CRITICAL INFORMATION INFRASTRUCTURE PROTECTION: ANALYSIS, EVALUATION AND EXPECTATIONS

Eugene NICKOLOV

Abstract: The article provides a brief description of critical information infrastructure and analyzes the extent to which organizations depend on the proper functioning of banking and financial services, electricity, fuel and water supply networks, as well as information and telecommunication networks. The consequences of attacks on specific elements of these infrastructures are examined, as well as the initiatives and problems that arise with their protection on national and international level. Special attention is paid to the state of critical infrastructure protection in Bulgaria, with analysis of the reasons for its poor level and recommendations for improvement.

Keywords: Critical Information Infrastructure Protection, Information Security, Malware Attacks, Vulnerabilities, National Cybersecurity.

Introduction

The information revolution and the spread of Internet are stimulating globalization and allowing corporations to conduct business around the world. Communication technologies improve the productivity, efficiency and competitiveness of organizations around the globe. Today, organizations are outsourcing much of their business, consolidating operations by tunneling data to one central processing location, and using the Internet to cut down operation costs and overhead. With the increasing number of transactions, enormous amounts of data with varying degrees of protection are flowing over the Internet.

On the other hand, modern society has become much more dependent on the availability, reliability, safety and security of many technological infrastructures. Both because of the significant social and economic benefits they provide as well as because of the serious consequences of their malfunctioning, information systems have become a necessity for human well-being. Infrastructures considered critical are those physical and information-based facilities, networks and assets, which if damaged

would have a serious impact on the well-being of citizens, proper functioning of governments and industries or other adverse effects. The following infrastructures need to be functioning at least at a minimal level for the public and private sectors to be able to survive:

- Electricity, fuel and water supply;
- Transportation and communication systems;
- Food supply and waste management;
- Finance and insurance;
- Information and telecommunication networks;
- Military and defense systems, civil protection;
- Emergency, health and rescue services;
- Public agencies and administration, justice system;
- Media, major research establishments, etc.

The energy supply and the communication systems can be regarded as crucial since the rest of the infrastructures depend on them in order to function properly.

Although in the past many of these systems have been physically separated since the technology boom and the change of market dynamics in the 1970s, critical infrastructures have progressively converged and become dependent of information structures such as the public telephone network, the Internet, terrestrial and satellite wireless networks for a variety of information management, communications, and control functions. Technological progress has lead to more automation in the operation and control of critical infrastructures and the creation of a special information infrastructure. Recently, this infrastructure has emerged as one of the most important critical infrastructures because it is the base for managing and integrating all other critical infrastructures as well as new forms of communication, information exchange and commerce. This symbiosis is a national security priority, since the information infrastructure is crucial for economic progress, military and civilian government operations. In particular, the government and military information infrastructures depend on commercial telecommunications providers for everything from logistics and transport to personnel and travel functions. The extent to which these systems are intertwined increases the effects of any malfunctioning since they are spread across different infrastructures, affecting a wide range of users.

Furthermore, the greater role of information and the availability of electronic means to collect, analyze and modify it, have transformed information and information systems both into an invaluable asset and a lucrative target.

Following this train of thoughts, one should place the destructive potential of cyber-war in between nuclear and conventional war although currently tools for cyber attacks are developed in 120 countries, and nuclear arms – in 20 countries.

Vulnerability of Critical Infrastructure

The increased interdependency combined with greater operational complexity, has made critical infrastructures particularly vulnerable to natural hazards, human error and technical problems as well as new forms of cyber crime, terrorism and warfare. Each of these events can result in severe service deterioration or outright infrastructure failure. The technology development and the struggle towards complete automation have reduced our ability to incorporate the necessary safety features, including detection, prevention and mitigation standards and practices. The vulnerability created by these gaps affects not only utility services, but also databases and systems that maintain a variety of sensitive and confidential information.[1]

Many of our most critical systems are extremely vulnerable to natural disasters such as earthquakes, inclement weather, etc. Even when they are not physically impacted, sudden demand surges during crises can provoke blackouts, leading to loss or denial of service. Similar scenarios can occur through deliberate or accidental human action. The Critical Information Infrastructure (CII) has become especially vulnerable to fun-seeking hackers, criminals and even state actors and terrorists. The main tools used to attack critical systems are malware (computer viruses, worms, logical bombs, trojans) that modify and destroy information or block the computer systems. Tools for eavesdropping of information exchange in computer networks as well as tools for modifying the normal function of the computer network and blocking the access to its services are also widely used for destructive purposes.

