STRATEGIKON
Innovative Strategies

REPORT

2016 Cyber Security Law

Liberty, trust and security in the national and European cyber space

Executive Summary

- This report tackles in an interdisciplinary way the subject of public-private partnership in personal data management in the US, the EU, and Romania in the context of both the draft Cyber Law being currently discussed and the asymmetric threats and emerging risks on the national, European, Euro-Atlantic cyber infrastructure.

- Strategikon answers three important questions when talking about cyber regulations: what are the international trends and developments, what are the lessons to be learned, and what should policy makers keep in mind when drafting a cyber law? Thus, the document can contribute to the drafting process of a Romanian Cyber Security Law designed to protect the right to privacy and satisfy the need for a secure cyberspace.

- Having the highest internet speed in the EU and close to no cyber protection, Romania is a hacker's heaven. After the Romanian Constitutional Court stated that the Cyber Security law was unconstitutional (Decision 17/2015), the Ministry of Communications and Informational Society (MCSI) published on its website an amended draft law which is (again) a hot topic in the public debate.

Bucharest, JULY 2016

STRATEGIKON REPORT, *JULY 2016, Copyright @ www.strategikon.ro . Report drafted by Bebe-Viorel Ionică, Claudiu Săftoiu, Corneliu Vișoianu, Denis Kurunczi, Filofteia Repez, Florin Necula, Gabriel Mihăilescu, Mădălina Neacșu, Mihai Popa.*

CONTENTS

INTRODUCTION

Is it possible to have sustainable security enshrined in national legislation, in such a manner, so as not to affect democracy? At the same time, can the cyber space remain free and also secure? The need for cybersecurity is acute especially given the fact that recent terrorist threats started mainly in cyber space and weakened national online systems. Systems of security institutions, national authorities and private companies are all mercilessly exposed to modern outlaws. Virtual terrorists misuse the liberty of the cyberspace to bring on its knees the liberty of the internet, nations and thousands of citizens using the internet.

Here, Romania`s case is relevant: faced with cyber risks, public opinion is unable to adapt, still fighting the legacy of oppression left by the former political police. Meanwhile, the US, Canada and other important European countries work together against hackers and criminal groups, the faceless criminals of the internet.

Strategikon exposes challenges, brings up significant comparisons and brings forward recommendations in the eve of the essential, secure and democratic Cybersecurity Law being discussed in the Romanian Parliament.

1. International trends, developments, and their lessons

1.1. The United States

The powers granted by Congress in the wake of 9/11 were vast but in the years after, the tide of judicial and public opinion turned against what many saw as vast overreach and even vaster failure to perform. In May 2015, the US Second Circuit Court ruled that the program to systemically collect Americans' phone records was never properly authorized. Not only was the law left to expire but in June 2015 Congress approved the USA Freedom Act, which included a ban on those collection activities. Even as the NSA has struggled to give the public and Congress more transparency into its workings, evaluations indicate that the bulk-collection program was a failure.[1]

Government and industry have talked about information sharing mechanisms for more than a decade. The House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA)—in 2013, but the bill's progress stopped when Pres. Barack Obama threatened a veto due to a lack of privacy protections. In October 2015, the U.S. Senate passed its Cybersecurity Information Sharing Act (CISA), a controversial measure to encourage businesses and government agencies to share information related to malicious hackers and their methods. High-profile cybersecurity breaches at Sony Pictures, Home Depot, the Office of Personnel Management and dozens of other organizations within the past year alone helped CISA make its way to the Senate floor. The thinking is that the shared information will help these different groups better prepare themselves to identify and defend against hackers trying to steal

[1] Cyber Risk Report 2016, Hewlett Packard Enterprise Security Research, http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/.

information from their computers. However, CISA in its current form does not clearly define how this information would be shared, who would manage such information or how it would be disseminated.[2]

Critics point out that information sharing will do little to prevent successful cyber-attacks. In fact, the federal government already has an organization for sharing cybersecurity threat information. The Department of Homeland Security established its United States Computer Emergency Readiness Team (US-CERT) in 2003 to collect, analyse, disseminate and respond to cybersecurity information shared among government agencies, the private sector and researchers. CISA's critics argue that information sharing must be combined with implementing encryption, patching outdated software and otherwise bolstering cyber defences.[3]

