Asociace pro mezinárodní otázky
Association for International Affairs

Briefing Paper 1/2014

Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge

–

April 2014

Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge

–

Tomáš Rezek

April 2014

The paper was prepared for the International Conference "Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge" held in Prague, Czech Republic, on May 28-29, 2014. The conference has been supported by the Ministry of Foreign Affairs of the Czech Republic.

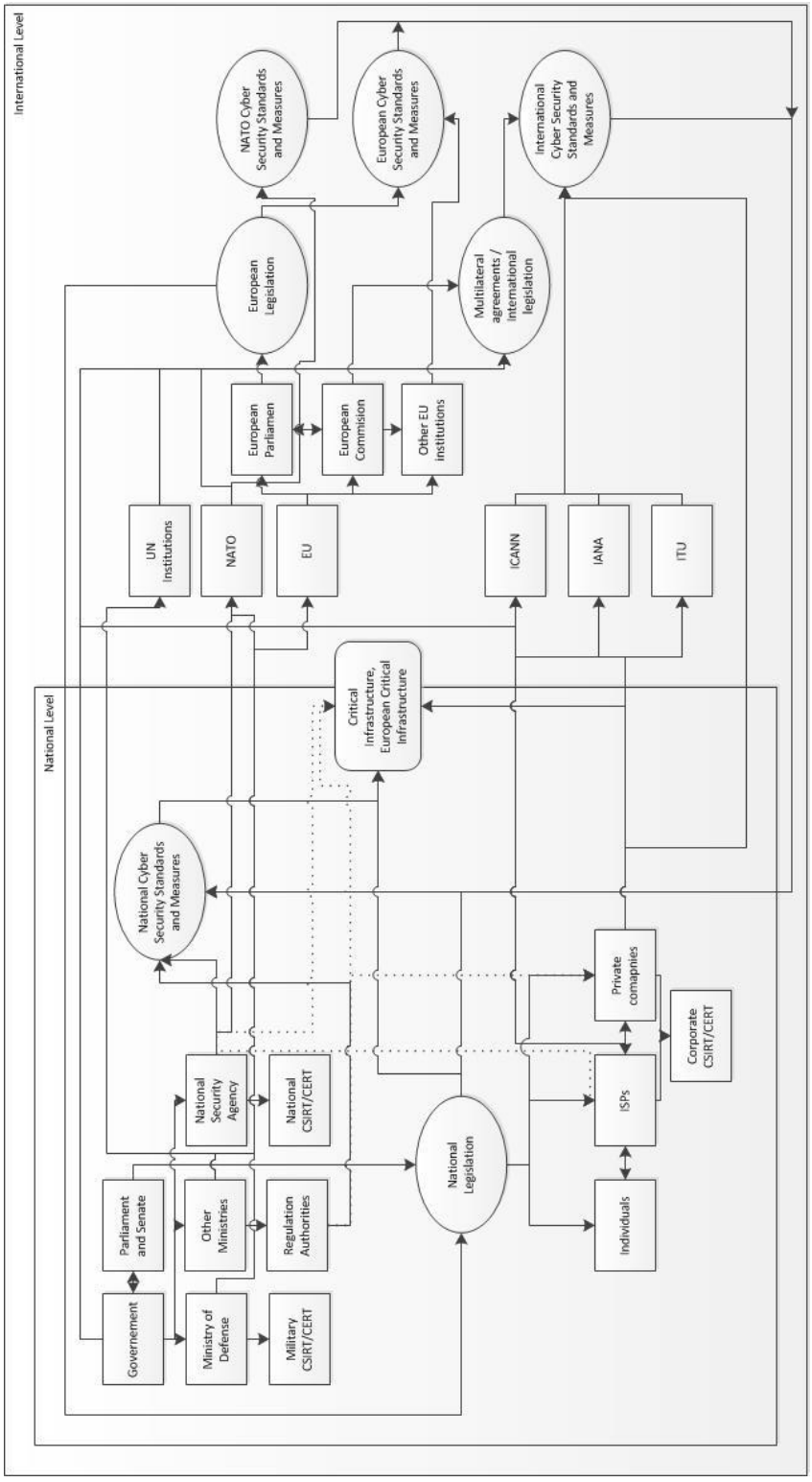
Ministry of Foreign Affairs of the Czech Republic

Introduction

The aim of this paper is to provide basic information on the four main topics that will be discussed during the International Conference **"Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge"**. Each of the four section focuses on one particular topic of one conference panel. It states basic definition and puts the topic into geopolitical circumstances in order to highlight the significance of given topic and the need for its discussion on an international level. Every chapter states some of the questions we would like to raise during the conference. These questions and subtopics are mentioned in order to initiate further discussion during the conference and possibly to help thematically shape contributions of invited panellists.

