The Armenian Center
for National and International Studies

Ռազմավարական եւ ազգային հետազոտությունների
հայկական կենտրոն

Армянский центр стратегических и
национальных исследований

ACNIS ANALYTICAL REPORT
Number One
July 2009

Richard Giragosian
ACNIS Director

THE STATE OF CYBER-SECURITY IN ARMENIA

Աշոտ Թուրաջյան
ՌԱՀՀԿ տեղեկատվական տեխնոլոգիաների մասնագետ

ՀԱՅԱՍՏԱՆՈՒՄ ՏԵՂԵԿԱՏՎԱ-ՀԱՄԱԿԱՐԳՉԱՅԻՆ ՏԵԽՆՈԼՈԳԻԱՆԵՐԻ ՄԱԿԱՐԴԱԿՆ ՈՒ ՁԱՐԳԱՑՈՒՄԸ

Карапет Каленчян
административный директор АЦСНИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЩЕСТВЕННО-ПОЛИТИЧЕСКИХ СИСТЕМ

Yerevan
2009

The views expressed here are those of the individual authors and do not necessarily coincide with those of the Center.

© 2009 Ռազմավարական եւ ազգային հետազոտությունների հայկական կենտրոն:
Հոդվածի կամ նրա առանձին հատվածների հրապարակումը առանց ՌԱՀՀԿ-ի գրավոր թույլտվության՝ արգելվում է:

© 2009 Армянский центр стратегических и национальных исследований.
Публикация статьи или отдельных ее частей без письменного разрешения АЦСНИ запрещена.

© 2009 Armenian Center for National and International Studies.
This publication may not be reproduced or published, in whole or in part, without the express written consent of the Center.

"The State of Cyber-Security in Armenia"

Prepared by

Richard Giragosian
Director
Armenian Center for National
and International Studies (ACNIS)

Introduction

The strengthening of cyber-security represents an effort of strategic importance for the Republic of Armenia. The strategic imperative for strengthening cyber-security in Armenia stems from three main factors: the need to be more deeply engaged in the globalized world, including "cyberspace," the challenges from newly emerging security threats, and the more specific need for ensuring adequate security for the development of Armenia's Information Technology (IT) sector.

There is also a degree of "peer pressure" from Armenia's neighbors, especially as the Azerbaijani government has become increasingly concerned with the need for enhancing its own cyber-security. There have also been reports that the Azerbaijani military has expressed a keen interest in bolstering its own cyber-warfare capabilities. From this regional perspective, there are also two important incentives for Armenia: the need to keep pace with cyber-security initiatives in the region, and the necessity to maximize Armenia's potential as a regional leader and pioneer in the IT sector.

The Concept of Cyber-Security

The concept of cyber-security is firmly rooted in the inherent role of the Internet as a bridge and link to the outside world. This role has expanded tremendously in recent years, as refelected in the vast expansion and diffusion of the Internet from its origins as a research project in the 1960s to a widespread commercial infrastructure with close to one billion Internet-connected users as of 2004. It is, therefore, a strategic imperative for Armenia to recognize and promote cyber-security as an urgent policy priority, in terms of keeping pace with globalization to overcome the thrat of isolation and to defend against the new security threats of the 21st century. More specifically, there are four principal components to Armenian cyber-security: to safeguard and defend national security, to engage and integrate more deeply with the globalized marketplace, to develop and expand a knowledge-based economy, and to ensure and modernize the military elements of its cyber-security.

A. National Security

The national security component of cyber-security is comprised of two maini elements: the need to protect Armenia from the threat of cyber-crime, such as money laundering and computer crimes, and the necessity to secure the country's critical infrastructure and communications systems. There is also a need for the monitoring and enforcement of cyber-security within the context of counter-terrorism, extremism and even terrorist financing that have recently redefined the parameters of Armenian national security.

Cyber-Crime & Money Laundering

The need to combat cyber-crime is an integral part of the overall effort to bolster Armenian cyber-security. Cyber-crime is also a national security consideration, as Armenia must prevent the creation of "cyber-crime havens" by enacting measures capable of fostering greater vigilance in countering any criminalization of cyberspace. The Armenian state is, therefore, called on to codify and criminalize any and all acts deemed to threaten the security and integrity of cyberspace. It should also recognize the scale and scope of cyber-crime, which almost always ignores national borders, surpasses legal systems and exploits weaknesses in multilateral cooperation.

Fighting cyber-crime also requires effective criminal investigation and prosecution. For Armenia, this also presents new opportunities, as there are a number of programs available that offer funding, training and technical assistance for fighting cyber-crime. The Armenian Central Bank and a few other government officials have already participated in such programs, but there is ample opportunity for greater involvement in international cyber-crime initiatives.

At the same time, there is a need to balance the law enforcement and national security demands of combating cyber-crime with the proection of civil liberties and societal rights. Such a policy balance needs to accommodate and appropriately protect privacy, with procedural safeguards governing the interception, preservation, production and seizure of data. In order to facilitate the protection of such societal norms, Armenia should look to the provisions of the "Council of Europe Convention on Cybercrime" as a useful basis for strengthening national legal frameworks dealing with cyber-crime. Armenia should also build upon its commendable decision to become a signatory state of the Council of Europe Convention on Cybercrime.

Although money laundering is not a new criminal threat, it has assumed an elevated importance in the wake of the attacks of September 11, 2001 and the subsequent "global war on terrorism." Although the traditional focus of money laundering has generally been driven by threats posed by international and domestic organized crime, and related narcotics trafficking, the new emphasis reflects the emerging threats to national security posed by the possible linkage of money laundering and terrorism, therefore, adding a new focus on tracking and blocking the financial flows of terrorist

groups and their supporting infrastructure network. The effort to counter money laundering has also had to adapt to newer, non-traditional facets of this challenge, such as the informal networks for remittances, and on the innovative use of the Internet and web-based financial transactions by both criminal and terrorist groups. For Armenia, the need is to demonstrate effective cyber-security policies sufficient to affirm Armenia's role as a responsbible partner in the fight against terrorism, money laundering and other related cyber-crimes.

Protecting Armenia's Critical Infrastructure

The protection of the country's national infrastructure and critical assets is also a fundamental requirement of Armenian national security. With the vital role of computer networks and sophisticated automated systems, the need for protecting the cyber-security of these operational components of Armenia's critical infrastructure is obvious. Given the natural reliance on the national infrastructure for much of Armenia's economic activity (the production and distribution of most goods and services), the identification of the "critical infrastructure" is an essential first step in assessing the vulnerabilities of such a wide array of physical assets. And as computer and communications systems and networks are increasingly vital bridges linking various sectors of the infrastructure, they are clearly "core critical infrastructures" mandating adequate cyber-security to safeguard against various vulnerabilities, including human error, natural disaster and even attack.

Moreover, Armenia's crucial infrastructure provides the "backbone" for the Internet wihin the country. In this context, the Internet should be seen as a complex "system of systems," composed of interconnected networks that use a common set of protocols, most commonly known as the Internet Protocol (IP). The Internet and its applications are dependent on the underlying physical infrastructure (or "backbone") and thereby require that this infrastructure is available, secure, well-managed and inter-connected, and has adequate capacity and service quality. Therefore, Armenia's critical infrastructure is a crucial consideration for cyber-security.

In terms of assessing the cyber-security needs of Armenia's critical infrastructure, there are six key areas in need of computer network/cyber protection:

1. **Telecommunications**: land-line and cellular telephone service networks, the processing, storage and transmission of data by facsimile and email;
2. **Energy**: operational and safety systems for essential services, such as electrical distribution and transmission and water supplies, among others, as well as the security of the Medzamor nuclear power plant;
3. **Banking & Finance**: systems governing financial exchange, transactions and settlements, stock trading, automated teller machines (ATMs);

4. **Transportation**: the aviation guidance, air traffic control and airspace monitoring system, the monitoring of transporting and handling of hazardous materials (such as nuclear waste from Medzamor) by road, rail or air;
5. **Government Services**: emergency systems for medical, police, fire, rescue and natural disaster response & recovery services, public health networks to monitor disease or bioterrorism, the continuity of government in crises (earthquake, incidents of terrorism or war);
6. **Defense**: command & control systems, lines of communication for air and land forces.

It is difficult to make a distinction between the physical security and cyber-security of the Armenian infrastructure, however. But it is the reliance on computer- and cyber-based systems for the operation, monitoring and safety of each of these six areas that presents a unique challenge to ensuring cyber-security. The need for cyber-security of the Armenian critical infrastructure further entails the protection of both physical and cyber assets from operational failure as well as from being compromised by either unauthorized access or problems in the operating software or systems. Moreover, the outdated condition of much of the physical assets of Armenia's critical infrastructure only compounds the inherent vulnerabilities in its computer- and cyber-based systems.

B. Globalization

Cyber-security is also a prerequisite for overcoming the constraints of the blockade and embargo imposed on Armenia by both Azerbaijan and Turkey. It is also necessary as a tool to overcome the isolation of Armenia and to help integrate the emerging Armenian economy into the globalized marketplace. On a national scale, cyber-security also holds an influential role in forging a deeper integration of Armenia's rural areas in the overall economy. Cyber-security is especially crucial in this regard, given the increasingly vital role of technology as a driver for future economic growth and job creation. Within a regional context, Armenia must also keep pace with its neighbors in developing its cyber-security. This is also essential to ensure that Armenia is no longer excluded from regional development projects or future technological initiatives.

C. A "Knowledge-Based" Economy

In addition to the role of cyber-security in negating Armenia's blockade and isolation, it is further important as a facilitator of the development of a knowledge-based economy in Armenia.[1] The protection of intellectual property, the prevention of cyber-crime and the promotion of sound national policies on technology, constitute the linkage between cyber-security and modern economic development.

[1] By the term "knowledge-based economy," I refer to the basic definition provide by the Organization for Economic Cooperation and Development (OECD), which states that a knowledge-based economy is "directly based on the production, distribution and use of knowledge and information."

This is clearly evident in Armenia's potential for hosting such "outsourced" services as software development, data entry and as "call centers" for foreign telemarketing, customer service and credit card companies. But effective cyber-security is also an important prerequisite for the development of future "start-up" businesses such as e-commerce, online banking, and biomedical research, among others.

D. Military Security

Cyber-security is also an essential element of overall Armenian military security. There are several facets of the relationship between cyber-security and military security, ranging from the need to protect against cyber-attack and cyber-warfare to the necessity of maintaing and protecting the integrity of secure military lines of communication and command and control.

Currently, the Armenian military faces two types of cyber-security threats: cyber-war and "netwar." Cyber-warfare involves information- or communications-system warfare waged by an opposing state's formal military forces. "Netwar," on the other hand, consists of an information- or communication-system conflict waged by networks of non-state actors. Both cyberwar and netwar utilize attacks an opponent's computer networks and military lines of communication.

Armenia has already been victim to such cyber-attacks, with "netwar" attacks successfully targeting and disrupting dozens of Armenian-related websites and their host computer servers in Armenia, Europe and the United States. One series of such attacks, in January 2000, have also targeted the web pages and computer networks of both the U.S. Embassy and the Soros Foundation office in Baku. The Azerbaijan cyber-attacks, carried out by hackers calling themselves "The Green Revenge" and "Hijack," were seen by some experts as being related to or even supported by the Azerbaijani government.[2]

And although the most extensive cyberwar capabilities are generally limited to the larger or more advanced military powers (China, Russia, Israel, the United States, etc.), the "start-up" or "entry" costs associated with acquiring more basic cyber-warfare capabilities are relatively modest and depend more on technical human capital than on financing. This has also been most clearly demonstrated by the record of cyber-attacks launched against the United States government and military, with cyber penetrations of some of the most "secure" U.S. systems by lone "hackers" and even school-age computer enthusiasts. The lesson for Armenia is to take nothing for granted, to not underestimate the ease of cyber-attacks and to prepare a defensive response *prior* to, and not simply *after* a cyber-attack.

---

[2] Strobel, Warren, "A glimpse of cyberwarfare," *U.S. News and World Report*, 13 March 2000.

The State of Armenian Cyber-Security

There are five main problems associated with the current state of cyber-security in Armenia. The first, and most pervasive, problem is rooted in the Soviet legacy of technology policy. Armenia faced a period of uncertainty and inexperience at the time of independence in the wake of the collapse of the former Soviet Union. Although the obstacles inherited from the Soviet system were profound, and ranged from a closed economic and political system to an overly managed centralized economy, it was the Soviet legacy of technology policy that seriously impeded the development of Armenian cyber-security.

