NEW REQUIREMENTS OF INFORMATION SYSTEMS IN TODAY'S CRITICAL INFRASTRUCTURE

Colonel (ret) Professor Gruia TIMOFTE, PhD*

This paper analyzes the cyber vulnerabilities, threats and risks to critical information infrastructure in the information age with large and intensive developments in information and communications technology. This virtual dimension is very important for information systems, communications networks, surveillance, control and warning systems and their critical information flows, which ensure the management of the global and national critical infrastructure. These systems are regarded as the backbone of critical infrastructures and as very necessary to the continuity of the information and knowledge management in order to provide specific services. Therefore, the information and communications technology systems must be robust, reliable, sustainable, secure, redundant, adaptive, etc. to meet the cyber threats and risks challenges.

Keywords: *critical information infrastructure, information systems, information and knowledge management, cyber threats, cyber security.*

The *Wikipedia* online dictionary defines cyberspace as an electronic medium of computer networks, in which online communication takes place. In current usage, the term "cyberspace" stands for the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems. As a social experience, individuals can interact, exchange ideas, share information, provide social support, conduct business, direct actions, create artistic media, play games, engage in political discussion, and so on, using this global network. The term has become a conventional means to describe anything associated with the Internet and the diverse Internet culture [1].

In the U.S.A., cyberspace is defined as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people [2].

* gruia.timofte@gmail.com

Cyberspace is better understood as a global information and communication environment, where technology is not only an entry point to the debate, but also a vitally important driver of change [3]. Cyberspace is a diverse arrangement of technology, products, collaborative environments and applications. These elements interact together in a constantly evolving system which is largely dynamic and unpredictable. Furthermore, this system is driven by a vast and diverse array of stakeholders – some more benign than others – including individual users, ad hoc communities, the private sector, the public sector, the national security community, etc. Self-evidently, technology and cyberspace evolve, so the threats and challenges which stem from them should also be expected to evolve.

1. Cyberspace and Critical Information Infrastructure

In most developed country critical infrastructure protection is an important political objective. For example, in the U.S.A., shortly after taking office, President Obama ordered the thorough analysis of federal efforts to defend the U.S. information and communications infrastructure, and the development of a comprehensive approach to securing U.S.'s digital operations in cyberspace, which encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure [4].

The near-term actions recommended are listed below:

- Appoint a cyber security policy official responsible for coordinating the nation's cyber security policies and activities.
- Prepare an updated national strategy to secure the information and communications infrastructure to be later approved by the president.
- Designate cyber security as one of the president's key management priorities and establish performance metrics.
- Designate a privacy and civil liberties official to the cyber security directorate.
- Convene appropriate interagency mechanisms to conduct legal analyses of priority cyber security related issues and formulate a coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cyber security related activities.
- Initiate a national public awareness and education campaign to promote cyber security.
- Develop U.S. Government positions for the international cyber security policy framework and strengthen the international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cyber security.
- Prepare a cyber security incident response plan; initiate a dialog to enhance public-private partnerships and to provide resources to optimize their contribution and engagement.

•Cooperate with other entities and develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure.

•Build a cyber security-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the nation.

In May 2009, the President accepted the recommendations of the resulting Cyberspace Policy Review and appreciated that the initiatives would play a key role in supporting the achievement of many of the essential recommendations from this document[5].

The Comprehensive National Cybersecurity Initiatives consists in a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace: *to establish a front line of defense against today's immediate threats, to defend against the full spectrum of threats, and to strengthen the future cyber security environment.*

The initiatives are as follows:

▪Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.

▪Deploy an intrusion detection system of sensors across the Federal enterprise.

▪Pursue the deployment of intrusion prevention systems across the Federal enterprise.

▪Coordinate and redirect research and development efforts.

▪Connect current cyber operations centers to enhance situational awareness.

▪Develop and implement a government-wide cyber counterintelligence plan.

▪Increase the security of our classified networks.

▪Expand cyber education.

▪Define and develop enduring "leap-ahead" technology, strategies, and programs.

▪Define and develop enduring deterrence strategies and programs.

▪Develop a multi-pronged approach for global supply chain risk management.

▪Define the Federal role for extending cyber security into critical infrastructure domains.