The cyber space is the only man made dimension where social, economic and political interactions take place. The increase in number and in volume of these interactions only highlights the need for international consensus on basic definitions. This first step will then allow more efficient governance of this domain both on national and global level. Unfortunately, the number of stakeholders related to the interactions taking place in the cyber space and to the modern technologies is very high. Therefore universally acceptable approach to the cyber security or Internet governance is possible only after intense negotiations on all levels. We are convinced that this conference is an excellent opportunity to exchange opinions and ideas on some of the important issues related to the cyber space and to the cyber security on the international level and more importantly also among public and private sector. Following chart picture illustrates the diversity of subjects taking part in the interactions in the cyber space; it also demonstrates the complexity of the topic:

Figure 1. Overview of stakeholders involved in the cyber space and relations among them



I. Internet regulation

I.1 Definition

The regulation of the Internet is a very sensitive topic, despite the fact that the understanding of this term significantly differs country from country. Since the Internet has become another domain for social and economic life in many countries across the globe it is no wonder that national authorities introduced the regulation of the Internet. The appropriateness of this term depends on the national approach to this problem, because national authorities regulate rather the access to the online content or behaviour of subjects in the online domain. Gartner study The Future of the Internet published in 2012 cites three main forces shaping the future of the Internet – the drive for profit, the desire for freedom and the demand for control. The study also mentions three elements of the Internet and the World Wide Web that are affected by the main forces – access, transport of data and content. Regulation of the Internet may affect all three elements and may arise from all three forces. Regulation based on the intention to increase the control of state authorities over the national cyber space domain and over domestic subjects is clear. But the regulation of the Internet may be based on the drive to maximize profits. Private companies might be motivated to provide access, particular content or services only on the basis of the customer – provider relationship. Private subjects may also push national authorities to increase the protection of their intellectual and property rights in the cyber space to increase their profits as well. Regulation of the Internet motivated by freedom would probably be reduced only into a form of control over particular subjects to ensure that the freedom is absolute.

Figure 2. Forces shaping the Internet and possible scenarios, Gartner Study on the Future of the Internet, 2012

The regulation aimed at content can be described as a censorship. This form of regulation is very common and it takes place in majority of countries. However, it is one of the most discussed aspects of Internet regulation in certain countries. The problematic aspect is the definition of illegal content. In many countries this regulation is restricted to children pornography or to propagation of extremism. But some countries apply broader definition, for instance banning content injuring the reputation of state institutions or inciting to overthrow the government. This kind of regulation applies to users and ISPs. Depending on the respective legislation, users might by prosecuted for trying to access illegal content as defined by the national legislation. The ISPs may be required by national authorities to cooperate on different levels to ensure the execution of the legislation. This cooperation might be in form of providing user's personal data, participating at the content filtering or removing the content. The involvement of private sector in this form of regulation depends on particular conditions on the local Telco market and infrastructure.

It is important to distinguish between the regulation focused on access and content. If the user is prevented from accessing particular site, e.g. Facebook, it is still a regulation of content. Only when particular user is denied the access to the Internet itself it is the regulation of access. The regulation of access has to overcome one significant obstacle – the attribution in the cyber space. Identification of a user in the cyber space is different from the identification of the individual. This kind of regulation requires extensive control and identity management regarding the access to the Internet. It also puts lot of responsibility on the companies providing access to the Internet as they have to provide necessary information about users to responsible authorities.

Regulation of data transport means control and potential regulation of data packets carrying the information over the Internet. Another option is the focus on the sides participating at the data transport. This means control and regulation of domain names (DNS) and IP addresses. There is a political pressure to keep the control over DNS and IP addresses independent, possibly under the supervision of U.N. Regulation of transport is more complicated than other forms of regulation.

I.2 Reasons for regulation

Certain level of regulation of the Internet is necessary. The main reason is that it is necessary to execute minimal level of regulation to ensure that basic human rights are respected. Another reason for certain level of regulation and control over the Internet is the fact that legislation valid in physical world can be used in the cyber space as well. Therefore it is necessary to enable the enforcement of law in regards to the cyber space. Let us presume that respecting basic human rights requires basic level of Internet regulation. This kind of regulation would probably consist of content control (e.g. racist content).

Another level of regulation is based on the premise that the regulation and control is necessary to grant national security. Increase in online surveillance and in the usage of personal data obtained from ISPs occurred due to terrorist attacks in 2001. Implemented security measures differ country to country, but in general related legislation enabled responsible authorities to monitor the Internet users. Surprisingly, the influence of these measures over the content has not been substantial. Nevertheless, the usage of personal and sensitive data from the cyber space by national security agencies in certain countries highlighted the fact that anonymity in the cyberspace is a myth.

National security is very often used as a pretext to execute regulation of the content and intense control over the users in order to strengthen the position of current establishment. It is difficult to alter this situation in countries where such approach is supported by valid legislation and democratic processes that could possibly change current situation are not applicable.