These automated tools allow intrusions from remote systems to be done within a few seconds which makes Internet attacks easy to launch and increasingly hard to trace.

The Enemy Is Really Dangerous

Underestimating the abilities, knowledge and experience of cyber terrorists could be fatal for critical infrastructures. Some Islamic fundamentalists declared that Al-Qaeda and other Islamic fundamentalist groups plan to use the Internet as a weapon against CII in the US and Western Europe. A leader of a fundamentalist organization said recently: "We will soon be the witnesses of attack to the stock exchanges in New York, London and Tokyo."

The variety of activities undertaken by hackers is enormous: attacks on systems with insecure perimeters, use of third-party web pages for nationalist propaganda, e-mail bombs that overwhelm servers at organizations they are protesting against, zombie

computers deployed across the Internet serve as remote controls for attacks. In some countries even the government is involved by approving official documents for the preparation and execution of cyber attacks.

Most cases of CII breach are easy to perform since the vulnerabilities or configuration errors as well as detailed how-to guides are available for everyone on the Internet. However, the background knowledge required to perform the intrusion is steadily decreasing, thus increasing the overall success rate of intrusions. All one needs in order to initiate an information structure attack is a personal computer connected to the Internet and an e-mail program, while organizations trying to prevent intrusions are usually constrained by both staff and equipment shortage. End-users are often left to train themselves; new employees may not possess the same level of knowledge as incumbents about system capabilities, potential vulnerabilities or risk reduction measures.

Due to the increasing pressure to reduce production time, a new surge in the number of computer and network vulnerabilities is to be expected. Therefore, one should plan for infrastructures that have built-in instability, critical points of failure, and extensive interdependencies. Furthermore, more and more CIIs are becoming privately-held or owned by foreign nations.

CII attacks include:

- Unauthorized access to sensitive or confidential information;
- Destruction, modification or substitution of software needed by critical infrastructures;
- Limited access for the agents able to prevent or mitigate the results of the attacks.

The possible consequences from critical infrastructure attacks include:

- Blocked transportation, electricity and water supply, communications, data transmission, nuclear power plants, air-traffic control;
- Bankruptcy of commercial structures and financial systems, failure of international business transactions, destabilization of markets and financial institutions, money and information theft;
- Loss of intellectual property or reputation (due to a worm attack the company for on-line payments PayPal was facing a bankruptcy in 2002);
- Human victims or material losses, provoked by the destructive use of critical infrastructure elements (cyber sabotage in the food industry, air or railway traffic);
- Unauthorized access and/or modification of personal information;

- Possibility for imputing terrorist acts to other country/government and aggravation of the tension in international relations.

While the actual restoration of the CII is often a quick and easy task, the indirect effects of even the shortest failures can be felt for a while. CII attacks can seriously undermine public and business confidence in electronic commerce and government initiatives. The human and economic costs associated with recovery or mitigation strategies are enormous. The loss of business and productivity is now measured in billions of dollars from each world-wide virus attack, and even the largest software vendors are hard-pressed to keep up with security enhancements.

Measures for CII Protection

The CII Protection (CIIP) has three strategic objectives [2]:

- Prevent cyber attacks against critical infrastructures;
- Reduce national vulnerabilities to cyber attacks;
- Minimize damage and recovery time from cyber attacks that do occur.

In order to achieve these objectives a new strategy is needed; one that incorporates more than just the technological issues and includes the following elements:

- Taking preventive measures at all levels;
- Improving early detection and rapid reaction capabilities, both for damage control and pursuit of the culprits;
- Limiting the impact of disruptions on government and society;
- Ensuring that the affected systems continue to function at a minimum level or can be restored within the shortest possible time.

Threats and vulnerabilities consist of physical, informational and psychological components; therefore, an open, non-hierarchical dialogue on newly recognized vulnerabilities is needed and physical, informational and psychological protective measures have to be defined.

Measures on National Level

Five national priorities can be defined:

1. Establishing a national cyberspace security response system.
2. Developing a national cyberspace security threat and vulnerability reduction program.
3. Creating national cyberspace security awareness and training program.
4. Securing government systems.