In February 2015, President Obama signed Executive Order 13691, which details a framework to expand both private sector and public-private sharing of information on threats and attacks. Such programs have long been the goal of a number of public and private efforts.[4]

1.2. Bridging the Atlantic - The EU

For enterprises, international data-privacy issues years in the making came to a head in October 2015 when the European Court of Justice struck down the EU-US Safe Harbor Agreement in place since 2000, that allowed US and European interests to share data that has privacy considerations. The Court's decision came in a tepid climate, made more so by Edward Snowden's data releases and Max Schrems's court complaint. Europe's top court found that the Safe Harbor Agreement did not adequately protect user privacy rights, because it allowed US officials to gain access to user data even when European law would forbid it and allowed for data to move to third-party nations with which the Safe Harbor agreement was not in force.[5]

In February 2016, the European Commission and the United States agreed upon the EU-US Privacy Shield, a new framework for transatlantic data flows. It provides for stronger obligations on companies in the U.S. to protect the personal data of Europeans and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities.[6]

In 2015, six of the top 10 countries that experienced the most Internet fraud were located in Eastern Europe and the former Soviet Union, some of the more pertinent criminal activities include:

- Malware: As of 2015, the three principal malware types that have been leveraged extensively by European cybercriminals are ransomware, remote access Trojans (RATs), and info stealers.
- Markets for Goods and Services: credit card data, e-mail spam, child pornography, fraud and phishing, cyber extortion, disclosure of

[2] Larry Greenemeier, A Quick Guide to the Senate's Newly Passed Cybersecurity Bill, The basics of the controversial Cybersecurity Information Sharing Act (CISA), 28 October 2015, http://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-passed-cybersecurity-bill/

[3] Larry Greenemeier, A Quick Guide to the Senate's Newly Passed Cybersecurity Bill, The basics of the controversial Cybersecurity Information Sharing Act (CISA), 28 October 2015, http://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-passed-cybersecurity-bill/

[4] Cyber Risk Report 2016, Hewlett Packard Enterprise Security Research, http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/.

[5] Cyber Risk Report 2016, Hewlett Packard Enterprise Security Research, http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/

[6] EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, Press release of the European Commission, 2 February 2016, http://europa.eu/rapid/press-release_IP-16-216_en.htm

personal and confidential data, compromise of resources and web defacements, compromise of network systems and websites, denial of service, and unlawful e-commerce and services.

- Bitcoin: Cybercriminals from Eastern Europe are also active in hacking Bitcoin, an untraceable crypto currency used online.[7]

Cyber security had a slower debut in the 2000s both within the Member States, with awareness raised by cyber-attacks and the growing reliance of modern economies on ITC, and at the level of the Union. The EU had at the time limited competences and focused on civilian rather than military aspects of cyber-security, reserved mainly to NATO.

The High Representative and European Commission's February 2013 Cybersecurity Strategy of the European Union, a first comprehensive EU policy framework established five priority areas for: cyber resilience and security of infrastructures; reducing cybercrime; cyber defence policy and capabilities related to CSDP; developing specific industrial and technological resources and an EU international cyberspace policy.[8]

The Digital Single Market is a priority of the Junker Commission and includes a key initiative on a public-private partnership on cybersecurity. The most significant achievement to date, the Directive on Network and Information Security (NIS) was adopted by the European Parliament and the Council. Member States will have 21 months to implement this Directive into their national laws and 6 months more to identify operators of essential services. The public-private platform on NIS will be a key mechanism to ensure a high common level of cybersecurity in the EU. The NIS Directive builds on three main pillars: 1) increasing the cybersecurity capabilities in the Member States; 2) ensuring cooperation among all Member States, by setting up a 'Cooperation Group' and 3) ensuring a high level of risk management practices in key sectors (such as energy, transport, banking and health).

While the NIS platform aims very high, there are considerable discrepancies between the Members State's (MS) cybersecurity policies, legal frameworks and operational capabilities. The European Network Security Agency (ENISA)[9] works closely with MS and the private sector to deliver advice and solutions and also facilitates dialogue among the public and private actors involved in cyber-security at EU level.