I.3 Problematic aspects of regulation

Boarders in the cyber space

There are no boarders in the cyber space. This important feature of the cyber space has been changing over the past years. National authorities have begun to execute regulation of the content in different ways. We are witnessing the creation of boarders in the cyber space based on the argument that national authorities have to protect national interests also in the cyber space. This regulation usually applies to legal and physical entities of given state being active in the cyber space and also users from this state. The definition of user applies to an individual accessing the cyber space from the physical location within boarders of given state, but it might be more sophisticated. Despite the legislation this regulation results in regulation of content provided by local subjects or branches. Another level is filtering the content accessible from the state, but being under jurisdiction of different state.

Creating boarders in the cyber space is sometimes motivated by financial profits. Users accessing the content from different state are obliged to pay certain fee for the access. In some cases boarders are set up to protect intellectual property rights. More interesting is the usage of boarders in the cyber space as a mean of foreign policy. Global sharing of information is one of the main benefits of the Internet. But on the national level it might be decided that from political reasons that certain information shall not be accessible from particular countries.

Role of ISPs in regulation

The role of private companies in any regulation is usually passive. National authority observes the obedience of the law and prosecutes potential violations. However, the situation is different in the case of cyber space regulation. National authorities in general do not have enough resources to execute the control. Of course that there are exceptions, but the state of national ICT industry and infrastructure in many countries does not allow to national authorities to execute the control. Private companies, particularly ISPs, are in some cases obliged not only to obey the law and refrain from posting illegal content, but they have to proactively participate at the regulation. ISPs in some countries are required to identify illegal content and delete it, or to block access to such content. This trend suggests that private companies are gaining the authority to decide which content is illegal. This is a very interesting precedent as such authority has been always granted only to courts.

Technical limits of regulation

Regulation of any form in the cyber space differs from the regulation in the physical world. Firstly, the time needed for a user to post or access a piece of information in the cyber space is only a fraction of the time needed for such action in the real world. Secondly, the nature of the internet allows users to search or post the information on a global level. Thirdly, the evolution speed of the Internet and of the information accessible online is incomparable to the physical world. New information is created or accessed every second. All this features of the cyber space make the regulation very difficult. Because of the speed, it has to be largely automated. But automation becomes obsolete and might have flaws which can be used by users to sneak past the regulatory measures. The pursuit of "perfect regulation" in some countries requires enormous effort, but the results are rather temporary.

Perception of regulation

It is actually very interesting how big response the regulation of cyber space receives. It is generally known that certain countries perceive the regulation of the cyber space in a more strict way. But this attitude towards regulation of the cyber space in these countries does not differ from other forms of regulation existing in the physical world. For instance the censorship of online content depicting nudity from religious reasons receives attention of media across the globe, albeit for a short time. However, the fact that same regulation is applied in broadcast and print is not mentioned. Similar situation applies to human rights. The fact that access to the Internet is regarded as a basic human right shifts the focus from off line problems with human rights in some countries. The reason might be that online content is global and therefore the situation or problem is easy to imagine, but it is important not to forget about other less virtual dimensions.

I.4 Questions for the conference panel

Certain level of regulation in the cyber space is inevitable in order to preserve basic human rights and freedoms. However, the attitude of particular states towards this regulation significantly differs. Discrepancies in taken measures create borders in the cyber space. Users cannot access certain content or the content is changed to comply with current legislation. Are EU member states coherent in their policies towards cyberspace so the "EU cyber space" is still without boarders? Is the future of the Internet impossible without national boarders? Should there be something like "international waters" in the cyber space?

Different legislation puts private companies, particularly ISPs into new role of collaborates with national authorities. In some cases they get also new powers. Is this trend dangerous? Should states invest more into national authorities to maintain their ability to control law obedience or will this "outsourcing" continue?

Regulation and control over the cyber space requires investments into equipment and skilled employees. Will states in the pursuit of efficient regulation disregard their budget constraints? Will the rapid development of the ICTs pose such a big threat to national authorities and to their task to control and regulate the national cyber space that stricter legislation will be issued to ease the job for national authorities?

Cyber space seems to be without boarder and universally accessible. However, the truth is different. Any governmental actions related to the regulation of the Internet incite reaction from media and citizens on a global level. How come that those more important issues related to human rights and freedoms fail to interest the same audience?

I.5 Topics for discussion

- Censorship of online content
- Private companies and their role in the regulation of the Internet
- Regulation or anarchy?
- National boarders in the cyber space
- Technical limits of regulation
- Regulation and its costs
- Future of the Internet governance
- Regulation of the Internet and human rights
- NETmundial conference and its implications
- ICANN and national interests

II. Internet and law

Internet and cyber space are a new dimension in which social, economic and political interaction takes place. These interactions have been increasing not only in number, but also in the importance with regard to national economy and social life. Cyber space and Internet have to be regulated consistently with other dimension where similar interactions take place. The general approach is that valid legislation can be applied to Internet and cyber space. But the cyberspace and the Internet have their particular characteristics which make the application of standard law more complicated and even influence the legal principles which have been unchanged for many years.