During the seven decades of Soviet rule, technology was dominated by the state and any and all technological innovation was driven by the state. This legacy of state-dominated technology resulted in an entrenched policy of limiting technological development and research and development (R&D) within the institutions of the state and the military. The current need for strengthening Armenian cyber-security, and for combating cyber-crime, must overcome this over-dependence on the state, however. Armenian cyber-security must now incorporate the private sector, and its emerging IT sector in particular, as a key driver for development. Moreover, it is the private sector, and not solely the state, that must be the primary innovator in cyber-security, technology and R&D.

A second problem facing the current state of Armenian cyber-security is the closed, monopolistic structure also defined as a Soviet legacy. But this problem is one of inherited hardware and not of inherited policy. Specifically, as with all former Soviet states, Armenia remains burdened by the limitations of a seriously outdated telecommunications infrastructure, in need of both modernization and investment. This Soviet-era system, dominated largely by outdated analog, rather than modern digital lines, is a challenge to bolstering cyber-security.

Although there has been some degree of progress following some infrastructural investments in recent years, serious structural shortcomings remain and the reliance on obsolete equipment continues to be commonplace. Thus, there is a continued need for further investment required to raise the Armenian system to minimum world standards. Unlike the first two Soviet legacy problems of Armenian cyber-security, the third obstacle arose more recently, and stems from the high cost of telephone and Internet services. The economics of this problem poses a significant challenge to Armenian cyber-security. It is also directly tied to the fourth problem, however, which center son the monopolistic nature of the Armenian telecommunications sector. And the fifth main problem defining the current state of Armenian cyber-security is the rather deficient set of state policies governing technology and telecommunications. There is a significant need for improvement to Armenia's regulatory framework and public policy in these areas as essential steps to supplement a truly viable and modern network of cyber-security and cyber-crime for Armenia.

Armenia's Emerging Information Technology (IT) Sector

Although an assessment of the Armenian IT sector is beyond the scope of this Analytical Report, the issue of cyber-security is important to Armenia because of the potential and priority of the emerging IT sector. But cyber-security is an essential requirement for the development of a stable IT sector in Armenia. The need for effective cyber-security is not only a prerequisite for IT sector expansion, but is a base requirement for any significant foreign investment in the Armenian IT sector.

A Proposed Cyber-Security Draft Action Plan

Mission Statement

This draft Cyber-Security Action Plan is based on an initial assessment of the reality and needs of the Armenian model, with an application of relevant cyber-security benchmarks and best practices judged to be most suitable for replication and adoption within the Armenian context. This consideration is particularly important, because the imposition of a standardized approach to cyber-security may actually serve to undermine, rather than bolster, security.

Moreover, cyber-security requires a holistic approach, incorporating measures that neither stifle innovation nor set arbitrary standards. This approach also recognizes the need to balance cyber-security against the minimum demands for data protection, privacy, consumer rights and the rule of law. It is this recognition of the need for balancing security against societal interests that limits the utility of other cyber-security models, such as the Russian, Chinese, European, or American case studies. The following Action Plan includes five steps identified as the most important policy measures to be introduced as part of the broader effort to strengthen Armenian cyber-security and bolster its capabilities to combat cyber-crime.

A Five-Step Action Plan

Step One: Securing IT Infrastructure

The first step in strengthening cyber-security and fighting cyber-crime is to address the challenge of the Armenian national telecommunications network. Although this is a complex issue in both a commercial and political sense, the current state of Armenian telecommunications poses a serious obstacle to even the first stage of strengthening cyber-security. The main problem is that a monopoly, exercised either by a state or company, which controls both the telecommunications network backbone and provides retail services to consumers has been found to result in higher prices, sub-standard quality and less competitive services.[3]

[3] Lurie, Peter and Chris Sprigman. "Broadband Marxism," *Foreign Policy*, March/April 2004. P. 83.

In addition to the national security implications of the foreign-held monopoly over the national telecommunications network, cyber-security is also hindered by three impediments directly related to the business conduct and performance of the telecommunications monopoly. The first stems from the blatantly expensive and poor-quality Internet service in Armenia. The high cost, poor quality problem is rooted in the serious record of overcharging and imposition of unreasonably high rates on other telecommunication service providers such as domestic cable company and Internet service providers (ISPs).[4]

The second impediment is the inconsistency and unreliability of the ArmenTel cellular telephone service. Although the Armenian government was able to partially open the mobile phone sector to competition in 2004, cellular phone subscription and area coverage remains far less than comparable data from neighboring Azerbaijan and Georgia.[5] And, as recently as July 2005, a near total paralysis of the small Armenian cellular network lasted for some three weeks, attributed by some analysts to the gross under-investment and under-development of its network.[6] The third impediment is the ArmenTel practice of importing inferior, outdated and, in some cases, defective equipment into Armenia while misidentifying it as an "upgrade" or as a new capital investment in the Armenian infrastructure.[7]

Open the IT Sector to Competition

Given these impediments, the Armenian government should seriously consider pursuing policies that would restore competition to the telecommunications sector and end the practice of satte-granted monopoly concessions. Such policies must strive to open the sector to competition, with transparent tender processes that would invite a significant degree of interest by foreign investors, crucial to providing the investment needed to complete the digitized upgrade of the Armenian telecommunications system.

The resulting competition would also result in lower costs and greater consumer choice for Internet service providers. The government would also be able to devise more prudent limitations, regulations and requirements on any bidders (foreign and domestic) that would satisfy national security concerns. Such negotiations could also lead to serious commitments by well-established foreign firms, such as Sweden's *Ericsson*, the Norwegian *Nokia* firm, or some leading Japanese firms, for example, to cooperate closely with the Armenian government in cyber-security efforts.

---

[4] Ibid.

[5] The partial opening of the sector led to the entry of the Lebanese *VivaCell* network which aims to provide coverage to all regions of Armenia by October 2005.

[6] Zakarian, Armen and Emil Danielyan, "Armenia's Main Cellphone Network Paralyzed," *Radio Liberty Armenia Report*, 18 July 2005.

[7] Information provided in interviews with an anonymous ArmenTel employee and Armenian government officials, Yerevan, June 2005.

While such a new policy option may be politically challenging in the short term, it is a significant longer term step toward ensuring the stability and security of the sector that are essential prerequisites for meaningful cyber-security. A number of leading Western experts have also advocated the concept of a "renationalization of network backbones" and have proposed that governments may ease the financial strain by "using long-term debt funded by revenues flowing from the operating lease. A properly structured public debt issuance would assuage foreign investors' fears of a broader nationalization campaign." [8]

Step Two: Securing Business and Economics

The second step in strengthening cyber-security and fighting cyber-crime is the need to secure the business- and economic-related aspects of cyber-security. This relates to the need to safeguard intellectual property and e-commerce. To date, Armenian legislation has tried to keep pace with these developments. Within the broader framework of harmonization with World Trade Organization (WTO) standards, Armenia has introduced several key amendments to its civil, criminal and customs codes, and has adopted laws on the protection of copyrights, database and computer programs (December 1999); trademarks, services marks, and the destination of places of origin (March 2000); and the protection of economic competition (June 2000). But aside from this record of Armenian intellectual property rights legislation, there is a lack of education, raining and preparatory guidance within the Armenian judiciary. There is still a gap in the enforcement of intellectual property rights in Armenia and an inadequate judicial capability to enforce and adjudicate infringement cases.

Intellectual Property Rights (IPRs)

The concept of intellectual property rights (IPRs) is of paramount importance in the age of the Internet, primarily because the Internet allows the relatively low cost duplication and easier worldwide distribution of works of intellectual property in digital form. It is the ease of duplication and distribution that also makes such digital products and work highly vulnerable to unauthorized copying, modification, tampering and outright theft and illegal re-sale. The term Intellectual Property Right (IPR) describes the legal rights covering intellectual activity in the industrial, scientific and artistic fields. The three main types of IPR are patents, copyright and trademarks, although other forms of intellectual property, such as trade secrets, are also relevant.

A related concern is the issue of consumer rights. Although usually defined and regulated by national legislation, in the context of the Internet, most consumers are unlikely to be aware of the country or jurisdiction regulating their transactions. And in addition, there are linguistic and cultural barriers to effective international protection of Armenian consumer rights. Therefore, the rights and duties of the users of digital

[8] Lurie and Sprigman, 2004.

content should be defined not only by consumer protection legislation, but also by mechanisms and stipulations in intellectual property law, such as software licenses and other end-user license agreements (EULAs).

Under these software licensing and end-user license agreements, however, it is usually the power of the "holders' of these rights to determine and grant the rights to their consumers. Thus, traditional rules normally applicable to the protection of consumer rights in the physical world often do not apply to transactions involving software and digital content. Additional developments in his field that require Armenian legislative and regulatory action include: new technologies such as "trusted computing," usually developed and self-regulated through industry consortia. Currently, there is no established mechanism to evaluate and address potential risks that might arise from the development and deployment of these new technologies.

A related requirement pertains to the utility of competition law and policy to address problems arising from vendors in a dominant position, such as with the case of *Microsoft*, for example. Efforts need to be made to define standard consumer rights and duties for the acquisition, use and sale of online digital goods, including regulations on consumer protection, IPR, competition law and on other related issues such as measures governing the freedom of expression and the regulation for websites.

E-Commerce and Trade

The term "e-commerce" refers to electronic commerce, including both business-to-business (B2B) and business-to-consumer (B2C) transactions. Electronic commerce consists of commercial transactions and the trading of goods and services that utilize electronic means, such as Internet- or web based sales, electronic funds transfers and share trading. The sheer growth in global electronic commerce, as demonstrated by such firms as *Amazon.com* and others, necessitates that Armenian business keep pace with the electronic marketplace.

The presence of Armenian businesses in cyberspace has been far too marginal to date, however. The potential of electronic commerce for Armenia is significant, especially given the geographic constraints on trade resulting from the blockade and embargo imposed by Azerbaijan and Turkey. It is an opportunity to both overcome the country's relative isolation and to negate the disruption of regional trade and export routes. Thus, although the Armenian government has adopted legislation conforming to World Trade Organization (WTO) standards in this area, there is a further need to adopt additional measures (legislative, statutory and regulatory) recognizing "digital signatures,"[9] electronic contracts and the admissibility of electronic evidence.

[9] In this report, 'digital signatures' is used generically to refer to an electronic or digital means to authenticate the identity of a party to an electronic transaction. While it is recognized that the term 'digital signature' is most commonly associated with public key infrastructure (PKI), it is used and intended here to be technology neutral.

As on-line security is a vital consideration in the use and development of e-commerce, Armenia needs to address the use of transaction encryption (or cryptography). The significance of encryption technology exceeds e-commerce considerations, however, as the Armenian government must also maintain vigilance over the sale and use of encryption software. There is a classified decree in place directing the proper use of encryption software by state agencies, bodies and ministries, and software manufacturers are required to submit encryption software to relevant national security authorities for certification. But more needs to be done to govern the import, export and production of such encryption software and there is a lack of a comprehensive policy on encryption.

Step Three: Securing the State

Applying elements of cyber-security to secure the Armenian state is the third step in this Action Plan. An effort to secure the Armenian state refers to the need to address cyber-security for the Armenian military, police and government. Although each of these three areas share a common vulnerability to some degree, their needs and requirements of cyber-security are fairly distinct, however.

Adopt & Adapt "Dual-Use" Technology

The state must also closely follow and adopt any and all relevant commercial technology and software and adapt it for its specific use in ensuring greater cyber-security. Such "dual-use" technology offers the Armenian military, police and government an opportunity to harness technological innovation and tailor it to its own needs.

Improve Defense against Military Cyber-Threats

One of the more recent innovations in modern warfare has been the adaptation of information technologies to war-fighting. The militarization of the Internet has been evolving through the last four decades and has reached an impressive degree of sophistication today. The military aspects of cyber-security, therefore, must be adept to meeting and confronting these emerging cyber capabilities. Cyber-warfare involves military operations that incorporate elements of information-related technology, such as disrupting or destroying an opponent's information and communications systems. Cyber-warfare utilizes a diverse range of technology, from the most rudimentary to the more sophisticated. It protects its own, and targets its opponent's systems for command and control, logistics, tactical communications, positioning, "friend or foe" identification, and "smart" weapons systems, among others. It may also include measures of electronic blinding, deceiving, intruding, jamming or overloading an adversary's information and communications systems.

Defending Against Cyber-Attack: Networks, Not Hierarchies

From a defensive position, there is a need for a new inter-organizational "network" within the Armenian military and government. A network-based approach is important, because the traditional military structure and organization is one of hierarchies (as in the standard "chain of command," for example), but with other low-intensity, asymmetrical threats like insurgencies and terrorism, the military cyber threat is posed by networks. And these networks enjoy the advantage of launching cyber-attacks at little cost and hold not only an advantage of surprise but also anonymity. It is as much a challenge to identify the cyber-attackers as it is to defend against them. Thus, it takes networks to defend against networks.