The EU is moving towards a better integration of its policies and a closer cooperation between its Member States. With the attacks in Paris and Brussels, the question "how did it came to this?" arose. Indeed, if Europeans have the framework for information sharing, they are aware that the threats go cross border and so the solution is to work together, how did we fail to predict the attacks, how were we left in the dark and what should we have done? The urgency of finding these answers and of the EU institutions filling the gaps, has never been more pressing.

Brief Overview in Key EU Member States

United Kingdom has a comprehensive cybersecurity strategy, which was released in 2011, that is complemented by a strong cybersecurity legal framework and two computer emergency response teams (CERTs). Furthermore, the UK also has a well-developed system of public-private

[7] The Global Cyber Crime Underground: Russia and Eastern Europe, LookingGlass Cyber Solutions, 14 April 2016, https://www.lookingglasscyber.com/blog/the-global-cyber-crime-underground-russia-and-eastern-europe/

[8] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[9] ENISA is a European agency established in 2004 (with a renewed mandate in 2008) that has seen its role gradually expanded to become a major actor in the European cyber-security community.

partnerships in which the private sector actively participates.[10]

France has an elaborate strategy on fighting cybercrime (with a strong emphasis on security measures), but lags behind in what concerns public-private partnerships. France has had a national cybersecurity strategy in place since 2011, although it has a strong focus on defence and national security issues. The National Agency for the Security of Information Systems (ANSSI) is a well-established authority dedicated to information security and is integrated with the country's computer emergency response team, CERT-FR. The cybersecurity strategy contains recommendations for closer cooperation with the private sector, but this has not been significantly developed. ANSSI has published sector-specific security measures, making France one of the few EU countries to adopt such a targeted approach to managing cybersecurity.[11]

Germany may be considered the European leader in cybersecurity since it places emphasis both on governmental strategy and private-public partnerships. Germany adopted a comprehensive cybersecurity strategy in 2011 and complemented it by a strong cybersecurity legal framework. The existence of the Federal Office for Information Security (BSI), in charge of managing computer and communication security for the German government, is a clear demonstration that cybersecurity is elevated to a high government level. Furthermore, the country has well-developed public-private partnership**s**, such as the Alliance for Cyber-Security and the UP KRITIS partnership, and its national policies and legal framework reflect this focus on cooperation.[12]

Italy updated its security laws in 2007 and adopted cybersecurity plans in 2013 and 2014, resulting in a strong legal framework supporting cybersecurity. The Italian cybersecurity strategy also calls for public-private partnerships as the intended direction for cybersecurity, but no formalised cooperation yet exists.[13]

1.3. Romania's tough neighbourhood: Eastern Europe

Not unlike its regional counterparts, the European cybercrime underground operates like a legitimate business marketplace, becoming increasingly more commercialized and services oriented. Eastern Europeans and Germans are some of the more active individuals in the European cybercrime eco-system. According to 2015 Interpol findings, Eastern European cybercriminals were among the most sophisticated. Notably, they highlighted the fact that while they may use exploits created by other hackers, they implement customized tools designed for the specific operation. These actors typically work in small teams focused on the projects at hand and are extremely cautious about preserving their anonymity.[14]

1.4.1. Romania - Context

In the current European context, Romania is the ideal launch pad for cyber-attacks against both internal and external targets, due to its internet speed (highest in the EU) and lack of cyber protection (both PCs and networks). The fact that there is no law stating responsibility for the cyber

[10] EU Cybersecurity Dashboard, Business Software Alliance (BSA), http://cybersecurity.bsa.org/assets/PDFs/country_reports/Cs_unitedkingdom.pdft

[11] EU Cybersecurity Dashboard, Business Software Alliance (BSA), http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_france.pdf

[12] EU Cybersecurity Dashboard, Business Software Alliance (BSA), http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf

[13] EU Cybersecurity Dashboard, Business Software Alliance (BSA), http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_italy.pdf

[14] The Global Cyber Crime Underground: Russia and Eastern Europe, LookingGlass Cyber Solutions, 14 April 2016, https://www.lookingglasscyber.com/blog/the-global-cyber-crime-underground-russia-and-eastern-europe/

infrastructure owned by private entities, transforms the national infrastructure's capabilities in real disadvantages in terms of cyber security at a local, regional and global level.

