1. European background

Two years ago, in February 2013, the European Commission published a cybersecurity strategy along with a Commission proposed directive on network and information security (NIS), which is still under debate.

The cybersecurity strategy, “An Open, Safe and Secure Cyberspace” presents the EU’s global vision on how best to prevent and manage cyber disruptions and attacks, with the aim of fostering the European values of freedom and democracy and ensuring the safe growth of digital economy.

The European strategy revolves around five priorities:

- Achieving cyber infrastructure resilience;
- Drastically reducing cybercrime;
- Developing a cyber-defence policy against cyber-attacks and the required capabilities related to the Common Security and Defence Policy (CSDP);
- Developing the necessary industrial and technological resources for cybersecurity;
- Establishing a coherent international cyberspace policy for the European Union and promoting core EU values.

The progress made by the European Union in this area covers the creation of a European Cybercrime Centre (IP/13/13), proposals of legislation on attacks against information systems (IP/10/1239) and the launch of a Global Alliance to fight child sexual abuse online (IP/12/1308). The Strategy also aims to develop and fund a network of national Cybercrime Centres of Excellence to facilitate professional training and capacity building.

Cybersecurity and the Romanian business environment in the regional and European context

Developing a cybersecurity culture for the users of digital and communications systems has become a mandatory requirement.
The growth and expansion of cyber-attacks have imposed the adoption of a new cyber-defence concept and policy by NATO as well.

Member states must adopt a network and information security strategy and appoint a national authority in this sector.

The proposed directive on network and information security represents the core component of the global strategy, requiring all member states, the main internet providers, critical infrastructure operators (for instance e-commerce and social networking platforms), service operators in energy, transport, healthcare and bank sectors, to ensure a secure and reliable digital environment in the entire EU. The measures set out under the proposed directive include the following:

1. Member States should adopt a network and information security strategy and designate a national NIS competent authority with adequate financial and human resources to prevent, handle and respond to NIS risks and incidents;
2. A cooperation mechanism should be created among Member States and the Commission to share early warnings on risks and incidents through a secure infrastructure, cooperate and organise regular peer reviews;
3. Operators of critical infrastructures in some sectors (financial services, transport, energy, health), enablers of information society services (notably: app stores, e-commerce platforms, Internet payment, cloud computing, search engines, social networks) and public administrations should adopt risk management practices and report major security incidents on their core services.

2. National background

In line with the European approach, Romania’s Government adopted GD 271/2013 on Romania’s cybersecurity strategy in May 2013.

The document contains an intricate description of the overall context and basic arguments underpinning the need to adopt such a strategy, one of which is the rapid advancement of modern information and communication technologies – a sine qua non requirement for the development of the information society – which has had a major impact on the social environment, sparking genuine mutations in the basic philosophy of economics, politics and culture, but also on individuals’ day-to-day life.

The Strategy calls attention to the fact that along with the undeniable benefits brought to modern society, information technology also comes with vulnerabilities and, therefore, cybersecurity must become a major concern for all the actors involved, in particular at institutional level, on whose shoulders rests the responsibility to develop and implement coherent policies in this field.

It is worth mentioning that the main purpose pursued by the Strategy is to develop a dynamic information environment, built on interoperability and services specific to the cyber society while ensuring adherence to fundamental rights and liberties and to the national security interests, under the umbrella of an appropriate legal framework.

The development of a cybersecurity culture for the users of digital and communication systems, who often are ill-informed about the potential risks or the means to fight them, has become a mandatory requirement.
A large-scale awareness of the risks and threats posed by cyber activities as well as of the means to prevent and combat cyber-attacks requires an efficient communication and cooperation between the participating players.

The cybersecurity incidents and major cyber-attacks recently targeting certain states and international organizations have raised international awareness about the need for cybersecurity strategies and policies. Thus, states such as Estonia, the United States, the Great Britain, Germany and France have developed national cybersecurity strategies that endorse the need for actions aimed at developing capabilities to counter cyber-attacks and lay down the foundations for cooperation between governmental and non-governmental entities acting to limit cyber-attacks consequences.

Against the background of increasing cyber-attacks, NATO has developed a new cyber defence concept and policy. Thus, the Alliance has redefined its role and strategic actions and has developed an action plan aimed at enhancing the protection capabilities of its own cyber infrastructure as well as at implementing mechanisms to ensure information sharing and mutual assistance with member states in the event of major cyber-attacks.

The European Union has equally recognised the need for a policy to fight cybercrime. Subsequent initiatives were boosted by the increasing number of cybercrime incidents, the enhanced involvement of organized crime groups in cyber criminality as well as by the need for coordinated efforts to combat such acts.

The cybersecurity incidents and major cyber-attacks recently targeting certain states and international organizations have raised international awareness about the need for strong cybersecurity strategies and policies.