5. Strengthening national security and international cooperation on cyber security.

The framework for CIIP at national level has to be considered in the wider context of the business, social, and technical environment. CIIP requires a multidisciplinary response incorporating technical, management and educational solutions. Both vendors and consumers need to prioritize better security in their products. Companies must adopt and share their best practices. The third approach is to promote better understanding of computer security and ethics through public education efforts. This program requires improved communication and coordination at three levels – within the industry, between the industry and the government, and within governmental structures and bodies.

Protection of the CII within Enterprises and among Industries

The most important factors for critical infrastructure vulnerability in the enterprises include:

- Large staff;
- Numerous physical facilities;
- Wide availability of phone numbers;
- Lack of security training;
- Lack of a system for data classification;
- Lack of procedure for reporting and reacting to incidents.

The measures that could be undertaken include:

- *Physical Protection of the Key Elements of CII.* Depending on the business, it may be necessary to install badge swipes, access codes or hire security guards. Cable locks, alarms, motion detectors, antitheft systems, biometric scanners, etc., could also come in useful. Electronic keypads on server rooms that are not shut off in the event of power loss may be necessary for some companies. These are just a few example physical security measures needed to secure a facility.
- *Technical Measures – Technical Security.* They include use of e-mail and file encryption to conceal the operations and prevent sensitive data from unauthorized disclosure, whether national security secrets or private customer account data or confidential proprietary information. Firewalls, intrusion detection systems, access control lists, strong password policy, and anti-virus software are also components that companies may need.
- *Social Measures - Staff Training and Control.* A background check on new employees is an excellent security measure. This is a good defense measure from

an information warfare standpoint. It informs employers whom they are hiring before the new employee has any physical access to a facility and sensitive documents.

User training is a huge step in the right direction. All employees have to be trained to lock their computer screens when they leave their desks, to use strong password management schemes, to know the methods of social engineering so that they do not end up revealing any confidential information. When employees feel personally involved in protecting the company or agency they work for, they tend to take more pride in what they do. The more they understand the policies set forth, the less potential problems will arise in future.

- *Security Policy*. All technical and social measures have to be implemented with a strong security policy that should:
    - Define what the user wants to protect;
    - Analyze what it is the user wants to protect it from;
    - Explain how the user intends to protect it.

  The policy must be updated regularly, signed off by management, and everyone in the IT department must be familiar with it.

  The overall security policy will address such areas as:
    - Physical security of the data and systems;
    - Access control to the data and systems;
    - Data integrity and availability;
    - Contingency and recovery plans.

  To be effective, the security policy must be both inclusive and dynamic. To be successful, it must have realistic goals and be phrased in a way that is simple and short enough to ensure it is understood and followed by all users.

Public / Private Cooperation between Industry and Government

Due to the large number of private actors that own or use CIIs, forming public-private partnerships is an important part of CIIP.[3] These partnerships should include:

- Problems and threats to national CII;
- Alerting software and hardware vendors to the security and the protection of their products;
- Fast and efficient reaction to all incidents related to the functioning of critical systems;
- Creation of systems for formal and informal sharing of information about computer related crimes and cyber terrorism.

Looking into more detail at the last item, it is clear that the private sector and law enforcement must gather and share information about threats, vulnerabilities, remedies and successful operating models of cyber security. To improve CIIP, industries have to share some information about incidents and damages with the government and the public, even when information sharing is damaging for the company itself. Only complete disclosure of information both in the private sector and the government could even the potential of the attackers and the defenders of the CII.

On the other hand, sharing CII has some negative side effects both to public and private interests. Information sharing could be regarded as price fixing, unreasonable restraint to trade, or systematic discrimination against certain customers. It also could raise privacy concerns, expose proprietary corporate secrets, and reveal weaknesses and vulnerabilities that erode public confidence and invite hackers. Retailers and credit card issuers often worry that disclosing any problems with the security of online transactions (e.g., hackers gaining access to credit card numbers or purchase history) may undermine public confidence in Internet commerce, to the detriment of their businesses. An ISP attack disclosure also could lead to a loss of customers and revenue.[4] Releasing a top ten vulnerabilities list to the public helps system administrators and computer users, but provides hackers with the information they need to successfully attack at-risk networks.