Current status of cyber security incidents in Romania:[15]

- 8% of the alerts processed by CERT-RO in 2015 occurred in vulnerable systems, meaning servers exposed to the internet, badly configured, not updated and used as a transit point during the attack.

- 21% of the alerts are malware. If a hacker wants to build a botnet network, he/she will choose victims in Romania, in the same context of technical high performance. Once the "host" got all set up on Romanian serves there is no stop in launching attacks and illegal activities on behalf of the infrastructure in Romania.

- According to CERT-RO, starting with the end of 2015, there was a spike in attacks targeted at Romanian local public authorities. The most frequent types of incidents are: compromised websites due to out of date and vulnerable platforms, work stations infected with different types of malware, especially ransomware.

- Cyber-attacks with a high level of complexity and threat, those in the Advanced Persistent Threat category, will increasingly manifest by identifying and exploiting new vulnerabilities in the systems of the targeted institutions, both public and private;
- Generally, public institutions are greatly affected by the lack of cyber security experts. Thus, IT systems are often times badly configured and poorly secured when compared to the existing threats.

Rising the cyber security level has been given a high priority. To this end, the following are considered:

- a joint public-private cyber exercise;

- the creation of a Cyber Security Innovation Centre;

- increasing the cyber security of local institutions' cyber infrastructure;

- starting CERT-RO's project regarding the extension of the early warning and real time monitoring system;

- educating high school students in the area of cyber security and online safety;

- drafting and approving the minimum criteria a CERT-type institution has to meet in order to be included in the Romanian CERT community;

- drafting and approving a public policy regarding the responsible disclosure of vulnerabilities.

1.4.2. The Cyber Security Law

The Romanian Cyber Security Law has come a long and difficult road through politics, NGOs' views on security and public analysts. It is an example of a good idea badly implemented and publicised. The Cyber Security law was one of the three "Big Brother Laws", a package, deemed unconstitutional. The first one mandated that phone and internet providers were to keep for six months their users' technical data whereas the second one required

[15] Report on the cybersecurity alerts processed by CERT-RO in 2015, CERT-RO, https://www.cert-ro.eu/files/doc/1068_20160411140422094789700_X.pdf

phone carriers to ask for and keep the personal data of those using pre-paid SIMs and pubic WI-FIs.

It is the authorities' second try to pass the law through Parliament, first in 2014 and again in 2015, the Romanian Intelligence Service (SRI) tried to single-handedly push the law through.

SRI's error delayed in an unreasonable manner the public debate and then Parliament's approval of a set of laws which were designed to tackle risks and threats, create a national framework of cooperation between the relevant institutions and the private sector, and strengthen the capacity to react to cyber incidents.

Despite both MCSI's and SRI's assurances that the law had nothing to do with privacy, the publicity generated lengthened the shelve life of vehement rhetoric. There are multiple reasons for this, all coming from the post-communism trauma still well alive in Romania. There is a fear going on, a type of urban legend of illegal intercepts of whomever, whenever. Media organisations, NGOs and opinion leaders keep alive the idea that the "system" is illegally listening, that intercepts are carried out without a warrant and at politicians' whim, and that the secret services act as they wish, being a state in a state.

The generalized fear is based on two developments. First, the current trend of a series of intercepts leaked to the media from prosecutors' cases. Second, the weight attached untill recently to the intercepts as necessary and sufficient proof in court. There have been quite a few cases when high ranking politicians accused the anticorruption institutions and the intelligence organisations which were doing the operative work, of doing less of their jobs and more that of a political police.

By politicizing the role and importance of the intelligence services, these institutions were demonised, at a time when the hot topics on the international agenda are hybrid war and the threats posed by terrorism.

