contingency Plan** is very important due to the growing and unpredictable cyber attacks. As mentioned above the Contingency Plan will include the guidance and development of procedures to be taken when a big cyber attack greatly affect negative the operation of critical information

infrastructures and telecommunications systems. Such a plan should include the following.

- Determining the level of protection.
- Creation of early warning systems.
- Create new secret, private and secure networks.
- Ensuring a confidential communication between critical services.
- Create disaster recovery plan.

The cyber security policy established by the state and should be actively supported by all federal agencies. This policy should regulate safety issues at all levels of government. The cyber policy should be accepted by all federal agencies. Then must be informed all the employees of federal agencies. There should be united response of any cyber threat. The security policy should include the following elements:

- Responsibilities and Roles.
- Cyber Security objectives.
- Scope of Cyber Policy.
- Cyber Security Legislation.
- Guidelines.
- Review and Audit.

The Cyber security rules must meet the characteristics of simplicity without unnecessary technical terms and specialized reports of clarity, applicability, will be generalizable and scalable and will require compliance by all employees in federal agencies independent hierarchy.

The review of Cyber security policy should be a very tactical level thinking always growing asymmetric digital threats and the need to anticipate and eliminate cyber attacks. The main factors to be covered in this direction are:

- Awareness of the problem size.
- Design periodic reviews and revisions of the measures.
- Duplication of measures. A combination of measures minimizes threats and increases the reliability of the protection system.
- The primary condition for the performance of a measure is to be active the right time.
- Identify potential risks and criteria for activating the plan.
- Identification of important operations and associated systems.
- Prioritization of activities and prioritization.
- Implementation plan by staff and scheduling operations.

System administrators of federal agencies in the U.S must comply with reverence the following rules and to comply with country Cyber security plan.

- Install, update, backup and identify security holes.
- Regular inspection of software implementation and system files.
- Check files and storage media for viruses.
- Filtering of incoming e-mails.
- Training employees.
- Checking the accuracy of the information.

Αν Cyber security plan should include policy management of telecommunications infrastructure. Employees of these systems must be bound by a contract, which will record the data requirements and the permissible level of access to perform their work to avoid violations and information modifications by unauthorized persons. The security policy that should be applied to these systems should be as follows:

- Access to communication services limited to specific entities.
- The available identification and authentication procedures should control all entities, using the communication infrastructure.
- Each access to the system should be recorded as well as any other activity.
- The of communications services users' passwords should be changed at regular time.
- Amended and sophisticated encryption methods should be used to prevent information leakage.
- No employee will not have access to network monitoring applications and systems.
- Where continuous unsuccessful access attempts to the access method must be deactivated.
- The system should be identified to the user.
- Traffic Analysis per employee.
- Double confirmation procedures.
- Apply remote booting, no local flash disks, hard disks, etc.
- Physical protection.

An attacker may be included in the set of authorized users but can also come from outside the organization, who is served by the system or not. The purpose of an unauthorized intrusion may be the disclosure, alteration and destruction of information, partial or total use-destruction of system resources.

The Cyber security policy along with the internal security policy to be applied by system administrators in a federal agency should be aimed to prevent threats which

are summarized below, and which must be prevented using the methods presented above.

- Message observation, copying all or part of them.
- Traffic Analysis (packet sniffing).
- Data Modification.
- Network Delay
- Break Privacy.
- Spoofing.

Federal agencies should create a customized software by the following characteristics:

- Object and data recognition.
- The system should monitor itself for the level of confidentiality.
- The system must record all actions involving or which may affect its safety.
- The system should provide technical arrangements to implement the ensuring policy.
- Continue monitoring.
- Security.
- Integrity.
- Capacity.
- Efficiency.
- Flexibility.
- Usability.
- Reliability.
- Extentability.
- Availability.

Ensuring continuity of the information system operation and the network after a cyber attack should apply Continuity Operation Plan which must be included in the country Cyber security plan which should include the following:

- Limiting the extent of damage and destruction, and prevent possible escalation of these.
- Seamless degradation.
- Installing alternative means of operation in advance.
- Education and familiarity of human resources.
- Rapid and smooth recovery operation.
- Minimize the economic impact.

The Continuity Operation Plan should initially include defining the conditions under which the state would be considered emergency. The federal Agency should conduct regular monitoring activities in its systems. The Continuity Operation Plan should include identification of important operations and respective systems. If it is found that there are security holes or glitches in the system, affecting essential requirements and obligations for the smooth operation and security, then it should be considered that there is a serious problem in security.

The economy and the strategy of a country is identified with the internet, mainly in America that most of the activities of public and private organizations conducted via the Internet, federal agencies must be considered paramount. What should concern and has as first target a government is the security of information systems and networks as government agencies including the army manage personal data of citizens. The security policy has to predict possible events and situations threatening the security thereof, and to propose a series of response measures. It has been shown that the mechanisms and techniques by themselves do not constitute a security

measures. It should also be given more scope in the analysis process of the systems of risk. The Cyber policy is the first step you need to do if a government wants to have a safe and trusted network.

Bibliography

Thomas Rid. 2013. **Cyber War Will Not Take Place** (1st Edition). Oxford University Press.

Brandon Valeriano, Ryan C. Maness. 2015. **Cyber War versus Cyber Realities: Cyber Conflict in the International System** (1st Edition). Oxford University Press.