Enhancing the capabilities to fight the cyber battle at national, European and international level, requires among other things:

- strengthening the cooperation and coordination of the units responsible to combat cybercrime, of other EU authorities and experts;
- creating a coherent cybercrime regulatory framework at EU level in cooperation with the Member States, as well as with the relevant European and international authorities in this field;
- raising awareness of cybercrime costs and threats.
Cyberspace, the new interaction environment of modern society, is offering a raft of opportunities generated by its very own idiosyncrasies. Thus, a number of opportunities have been identified that can be exploited by Romania through its cyberspace, such as:

- upholding its policies and promoting national interests;
- developing and bolstering the business environment;
- increasing life quality by strengthening the services offered by the cyber society;
- optimising understanding and upholding national strategic decisions in the digital age by ensuring adequate cyber capacities and tools;
- strengthening knowledge levels and prediction capabilities to enable early warning of risks and threats to national security;
- enhancing technical capacities and human resources skills to meet national security objectives.

3. Public and private sectors cooperation

The national Strategy on cybersecurity points out that developing the cooperation between public and private sectors to ensure cybersecurity is a primary course of action for international organizations or alliances to which Romania is a party, since cyberspace encompasses cyber infrastructure held and administered by both the state and private entities.

The main courses of action targeting cybersecurity to be undertaken by the public sector in cooperation with the private one will pursue to achieve:

- a trust based cooperation between the state and the business environment;
- higher protection of cyber infrastructure by correlating the measures undertaken with the resources available in the public and private sectors.

Romania can assume an active key role in the cooperation with the EU, NATO, USA as strategic partners, to successfully implement strategies and advance measures aimed at cybersecurity consolidation.

The responsibility to ensure cybersecurity rests with all the actors involved, with due consideration given to complementary interests in this sector, so as to secure the lawfulness of operations, a crackdown on cybercrime phenomenon and the protection of critical infrastructure interconnected with the cyberspace, based on enhanced mutual trust.
The cooperation between the public and the private sectors will target the following core objectives:

- share information on threats, vulnerabilities and specific risks;
- enhance early warning and response capabilities to cyber incidents and attacks;
- organize joint cyberspace security exercises;
- develop training and research programs in this field;
- create a security culture;
- prepare a joint response to major cyber-attacks.

Attaining these objectives presupposes a close cooperation between the public and the private sectors through, among other things, the adoption of prevention measures, awareness raising and advancement of cybersecurity opportunities.

However the Romanian business environment remains vulnerable and underprepared to face the current multifarious cybersecurity risks. Globalization and the Internet as well as the fast progress of information technology towards centralized systems serving transnational corporate structures pose a high risk to the private environment which is directly exposed to potential cyber-attacks. Furthermore, client databases (especially in the banking, telecom and health sectors), but equally so employees’ records of big size employers, contain legally protected personal data whose safety is not always secured. The local economic environment has financial, economic and resource ties at European and international level, but not all the participants are well-informed and properly prepared to prevent or react in case of need.

Quite a large number of private business entities with foreign or domestic capital, national companies, government business enterprises or other state owned entities active on the market lack a Business Continuity and Disaster Recovery Planning, or adequate human and technical resources to reliably implement such solutions. Apart from banks and entities acting in strictly regulated sectors, companies have no legal obligation to have their IT systems and their protection capabilities audited nor are they required to have a system penetration testing. The overall national awareness level is low, while the basic means available to SMEs, for instance, are non-existent. Against the backdrop of the still persisting economic downturn, the aggravating regional security climate, with Romania still lagging behind (in infrastructure, healthcare, education, EU funds absorption etc.), the private sector is still prone to disruptions.

The proposed directive is still under debate, but no major amendments are expected. Five main concepts are at the core of the directive: obligation of each European state to adopt its own national cybersecurity strategy; creation of an institutionalized cooperation network; development of uniform/standardized requirements; and consistent application/implementation of these rules by Member States.
At the end of year 2014, public eye was drawn to the draft law on cybersecurity, as part of the national strategy and submitted for approval to the Parliament. Despite being voted by both Chambers of the Parliament, the draft law was held to be unconstitutional in its entirety under Decision no. 17/2015 of the Romanian Constitutional Court.

The draft law, drawing on the NIS Directive (Network & Information Security), which is not yet in effect, must be resumed with celerity, under terms that should ensure compliance with best practices and standards and the protection of rights deriving from personal data protection, professional secrecy, the rule of law and an impartial justice.

While policymaking may be a complex and time-consuming process at both national and European level, Information technology has an explosive and unceasing advancement. In this context, the authorities, but equally so the private sector, should be aware of and prepared to respond to the raft of severe risks generated by cybercrime manifesting in the growth of massive and focused attacks, by espionage operations facilitated by intelligence leaks/information loss, by the exposure driven by social media and outdated versions of systems/software or source codes. Specialist opinions raise a red flag, pointing to worrying signs in health and utilities infrastructure, vulnerabilities in the Internet of Things growth areas but also in less targeted sectors such as retail.

Indicative Bibliography:
GD 271/2013 regarding Romania’s national cyber security strategy
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2015 NTMO sprl, a Romanian law firm and a member firm of the KPMG Legal network of independent firms. All rights reserved. Printed in Romania.