Therefore, trust with respect to how the information will be used, how it will be protected from disclosure, and whether legal tools can be used by the government and private parties against those sharing information is needed among those sharing information in order to achieve successful protection of the national CII.

Tasks on Governmental Level

The most important task is the creation of a national security policy which has to include:

- Security policy for strategic objects controlled by computer networks, based on the risk analysis of possible attacks;
- Programs for practical implementation of security policy and operational measures to ensure the rules are followed;
- Strict adherence to the assessment standards of products and systems prone to cyber attacks;
- Analysis of the current reaction abilities of network elements and systems based on their reaction to possible attack scenarios;
- Assessment of the efficiency of protection tools by:
    - Reliable verification (reasonable balance between confidentiality and access to common data);

- Protection of all systems and subsystems using testing (honey pots and honey nets) and specific criteria ("Orange book," Canadian criteria for security estimation of information technologies, harmonized European criteria).

The best practices and resources on cyber security policy developed in the last years provide valuable guidance both to industrialized and developing countries. The forerunner, the British Standard 7799, has now evolved into the International Standard ISO/IEC 17799. A number of other IT security standards have been developed, including ISO/IEC 13335 which relates to the Guidelines for the Management of Information Technology Security.

One of the most important aspects of effective organization of CIIP is government funding. Often the security measures undertaken by businesses are not very effective – or effective enough to outweigh the investment. Government investments in research and development of computer security measures resolve this problem to a certain extent. The second important task to be performed on the governmental level is the elaboration of common policy in the control of computer systems especially for the vital branches of national defense and business. This policy has to be founded on a legal framework for CIIP to be considered in the larger context of the business, social, and technical environment. CIIP has to be seen as a part of society's (cyber) crime prevention. Cyber crime is a very broad concept that has various meanings, ranging from technology-enabled crimes to crimes committed against individual computers, and includes issues such as copyright infringement, computer fraud, child pornography, and network security violations. Cyber crime is generally fought with traditional law-enforcement strategies that include adopting appropriate legislation and fostering international cooperation.

Only governmental institutions could create a united front against cyber attacks. This front needs a central unit for infrastructure protection – a body that is already created in some countries. It must focus on the collaboration of the private sector, law enforcement, prosecution and the intelligence community and provide support in the following four areas:

- Management of the computer emergency response teams (CERT) and virus centers in the country;
- Investigations on the Internet to identify criminal misuse and to monitor dangerous situations, such as the vulnerability of widely used hardware and software products;
- Verifying whether the reported matter constitutes a criminal offence, coordinating with ongoing proceedings and referring the case to the relevant prosecution authorities at home and abroad;

- Analyzing the interconnectedness of critical sectors and their dependence on information technology, and developing measures for prevention, response, and comprehensive security management of the national critical information structure.

These tasks include systematic examination of all infrastructure areas for possible weaknesses and improvement possibilities in terms of IT dependencies and security. Further, they necessitate the appropriate solutions, recommendations for each individual sectors, as well as indications of technical or organizational support needed in order to be executed.

The US was the first country to broadly address the new vulnerability of the vital infrastructures.[5] The Presidential Commission on Critical Infrastructure Protection (PCCIP) defined in 1997 the CII, its particularities and vulnerabilities. Following the PCCIP's publication, US President Bill Clinton started initiatives to increase the protection of critical infrastructures in the US, on the premise that a joint effort by government, society, organizations, and critical industries was needed to defend these vital assets.

Recently, following the example of the US, many countries including Australia, Canada, Germany, The Netherlands, Norway, Switzerland, the U.K., and Japan have taken steps on their own to better understand the dangers to their CII, and have proposed measures for the protection of these assets.

Computer Emergency Response Team (CERT) coordination centers are also being established around the globe and provide assistance in handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing security information and training materials.

Problems in CIIP on National Level

The main difficulty is that vendor product development and testing cycles are decreasing, thus leaving exploitable vulnerabilities. There are infrastructures with fundamental security design problems that cannot be quickly addressed. Vendors produce software with vulnerabilities, even such that can be easily avoided and computer source code often is not required to find them. In addition, the sophistication of attacks and intruder tools is increasing and many are designed to support large scale attacks.