II.1 Basic problems

One of the basic problems related to the application of current legislation on cyber related issues is the legislative process itself. Even if the intention of national authorities is to introduce new laws or amendments to existing legislation, this process takes lot of time. In the Czech Republic, this process involves the creation of a draft that has to be discussed in the Parliament in several rounds, then accepted and submitted to the Senate for discussion. After acceptance in the Senate the future law must be signed by the President and then published in the law collection. Even if the process is smooth it can take months. The situation might be different in some countries, but the general problem is that the evolution of ICTs and the cyber space is much faster than the ability of national authorities to analyse and address these changes.

This is also one of the reasons why current legislation is applied – to create new legislation addressing only cyber space would take too much time. But the application of current legislation on cyber related issues or relations create problems. It might be gaps in terms of new type of entity or subject present in relations among subjects in the cyber space or simply the problem of definitions. In such cases the application of the law by particular judge is crucial. The problem is that if there is no official explanation of the law for similar case from the Supreme Court, the verdicts of individual judges may differ in the Czech Republic. Of course that there are legal remedies when one of the sides feels injured by the verdict. But again this process takes a lot of time. The average length of the first instance trial related to commercial relations in the Czech Republic is one year. Waiting couple of years for a verdict in such a dynamic environment as the cyber space is can be lethal for small and medium companies. However, it is important to highlight the fact that this situation in some countries is simply derived from the current situation in the justice.

Number of parties involved in commercial relationship in the cyber space can be very complex. Apart from specific role of Internet Service Providers (ISPs), there can be very

specific relations related to cloud computing or other special services, for which there is no analogy within the physical world. The application of legislation might be problematic in such cases. Identification of the parties involved in the relationship can be also complicated. The chain may involve web hosting companies from abroad, virtual servers and online companies registered abroad. One problem might be identifying the actual legal entities and physical individuals involved in particular relationship in the cyber space, because of the attribution problem. The court jurisdiction can be also tricky as the cyber space seems to be borderless. These aspects of the cyber space might worsen the enforceability of the law and decrease the trust in the cyber space.

II.2 Sensitive data

The evolution of the cyber space and of the modern technologies has changed the perception of privacy. The former perception of privacy focused on the right not to be surveyed in the physical world and to be undisturbed in home and other private locations. Even this perception changed as increased surveillance in public spaces was introduced in reaction to the threat of terrorism. But there is virtually no safe haven in the cyber space, at least not for an average user. The activity of an every Internet user is logged by a browser or by an ISP. Visited web pages also collect data about users who accessed them, their history, settings and other data from cookies data. Users in general voluntarily or unknowingly provide their data in exchange for a service. It might be the service in a form of web search, customized commercials or even a discount. The number of users trying to avoid providing their data is still low. The volume of this kind of data is increasing in proportion to new ways of using the cyber space. Given the fact that also capabilities to analyse this data increased substantially, the value of this data increased, at least for interested companies. But has the value increased also for the users? This data can be compared to a surveillance report in the physical world – it lists every movement in the cyber space. Should the users be protected from companies using their data? Who is actually the owner of the data, if the data were created by visited website? Is there any control that this data are not abused? Of course, users can make the choice not to use particular web browser or webpage or even not to use the Internet. But is this still an option?

Cyber space does not contain only the data about out virtual activities. Increased connectivity of tools provided manufacturers and other companies with large amount of data about the users. We can take for an example the GPS functionality of Smartphones. It tells you where you are, if you want to know. But it also tells the service provider where the phone is, even if you do not want to. Who is the owner of this data? Can the owner of the phone make any decisions regarding the usage of this data? Should the usage of this data be retrained by a law?

All the data related to the usage of the cyber space practically removes the anonymity from the Internet and the cyber space in general. How important is the anonymity for the Internet and potentially for the democratization processes in some countries?

II.3 Internet freedom and basic human rights

The relation between the cyber space and the law has a very strong international aspect. Let us now forget the application of national legislation in regards to foreign subjects as we will focus on the international law itself. Group of states recently achieved a great success on the grounds of UN. The resolution of the Human Rights Council put the online human rights on the same level as the more common "offline" option. This can be regarded as a success in a certain way. But the resolution itself does not change anything for states where human rights are not respected. It is true that this resolution makes a difference in cases where the country is going through difficult political situation and the right on freedom of speech is often violated in the cyber space. Still, what difference will this resolution make in such situations?