Such a defensive position against cyber-attack would involve a small unit, similar to the existing signal corps within the Armenian military, assigned to monitor the military communications networks and develop tactical defensive response plans in the event of cyber-attack. From a military perspective, the goal would be system integrity and survivability, and not necessarily counter-attack. This unit would also adopt "red team versus blue team" cyberwargame simulations that would bolster unit readiness and also reveal system cyber vulnerabilities. Specific assistance and training may also be sought through the NATO Partnership for Peace (PfP) program, as well as through bilateral arrangements with the relevant U.S. and/or Russian military units.

Structurally, cyber-security for the Armenian military is dependent on cyber-security for all. Even the advanced and technologically sophisticated U.S. military structure is dependent on the critical infrastructure. The U.S. military, for example, still relies on the same telephone, fax and electrical networks as the ordinary American for over 90 percent of all military communications. For communications, the U.S. military typically uses its Non-Classified IP Router Network (NIPRNET) for routine administrative operations, while its Secret IP Router Network (SIPRNET) allows military access to classified databases and conduct secure messaging. Over 70 percent of NIPRNET traffic uses the civilian Internet, however, while SIPRNET is isolated from the more open Internet. For the Armenian military, therefore, cyber-security is also inherently tied to cyber-security for all of Armenia, especially as the Armenian military is a stakeholder in cyber-security.

Over the medium-term, senior Armenian military staff officers, in conjunction with the Minister of Defense, should increase cooperation and even lead collaborative efforts with the private sector to enhance the cyber-security of the sections of the public infrastructure that the military relies upon. There should also be greater attempts to leverage opportunities for international cooperation in this field, with specific financial and training assistance from the U.S. military, NATO's Partnership for Peace (PfP) program, and from the Collective Security Treaty Organization (CSTO), as well as within multilateral programs of the OSCE, the United Nations, European Union (EU), World Bank and European Bank for Reconstruction and Development (EBRD).

Cyber-security is also in need of increased attention for the Armenian police and emergency services. As both are the first lie of defense or "first responders" in cases of national emergency, the integrity, security and inter-operability of their cyber systems are crucial. The priority of cyber-security for e-governance and related services is also an important consideration. Armenia is the second country in the world, second only to Australia, to have introduced an electronic visa system. It has also been recognized as a pioneer in the establishment of several governmental websites, with one of the most impressive being the Ministry of Foreign Affairs' webpage. Ironically, in the event of cyber-attack, these systems may invite a coordinate attack, as they are natural targets as the moe official "cyber representatives" of the Armenian state.

Step Four: Leverage New Opportunities for Funding and Training

In recognition of the existing financial and budgetary limitation facing Armenia, there is a need to leverage existing programs that provide financial and technical assistance and training in the field of cyber-security. One of the largest and most significant opportunities is provided by the U.S. National Infrastructure Protection Center (NIPC), an interagency effort within the U.S. Federal Bureau of Investigation (FBI). The NIPC regularly provides cyber-crime investigation training to interested foreign counterparts and holds training sessions at the International Law Enforcement Academies in Budapest and Bangkok, with additional training seminars held for foreign cyber-crime officials. The NIPC also offers to hold workshops with foreign governments in their countries to reach larger numbers of officials involved in fighting cyber-crime.

Other opportunities for Armenia to benefit from such international cyber-crime assistance are found in the U.S. Department of Justice's Computer Crime and Intellectual Property Section (CCPS), and its National Cybercrime Training Partnership (NCTP), both of which have been expanding their scope to include foreign training and funding programs. More recently, the U.S. Customs Service has also launched a program on international cooperation. Within the U.S. Department of Homeland Security (DHS), this program provides targeted financial assistance and technical training to a number of foreign cyber-crime personnel.

Forge Public-Private Partnerships

Ensuring cyber-security also requires an active and collaborative relationship between the government and the private sector. This is increasingly essential, as much of the computer and telecommunications systems that constitute Armenia's critical infrastructure are owned, controlled and managed by private companies. The Internet Service Providers (ISPs) must also be integrated into a comprehensive cyber-security strategy. One of the first challenges to establishing an effective public-private partnership for cyber-security is the reluctance of companies to report or share data concerning cyber-attacks. This reluctance is grounded in a fear of disclosing sensitive

corporate information and data and is the most common limitation to establishing a "climate of security consciousness."[10] In order to overcome this private sector hesitation and to foster an effective public-private cyber-security partnership, the government must, therefore, craft polices capable of preventing the unnecessary and unrestricted disclosure of sensitive commercial information, trade secrets or other digitized propriety data.

Create a Public-Private Cyber-Security Forum

One of the more promising avenues to forge an atmosphere of trust and confidentiality within a context of public-private cyber-security would be the creation of a confidential venue or forum that would foster an open and free exchange of data and information regarding cyber-attacks and system vulnerabilities. Such a "public-private cyber-security forum" would encourage private companies to feel comfortable in disclosing relevant information while benefiting from government efforts aimed a protecting them and their business. And, in turn, the government would gain "real time" information on any new cyber-attacks or cyber-crime. Such an effort would be especially important to Armenia, as the state could maintain an active dialogue with the rapidly emerging new firms in the IT sector at a pace consistent with the fast-paced and unpredictable rate of cyber-attacks and cyber-crime.

Such an approach is also beneficial to allow for a closer relationship between the state and the strategically important Internet Service Providers (ISPs). The ISPs should be required to establish national network operations center capable of working with and supporting the government's cyber-security teams. This is especially important as the ISPs are usually the first-line of defense for both cyber-attacks and cyber-crime. They are also in the best position to monitor, track and report attempts at computer system infiltration, penetration or manipulation. The Public-Private Cyber-security Forum concept is modeled on similar computer emergency response centers, officially known as a Computer Emergency Response Team (CERT). This would also allow Armenia to join the Forum of Incident Response and Security Teams (FIRST), and international organization that links foreign CERTs in a global network of cooperation.

Step Five: Preparing for the Future

As this Cyber-Security report has attempted to demonstrate, the future of Armenian economic, military and national security is largely dependent on broader trends that are generally well beyond the parameters of any one country. These trends, exhibited in terms of broad economic and commercial globalization, dynamic new military technology and rooted in the rapid global change of the Internet era, require a new focus on security. It is from this starting point that Armenia must recognize and act

[10] "The Cyber-Dimension of Emerging National Security Threats." The Marshall Center for Security Studies, Conference Report, 2-5 December 2002.

upon the demands of cyber-security. Thus, it is essential for Armenia to prepare for the future in order to guarantee its own future as a secure and stable nation capable of withstanding and exploiting these larger global trends.

The Need for Internet Governance

A core requirement for developing sustainable cyber-security is the need for Internet governance. The need for Internet governance has intensified as the Internet underwent a broad transformation from a research and academic facility into a general purpose communications medium widely available to the public and used for an expanding range of private and public purposes. Although the definition of Internet governance has been underway for over a decade, it has not been free of debate.

The founders of the Internet rejected any suggestion of governance and only called for coordination in a bottom-up, collaborative, largely voluntary fashion. But as the invention of the World Wide Web expanded the Internet and made it accessible to a wide range of users from the mid-1990s on, the need for governance emerged from the increasing commercial value of the Internet, its growing importance to business and government users in all countries, and from the emergence of threats to the security of both individual users and the Internet as a whole.

For the purposes of strengthening cyber-security and combating cyber-crime, Internet governance represents a continuation of the "corporate governance" that relates to the management and operation of private companies and relations between shareholders, directors and managers, as well as with both the state and civil society as a whole. And for the unique context of Internet governance in Armenia, the effort should be transparent and democratic, with the full involvement of the state, the private sector, civil society and relevant international organizations and multilateral institutions.

The Need for Competition Policy

As the Internet and its applications run primarily through the "backbone" telecommunications networks, there is a direct relationship between telecommunications policy and cyber-security. The history of the Internet has demonstrated that its growth was due to in large part to pro-competition and pro-private sector policies in the telecommunications sector.

In a June 2005 report by the United Nations Working Group on Internet Governance tracing the course of the development of the Internet, the evidence demonstrated that state-owned telecommunications operators were privatized, markets were liberalized, and new independent regulatory authorities were established. As the Internet and cyber-activity expanded, regulation shifted from technology-oriented and sector-specific regulation to more competition-oriented regulatory frameworks. In the last ten years, the transformation of the global telecommunications sector also coincided with the

transformation of the Internet (and the World Wide Web) from a medium primarily used by the research and academic communities into "a global facility available to the public."[11]

These transformations were mutually dependent and resulted from shifts in policies affecting the enabling environment. For Internet users, these policies enabled greater access to higher quality services and greater affordability, and lower barriers to entry for network operators and service providers, first in the developed world, then increasingly in developing countries. The next stage in the transformation of telecommunications and the Internet will also feature an extension of IP-based technologies and services to networks previously served only by traditional (analog or digital but non-IP) telephony, and to those characteristic of radio and television broadcasting. The convergence on IP platforms, also referred to as "next generation networks" (NGNs) is already raising new challenges to competition policy and regulation, especially *vis-à-vis* traditional technical regulation and will affect a new array of consumers and mostly private sector operators and service providers and suppliers.[12] For Armenia, there is opportunity to align its telecommunications competition policy with existing inter-governmental organizations that handle Internet governance, such as the International Telecommunications Union (ITU), the Organization for Economic Cooperation and Development, and the World Trade Organization (WTO).[13]

The Fiber-Optic Imperative

Since gaining independence in the wake of the collapse of the Soviet Union, Armenia has been faced with several fundamental challenges, including the disruption of trade, transport and energy links resulting from the imposition of an East-West blockade and related trade embargo by Azerbaijan and Turkey that further distorted Armenia's natural socioeconomic development. Armenia was also excluded from several elements of regional energy and transport development plans, including the Baku-Ceyhan and Baku-Erzerum oil and gas pipelines, as well as more recent projects to modernize the regional railway network. But the most significant imperative for Armenia today is to ensure that it is not excluded from the newest regional development plan. And this imperative is again one of "pipelines," but does not involve energy. This new imperative for regional *inclusion* over *exclusion* stem from the new projects to develop the fiber-optic network in the region (and beyond). It is this fiber-optic "pipeline" that will be key to not only Armenian cyber-security, nor even its economic development, but will determine the future of Armenian national security.

---

[11] United Nations Working Group on Internet Governance. Background Report. June 2005.
[12] Ibid.
[13] The principal governance mechanism of the WTO is through the General Agreement on Trade in Services (GATS), and in particular the agreements on trade in enhanced and basic telecommunication services that form part of the GATS.

There are two ongoing projects aimed at forging regional telecommunications development. The first project, focusing on the "Silk Road" countries, is called SILKSAT and involves the participation of the U.S. satellite corporation *Orbital*. This project has already attracted the interest of Ukraine, Georgia, Azerbaijan and Russia. Within this project, Georgia has positioned itself as the regional hub for the interconnection of the telecommunications networks.

A number of fiber-optic lines, both projected and existing, converge in Georgia. These include four strategic routes Sochi-Poti fiber-optic line, financed by *Rostelecom* to connect the two Black Sea ports; FOPNet's nation-wide trunk telephone network, which will connect Poti with Tbilisi and branch off to Azerbaijan (and theoretically to Armenia); the Trans-Asia-Europe Line (TAE), an 18,000 km fiber-optic network that runs from Frankfurt to Shanghai, via Turkey, Iran and the Central Asian states of the former Soviet Union; and the Black Sea underwater fiber-optic cable, which connects the networks of Bulgaria, Russia, Ukraine and Georgia. The second project, financed by the European Union, is the "Traceca Silk Road" project, which consists of a fiber-optical communication cable running alongside the regional railway network, linking 133 rail stations and providing signaling along the South Caucasus railway tracks. The World Bank has estimated that up to 80% of the network capacity could be leased to public and private telecom operators for general telecommunications purposes.

Armenian participation in both projects is already only marginal at best. Thus, Georgia has emerged as the one state in the region serving as the center for the development of the region's infrastructure strategy that looks to the future of the development of the IT and telecommunications sectors. The imperative, therefore, is clear and Armenia once again faces exclusion from one of the most important regional development plans. This danger of exclusion from the region's expanding fiber-optic network is one of the most serious, yet under-recognized threats to the future of Armenian cyber-security.

Conclusion

Defining a country's national security is one of the more basic obligations of a state. The concept of national security is essentially defined by a state's mission to meet possible threats, both internal and external. This state mission is comprised of three main pillars: to protect its territorial integrity and state borders; to provide security for its population; and to preserve stability, in both political and economic terms. The challenge of national security, especially in today's complex environment of multiplying threats, is to ensure that both the *definition* and *defense* of national security is a dynamic, not static, process of constant vigilance and preparation. For Armenia, small in both size and population, national security holds an even greater role in the face of the threats of isolation and blockade. The imperative for cyber-security, therefore, is merely one element of a broader long-term mandate to ensure the viability of Armenia's overall national security. And as this draft Cyber-security Action Plan envisages, this is only the beginning of such a longer-term effort.