The security and the effective operation of the U.S.'s and other countries' critical infrastructure rely on cyberspace, industrial control systems, and information technology that may be vulnerable to disruption or exploitation. Along with the rest of the U.S. government, the Department of Defense depends on cyberspace to function. It is difficult to oversee this reliance; it operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. The Department of Defense uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full

spectrum of military operations. To this end, it establishes five strategic initiatives, as follows[6]:

(1). *Department of Defense will treat cyberspace as an operational domain to organize, train, and equip so that it can take full advantage of cyberspace's potential.*

•Manage cyberspace risk through efforts such as increased training, information assurance, greater situational awareness, and design of secure and resilient network environments;

•Assure integrity and availability by engaging in smart partnerships, building collective self defenses, and maintaining a common operating picture; and

•Ensure the development of integrated capabilities to rapidly deliver and deploy them where they are needed the most.

(2). *Department of Defense will employ new defense operating concepts to protect its networks and systems.* As a first step, Department is enhancing its cyber hygiene best practices to improve its cyber security. Second, to deter and mitigate inner threats, it will strengthen workforce communications, workforce accountability, internal monitoring, and information management capabilities. Third, it will employ an active cyber defense capability to prevent intrusions onto its networks and systems. Fourth, Department is developing new defense operating concepts and computing architectures.

(3). *Department of Defense will partner with other government departments and agencies and the private sector to enable the cyber security strategy.*

(4). *Department of Defense will build robust relationships with U.S. allies and international partners to strengthen collective cyber security.*

(5). *Department of Defense will leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.*

The Department's five strategic initiatives offer a roadmap for it to operate effectively in cyberspace, defend national interests, and achieve national security objectives.

In official publications, the term Critical Infrastructure Protection (CIP) is frequently used even if the document only refers to the information aspects of the issue. The reason for this is that the two cannot and should not be discussed as completely separate concepts. In our view, CIP is more than Critical Information Infrastructure Protection (CIIP), but CIIP is an essential part of CIP. An exclusive focus on cyber-threats that ignore important traditional physical threats is just as dangerous as the neglect of the virtual dimension – what is needed is a sensible handling of both interrelated concepts [7]. While CIP comprises all critical sectors of a nation's infrastructure, CIIP is only a subset of a comprehensive protection effort, as it focuses on measures to secure the critical *information* infrastructure (CII). Generally, the CII is that part of the global or national information infrastructure that is essentially necessary for the continuity of a country's critical infrastructure services. The CII, to a large degree, consists of, but is not fully congruent with, the information and telecommunications sector, and includes components such as telecommunications,

computers / software, the internet, satellites, fiber-optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows. Due to their role in interlinking various other infrastructures and also in providing new ways in which they can be targeted, information infrastructures do play a very specific role in the debate, as we have already mentioned. They are regarded as the backbone of critical infrastructures, given that the uninterrupted exchange of data is essential to the operation of infrastructures in general and to the services they provide.

2. Information Systems and Cyberspace

An information system can be any organized combination of people, hardware, software, communications networks, data resources, and policies and procedures that store, retrieve, transform, and disseminate information in an organization. People rely on modern information systems to communicate with each other using a variety of physical devices *(hardware),* information processing instructions and procedures *(software),* communication channels *(networks),* and stored data *(data resources)* [8].

Conceptually, the applications of information systems that are implemented in today's critical infrastructure can be classified in different ways. For example, several types of information systems can be classified as either operations or management information systems.

a. Such operations support systems produce a variety of information products for internal and external use. However, they do not put on emphasis on the specific information products that can be best used by managers. Further processing by management information systems is usually required. The role of the organization's operations support systems is to efficiently process transactions, control industrial processes, support enterprise communication and collaboration, and update corporate databases. The main operations' support systems are as follows:

•*Transaction processing systems* - process data resulting from business transactions, update operational databases, and produce business documents.

•*Process control systems* - monitor and control industrial processes.

•*Enterprise collaboration systems* - support team, workgroup, and enterprise communications and collaboration.

b. When information system applications focus on providing information and support for effective decision making by managers, they are called management support systems. Conceptually, several major types of information systems support a variety of decision-making responsibilities: (1) management information systems, (2) decision support systems, and (3) executive information systems.

•*Management information systems* - provide information in the form of pre-specified reports and displays to support business decision making.

•*Decision support systems* - provide interactive ad hoc support for the decision-making processes of managers and other business professionals.

•*Executive information systems* - provide critical information from management information systems, decision support systems, and other sources tailored to the information needs of executives.

c. Several other categories of information systems can support either operations or management applications. For example, expert systems can provide expert advice for operational chores like equipment diagnostics or for managerial decisions such as loan portfolio management. Knowledge management systems are knowledge-based information systems that support the creation, organization, and dissemination of business knowledge to employees and managers throughout an enterprise. Information systems that focus on operational and managerial applications in support of basic business functions such as accounting or marketing are known as functional business systems.