In some EU countries the access to the Internet is regarded as one of the basic human rights. Nevertheless, this right cannot be spread to other countries without necessary infrastructure. However, the question itself remains the same – should be the access to the Internet regarded as a basic human right? In this case it is necessary to mention the influence of the boarders in the cyber space – should the access to the Internet and to the information be based on the location of the user? The freedom of the Internet is often stated as a necessary part of a democratic process helping to develop political awareness of citizens. On the other hand some states argue that it is only a tool of foreign policy serving national interests – they proclaim freedom of the Internet in foreign relations, but execute strong regulation on the national level.

II.4 Transition of power

The usage of modern technologies in the cyber space increased the number of subjects involved in commercial and other relations in this virtual domain. So has increased the number of such relations. The increase in volume of the virtual life and relations creates pressure on national authorities in terms of supervision and law enforceability. Police and other responsible national authorities are supposed to keep up the pace of the cyber space development, but this is not happening. The spontaneous process in the cyber space is much faster than rather a rigid evolution in the public sector. Despite indisputable progress in the public sector, there are still important gaps that make the cyber space safer for criminal activities than the physical world. One of the reasons is the mere size. The volume of transactions realized in the cyber space is rising every day. The same counts for the size of the content available in the national cyber space. National authorities can hardly monitor all

such activities and efficiently fight cybercrime. One possible approach is to involve private sector into the process. ISPs and other subjects may become more responsible. Sometimes it is impossible to reveal the identity of the author of illegal content, but it is much easier to identify the provider of the service, as in the Megaupload case[1]. This step makes the ISPs more responsible, but it also shifts the power in the direction of private companies. If the ISP is going to be held responsible for the illegal content it holds, the ISP will monitor the content and will decide what content is illegal in order to prevent any possible trials in the future. Users can defend against such actions in the court, but is this a desirable direction?

II.5 Questions for the conference panel

The development of the Internet and related services has created a pressure on current legislation in many countries. It resulted into a temporary period of instability when needed amendments were being prepared. We can say that this period is over and that current legislation and the explanation of the law with regard to the cyber space significantly improved. But another step is to improve the enforceability of the law in the cyber space. Probably the most important step is going to be to keep the legislation up to date with the rapid evolution of the cyber space and related services. The process of law application on the cyber space has raised some important questions discussed above. Answers to these questions should help us to better understand the complexity of the cyber space and the need for improvement of the current legislation. The increase in importance of the cyber space might require a dedicated authority to oversee the application of the law, for instance an ombudsman for the cyber domain.

II.6 Topics for discussion

- Current legislation and cyber space
- Cyber crime
- Anonymity in the cyber space
- Private data and sensitive information in the cyber space
- Customer protection and free services
- Freedom of the Internet – political tool or necessity?
- Human rights in the cyber space
- Law enforceability in the cyber space
- Private companies and legal obligations
- Transition of power to private companies

[1] Famous file-hosting site Megaupload.com was closed by the US Department of Justice in 2012 on the basis of legal actions against the owner and other individuals. The case was based on the illegal content shared by the users of the service using this site without any restraints from the administrators.

III. Safeguarding critical infrastructure

III.1 Definition

Definition of the critical infrastructure by the Commission of the EU is as follows: "Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens."

This definition is also accompanied by instructions how to identify the critical infrastructure in the EU. These instructions were introduced in the Directive on the European Critical Infrastructure in 2008. This directive also distinguishes between the critical infrastructure and the European critical infrastructure (ECI). The ECI has to have an important role for at least two member states of the EU. Apart from the instructions how to identify the ECI and the critical infrastructure, the directive from 2008 strongly emphasizes the need to communicate with other states especially in regard to the ECI. The identification of all parts of critical infrastructure is necessary for increased protection, security and stability both on the national and the EU level. It is the responsibility of every state to identify its critical infrastructure and ensure adequate level of protection. However, there is no control mechanism on the EU level. If any state declares that there are none of ECIs within its borders, it is virtually impossible for other states to prove this statement wrong, unless some serious accident with foreign consequences happens.

III.2 Identification of critical infrastructure

The identification of critical infrastructure is the first step in the process of securing stability and security both on the national and international level. However, it is important to highlight the fact that also the understanding of critical infrastructure is evolving in the time; therefore the list of critical infrastructure has to be regularly revised. One of the reasons is the definition itself – essential for the maintenance of vital societal functions. Of course, that the vital societal functions remain relatively stable, but the rapid development of the society in relation to the cyber space influences the perception of vital societal functions. The ultimate question is, whether national authorities successfully manage to include this evolution of the society into the process of critical infrastructure identification.

III.3 Cyber aspects of critical infrastructure

Cyber space and modern technologies have influenced whole society in all aspects, especially in developed countries. Critical infrastructure has been also influenced in several

aspects by the rise of the cyber space and modern technologies. ICTs and other technologies enabled an increase in the efficiency in many industries, including energy. Given the fact that at least nuclear power plants and transmission network are usually part of national critical infrastructure, the cyber aspect in the critical infrastructure is indisputable.