The controversies over the cyber law package, highlight three issues, still very much current:

1. The weak security culture in the media, and of both opinion leaders and decision makers, politicians with limited terms in office and little appetite for deepening their understanding of new security concepts.
2. The way in which by politicizing an issue, rivalries are heightened whereas joint efforts towards initiatives of national interest are weakened.
3. Citizens' lack of trust in the security institutions and their initiatives.

For this reason, in the latest draft of the Cyber Security Law, important corrections were made regarding the judge's warrant in investigating cyber security incidents:

- Private data necessary for specific activities will be accessed only with a court order.
- When activities thought to be indicative of a cybercrime are identified, the prosecutor's office shall be notified.
- The system's oversight was changed from the military (SRI) to the civilian (MCSI).

In terms of public image, an important step was to split the public debate along the lines of each of the "Big Brother" laws. It is a good sign the fact that the government promoted separately the Cyber Security Law and allowed for two public debate sessions.

A key pillar in promoting the Cyber Security Law was to promote the idea that it is NOT targeting the individual user but national entities, owners of personal data or data relating to the national security infrastructure. By strongly addressing this issue, the frequency with which the law was accused of meddling into the private life was decreased.

2. Advice for Key Decision Makers

Article 19 of the International Covenant on Civil and Political Rights states the freedom of expression, under different forms and manifestations. One could argue that the internet has become an indispensable tool for our freedom of expression. Thus, we could argue that the online freedom of expression is guaranteed. And if we add the fact that an increasingly larger part of our lives is dependent on the internet, we could also argue that **the right to be connected, in other words the right to the internet, must be guaranteed.**

When horrific events occur impacting the lives of many, there is a natural reaction to do something to try to prevent future occurrences. Too often, the "something" (legislation) incurs unwanted consequences to go along with the intended result. This is the case with various proposed regulations governing cybersecurity. While the intent to protect from attack is apparent, regulations must keep in mind the bigger picture.

2.1. Motivation: Why?

When it comes to the cyber space, restrictions cannot be imposed over the internet as a whole. The cyber space is a system and thus not controlled by any one institution, so the only restrictions which can be imposed refers to the effects of this space and the effects of the relationships in this space. In the end, these restrictions can only be imposed on the physical dimension. Thus, a state can geo block access to some information, by itself or by having internet service providers do it. Even so, that information is blocked, not erased from the internet and it continues to be accessed by other users.

When drawing up a policy, the government has to clarify the objective of said policy. When it comes to cyber security laws, the stated objective is to protect the integrity of internet infrastructure and of data hosted and transiting said infrastructure. This objective is fair and worthy.

In the case of Internet policy implementation there are some clear implementation mechanisms: The Law, Social Norms, the Market and Architecture which have to work together.[16]

Furthermore, policy makers have to take into consideration the existing legal and social context. Internet and technology are part of the status-quo and the way people use it can be considered as part of the current legal and social context. This is because people developed habits and have expectations when interacting with Internet technology.

Thus, Internet policies have to use law, social norms, the market and architecture to secure connections and data while not affecting the current way people express themselves and communicate on the web.

In order for limitations to be perceived as reasonable and their implementation possible, states have to make sure these limitations are according to the principles of legality (anything not forbidden is allowed), legitimacy (the belief that authorities, institutions and social agreements are adequate, appropriate and fair) and proportionality (the equilibrium between what is being imposed and the value to be defended by the imposition).

2.2. Means: How?

Governments should enact and keep up-to-date a comprehensive legal and policy framework, based on a solid national cybersecurity strategy, built upon the following key principles.

1. **Risk-based and prioritized**: Cyber-threats come in many shapes and magnitudes with varying degrees of severity. Establishing a hierarchy of priorities — based on an objective

[16] Regulating the Internet, 19 February 2015, http://mysmartcity.ro/en/regulating-the-internet/

assessment of risk — with critical assets and/or critical sectors at the top.