Finally, strategic information systems apply information technology to an organization's products, services, or business processes to help it gain a strategic advantage over its competitors. It is also important to realize that business applications of information systems in the critical infrastructure are typically integrated combinations of the several types of information systems. The conceptual classifications of information systems are designed to emphasize the many different roles of information systems. In practice, these roles are combined into integrated or cross-functional informational systems that provide a variety of functions. Thus, most information systems are designed to produce information and to support decision making for various levels of management and business functions, as well as to do record-keeping and transaction processing chores. Whenever is analyzed an information system, we will probably see that it provides information for a variety of managerial levels and business functions.

A model of an information system consists of five major resources: people, hardware, software, data, and networks:

▪*People resources* – specialists (systems analysts, software developers, system operators), end users, and anyone else who uses information systems.

▪*Hardware resources* – machines (computers, video monitors, magnetic disk drives, printers, optical scanners), and media (magnetic tape, optical disks, plastic cards, paper forms).

▪*Data resources* -product descriptions, customer records, employee files, inventory databases.

▪*Network resources* - communications media, communications processors, network access and control software.

▪*Information products* - management reports and business documents using text and graphics displays, audio responses, and paper forms.

As computer technology has advanced, agencies and the nation's critical infrastructures as power distribution, water supply, telecommunications, and emergency services – have become increasingly dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Public

and private organizations rely on computer systems to transfer increasing amounts of money and sensitive and proprietary information, conduct operations, and deliver services to constituents. The security of these systems and data is essential to protecting national and economic security, and public health and safety. Conversely, ineffective information security controls can result in significant risks, including the loss of resources, such as national payments and collections; inappropriate access to sensitive information, such as national security information, personal information on taxpayers, or proprietary business information; disruption of critical operations supporting critical infrastructure, national defense, or emergency services; and undermining of agency missions due to embarrassing incidents that diminish public confidence in government [9]. Threats to systems supporting critical infrastructure and national information systems are evolving and growing. The connectivity between information systems, the Internet, and other infrastructures also creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services.

There are many processes meant to verify actions taken to implement the standards and recommendations. In addition, there is ongoing preoccupation regarding cyber CIP efforts in several other areas including (1) cyber security-related standards used by critical infrastructure sectors, (2) national efforts to recruit, retain, train, and develop cyber security professionals, and (3) national efforts to address risks to the information technology supply chain. In addition to improving the national capability to address cyber security, executive branch agencies also need to improve their capacity to protect against cyber threats by, among other things, advancing cyber analysis and warning capabilities and strengthening the effectiveness of the public-private sector partnerships in securing cyber critical infrastructure.

An appreciated American scientist presents, in a recent printed book, a new method to analyze and protect critical infrastructure against cyber attacks using 10 basic principles, as follows [10]:

a. *Deception* - involves the deliberate introduction of misleading functionality or misinformation into critical information infrastructure for the purpose of tricking an adversary. The openly advertised use of deception creates uncertainty for adversaries because they will not know if a discovered problem is real or a trap. The method is useful for real-time behavioral analysis if an intruder is caught in a trap.

b. *Separation* - implies enforcement of access policy restrictions on the users and resources in a computing environment. Network separation is currently accomplished using firewalls, but programs of critical infrastructure protection will require three specific changes: network based firewalls on high-capacity backbones, internal firewalls, and firewalls for specific applications and protocols.

c. *Diversity* requires the selection and use of technology and systems that are intentionally different in substantive ways. The diversity in the products, services, and

technologies supporting national infrastructure reduces the chances that one common weakness can be exploited to produce a cascading attack. Therefore, a program of coordinated procurement and supplier management is required to achieve a desired level of national diversity across all assets.

d. *Commonality* - necessitates uniform attention to security best practices across critical infrastructure sectors. The consistent use of security best practices in the management of critical infrastructure ensures that none of the components is poorly managed or left completely unprotected. For this purpose, programs of standards selection and audit validation are required.

e. *Depth* - involves the use of multiple security layers of protection for critical infrastructure assets. The use of defense in depth in critical infrastructure assures that no important asset is reliant on a single security layer. At the national level, analysis is required to ensure that all critical assets are protected by at least two layers, and if possible more.

f. D*iscretion* - implies individuals and groups making good decisions to obscure sensitive information about critical infrastructure. Large-scale infrastructure protection can not be done correctly unless a national culture of discretion and secrecy is promoted.