The first aspect is the systems used for running the critical infrastructure. These critical infrastructure systems have to be coherent with special security requirements, as discussed below.

The second aspect is based on the usage of cyber space and modern technologies as a part of standard procedures to monitor the activity of critical infrastructure or to manage its functions. In other words, critical infrastructure is dependent on its special systems, but also on the cyber space that is used to access such systems. For example, if very specialized and secured system running a gas pipeline is accessed via Internet, the inability to access the Internet or crucial login page is a risk and dependency. Similar dependencies can become very dangerous if there is no emergency workaround or a backup solution not relying on similar technologies.

Another form of the cyber aspect in the critical infrastructure is the intersection of the physical and virtual world. In some cases the physical protection of critical infrastructure is not enough. Cyber security of critical systems comes in mind, but there is still one missing part. It is the physical protection of infrastructure running the critical systems. Physical protection of a power plant is the basic level. Recent development introduced also the necessity to protect the systems running the power plant both in the cyber space and in the physical world.

Critical infrastructure systems

Systems used in critical infrastructure are a vital part. The facility or network would not be operable on the same level without such systems. Therefore security requirements concerning these systems are more strict that in public institutions or other facilities. Systems have to resists not only cyber attack from outside of the facility, but have to be reliable and remain operational even during extreme situations. In some cases, public authorities or private companies prefer to use over the shelf solutions with minimal customizations in order to minimize the costs. But such solutions can be vulnerable to the same cyber attacks as ordinary PCs. But the fundamental question is if responsible authorities are aware of the relation between critical infrastructure and its system and the requirements for these systems are reflecting this importance.

Dangerous dependency

Global economic crisis increased the pressure on the efficiency in all sector, including the public administration. This only increased the pace of modern technologies implementation in the sector, in some cases including the critical infrastructure. The implementation of modern technologies itself is a step in the right direction. It brings new opportunities and new service, introduces new means for interaction among the state and the citizens and it also reduces the costs. However, it is important to bear in mind that systems might collapse and backup solution must be ready to be used in the case of emergency. The problem is that backup solutions independent from the modern technologies might be costly. If the critical infrastructure is dependent on a system or on a cyber space, the backup solution has to be free of such dependency. These backup solutions are often primitive, but efficient (e.g. diesel aggregates in nuclear power plants). The political pressure on cost reduction might force national authorities to change their attitude towards needed backup solutions. Political will is needed for the implementation of modern technologies in the public sector. But is there an apolitical authority supervising that there are no necessary risks taken in order to increase the costs savings in this field?

Cyber and physical

The tight relationship between cyber space and physical world creates intersection in the critical infrastructure protection. It also enlarges the number of facilities that can be regarded as a national critical infrastructure and therefore protected appropriately. It is clear that critical infrastructure has to be physically protected. Necessary measures have been implemented to protect also systems running this infrastructure in the cyber space, but it is still necessary to protect the physical infrastructure running theses critical systems. This might be a problem, as the physical location of the facility and system's hardware might and should be different. It is not sufficient to protect the electric grid from physical attack and systems running the grid from a cyber attack. The hardware running the system has to be protected as well, because its destruction might have similar effects as damaging the grid or disabling the system. The question is whether this aspect has been considered in the process of critical infrastructure protection. Another interesting aspect is the international feature – the hardware on which the system is running might be located in a different country. In case of critical infrastructure systems using data from cloud storage, the situation might be even more difficult as the location of the data is practically unknown. Is it the responsibility of the state in possession of the critical infrastructure to identify this risk in a different state? And what should be the role of the private sector in such cases?

III.4 Costs and private companies

The security of critical infrastructure is not a state, but rather a process. It involves many subjects and it is very expensive. In some cases the critical infrastructure is in the hands of the private sector. State exercises its control and supervision through responsible authority,

which is setting the security standards and making audits. Private sector may be part of the critical infrastructure in more stages due to the usage of modern technologies and cyber space. It is important to highlight the fact that the primary task of the private company is to make profit for its shareholders. Implemented security measures are based on the legislation and on simple mathematics. If it is more profitable to take the risk, the private company will in many cases do so. Voluntarily implemented security measures are not an option for private companies, unless they increases or ensures the profit. Similar reasoning was used in the draft of the EU directive on cyber security and it is important to bear in mind that the most effective tool national authorities have to ensure the security of critical infrastructure is the legal obligations. Nevertheless, this approach has several disadvantages.