A Cyber-Security Action Plan for Armenia

Step One: Seek a negotiated settlement ending the monopolistic structure of the national telecommunication sector and open it to competition after crafting adequate regulatory and national security safeguards;

Step Two: Educate and assist the judiciary to recognize and enforce intellectual property rights; and adopt additional legislative and regulatory measures on "digital signatures," electronic contracts and the admissibility of electronic evidence.

Step Three: Secure state functions of the military, police and government services by adopting and adapting "dual-use" technology; leverage international funding and training; and ensure greater interoperability in times of crisis.

Step Four: Leverage new opportunities for funding and training by international and U.S. cyber-crime programs; forge public-private partnerships and create a Public-Private Cyber-security Forum; and follow-up on its ratification of the Council of Europe Cybercrime Convention.

Step Five: Develop new policies of Internet Governance and Competition Policy; and integrate the country more closely into global- and regional-based fiber-optic network development projects.

References

Andonian, Andre, Avetik Chalabyan and Pierre Gurdjian. "Armenia's Software Advantage." *The McKinsey Quarterly*, Number 1, 2004.

"Armenia: Brief Overview of the Communications Sector," U.S. Embassy Factsheet, Yerevan, Armenia, January 2003.

Arquilla, John and David Ronfeldt. "Cyber War is Coming." *Comparative Strategy*, Vol. 12, 1993.

Bollier, David. "Why the Public Domain Matters. The Endangered Wellspring of Creativity, Commerce and Democracy." The New America Foundation, May 2002.

Center for Strategic and International Studies (CSIS). Cybercrime. Cyberterrorism. Cyberwarfare. Averting an Electronic Waterloo. CSIS Global Organized Crime Project. 1998.

Congressional Research Service (CRS). Cyberwarfare. 19 June 2001.

Congressional Research Service (CRS). Critical Infrastructures: Background, Policy and Implementation. 30 July 2002.

Congressional Research Service (CRS). Information Warfare and Cyberwar: Capabilities and Related Policy Issues. 19 July 2004.

de Borchgrave, Arnaud, Frank Cillufo, Sharon Cardash and Michele Ledgerwood. "Cyber Threats and Information Security. Meeting the 21st Century Challenge," Report of the CSIS Homeland Defense Project, Center for Strategic and International Studies (CSIS), May 2001.

DeRosa, Mary. "Data Mining and Data Analysis for Counterterrorism." Center for Strategic and International Studies (CSIS), March 2004.

"Information Operations," *Perspectives*. Canadian Security Intelligence Service. Report 2001/11, 6 May 2002.

"ISA Armenia: Market of Personal Computers in Armenia," U.S. Embassy Factsheet, Yerevan, Armenia, August 2003.

Khazhakian, Gourgen. "Armenia and the Global Information Society," *Noyan Tapan Highlights*, 21 June 2004.

Lewis, James, Ed. "Cyber Security. Turning National Solutions into International Cooperation," Center for Strategic and International Studies (CSIS), 2003.

Lurie, Peter and Chris Sprigman. "Broadband Marxism," *Foreign Policy*, March/April 2004.

Marshall Center for Security Studies. The Cyber-Dimension of Emerging National Security Threats. Conference Report, 2-5 December 2002.

National Research Council. Science and Technology in Armenia. Toward a Knowledge-Based Economy. 2004.

Samuelian, Thomas J. "E-Governance in Lawmaking and Judicial Decision Making. Some Practical Steps toward the Rule of Law and Due Process in Armenia," *Armenian Forum*, No. 4, 2003.

Shimeall, Timothy. "Countering cyber war," *NATO Review*. Winter 2001/2002.

Solomon, Anne, Ed. "Technology Futures and Global Power, Wealth and Conflict," Center for Strategic and International Studies (CSIS), May 2005.

Strobel, Warren. "A glimpse of cyberwarfare," *U.S. News and World Report*, 13 March 2000.

United Nations Working Group on Internet Governance. Background Report. June 2005.

Wallsten, Scott. "Regulation and Internet Use in Developing Countries," AEI-Brookings Joint Center for Regulatory Studies. May 2003.

Zakarian, Armen and Emil Danielyan, "Armenia's Main Cellphone Network Paralyzed," *Radio Liberty Armenia Report*, 18 July 2005.

Հայաստանում տեղեկատվա-համակարգչային տեխնոլոգիաների մակարդակն ու զարգացումը

Կովկասյան տարածաշրջանի երկրների, ինչպես նաեւ հետսովետական ողջ տարածքի (բացառությամբ մերձբալթյան երկրների) համար այսօր բնորոշ են ընդհանուր տենդենցներ, ինչպիսիք են՝ գիտական հետազոտությունների բյուջետային ֆինանսավորման նվազեցում, պետական համակրթական ծրագրերի կրճատում կամ սեղմում եւ յուրաքանչյուր երկրի ներսում տեղեկատվական անհավասարության մեծացում: Դա չի կարող չազդել մասնագետների նախապատրաստման եւ կրթության ոլորտում արդի տեխնոլոգիաների օգտագործման վրա:

1984թ. էլեկտրակապի միջազգային միության (ԷՄՄ) կողմից հրատարակվեց «Պակասող օղակ» («Недостающее звено») զեկույցը, որտեղ նշվում էր, որ էլեկտրակապի ինֆրակառույցի բացակայությունը զարգացող երկրներում, որոնց թվին այսօր նաեւ դասվում են Կովկասյան նոր պետությունները՝ Ադրբեջանը, Հայաստանը եւ Վրաստանը, խոչընդոտում է դրանց տնտեսական աճին: Այդ ժամանակահատվածի համար զեկույցը նվիրված էր միայն հեռախոսակապի հասանելիության հիմնախնդիրներին: Քսան տարի անց աշխարհում «պակասող օղակ» կարելի է անվանել թվային տեխնոլոգիաների ճեղքումը[1]:

90-ական թվականներին Կովկասյան տարածաշրջանում նոր պետությունների կայացումը տեղի ունեցավ ամբողջ հետսովետական տարածքին բնորոշ ընդհանուր տնտեսական անկման ֆոնի վրա: Այսօր էլ տվյալ տարածաշրջանի պետությունները չեն ապահովում իրենց տնտեսական վերելքի համար անհրաժեշտ միջոցներով, իսկ տեխնիկական սպասարկման ծախսերը բոլոր երկրներում չեն համապատասխանում իրական պահանջներին: Աճում է արտադրական բազայի մաշվածությունը, որն ուղեկցվում է փոխարինմանն ու արդիականացմանն ուղղված անբավարար ներդրումներով: Դա չէր կարող չազդել տեղեկատվա-համակարգչային տեխնոլոգիաների (ՏՀՏ) կայացման եւ զարգացման վրա, հատկապես այն հատվածում, որը կապված է կրթության եւ դրա համար անհրաժեշտ տեխնիկական ու մեթոդական հիմքի ստեղծման հետ:

XXI դարի սահմանագծին կովկասյան տարածաշրջանի երկրները հանգեցին տարբեր արդյունքների: 2002թ. աշխարհի առաջին 60 երկրների ցանկում ըստ Ինտերնետի օգտագործման թվի ցուցանիշի մտել էին Ադրբեջանն ու Վրաստանը, իսկ Հայաստանը չէր ընդգրկվել: Միեւնույն ժամանակ, յուրաքանչյուր երկրում կա որակավորված մասնագետների մի մեծ ջոկատ, իսկ Ինտերնետից օգտվելը դառնում է սովորական երեւույթ:

[1] Հաշվետվություն համաշխարհային էլեկտրակապի վերաբերյալ: ԷՄՄ: 2002

Այսօր կովկասյան տարածաշրջանի երկրների համար պրոբլեմային հարցեր են մնում հեռահաղորդակցության ոլորտում ներդրումների որոնումը եւ այդ ոլորտի ծառայությունների վճարունակ պահանջարկը: Այնուամենայնիվ, տարածաշրջանում տեղեկատվական տեխնոլոգիաների (ՏՏ) հեռանկարները հսկայական են՝ ստեղծվում եւ զարգանում են ՏՏ-ընկերություններ, բնակչության եւ պետական սեկտորում աճում է համակարգիչների քանակությունը: Տարածաշրջանում ընկերությունների ու մասնավոր անձանց էլ ավելի մեծ քանակություն է միանում Ինտերնետին եւ օգտագործում ՏՏ իրենց գործունեության մեջ:

Տարածաշրջանում առավել բարենպաստ վիճակում է հայտնվել Ադրբեջանը: Այդ երկրի նաֆթային եւ աշխարհագրական-քաղաքական ներուժը անհամադրելի է մերձավոր հարեւանների հնարավորությունների հետ: Այդ իսկ պատճառով, չնայած ներկայիս առկա բարդությունների, այդ երկրում ՏՏ-սեկտորը զարգանում է բավականին արագ եւ պահանջված է դառնում բիզնեսի, խոշոր ներդրողների ու գիտական ինստիտուտների կողմից:

XX դարի վերջում Հայաստանի կառավարությունն իր ուշադրությունը բեւեռեց տեղեկատվական տեխնոլոգիաների վրա: Իսկ 2003թ. երկրի վերստին ընտրված նախագահ Ռոբերտ Քոչարյանը հռչակեց մի պատվախնդրային նպատակ՝ Հայաստանը պետք է դառնա ինտելկտուալ ծառայությունների եւ տեղեկատվական տեխնոլոգիաների տարածաշրջանային առաջատարը:

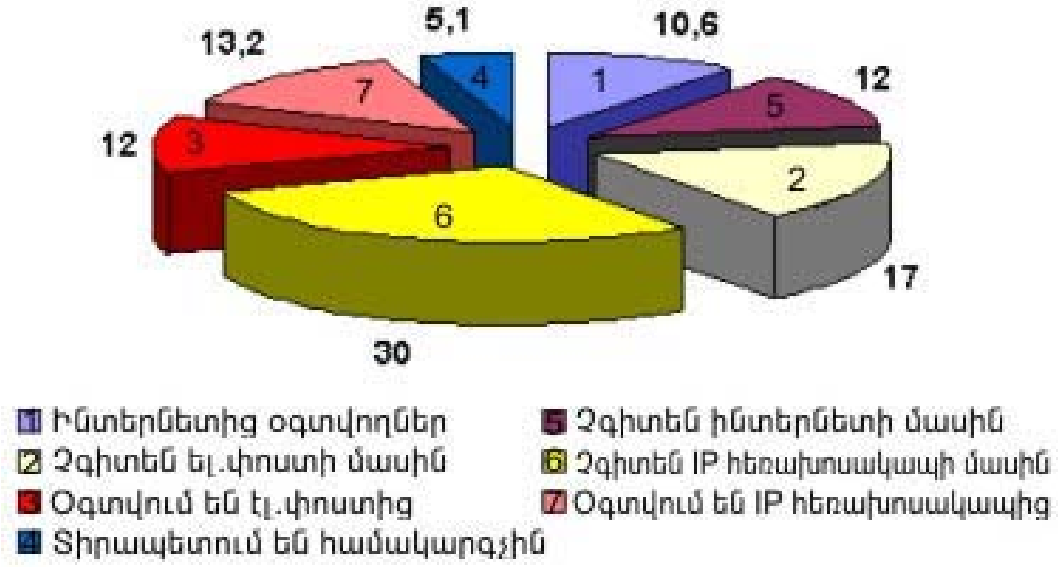
Դժվար խնդիր է, եթե հիշենք, որ այսօր Հայաստանի Հանրապետությունում բնակվում է 3,8 միլիոն մարդ, միջին աշխատավարձը կազմում է 270 ԱՄՆ դոլար, իսկ բնակչության մոտ 45% ապրում է աղքատության սահմանագծից ցածր[2]:

Մինչեւ 1997թ. Հայաստանում դեռ պահպանվում էին էլեկտրաէներգիայի հետ կապված խնդիրներ, եւ միայն Մեծամորի ԱԷԿ[3] մեկնարկումից հետո երկրի ցանցային տեխնոլոգիաները սկսեցին արագ զարգանալ: 2001թ. սկզբին Հայաստանում արդեն գործում էին մեկ առաջին եւ ութ երկրորդ մակարդակի ISP-ներ (Ինտերնետ ծառայության պրովայդեր): 2003թ. կեսերին Ինտերնետից

[2] 2008թ. դրությամբ Հայաստանի ազգաբնակչությունը կազմում էր 3,8 մլն. մարդ: Նրանցից 1,254 մլն. բնակվում էին Երեւան քաղաքում:

[3] ԱԷԿ սուղ էներգետիկ ճգնաժամի պատճառով 1989թ. մարտին կանգնեցվել էր եւ վերստին գործարկվել 1995թ. նոյեմբերին: ԱԷԿ երկրորդ բլոկը, որը համալրված էր սովետական ВВЭР-440 առաջին սերնդի ռեակտորով, արտարդրում է հանրապետությունում արտադրվող էլեկտրաէներգիայի 30-40%: 2003թ. ստորագրվեց պայմանագիր, ըստ որի ԱԷԿ-ն 5 տարի ժամկետով փոխանցվել է «Ռուսաստանի Միասնական էներգետիկ Համակարգեր» Ռուսաստանի Բաժնետիրական Ընկերակցության հավատարմական կառավարմանը: 2008թ. դեկտեմբերի 4-ին ստորագրվեց Հայկական ԱԷԿ-ի հավատարմական կառավարման նոր պայմանագիր՝ եւս 5 տարի ժամկետով:

օգտվողների քանակն արդեն կազմում էր մոտ 50 հազար: Այնուամենայնիվ, ելնելով տարբեր պատճառներից, որի թվին է պատկանում նաեւ առաջին մակարդակի ISP «ԱրմենՏել» ընկերության բարձր սակագները, Ինտերնետի հասանելիությունն երկրում չի կարելի անվանել էժան եւ հասանելի բոլորի համար:



Նկ. 1. Հայաստանում տեղեկատվա-համակարգչային զարգացման մակարդակը

Ըստ ԱՄՆ Միջազգային զարգացման գործակալության փորձագետների գնահատման, Ինտերնետի գների, կապի որակի ու արագության հարաբերակցությունը թույլ է տալիս ասել, որ ISP ծառայությունները Հայաստանում շատ ավելի թանկ են, քան հարեւան երկրներում ու անհամեմատ թանկ են, քան ԱՄՆ-ում: Բարձր արագությամբ Ինտերնետը նույնիսկ Հայաստանի մայրաքաղաքում ունի աննշան զարգացում եւ բավականին թանկ է: Հիմնականում դա կախված է այն բանից, որ «ԱրմենՏել» (Beeline[4] ապրանքանիշ) 1997թ-ից օժտված էր կապի միջազգային ուղիների բացառիկ իրավունքով: Կապի օպերատորի մենաշնորհային դիրքը բացասաբար է անդրադարձել երկրում հեռահաղորդակցման սեկտորի զարգացման վրա, եւ Հայաստանը հետ է մնում բջջային կապի ծառայությունների մատուցման մակարդակով՝ ի համեմատ տարածաշրջանում մյուս երկրների:

Թեեւ 2003թ-ին Հայաստանը դարձավ ՀԱԿ (համաշխարհային առեւտրային կազմակերպություն) անդամ, այնուամենայնիվ հեռավոր կապի շուկան մինչ

[4] «ԱրմենՏել» (Armenian Telecommunications Company, սկսած 2008թ. գործում է «ԲիԼայն» ապրանքանիշի ներքո) գործում է ՀՀ կապի եւ տրանսպորտի նախարարության թիվ 60 արտոնագրի համաձայն, ըստ որի սահմանվել է միջազգային հաղորդակցությունների մենաշնորհային իր իրավունքը եւ դրանք տեղական «պատշաճ կերպով գրանցված եւ ՀՀ օրենքներին համապատասխան գործող իրավաբանական անձանց» տրամադրելու իրավունքը՝ ինտերնետ-ծառայություններ իրականացնելու համար:

օրս չի լիբերալիզացրել: 1997թ. սեփականաշնորհման արդյունքում «ԱրմենՏել» հայկական մենաշնորհային ընկերությունը բացառիկ իրավունքներ ստացավ թե տեղական, եւ թե հեռավոր կապի համար՝ մինչեւ 2013թ.՝ 15 տարի ժամկետով: Չնայած այն խոստումների, որ մալուխային եւ բջջային ցանցերի, ինչպես նաեւ մալուխային հեռուստատեսության ինֆրակառույցի որակը կբարելավվի, Հայաստանում հեռախոսակապի որակը դեռեւս շատ ցածր է բավականին բարձր գների պայմաններում: Միակ բանը, ինչին կարողացավ հասնել Հայաստանի տրանսպորտի եւ կապի նախարարությունը՝ դա «ԱրմենՏել»-ի արտոնագրի պայմանների փոփոխումն էր՝ սահմանափակելով ընկերության ֆիքսված կապի ծառայությունների մասով մենաշնորհային կարգավիճակը մինչեւ 2009թ.:

Հենց ՀԱԿ-ի պահանջով 2003թ-ին ստեղծվեց Հասարակական ծառայությունների կարգավորման անկախ պետական հանձնաժողով (այսուհետ՝ Հանձնաժողով): Այդ մարմինը այսօր նույնպես կոչված է կարգավորելու բնական մենաշնորհների գործունեության հետ կապված վիճելի հարցերը եւ ստեղծելու նախադրյալներ հետգհետե նորմալ մրցակցության անցնելու համար:

Հանձնաժողովի գործունեությունը ոչ մի կերպ անարդյունավետ չենք կարող անվանել: Վերջերս Հանձնաժողովն ընդունեց որոշում «ԱրմենՏել» ՓԲԸ արտոնագրում փոփոխություններ մտցնելու վերաբերյալ (փաստաթուղթ №60), որի արդյունքում ընկերությունը զրկվեց դեպի Ինտերնետ միջազգային ելքի տրամադրման բացառիկ իրավունքից: Մասնավորապես, ընկերությունը զրկվեց ինտերնետ-տվյալների եւ ձայնային հաղորդագրությունների փոխանցման մասով միջազգային ծառայությունների տրամադրման մենաշնորհային դիրքից: Տվյալ որոշումը թելադրված էր ռուսաստանյան «ՎիմպելԿոմ»՝ ներկայիս «ԱրմենՏել»-ի սեփականատիրոջ դիմումով այն բոլոր տեսակի մենաշնորհներից հրաժարվելու մասին, որոնք նախկինում պատկանում էին «ԱրմենՏել» ընկերությանը: Այսուհետ Հայաստանի պրովայդերներն իրավասու են ինքնուրույն ապահովել Ինտերնետի միջազգային մուտք արբանյակային կապի կամ որեւէ մեկ այլ ընկերությունից վարձակալված կապի միջոցի օգնությամբ:

Տվյալ պահին Հայաստանում գոյություն ունեն Ինտերնետի միջազգային մուտքի 2 վերգետնյա «մայրուղիներ»՝ դա «ԱրմենՏել»-ի ու «Fibernet»-ի օպտիկամանրաթելային մալուխներն են, որոնք անցնում են Վրաստանի տարածքով ու Սեւ Ծովի հատակով եւ արբանյակային կապի մի քանի «պաշարային» ուղիներ, որոնք օգտագործվում են հիմնականում «վթարային» նպատակներով: Սկսած 2005թ. գոյություն ունի նաեւ իրանական «մայրուղի», որն անցնում է Մեղրիի տարածքով, սակայն մինչ օրս այդ մալուխը հնարավոր չէ օգտագործել լայնաշերտ Ինտերնետի

միացման համար: Նույնիսկ վթարների ժամանակ իրանական ուղին չի հաջողվում գործածել, եւ դեռեւս այն համարվում է «մեռյալ»:

Այնուհանդերձ, գոյություն ունի ահաբեկչական ոտնձգությունների եւ Հայաստանի արտաքին ինտերնետ-մայրուղիների վնասման մեծ ռիսկ, ինչպես նաեւ կա բազում այլ խնդիրների վտանգ, որոնք կարող են հանգեցնել երկրում «Համաշխարհային սարդոստայնի» անգործությանը:

Հայաստանի կիբեռ-անվտանգությունը

Ադրբեջանական կողմն արդեն չորս տարի է, ինչ ակտիվ պատերազմ է վարում Ինտերնետի հայկական սեգմենտի դեմ: Պարբերաբար ադրբեջանցիներին միանում են նաեւ թուրք խակերները: Այսպես, 2007թ. փետրվարին ինտերնետ-գրոհի արդյունքում «ջարդվել» են օմբուդսմենի, Ազգային վիճակագրական ծառայության, «Դե Ֆակտո» գործակալության կայքերը: Կայքերի տերերին ուղարկված նախազգուշացումները ցույց տվեցին, որ կատարվածից հետո անգամ մի քանի ժամ անց այնտեղ «ներթափանցման» փաստ չի նկատվել: Անցած տարի ադրբեջանցիներն օգտվեցին հայկական «Web» անվամբ պրովայդերի զգոնության բացակայությունից եւ վերահսկողության տակ վերցրեցին Հայաստանյան տասնյակ կայքեր, ներառյալ «Մեդիամաքս» գործակալության ինտերնետ-նախագծերը, որոնք տեղադրված էին ընկերության սերվերի վրա: Մի քանի շաբաթ շարունակ ընկերությունը չէր շտկում իր անփութությունը՝ ամբողջ մեղքը գցելով կայքերի տերերի վրա: Փաստորեն պարզվեց, որ անվտանգության համար պատասխանատու պետական կառույցները ոչ մի կերպ չմիջամտեցին իրադրությանը, եւ միայն մշտական բողոքները վերջ ի վերջո ստիպեցին ընկերությանը երկար ժամանակ անց շտկել սերվերների անվտանգության համակարգում առկա խնդիրները: Առայժմ ադրբեջանցիները բավարարվում են կայքերի «ջարդմամբ» կամ հակահայկական տեղեկատվությունների տեղադրմամբ: Սակայն, եթե հաշվի առնենք, որ այդքան նշանակալից կայքերի տերերը չեն նկատում ներխուժման փաստերը, ապա դա կարող է թույլ տալ ադրբեջանցիներին իրենց համար հարմար պահին տարածելու նախապես պատրաստված ապատեղեկատվությունն անմիջապես հայկական կայքերի միջոցով:

Հայկական կայքերի վրա նմանատիպ զանգվածային գրոհների դեպքեր տեղի են ունենում տարին մեկ անգամ: Ընդ որում, գրոհները դառնում են էլ ավելի արհեստավարժ, ադրբեջանական կողմից ավելի շատ են ներգրավվում մարդկային եւ, բնականաբար, ֆինանսական պաշարներ, իսկ գրոհների օբյեկտ են դառնում առավել նշանակալից հայկական կայքերը: Համապատասխանաբար հրատապ խնդիր է դառնում Հայաստանի ոչ միայն պետական, այլեւ ընդհանրապես կարեւոր նշանակություն ունեցող կայքերի եւ սերվերների պաշտպանությունը: Ստեղծվում է տպավորություն՝ մասամբ ամրագրված փաստերով, որ Ադրբեջանի հատուկ ծառայությունները

վերահսկում են մի շարք խակերային խմբեր, իսկ հայկական կայքերի գրոհներն իրականացվում են թույլ կողմերն ի հայտ բերելու, այլ ոչ միայն պարզապես վնասարարության համար: Այսպիսով, Բաքվում, ամենայն հավանականությամբ, հիմքեր են ստեղծվում, որպեսզի պետք եղած ժամանակ փորձեն լիարժեքորեն քանդել Ինտերնետի հայկական սեգմենտը: Նման վտանգին դիմակայելու, ինչպես նաեւ հզոր հակագրոհների հնարավորության համար Հայաստանը պետք է համալրված լինի անհրաժեշտ պատրաստված կադրերով, ինչպես նաեւ գործողությունների մշակված ռազմավարությամբ:

Ներքին ցանցերի անվտանգությունը

2007թ. դեկտեմբերին Հայաստանի Արտաքին գործերի նախարարության ներքին ցանց ներխուժումը դարձավ հայկական կողմի անփութության եւ ադրբեջանցիների պլանաչափ գործողությունների տրամաբանական շարունակությունը: Անգամ մամուլում բաց հաղորդագրություններից կարելի էր հետեւություններ անել այն մասին, որ Ադրբեջանում հատուկ ծառայությունները վերահսկում են մի շարք խակերային խմբեր, որոնք օգտագործվում են Հայաստանի դեմ գրոհների համար:

Ոչ պակաս լուրջ վիճակում է էլեկտրոնային նամակագրության պաշտպանության խնդիրը: Ըստ էության, այդ հարցը մեր երկրում դեռեւս չի արժանանում պատշաճ ուշադրության: Այսպես, Հայաստանի պաշտպանության նախարարության մամլո-քարտուղարն արդեն երկար տարիներ ի վեր մամլո-հաղորդագրությունների ուղարկման համար օգտագործում է mail.ru ռուսական անվճար սերվերի էլեկտրոնային փոստը, որի «ջարդումն» անգամ բացահայտ կերպով գովազդվում է Ինտերնետում եւ արժե մոտ 50 ԱՄՆ դոլար: Չկա որեւէ երախշիք, որ տվյալ պահին նույնպես այդ փոստարկղը չի գտնվում ադրբեջանցիների գաղտնի հսկողության ներքո եւ հարմար պահին չի օգտագործվի իրենց նպատակների համար:

Լրիվ ակնհայտ է, թե ինչպիսի լուրջ վնաս կարող է հասցվել բարձրաստիճան պաշտոնյաների էլ.փոստ ներխուժելու եւ էլեկտրոնային նամակագրությունը ջարդելու դեպքում: Ընդհանուր առմամբ պետք է գոյություն ունենա պետական ներքին ցանցերի, փաստաթղթերի էլեկտրոնային շրջանառության պաշտպանության միասնական ռազմավարություն: Հատկապես, եթե հաշվի առնենք այն, որ երկրում էլ ավելի շատ են ներդրվում էլեկտրոնային կառավարման համակարգեր, ապա դեպի այդ համակարգեր չթույլատրված մուտքի վտանգն ավելի է ուժեղանում: Ոչ պակաս կարեւորություն է իրենից ներկայացնում ռազմավարական նշանակության ոչ պետական առեւտրային ցանցերի, օրինակ՝ էներգահամակարգերի, պաշտպանությունը, որոնց խոցելիությունը կարող է հանգեցնել աղետալի հետեւանքների:

Քարոզչություն

Փաստորեն, ադրբեջանական եւ թուրքական քարոզչության դեմ հայկական կողմի կողմից որեւէ քայլեր չեն ձեռնարկվում: Այս առումով հիմնական գործողությունները ձեռնարկվում են Հայաստանի եւ սփյուռքի հայ անհատների կողմից, որոնք գործում են ելնելով անձնական հայրենասիրությունից ու խանդավառությունից: Օրինակ, ադրբեջանական ԶԼՄ-ների ապատեղեկատվության դեմ ուղղված գործողություններն այն մասով, որ Լվովի հայերը պահանջում են վերանվանել քաղաքը «Առյուծ»-ի, ձեռնարկվել էին բացառապես հայկական կողմի ինտերնետ-ընկերակցության կողմից, որին հաջողվեց ստիպել ուկրաինական ԶԼՄ-ների մեծամասնությանը հանել այդ նյութը ինտերնետ-կայքերից: Մինչդեռ Ադրբեջանում եւ Թուրքիայում այդպիսի հարցերով լայնամասշտաբ կերպով զբաղվում են պետական կառուցվածքները: Ընդ որում, հայկական կողմի մասնագետների մի փոքր անձնակազմը կարող էր կատարել ադրբեջանական քարոզների եւ ապատեղեկատվության մոնիտորինգ՝ անցկացնելով պատասխան միջոցառումներ: Հաշվի առնելով մասնավոր մակարդակով տեղեկատվական պատերազմում ներգրավված հայերի մեծ քանակությունը, նման կառուցվածքը կարող էր իրենց ներգրավելու եղանակով արդյունավետ կերպով եւ նվազագույն վնասներով հասնել այդ բնագավառում հաջողությունների:

Հայկական մամուլում անընդհատ գովազդվում են ադրբեջանական եւ թուրքական ԶԼՄ-ները, մասնավորապես Ինտերնետում ներկայացվածները: Ընդհանուր առմամբ կարելի է ասել, որ ըստ վիճակագրական տվյալների, հայկական հեռուստատեսությունը եւ թերթերը ավելի շատ գովազդում են ադրբեջանական ցանցային ռեսուրսները, քան հայրենականները: Ավելին, հայկական ԶԼՄ-ներն առանց ստուգման վերատպում են ադրբեջանական եւ թուրքական ապատեղեկատվությունները՝ դրանով իսկ ավելացնելով տպաքանակը հայ լսարանի շրջանում: Էլ չենք ասում այն մասին, որ հաճախ ադրբեջանական նորությունները պարզապես կրկնօրինակվում են՝ պահպանելով այնպիսի արտահայտություններ, ինչպիսիք են «ղարաբաղյան սեպարատիստներ», «հայկական ֆաշիստներ», չակերտավոր օգտագործվում են «ցեղասպանություն», «ԼՂՀ» եւ այլ բառեր:

Բացի այդ, չկա անգամ պետական խորհրդանիշների հետ աշխատանքի ընդհանուր մոտեցում: Հայկական ԶԼՄ-ներում անընդհատ պրոպագանդվում են Ադրբեջանի եւ Թուրքիայի պետական խորհրդանիշները ամենաձեռնտու լույսի տակ: Միեւնույն ժամանակ, հայկական մամուլում անգամ չկա մեկ միասնական մոտեցում ԼՂՀ քարտեզի պատկերի նկատմամբ: Հաճախ հայ հանդիսատեսը էկրանին տեսնում է նախկին ԼՂԻՄ, որը որեւէ կապ չունի Հայաստանի հետ: Այն, որ երկրում ուշադրություն չեն դարձնում այդպիսի «մանրուքների» վրա, խոսում է ինչպես ներքին, այնպես էլ արտաքին

պրոպագանդայի նկատմամբ պետական մոտեցման կարեւորության ըմբռնման պակասի մասին:

Ներքին շուկայում, իր հերթին, լրիվ բացակայում է պետական մոտեցումը. տեղական ԶԼՄ-ները գործնականում չեն լուսաբանում կյանքը Լեռնային Ղարաբաղում, Հայաստանի մարզերում, թեեւ խնդրի կարեւորության ընկալմամբ ցանկացած հրատարակություն պետք է ունենար իր մամլո կետերն ինչպես Ստեփանակերտում, այնպես էլ տարածաշրջանային կենտրոններում: Փաստորեն, Ինտերնետում գոյություն ունի լոկ մեկ ղարաբաղյան գործակալություն՝ Karabakh-Open.com, որն օպերատիվ կարգով տեղեկացնում է ԼՂՀ-ում տեղի ունեցող իրադարձությունների մասին: Ընդ որում հայկական մյուս ԶԼՄ-ները գործնականում ուշադրություն չեն դարձնում այդ ռեսուրսի վրա՝ շարունակելով տեղեկատվություն քաղել ադրբեջանական աղբյուրներից:

Ստեղծվել է պարադոքսալ իրավիճակ, երբ հայերի մեծամասնության համար Ինտերնետում տեղեկատվության հիմնական աղբյուր է հանդիսանում ադրբեջանական տեղեկատվական Day.az պորտալը, որն ըստ այցելության եւ մեկնաբանման ցուցանիշների գերազանցում է բոլոր նմանատիպ հայկական ռեսուրսները՝ բոլորը միասին վերցված: Հարկ է նշել, որ «արտակարգ իրավիճակի» ժամանակահատվածում Day.az-ն առանձնահատուկ համբավ ունեցավ հայերի շրջանում, քանի որ հմտորեն օգտվում էր Հայաստանյան բոլոր՝ ինչպես պաշտոնական, այնպես էլ ընդդիմադիր աղբյուրների նորություններից, ինչը չկարողացավ իրականացնել ոչ մի հայկական հրատարակություն:

Վերջաբան

Պահպանելով ներկայիս տենդենցները՝ Հայաստանը մոտ ժամանակներում լրիվ կկորցնի իր նախաձեռնությունը Ադրբեջանի եւ Թուրքիայի դեմ տեղեկատվական պատերազմում: Կենսականորեն անհրաժեշտ է դառնում միջգերատեսչական մարմնի ստեղծումը, որը կհամակարգի ԱԱԾ (Ազգային անվտանգության ծառայության), ԱԳՆ, ՊՆ եւ այլ գերատեսչությունների տեղեկատվական գործունեությունը՝ հակամարտության եւ, ինչը շատ կարեւոր է, այդ ուղղությամբ նախաձեռնվող գործողությունների համար:

Աշոտ Թուրաջյան
ՌԱՀՀԿ տեղեկատվական տեխնոլոգիաների մասնագետ

Информационная безопасность общественно-политических систем

Информационная безопасность является основой жизнедеятельности любой общественно-политической системы. В частном случае, жизнедеятельность государства можно отнести к общественно-политической системе. Если любая система имеет внутреннее самоуправление, то такая система называется самоорганизующейся.

Системы, жизнедеятельность которых подчинена определенной, наперед заданной программе существования с учетом воздействий на них внешних сил или факторов, изменяющихся во времени, можно назвать самоорганизующимися. Это относится как к техническим, так и к биологическим и общественно-политическим системам.

Впервые объединить и обобщить науку управления технических и биологических видов самоорганизующихся систем предложил Норберт Винер и назвал свою теорию кибернетикой[1]. Необходимо отметить, что само слово “кибернетика” встречается уже у Платона, который под этим словом понимает науку об управлении кораблем. В 1834 г. французский физик Ампер назвал кибернетику наукой об управлении государством. Заслуга Винера заключалась в том, что он вывел общие принципы и механизмы управления техническими и биологическими системами. Винер предложил рассматривать самоорганизующуюся систему как **Объект управления** с воздействующими на него внешними связями (силами или факторами). При этом сам объект управления он назвал «черным ящиком», этим дав понять, что в общем случае нас не интересует, что происходит внутри этого черного ящика. Нас только интересуют внешние воздействия или связи на объект и контролируемые нами выходные величины. Эти связи подразделялись на три группы – контролируемые внешние воздействия, неконтролируемые внешние воздействия и управляющие внешние воздействия. На выходе из объекта мы получаем контролируемую величину или величины, которые заранее определены человеком для его безопасной жизнедеятельности. Изучение и анализ общественно-политических систем приводит к выводу, что эти системы также являются самоорганизующимися системами. Поэтому принципы управления и безопасности подобных систем те же. Само собой разумеется, что выходные параметры самоорганизующихся систем определяются человеком только в случае технических или общественно-политических систем. В случае биологических систем эти параметры поддерживаются независимо от воли человека и программа их жизнедеятельности предопределена Творцом. Например, нормальная температура тела человека равна 36,6±0,3°С и она поддерживается организмом независимо от воли самого человека и независимо

[1] Норберт Винер. Кибернетика. М, 1980.

от времени года – зимой, когда холодно, или летом, когда температура окружающей среды может быть даже выше, чем температура тела человека.

Для того чтобы осознанно воздействовать на объект управления для поддержания его в заранее определенных параметрах, которые обеспечивали бы его безопасность и устойчивость, необходимо **Устройство управления**. Устройство управления принимает информацию о состоянии объекта управления (или черного ящика), сравнивает эту информацию с имеющейся у него заданной программой или параметрами (это находится в задающем устройстве ЗУ) и затем принимает решение о воздействии на объект с целью корректировки его состояния. Задающими устройствами в государстве могут быть Конституция и Конституционный суд, парламент, который принимает законы, регламентирующие в каких общественно-политических границах может существовать государство, его, правительство и президент. Например, если парламент принимает, а президент утверждает бюджет государства на следующий год, то он уже является Законом и никакая структура не имеет права его нарушить, ибо за его исполнением четко следит Центральный банк.

В частном случае, если объект управления находится в заданных пределах заранее установленных параметров, то никаких воздействий на объект управления со стороны устройства управления не поступает. Управляющие воздействия осуществляются с помощью **исполнительного органа**.

В простейшем случае для наглядности представления о работе самоорганизующихся систем, можно представить схему работы такой системы.

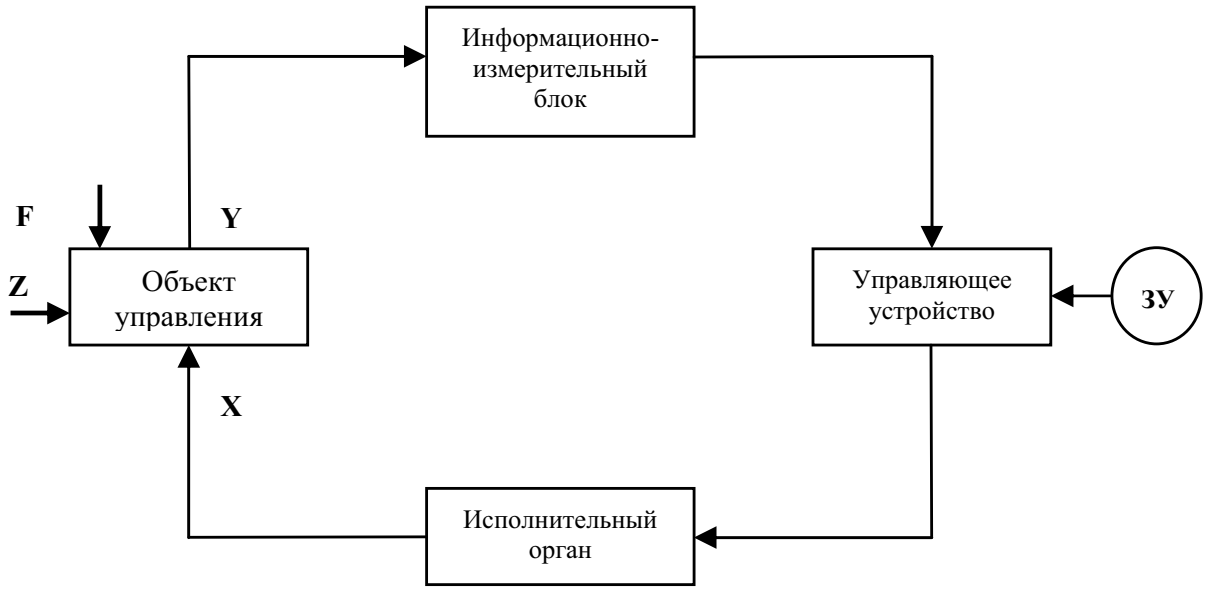


Рис.1. Обобщенная схема работы самоорганизующейся системы.