g. *Collection* - involves automated gathering of system-related information about national infrastructure to allow security analysis. National infrastructure protection will require a data collection approach that is acceptable to the citizens and provides the requisite level of detail for security analysis.

h. *Correlation* - implies a specific type of analysis that can be executed on factors related to national infrastructure protection. This principle is the most fundamental of all analysis techniques for cyber security, but modern attack methods such as botnets greatly make difficult its use for attack-related indicators. National-level correlation must be performed using all available sources and the best available technology and algorithms.

i. *Awareness* - requires an organization understanding the differences, in real time and at all times, between observed and normal status in national infrastructure. A program of national situational awareness must be running to ensure correct management decision making for national assets.

j. *Response* - involves ensurance that processes are in place to respond to any security-related indicator that becomes available. Incident response for critical infrastructure protection is especially difficult because it generally involves complex dependencies and interactions between disparate organizations. This is best completed at the national level when it focuses on early indications, rather than on incidents that have already begun to damage national assets.

For the individual user, cyber security is best understood as a combination of computer security and network security. *Computer security* is concerned with the protection of the system (both hardware and software) and the information it carries from theft, corruption or interdiction. It can therefore involve both physical measures, such as limiting

access to information and communication technology (ICT) systems and controlling the user base, as well as digital security enhancements, such as the creation of a secure ICT architecture and operating system, and the use of secure coded software and anti-virus software. To an extent, the goal of computer security is to ensure security at the level of the component parts of the system. This approach should as a consequence improve the security of the ICT system as a whole [11].

Computer security is complemented by *network security*. Network security is achieved through a combination of physical measures to prevent unauthorized access to the network and to network-accessible resources and equipment, and electronic measures to protect the computing network infrastructure. Network security therefore encompasses a wide range of tools, including administrative and physical controls, and on the electronic side firewalls, encryption and authentication software, anti-virus and intrusion detection systems.

At one level, both the private commercial sector and national governments have adopted a technological approach to cyber security, usually summarized by the term *information security*.

The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide — (a) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; (b) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (c) availability, which means ensuring timely and reliable access to and use of information.

Information assurance is usually understood to be very closely related to information security. If information security can be understood as a largely reactive policy of defense and denial, with an emphasis on technological and physical solutions to the security of data and data systems, then information assurance is more qualitative, in both method and outcome. Giving some sense of this qualitative shift, the goal of information assurance is defined as 'the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Information assurance takes an approach which is more strategic than information security, in that information assurance might, for example, address the consequences of and the recovery from an information attack, and might offset (i.e. accept) a data risk in one area by achieving a level of security in some other area. Information assurance should therefore be understood as the *management of risk* where the quality, reliability and availability of information are concerned, using the standard tools of mitigating, excluding, accepting or transferring risk, and doing so cost-effectively. As such, information assurance should be expected to make more of a contribution than the narrower information security approach to the development of cyber security strategy.

3. Secure Control and Warning Systems

The widespread interconnectivity poses significant risks to the organizations' and the nation's computer systems and, more importantly, to the critical operations and infrastructures they support [12].

Control systems are computer-based systems that are used within many infrastructures and industries to monitor and control sensitive processes and physical functions. Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment.

There are two primary types of control systems. Distributed control systems typically are used within a single processing or generating plant or over a small geographic area. Supervisory Control and Data Acquisition (SCADA) systems are typically used for a large geographically dispersed distribution operations.

Historically, *security concerns about control* have been related primarily to protecting them against physical attack and preventing the misuse of refining and processing sites or distribution and holding facilities. However, more recently, there has been a growing recognition that the control systems are now vulnerable to cyber attacks from numerous sources.

Several factors have contributed to the escalation of risk to control systems, including (1) the adoption of standardized technologies with known vulnerabilities, (2) the connectivity of control systems to other networks, (3) insecure remote connections, and (4) the widespread availability of technical information about control systems.

a. Today, however, to reduce costs and improve performance, organizations have been transitioning from proprietary systems to less expensive, *standardized technologies* and the common networking protocols used by the Internet. These widely-used, standardized technologies have commonly known vulnerabilities, and sophisticated and effective exploitation tools are widely available and relatively easy to use. As a consequence, both the number of people with the knowledge to wage attacks and the number of systems subjected to attack have increased. Also, common communication protocols and standards can make it easier for a hacker to interpret the content of communications among the components of a control system.