Firstly, some security measures become obsolete and do not correspond to current threats. Therefore it is important that the responsible authority continuously update the security requirements. But in case of the cyber space, the evolution is so fast that keeping up the pace of the evolution with rather rigid process of the public sector is very difficult. Secondly, these requirements increase costs. State may choose to participate to lighten the financial burden for the private sector. If not, it is very probable that if possible, the users of the service will have to bear the costs in the form of increased price of the final service or product. These costs may also influence the situation in the market and act as a barrier to entry the market. The question is how state should motivate private companies to flexibly increase their security measures when dealing with critical infrastructure. Another issues is the state participation on such costs as in the end, it is a national interest to have a secured critical infrastructure.

III.5 Topics for discussion

- Development of critical infrastructure's characteristics
- Responsibility for cyber security of critical infrastructure and its systems
- Critical infrastructure on EU level
- Stakeholders and their responsibilities
- Costs versus security in the cyber space
- Public sector and cyber security
- Security of cloud solutions
- Regulation of private companies in the name of security
- Bearing costs for the security
- Cyber aspects of critical infrastructure

IV. Virtual war and casualties

IV.1 Definition

The term cyber war was created using the method of genus and differentia, when a new term is created by specifying the more general term (genus) by another word (differentia). Logical explanation could be that in this case the genus is the war, whereas the differentia is specifying the dimension in which the war takes place. Unfortunately, the explanation of this term is not as easy as it seems. The nature of the war in this definition is dramatically changed by the cyber space. The genus de facto loses its original meaning. The war involves soldiers, weapons, destruction and physical violence among other aspects. Only part of this meaning can be transferred into the cyber space. Important fact is that the physical violence, which is inseparable part of the war, cannot be reproduced in the cyber space, unless we change the common understanding of the term violence. Therefore the term cyber war can be understood as a new term and definition, rather than a term based on the common definition of war projected into the cyber space using genus and differentia method. We can say that the cyber war is not a war in the cyber space with all the meanings we attribute to the term war, but it is rather a new term using "old" words.

What is the cyber war then? Definitely it is a conflict of two or more parties. If we accept the premise that only states can engage in a war and similar conflicts, all other attacks perpetrated by other subjects (e.g. extremists groups or hackers) would have to be regarded as terrorist or criminal acts. This conflict takes part in the cyber space or the cyber space has to be at least involved in the conflict. The usage of the term war suggests destruction. Systems and networks can be damaged in the cyber war by cyber attacks. Interestingly, if a network is shut down during a war because of a missile attack, it would be still regarded as a part of conventional warfare, even if the cyber space is involved. But if a missile silo during a war is not operational due to a cyber attack, would this attack be regarded as a part of conventional warfare? The complexity of the cyber space and tools that can be used for attacks with different consequences complicates the explanation of the term cyber war. Unfortunately, the term itself is used so often that it is virtually impossible to start using a better term for this new type of conflict. It is imperative to agree on the definition of the cyber space and cyber attacks, before approaching the definition of the cyber war. However, the cyber war cannot be explained simply as a war in the cyber space. In the meantime we can use the Oxford dictionary definition: "Cyber war: The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of communication systems by another state or organization."

IV.2 Rules

The ambiguity in the explanation of the term cyber war has not stopped academics and officials from analysing possibilities and more importantly the rules of such conflict. One approach is based on the premise that cyber war is simply a war just in a different domain. Supporters of this approach state the Law of Armed Conflicts (LOAC). LOAC is based on three principles – military necessity, distinction and proportionality. Military necessity requires combat forces to engage in only those acts necessary to accomplish a legitimate military objective. Distinction means discriminating between lawful combatant targets and non-combatant targets such as civilians, civilian property, POWs, and wounded personnel who are out of combat. The central idea of distinction is to engage only valid military targets. Proportionality prohibits the use of any kind or degree of force that exceeds that needed to accomplish the military objective. Proportionality compares the military advantage gained to the harm inflicted while gaining this advantage. LOAC is also related to the Geneva Conventions. Application of Geneva Conventions on the cyber war or on a conflict in the cyber space was the topic of a study called Tallinn Manual, published by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). CCD COE is currently preparing the follow up publication called Tallinn 2.0.

We can argue if the application of "old" rules and principles on the "new" domain makes sense. But since there is no global consensus needed for the creation of a new international legal measure to regulate cyber war, it is probably the best we can do.

IV.3 Arms race

Cyber war requires cyber weapons. This is another term whose explanation is understood differently. The main problem is that the variety of tools that can be used for a cyber attack is so wide that the category of cyber weapons is too general and needs to be more structured. Cyber weapons can range from malicious software used for traffic overflow, simple viruses, sophisticated code like Stuxnet or even botnets for possible use against military targets. But it can be also special hardware providing back door entrance or logic bombs in software. Again, the definition of the cyber weapons is too ambiguous to be properly used.