Из этой схемы видно, что на объект управления могут действовать силы Z – контролируемые внешние воздействия, F – неконтролируемые внешние

воздействия и X – управляющие воздействия со стороны управляющего устройства через исполнительный орган, а Y – выходная величина, которую можно охарактеризовать как продукт жизнедеятельности системы. Здесь линии со стрелками схематически обозначают каналы, по которым осуществляется связь между ними. Для того чтобы система работала как самоорганизующаяся, необходимо наличие обратной связи, которая бы замыкала цикл. Под обратной связью мы понимаем связь, которая ставит в зависимость причины от следствия. При управлении по замкнутому циклу управляющее воздействие ставится в зависимость от величины отклонения регулируемой величины. Из рис.1 видно, что схема управления самоорганизующейся системы представляет собой замкнутую цепочку: объект управления - информационно-измерительный блок - управляющее устройство - исполнительный орган - объект управления. В этой замкнутой цепи блоки: управляющее устройство - исполнительный орган - объект управления – представляют собой обратную связь. Если мы хотим, чтобы система работала безопасно для себя и для окружающих ее систем, мы должны определить совокупность верхних и нижних выходных параметров, в которых жизнедеятельность этой самоорганизующейся системы будет устойчивой и находиться в состоянии устойчивого равновесия (под устойчивостью самоорганизующейся системы понимают ее свойство возвращаться к прежнему или новому равновесному состоянию). Другими словами, мы должны определить максимальные и минимальные величины выходных параметров системы Y, выше или ниже которых она может выйти из состояния устойчивого равновесия и саморазрушиться. Это наглядно видно из рис.2. Математически это можно выразить следующим образом: $Y_{min} \leq Y \leq Y_{max}$.

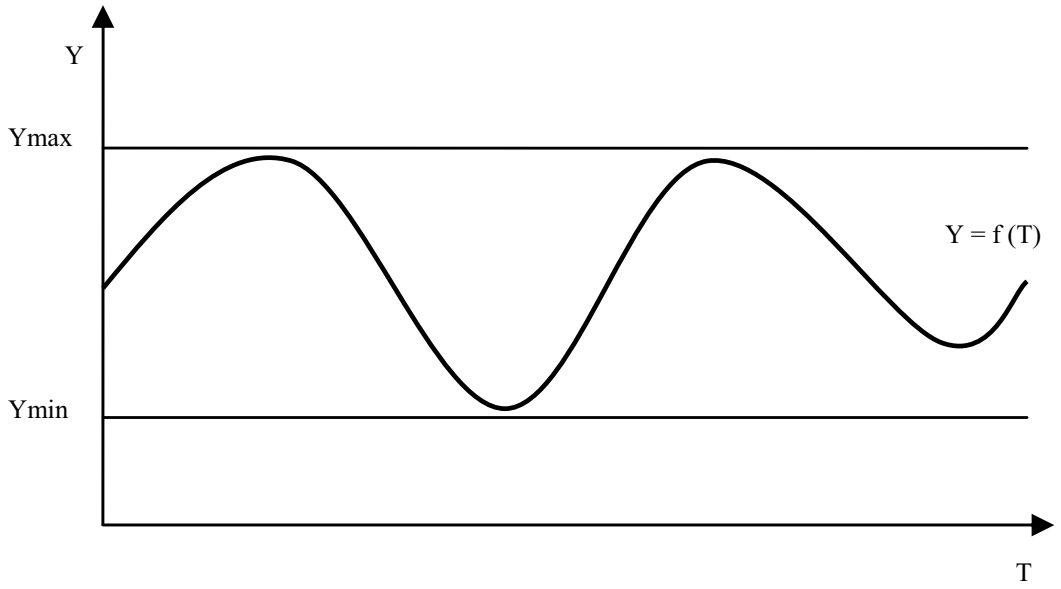


Рис.2. Устойчивая жизнедеятельность самоорганизующихся систем.

Здесь T – время, Y_{max}, Y_{min} – верхний и нижний выходные параметры системы, выше и ниже которых ее жизнедеятельность может быть прекращена, то есть система может разрушиться. Жизнедеятельность самоорганизующихся систем

представляет собой колебательный процесс. Если продукт жизнедеятельности системы (значение выходного параметра) достигает Y_{max}, поступает управляющее воздействие на его уменьшение, а если Y_{min}, то наоборот. При этом если частота колебаний выходных параметров системы находится в заданных пределах, то можно говорить, что система устойчива. Если же частота колебаний выходит за пределы расчетных значений, в сторону ее увеличения, то система неустойчива и способна к саморазрушению. Наиболее сложной и ответственной задачей в разработке самоорганизующихся систем является определение максимальных и минимальных величин выходных параметров системы Y. В данном случае мы рассматриваем простейшую систему с одним параметром. В реальности самоорганизующиеся системы имеют десятки тысяч и более выходных параметров, которые они должны контролировать и управлять и для каждого из этих параметров должны быть четко установлены верхние и нижние интервалы значений, выйдя за которые система может быть разрушена. Особенно это относится к биологическим и общественно-политическим системам. Для того, чтобы любая система работала в вышеуказанном режиме, необходимо, чтобы между ее звеньями существовала не просто обратная связь, а **отрицательная** обратная связь. Понимается это следующим образом. Если значение выходного параметра увеличивается и достигает максимума, то есть верхнего предельного значения (как это видно на рис.2), то обратная связь: управляющее устройство - исполнительный орган - объект управления будет воздействовать на объект управления так, чтобы понизить значение выходного параметра и наоборот. Если значение выходного параметра уменьшается и достигает минимума, то есть нижнего предельного значения, то обратная связь будет воздействовать на объект управления так, чтобы повысить значение выходного параметра. И в том, и в другом случае меняется знак или направление воздействия. В этом случае мы говорим, что в самоорганизующихся системах существует отрицательная обратная связь.

Самым важным органом в самоорганизующихся системах является **информационно-измерительный блок** или, проще говоря, **информационная подсистема**. Она должна обладать объективностью, помехозащищенностью и высокой скоростью передачи информации. Если хотя бы один из этих принципов будет нарушен, управляющее устройство будет принимать неадекватные решения по воздействию на объект управления, в результате чего самоорганизующаяся система разрушится.

Помехозащищенностью и высокой скоростью передачи информации должны обладать и каналы связи, по которым передается информация, потому что если информация об объекте объективна, а канал связи не защищен и передача по каналам связи задерживается, последствия будут те же. Методами передачи информации в общественно-политических системах являются печатные издания (газеты, журналы, бюллетени и различные документы печатного или рукописного типа), а также электронные виды информационного пространства –

телефонная, телевизионная, радиотехническая, спутниковая и, самое важное, интернетная связь (всемирная паутина). Об интернетной связи нужно сказать отдельно, ибо современные его возможности поистине неограниченны. На сегодняшний день интернетная связь является самым мощным источником информации, которая получила колоссальное развитие и продолжает совершенствоваться буквально каждый день.

Говоря от телекоммуникационной связи, необходимо отметить, что всемирная паутина или попросту Интернет позволила создать некое киберпространство, с помощью которого не только революционным методом изменилась вся философия информационного пространства и связи, но и представилась возможность всему населению земного шара получить прямой доступ к колоссальным информационным потокам. Более того, на качественно новый уровень вышел поиск необходимой информации. Если буквально каких-нибудь 30 лет назад чтобы получить наиболее полную информацию о каком-либо процессе студенту или научному работнику необходимо было проводить месяцы в специализированных библиотеках, то сейчас ту же информацию можно получить за несколько секунд. На принципе Интернета кардинально изменилась телеграфия, телефонная и видеосвязь. Наряду с качеством связи, понизилась и ее стоимость. Сейчас почти полностью междугородние телефонные разговоры осуществляются через Интернет и при этом обеспечивается видеосвязь с абонентом. Однако доступность интернетной связи, с помощью которой практически вся информация поступает в Армению и выходит из нее, оставляет желать лучшего.

При передаче информации с помощью Интернета очень важна информационная безопасность в самой системе Интернета. Данный вид информационной безопасности в настоящее время стал наиболее актуален по той причине, что практически все компьютеры мира, независимо от того, работают они в государственных учреждениях или находятся дома у пользователя, связаны меж собой через Интернет. Здесь открывается море возможностей для проникновения в секретные базы данных военных ведомств, банков, проведению промышленного шпионажа, взламывания сайтов, насаждения дезинформации и многого другого. С этой целью пишутся всевозможные вирусные компьютерные программы, которые проникают в любой компьютер и могут сидеть там до наступления часа X. В нужный момент они по команде с какого-либо центра начинают работать и разрушать любую операционную систему. Поэтому государства, которые заботятся о своей информационной безопасности, имеют специальные службы программного обеспечения, которые позволяют распознавать и уничтожать новые вирусы или разрабатывать их для проникновения в компьютерные сети вероятного противника.

Понятие информации в кибернетике родственно понятию отражения в диалектике. Свойство отражения присуще не только объектам, но и процессу и

заключается в том, что между состоянием взаимодействующих объектов существует определенная связь. Однако философию прежде всего интересуют качественные различия между типами отражения, а кибернетику – количественные описания. Поэтому имеются ли в виду соответствия между ощущениями и реальностью или положением стрелки вольтметра и напряжением на его клеммах, в подобных ситуациях один объект отражает другой, один объект содержит информацию о другом. Поэтому можно сказать, что **информация** есть отражение одного объекта другим, проявляющееся при наличии соответствия их состояний. Один объект может быть отражен несколькими другими объектами. **Информацию**, фиксированную в определенной форме, можно назвать **сообщением**. Сообщение может иметь самое различное содержание, но независимо от этого, всегда отображается в виде сигнала (электрического, звукового, текстового и др.). Формирование любого сигнала связано с передачей сообщения от отправителя к получателю, которые в общем случае разделены пространством и временем. **Сигнал** можно охарактеризовать как средство передачи информации в пространстве и времени. Анализ ситуаций, в которых участвует сигнал, приводит к выводу, что хотя сигнал связан всегда с материальным объектом, большинство конкретных свойств этого объекта несущественно. Например, при ознакомлении с содержанием печатного текста неважно, каким шрифтом или на какой бумаге он напечатан. Для соответствия между сообщением и сигналом, т.е. возможностью извлечения сообщения из полученного сигнала, последний должен формироваться по определенным правилам. Такое построение сигнала называют **кодированием**. В любых самоорганизующихся системах информация кодирована. Например, в общественно-политических системах кодированием может быть язык общения, его звучание и правописание. Сообщение о том, что, например, «стена белая» можно передать и написать на различных языках, – «պատը սպիտակ է» или «the wall is white». Содержание то же самое, но кодирование (в данном случае, язык общения) – различно.

Особо важно обратить внимание на кодировании информации. Если информация конфиденциальна, то она должна иметь несколько степеней защиты от несанкционированного входа в канал связи и расшифровки оппонентом сообщения или какой-либо базы данных, которые являются основой безопасности любой общественно-политической системы. При этом информация может нести в себе сведения оборонного, экономического, промышленного, экологического, демографического и социального характера. Если же оппоненты будут заранее знать стратегическую информацию, принадлежащую данной общественно-политической системе, то впоследствии довольно легко разработать неконтролируемые внешние воздействия на объект управления и привести его к гибели или разрушению.

Классически считается, что обеспечение безопасности информации складывается из трех составляющих: Конфиденциальности, Целостности и Доступности (рис. 3).