2. **Technology-neutral**: A technology-neutral approach to cybersecurity protection will allow security controls and best practices to evolve and keep up with the evolving threats.
3. **Practicable**: Any strategy is only as effective as it is adoptable by the largest possible group of critical assets and implementable across the broadest range of critical actors. Overly burdensome government supervision of private operators, or disproportionately intrusive regulatory intervention in their operational management of cybersecurity risk would most often prove counterproductive, diverting resources from effective and scalable protection to fragmented administrative compliance.
4. **Flexible**: Managing cyber risk is a cross-disciplinary function and no one-size-fits-all approach exists. Each industry, system and business faces distinct challenges, and the range of actors must have flexibility to address their unique needs.
5. **Respectful of privacy and civil liberties**: Security requirements should be duly balanced with the need for protection of privacy and civil liberties. Ensuring that requirements and obligations are proportionate, do not represent more intrusion in fundamental rights than what is strictly necessary, follow due process and are supported by adequate judicial oversight are all important considerations to address in any cybersecurity framework.
6. **Partnering with the private sector:** Most infrastructure is owned by the private sector, making effective public-private cooperation essential. Cooperation also improves the effectiveness of risk management by improving the sharing of information, experience and perspective of multiple sources. Particular efforts are needed to foster trust and avoid legal obstacles that may hinder it.
7. **Global rather than isolated**: Given that cyber threats are global, effective cybersecurity policies and strategies need to maintain an international outlook, building on joint efforts with partners and allies. They should also leverage international, voluntary and market-driven standards in order to maximise pan-regional and global information sharing and protection.
8. **Foster Education and Awareness about Cybersecurity Risk:** Awareness raising, education and training about clearly articulated cybersecurity priorities, principles, policies, processes and programs are essential components of any cybersecurity strategy.
9. **Establishing an appropriate framework for meaningful information sharing:** Cybersecurity incidents or breaches can have a major impact on governments, private entities, as well as individuals. The exchange and sharing of the appropriate information at the right time — and the coordinated effort among relevant actors it enables — is considered the best way to reduce and mitigate risks and respond to cyber incidents.

Accordingly, the key question is how to best achieve meaningful and effective information sharing among relevant stakeholders. While some countries have considered mandatory incident notification systems, these alone would not suffice to address the issue of collective awareness and preparedness. When it comes to that, voluntary information exchanges based on trust have proved to be the most efficient way to achieve successful information sharing. Some of the fundamentals of such an environment are the following:

- **Create an environment of trust**: Information sharing, as well as incident reporting, require safeguards and incentives.
- **Ensure a high level of confidentiality**: Given the sensitive

nature of the information shared about an incident or cyber threat affecting any critical infrastructure, it is crucial to ensure that confidentiality and security of the communications between the infrastructure operator and any supervisory authorities are respected and maintained, subject to transparent reporting by the authority, as appropriate.

- **Ensure an in-depth dialogue** between the entities suffering a breach and the authorities before any disclosure in order to avoid increasing the attack footprint, multiplying the impact of the incident, creating panic, or leading to undue public shaming.
- **Ensure reciprocity**: While the private sector owns and operates much of the countries' critical infrastructure, information sharing should not be seen as a one-way provision of relevant data from private to public entities. It should be regarded as a real and mutual exchange of information, based on trust and mutual benefits.
- **Make requirements clear and consistent across jurisdictions**: As mandatory notification requirements cover an ever-increasing number of areas and geographies, the likelihood of facing conflicting legal obligations increases. As various organizations operate in multiple sectors across different countries and regions, the questions of what to report when and to whom already pose important compliance challenges. Therefore, to the extent a mandatory notification system should be introduced, it is imperative to strive for as much consistency as possible not only among the different notification obligations, but also among the various national and regional requirements.
- **Clearly define the terms** on cyber threats and their standardization in the context of a similar and uniform interpretation (across institutions), potentially by creating an international standardized language of cyber security.
- **Harmonize the provisions and principles** of the cyber security laws with those of the national laws (constitution) and official documents (national strategy).
- As technology evolves, its effects and usage must be understood so that it can be properly regulated. Thus, **new research** should be encouraged on: encryption; group behaviour psychology; social engineering and development studies on the evolution of new technologies in relation to attitudes and dialogue with citizens.

Annex

Terms

The following terms and concepts appear throughout the report. For a better understanding we provide here their definition, as they are seen by Strategikon's rapporteurs in the context discussed. A distinction is made between "conceptual" terms and "technical" ones. The former need defining due to their broad meaning and sometimes misleading usage. The latter need defining for a non-IT specialist's understanding.