There are also several other factors that complicate efforts to improve CII security. First, there is an inequality between the low cost performing an attack and the high cost of protection mechanisms. Therefore, there are indeed well-known technical vulnerabilities inside many infrastructures, but because of the prohibitive costs not enough has been done to address them.

Sometimes, losses from security breaches can be dealt with only if large numbers of parties coordinate to make the necessary investments. The incentive that one conscientious network owner has to invest in security measures is reduced if the owner believes that other connected networks are insecure, which would undermine the impact of the conscientious owner's measures. Moreover, assigning liability for security breaches is difficult – a user cannot easily identify the source of the problem (e.g., whether it was due to the user's software, the ISP, the backbone to which the ISP is connected, or software used by others).[6]

Another complicating factor is that computer network externalities are international in scope and implementation of a strong security policy conflicts with efforts to promote open communication environment. Furthermore, current highway net infrastructures connect countries with different levels of technological development; the "weak points" are vulnerable in two different ways: by themselves and as an initial point for attacks (zombing).

International Level

CII attacks are becoming a growing transnational phenomenon, making prosecution extremely difficult. Therefore cyber security must be approached from an international perspective, taking into account:

1. National and international initiatives;
2. Legal developments;
3. Best practices and resources;
4. Guidance on developing and implementing effective security programs;
5. Technological considerations.

Achieving cyber security requires a global effort; it cannot be achieved by a few nations. It requires the input from all information and communication technologies users, including citizens, governments, businesses, and organizations. On the multinational front, the Group of Eight (G8), the Asia-Pacific Economic Conference (APEC), the European Union (EU), the Council of Europe (CoE), the Organization for Economic Cooperation & Development (OECD), the Organization of American States (OAS), and the United Nations (UN) are each working towards solving this problem. As early as December 1998 the General Assembly of the United Nations approved Resolution 53/70 on cyber crimes, cyber terrorism and cyber war. It appeals to the member states to inform the UN Secretary General of their opinions on the following issues:

- The problems related to information security;
- Basic notions related to information security;

- Development of international principles of the global information space and telecommunications, which help combat cyber terrorism and cyber crimes.

The EU has adopted the *Proposal for a Council Framework Decision on Attacks against Information Systems* that recommends a harmonized approach to attacks against information systems through uniform prohibitions against illegal access to information systems, as well as instigating, aiding or abetting such acts. The Council of Europe developed the Convention on Cyber crime (with the United States participating as an observer), which has since been signed by 42 countries.[7]

In October 2004 the General Assembly adopted a resolution about the creation of a global culture of cyber security and the protection of CII which recommends:

- The creation of emergency warning networks and crisis communication networks regarding cyber-vulnerabilities, threats and incidents;
- Public and private partnerships to share and analyze critical infrastructure information;
- The adoption of adequate substantive and procedural laws to enable states to investigate and prosecute attacks on CII and coordinate such investigations with other states when necessary.

In addition, many bilateral and multilateral documents have been signed for legal help, extradition, and law unification, guaranteeing transnational and international prosecution of cyber criminals. For example, the U.S. has held bilateral meetings on critical infrastructure protection (CIP) with Germany, Japan, Australia, Canada, China, and India. The European Commission recently held a conference at which EU-Russia cooperation regarding cyber security was highlighted. The case of *U.S. v. Gorshkov*,[8] in which an FBI agent conducted a cross-border search of a Russian computer to obtain evidence to indict a Russian citizen on extortion charges, is an example of how international cooperation helps cross-border searches in the current environment and how it might become the norm in the absence of formal international coordination.

Problems of CIIP in Bulgaria

The most important problems of CIIP in Bulgaria could be summarized as follows:

- Lack of legal acts for cyber criminal proceedings;
- Lack of trained staff;
- Lack of the necessary technical tools for response to cyber attacks;
- Lack of reliable system for interaction with special organizations from other countries;

- Lack of national organization on governmental level coordinating the CIIP;
- Lack of national strategy aimed at funneling the modest financial resources of the country to the development of such an organization;
- Lack of national action plan binding the national funds with international projects on regional level for the development of such organization.