b. Enterprises often *integrate their control systems with their enterprise* networks. This increased connectivity has significant advantages, including providing decision makers with access to real-time information and allowing engineers to monitor and control the process control system from different points on the enterprise network. In addition, the enterprise networks are often connected to the networks of strategic partners and to the Internet. This convergence of control networks with public and enterprise networks potentially creates further security vulnerabilities in control systems.

c. Vulnerabilities in control systems are exacerbated by *insecure connections*. Organizations often leave access links—such as dial-up modems to equipment and control information—open for remote diagnostics, maintenance, and examination of system status. If such links are not protected with authentication or encryption, the risk increases that hackers could use these insecure connections to break into remotely controlled systems. Also, control systems often use wireless communications systems, which are especially vulnerable to attack, or leased lines that pass through commercial telecommunications facilities.

d. Public *information about infrastructures and control systems is readily available to potential hackers and intruders*. In addition, significant information on control systems is publicly available—including design and maintenance documents, technical standards for the interconnection of control systems, and standards for communication among control devices—all of which could assist hackers in understanding the systems and the ways to attack them. Moreover, there are numerous former employees, vendors, support contractors, and other end users of the same equipment worldwide who have inside knowledge about the operation of control systems.

Control systems can be vulnerable to cyber attacks. Entities or individuals with malicious intent might take one or more of the following actions to successfully attack control systems [13]:

• disrupt the operation of control systems by delaying or blocking the flow of information through control networks, thereby denying availability of the networks to control system operators;

• make unauthorized changes to programmed instructions devices, change alarm thresholds, or issue unauthorized commands to control equipment that could potentially result in damage to the equipment, premature shutdown of processes, or even disabling control equipment;

• send false information to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators;

• modify the control system software, producing unpredictable results; and

• interfere with the operation of safety systems.

The control systems community faces several *challenges to securing control systems* against cyber threats. These challenges include (1) the limitations of current security technologies in securing control systems, (2) the perception that securing control systems may not be economically justifiable, and (3) the conflicting priorities within organizations regarding the security of control systems.

Efforts to strengthen the cyber security of control systems are made in the following directions:

• Research and development of new security technologies to protect control systems.

• Development of requirements and standards for control system security.

• Increased awareness of security and sharing of information about the implementation of more secure architectures and existing security technologies.

• Implementation of effective security management programs, including policies and guidance that consider control system security.

In conclusion, information systems play an important role in critical infrastructure protection against cyber attacks. Therefore, any organization must develop documented and implemented programs to provide information security and systems security including the following measures: periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems; risk-based policies and procedures that reduce information security risks in a cost-effectively way and to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system; coordinated plans for providing adequate information security for networks, facilities, and systems or groups of information systems; security awareness training for enterprise personnel, including contractors and other users of information systems that support the operations and assets of the enterprise; periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, testing of management, operational, and technical controls for every system identified in major information systems; a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the enterprise; procedures for detecting, reporting, and responding to security incidents; and plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the enterprise.

NOTES

[1] http://en.wikipedia.org/wiki/Cyberspace/

[2] The White House. *The Comprehensive National Cybersecurity Initiative* (Washington, D.C.: March 2, 2010).

[3] Paul Cornish, Rex Hughes and David Livingstone. *Cyberspace and the National Security of the United Kingdom Threats and Responses* (A Chatham House Report, London, March 2009).

[4] The White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: June 19, 2009).

[5] *The Comprehensive National Cybersecurity Initiative*.

[6] U.S. Department of Defense. *DoD Strategy for Operating in Cyberspace* (Washington, D.C.: July 20, 2011).

[7] Elgin M. Brunner and Manuel Suter. *International CIIP Handbook: An Inventory of 25 National and 7 International Critical Infrastructure Protection* (Center for Security Studies, Zurich, 2008).
[8] James A. O'Brien, George M. Marakos. *Introduction to Information Systems* (McGraw Hill, New York, 2007).
[9] U.S. General Accounting Office. *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems,* GAO-11-463T (Washington, D.C.: March 16, 2011).
[10] Edward G. Amoroso. *Cyber Attacks: Protecting National Infrastructure* (Elsevier Inc., New York, 2011).
[11] *Cyberspace and the National Security of the United Kingdom Threats and Responses.*
[12] U.S. General Accounting Office. *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems,* GAO-04-628T (Washington, D.C.: March 30, 2004).
[13] U.S. General Accounting Office. *Federal Information Systems Controls Audit Manual*, GAO-09-232G (Washington, D.C.: February 12, 2009).