Conceptual terms

- **Culture of security =** the general population's understanding of the threats it faces when using cyber devices and services and ownership of the ways and means of cyber protection. A culture of security is a means of achieving proper use of information, increase transparency and trust in IT systems and cyber regulation, and ease compliance with laws and regulations.
- **Cyber infrastructure owned by private entities =** assets, systems, and networks, physical (servers) or virtual (the internet), providing essential services to a considerable number of people. The infrastructure is owned by private entities but regulated by the state due to the magnitude of its possible disruption.
- **Cyber rights and liberties =** unrestricted and secure usage of cyber infrastructure, the guaranteed freedom of speech, access to information, and privacy, when accessing cyber infrastructure.
- **Cyber protection =** methods of assuring a safe usage of cyber devices and services, either through IT means (software) or laws and regulations (cyber security law).
- **Cyber security law =** a regulation accepted by the society as fairly and legally imposing restrictions on its rights and liberties in order to assure its safe usage of cyber devices and services.
- **Information sharing mechanisms =** public-private partnerships creating transparent and safe protocols aimed at informing each other on threats and acting together on risk mitigation, threat assessment, intervention, and prevention.
- **Personal data =** piece of information that can identify a person, either by itself or by corroborating it with other pieces of information.
- **"Securitate" =** secret police agency of Communist Romania.

Technical terms

- **Malware =** a variety of forms of hostile or intrusive software
- **Remote Access Trojans (RATs) =** software which once on a computer gives access to a hacker information or to install other malicious software
- **Ransomware =** malware restricting access to the infected system for ransom.
- **APT – Advanced Persistent Threat =** a set of stealthy and continuous cyberattacks, often targeting a specific entity.
- **Phishing =** attempt to acquire sensitive information (usernames, passwords, credit card details) by posing as a trustworthy entity in an electronic communication.
- **DoS attack =** an attempt to make a machine or network resource unavailable to its intended users

- **Distributed Denial of Service (DDOS) =** infected systems, used to target a single system causing a Denial of Service (DoS) attack.
- **Botnet =** interconnected computers infected with malware without the user's knowledge and controlled by cybercriminals

About the Authors:

Bebe-Viorel Ionică is an IT systems specialist. He served as Secretary of State in the Ministry of Communications and Informational Society where he was in charge with the overall direction, coordination, and supervision of ICT activities

Claudiu Săftoiu is a communication and political campaigns specialist. He served as Director of the Foreign Intelligence Service and as Adviser to the Romanian President, on domestic political issues.

Corneliu Vișoianu is a PhD candidate at the National Defence University and former Advisor to the Prime Minister. Currently, he serves as Strategikon Vice-President.

Denis Kurunczi is a law graduate with expertise on government and civil rights and liberties. He serves as Legal Adviser for the National Institute for Research and Development in Informatics.

Filofteia Repez is an Associate Professor within the Security and Defense Faculty of the National Defense University where she teaches joint operations, national and Euro-Atlantic security, political-military doctrine, and strategic studies.

Florin Necula serves as Counselor to the Ministry of Economy, Commerce and Relations with the Business Environment. Previously, he served as Counselor to the Ministry of Communications and Informational Society

Gabriel Mihăilescu is a senior IT professional with experience in system administration and strategy development and implementation. Prior to joining the Ministry of Foreign Affairs' IT Department he served as Informatics Site Head for Roche Romania.

Mădălina Neacșu is President and Founder of AGROINTELLIGENCE, the Information System on Food Security Program. She is an expert on international security and regulation.

Mihai Popa is a corporate law expert, with expertise on compliance practices, international and European law, and corporate compliance regulations and contracts.

About the report:

This Strategikon report reflects only the views of its authors. Copyright of this publication is held by Strategikon. You may not copy, reproduce, republish or circulate in any way the content from this publication except for your own personal and non-commercial use. Any other use requires the prior written permission of the Strategikon team (www.strategikon.ro). We welcome feedback on our reports: please send us your comments, improvement ideas as well as criticism, to office@strategikon.ro.