Bulgaria needs a legal framework that would authorize governmental agencies to read e-mails, intercept wireless communications, monitor computer use, etc. A special law could make it illegal to intentionally crack a computer, or to deliberately cause damage launching a malicious program that harms a system. Hacking could be included in the definition of terrorism and may even face life imprisonment, as under the provisions of USA Patriot Act of 2001.

Recommendations and Suggestions

The following recommendations and suggestions could be given:

1. Organization of effective collaboration between the judicial bodies and special services of Balkan and European countries and international organizations.
2. Creation of a national strategy for prevention and combat against cyber crimes.
3. Creation of a national service against cyber criminality and international contact point for reaction and help during transnational computer incidents.
4. Extension of international collaboration in the field of judicial aid in the struggle against cyber criminality.
5. Creation of special laws in the area of telecommunications and computer networks in accordance with the current international standards and the Convention of EC for cyber criminality.

The best governmental approach would be to facilitate the establishment of a single technical point of contact that would enable the administrators at the backbone ISPs to share, in real time, information to combat a cross-industry attack (such as Bagle, Mydoom, Netsky, Sasser, Korgo, Sober). Coordination among the technical experts during a distributed denial-of-service (DDOS) attack, for example, would help them identify the source of the attack, as well as potential solutions to block the attack, and restore the network to operational capacity faster. Informal communication and coordination do take place, but with the evolution of the Internet itself there is a need to increase the scope and scale of such activities.

Conclusion: Towards Practical CII Protection

One of the key features of our networked environment is that individuals, corporations and governments all share a responsibility in securing this environment. Therefore, the private sector, law enforcement, intelligence agencies and competence centers in certain fields, such as the CERTs in the domain of information infrastructures, must be brought together to ensure an integral and therefore successful protection of the national critical infrastructure.

Since usually the majority of a nation's critical infrastructure is operated and owned by the private sector, public-private partnerships are the key. In order to accomplish this, however, the government, which is usually in charge of the protection of the national critical infrastructure, should offer a well organized, efficient and reliable network to the private sector, covering all relevant fields from battling misdemeanors and early warning, to technical expertise and support.

Notes:

[1] John Moteff, Claudia Copeland, and John Fischer, "Critical Infrastructures: What Makes an Infrastructure Critical?" Report for Congress RL31556 (Congressional Research Service, Library of Congress, 21 Jan 2003).

[2] Andreas Wenger, Jan Metzger, and Myriam Dunn, eds., *International CIIP Handbook* (Zurich: Center for Security Studies at the Swiss Federal Institute of Technology, 2004), <www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf>.

[3] *U.S. The National Strategy to Secure Cyberspace* (US Government, February 2003), <http://www.whitehouse.gov/pcipb> (18 July 2005).

[4] Paolo Donzelli, "A Goal-Driven and Agent-Based Requirements Engineering Framework," *Requirements Engineering* 9, no. 1, Springer-Verlag London (February 2004): 16-39.

[5] Patrick L. Anderson and Ilhan K. Geckil, "Northeast Blackout Likely to Reduce US Earnings by $6.4 Billions," AEG Working Paper 2003-2 (Anderson Economic Group, 19 August 2003).

[6] Paolo Donzelli and Roberto Setola, "Putting the Customer at the Center of the IT System – A Case Study" (paper presented at the *Euro-Web 2001 Conference – The Web in the Public Administration*, Pisa, Italy, 18-20 December 2001).

[7] <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG> (18 July 2005).

[8] *U.S. v. Gorshkov*, 2001 WL 1024026 (Western District of Washington).

EUGENE NICKOLOV, Prof. DSc. PhD Eng. Mag., has been Director of the National Laboratory of Computer Virology in the Bulgarian Academy of Sciences since 1991. He is Professor of Informatics, Doctor of Mathematics, Doctor of Computer Sciences, Engineer of Radioelectronics and Master of Sciences in Microelectronics. His main scientific interests are in informatics: algorithms, effectiveness, protections of operating systems; abstract models of computer systems, theory of programs; simulation and modelling of computer and communication technologies; theory of information and cryptographics; data security, computer security, communication security; analysis, synthesis, protection of stegano objects. *Address for correspondence*: Acad. G. Bontchev Str., Building 8, Office 104, 1113 Sofia, Bulgaria; *Phone*: +359-2-9733398; *E-mail*: eugene@nlcv.bas.bg.