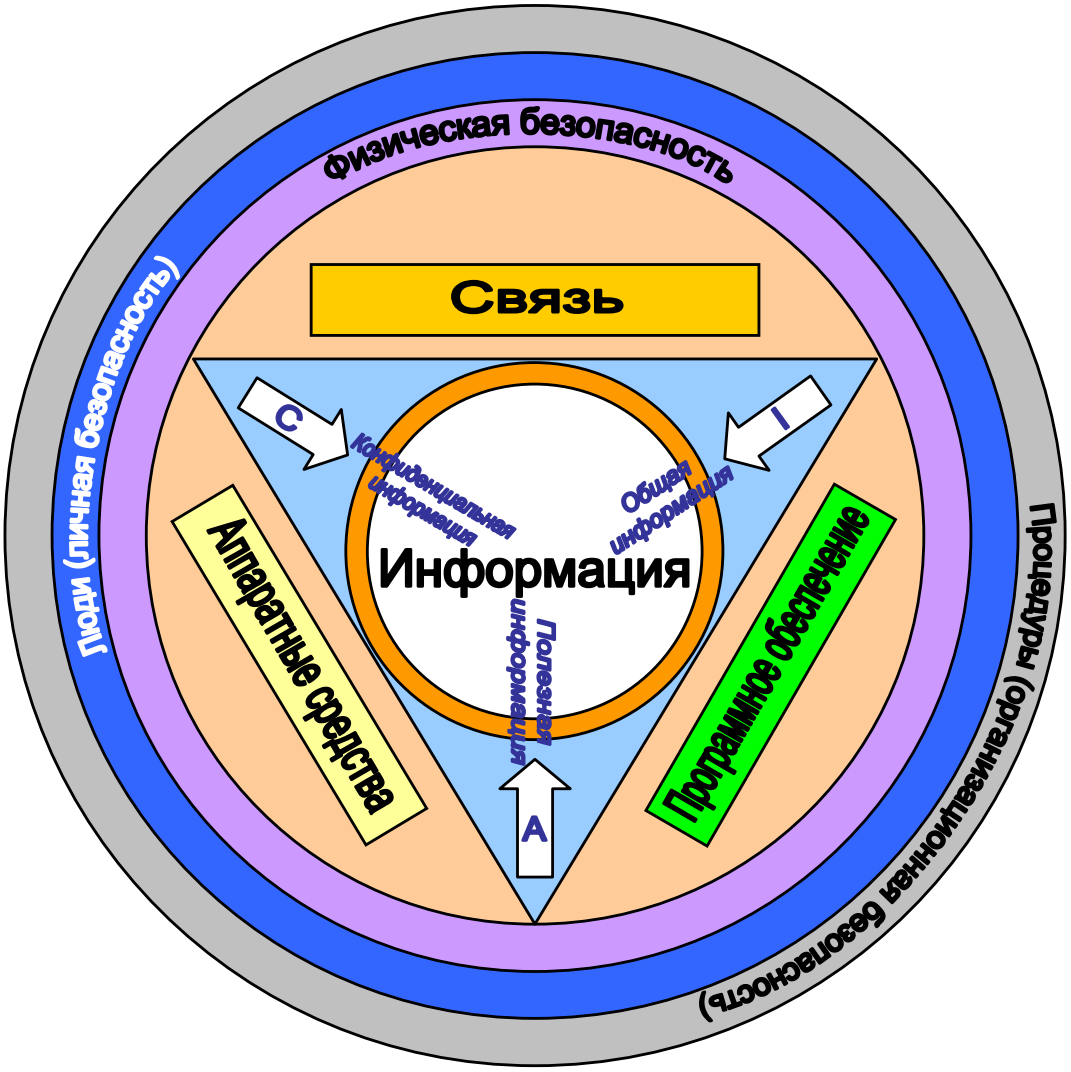


Рис. 3. Информационная безопасность общественно-политических систем.

Точками приложения процесса защиты информации к информационной системе являются аппаратное обеспечение, программное обеспечение и обеспечение связи (коммуникации)[2] Сами механизмы защиты разделяются на защиту физического уровня, защиту персонала и организационный уровень. Если по конфиденциальности и целостности информационной безопасности страны прямая ответственность лежит на спецслужбах и Совете национальной безопасности страны, то доступность информации это сугубо политический аспект и ответственность за него прямым образом лежит на правительстве и президенте страны. В данном случае нас интересует политический аспект информационной безопасности.

[2] Информационная безопасность. Википедия. http://ru.wikipedia.org

Для нормальной жизнедеятельности любого общества необходима объективная информация, которая бы отображала его состояние. Для получения объективной информации необходимо, чтобы средства массовой информации (СМИ) работали в свободном режиме и на них не оказывалось бы никакое давление со стороны. Но это не говорит о том, что какая-либо общественная организация или партийный орган не имеет права иметь свое собственное СМИ и пропагандировать свои взгляды на жизнь по тому или иному вопросу жизнедеятельности общества. Важность заключается в том, что общество имеет право выбора и свободного доступа к информации, кроме тех видов информации, которая засекречена и содержит в себе секреты оборонного, дипломатического характера или же пропагандирует идеи, входящие в противоречие с законом – например, расизм, вероненавистничество и другие. Потребитель сам вправе выбирать тот или иной информационный канал, к которому питает доверие. Таким образом, для каждого индивидуума происходит естественный отбор информационных источников и предпочтение тому или иному информационному каналу. Если нарушен этот принцип и в обществе информационная политика находится под жестким контролем одного человека или группы лиц (например, тоталитарное государство), то такое общество является больным. В таком обществе теряется вера в объективность информации и это чревато тяжелыми последствиями не только для общества, которое живет в государстве, но и для самого государства.

В разведывательных целях информация об объекте должна поступать тщательно проверенной и, как правило, от нескольких, независящих друг от друга, информационных источников. Для чего это необходимо? Обычно контрразведка занята не только обнаружением и устранением агентов иностранной разведки. Она работает более тонко. Обнаружив иностранного агента, она его не устраняет, а ведет за ним тщательное наблюдение, входит к нему в доверие и «предоставляет» ему дезинформацию для ее последующей передачи получателю. В этом случае делать объективные выводы о том или ином процессе уже не представляется возможным и тем самым разрушается процесс управления и принятия адекватного решения по тому или иному вопросу.

Представим себе, что есть два соседних государства, у которых примерно равные экономические, военно-технические и людские ресурсы. Другими словами, по всем своим параметрам они равны. В этом случае маловероятно, что одно государство осмелится начать военные действия против другого государства. Однако при всех прочих равных условиях в современной войне побеждает тот, у кого информационная безопасность выше. В данном случае на первый план выходит информационная война между соседними государствами, куда входит разрушение военных и гражданских каналов связи, полное разрушение киберпространства противника и информационный терроризм. Ярким примером информационного терроризма являются последние два землетрясения в Армении, толчки которого ощущались в Ереване. Сразу после толчков люди в панике бросились оповещать друг друга о том, что ровно через 2 часа (якобы радио и телеканалы сообщили) землетрясение повторится и надо всем выйти из своих домов. Кто-то преднамеренно пустил дезинформацию, а СМИ, в свою очередь, опоздали с ее опровержением. Тот же самый терроризм может наблюдаться в военное время, когда в войска спецсредствами связи противника

может вбрасываться заведомо ложная информация о том, что на соседнем участке прорван фронт и все убегают со своих позиций. Это приводит к панике в войсках и сражение, а впоследствии и весь исход войны, может быть проигран.

С помощью информационной войны можно дестабилизировать общество и довести его до революционных действий и даже этим способом разрушить само государство. В этом случае в силу вступает закон резонанса, когда с помощью тщательно просчитанной и вовремя вбрасываемой дезинформацией разрушается стабильность общества и народ провоцируется на экстремальные действия. На рис. 3 представлена динамика резонансного разрушения любой самоорганизующейся системы и в частности общественно-политической.

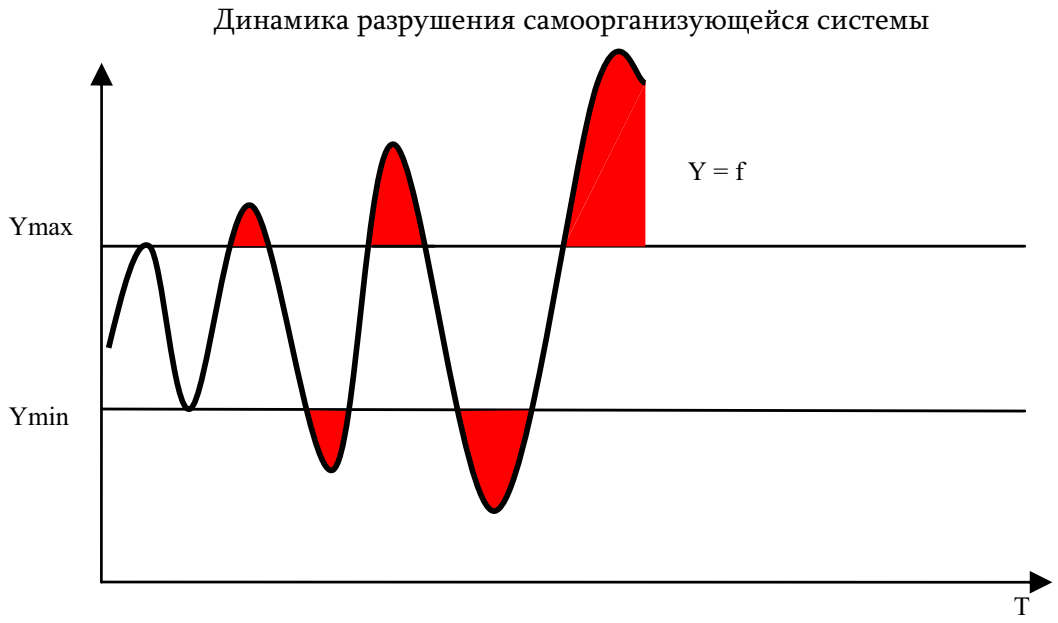


Рис. 3. Резонансное разрушение общественно-политической системы с помощью информационного воздействия

Не вдаваясь в техническую сторону вопроса, попробуем разобраться в каком состоянии находится доступность и достоверность информации для граждан Армении, какие проблемы стоят перед властями и общественностью для обеспечения доступности информации. Наиболее массовый вид информационного обеспечения – телевидение – по факту управляется из одного центра. Двадцать с лишним каналов отечественного телевидения преподносят обществу тщательно идеологически обработанную и однобокую информацию, усвоив которую делать более-менее объективные выводы о том или ином процессе, не представляется возможным. Единственный телеканал А1+ по причине своей объективности и освещению различных мнений был закрыт после теракта в Национальном собрании Армении. Ультракоротковолновые радиостанции (так называемые FM радиостанции), в основном, заняты развлекательными программами и рекламой товаров. При этом они не охватывают всю территорию республики и зона их действия распространяется в основном на столицу. Общественное радио постепенно утрачивает свою

значимость, поскольку при строительстве новых домов проводка линии радио не проводится. Телефонная связь, как информационная система, до недавнего времени находилась в весьма плачевном состоянии, поскольку единственный монополист в этом виде «Арментел» кроме как получением неконтролируемых со стороны общества сверхприбылей практически ничего не делал. Только появление других операторов связи, да и то только в части мобильной телефонии, заставили этого монополиста чуточку зашевелиться. Но до сих пор качество связи и обслуживания по сравнению с Vivacell оставляет желать лучшего. Есть надежда, что с появлением третьего оператора связи в стране картина изменится в лучшую сторону.

Сейчас в Армении наиболее свободным является Интернет, поскольку пока только в нем могут создавать свои информационные сайты издания, образ мысли которых отличается от правящей партии. Однако опыт постсоветских стран показывает, что со временем, эти сайты будут также закрываться и под это будет подводиться законодательная база. Например, как сообщает «Комсомольская правда» от 14.07.09, «Казахстанские юзеры переживают не лучшие времена. Теперь за смелое, опрометчиво оставленное в Сети слово им придется нести ответственность – вплоть до уголовной. Радея за урегулирование «всемирной паутины», Нурсултан Назарбаев приравнял абсолютно все Интернет-ресурсы к СМИ. Отныне чаты, блоги, Интернет-магазины и прочие веб-сайты должны формировать свой контент с оглядкой на законодательство. Причем это же мерило будут применять и по отношению к зарубежным сайтам. В случае чего доступ к любому противоречащему законодательству Казахстану сайту немедленно заблокируют». Анализ показывает, что по этому пути может пойти и Армения. Ведь закрыл же Роберт Кочарян на территории Армении российский телеканал НТВ только за то, что тот дал нелицеприятную информацию о его сыне.

В заключение необходимо отметить, что президент, правительство, служба национальной безопасности Армении и Совет национальной безопасности должны самое тщательное внимание уделять информационной безопасности Армении, поскольку только надежность информационной безопасности может обеспечить военную, экономическую, экологическую, промышленную и продовольственную безопасности любой общественно-политической системы и Армении в частности.

Карапет Каленчян
административный директор АЦСНИ