Despite the problems with the definition, some states confirmed intentions to include the building of offensive cyber capabilities as a part of their complex cyber security strategy. This confirmation is often made in relation to the Confidence Building Measures (CBMs) introduced by OSCE for nuclear weapons during the cold war as one of them highlights the importance of transparency. As the definition of cyber weapons and cyber capabilities is different in many countries, some states might feel insecure when other states proclaim the pursuit of building offensive cyber capabilities,. The confirmation done in the name of transparency can be regarded as a proof that the probability of a state sponsored cyber attack is increasing and it is necessary to be prepared for the cyber war, whatever it may mean. Some academics argue the efficient defence cannot be done without the study of the attack

tools and methods, which can be regarded as a building of offensive capabilities. Are we witnessing the beginning of another arms race, this time in the cyber space?

The economic costs related to the building of offensive capabilities in the cyber space are much lower than costs related to conventional weapons. Many states can therefore afford to build the offensive capabilities in the cyber space. But is this a desirable option? Is it a step in the right direction – having states with offensive cyber arsenal without common understanding of the basic definition needed for the application of the international law? If not, is it even possible to introduce any measures for the non-proliferation of cyber weapons among states? And what about cyber weapons in possession of individuals or terrorist groups?

IV.4 Asymmetrical warfare

The usage of the cyber space creates dangerous dependency in some states, when a disruption of some systems or networks could result in major economic damage. This dependency can be regarded as a weakness that can be exploited by a terrorist group or by a state during a conflict. The attribution problem in the cyber space theoretically enables attackers to remain unknown. This may provoke attacks on critical infrastructure systems or other important systems. If the cyber attacks are used during a general conflict, the attribution might be politically defendable, but from the technical point the identity of the attacker cannot be revealed without international cooperation. For example, cyber attacks during the Russian conflict with Georgia. In this case, it is universally acknowledged that the attacks were initiated by Russia to support military operations. However, there is no proof of this statement. But if such attacks occur without conventional conflict, the identification of the perpetrator is very difficult. Attribution problem in combination with the increase usage of modern technologies and cyber space in some countries creates conditions of asymmetrical warfare in the cyber space. The attacker may focus on the weakest point whereas the defenders have to secure the entire critical infrastructure and other crucial networks.

Increased cooperation on the international level is needed to improve the attribution of the cyber attack in order to deter possible perpetrators from committing cyber attacks.

IV.5 The role of the army

The term cyber war suggests that army and soldiers should be involved. There is a general agreement on the level of offensive actions in many states – only the army has the authority to execute offensive actions against other state, including the cyber attacks. Nevertheless, the role of the army in the cyber defence is not so clear.

The ambiguity arises from the differences among two terms – cyber security and cyber defence. Usually it is a national security authority responsible for cyber security on a national level. It might be a dedicated office in the structure of a ministry or a completely independent office. This office manages national Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Team (CSIRTs), facilitates cooperation among major stakeholders and monitors possible security threats. Cyber defence is the responsibility of the army. It often means that dedicated military units are responsible for the defence of military networks and related systems.

But it is highly improbable that only military networks and systems will be targeted by cyber attacks. Disrupting private networks and systems supporting military facilities or systems can occur during a conflict. But in such case, it would be the national authority responsible for the cyber security facing the attack in the first place. Another important aspect of the cyber space is the time. Attacks can be executed in seconds. That is why some academics argue that handing over the responsibilities to the army in the event of serious cyber attack is not efficient and that the dedicated military units should participate on the cyber security.

IV.6 Topics for discussion

- Cyber war and its definition
- Cyber attacks as a part of conventional warfare
- Cyber weapons and their definition
- Cyber attacks and the international law
- Cyber arms race – fiction or reality?
- Non proliferation of cyber weapons
- NATO Smart Defence and the cyber war
- Attribution problem in the cyber war
- Cyber defence vs. cyber security
- Role of the army in the cyber security

Summary

Cyber space and modern technologies are shaping our world. It is necessary to continue in discussion and negotiations to actually reach a consensus on various topics, some of which will be discussed during the conference. Only when there is an international consensus, we will be able to benefit from the opportunities the cyber space offers without the need of taking too high risks related to the cyber security issues. We believe that the conference will increase mutual understanding on cyber security problematic not only among different states but also among different sectors. We are convinced that events like this conference are needed to actually make progress both on national and international level towards secured cyber space.

ASSOCIATION FOR INTERNATIONAL AFFAIRS – AMO

The Association for International Affairs – AMO is a preeminent independent think-tank in the Czech Republic in the field of foreign policy. Since 1997, the mission of AMO has been to contribute to a deeper understanding of international affairs through a broad range of educational and research activities. Today, AMO represents a unique and transparent platform in which academics, business people, policy makers, diplomats, the media and NGOs can interact in an open and impartial environment.

In order to achieve its goals AMO strives to:

- formulate and publish briefings, research and policy papers;
- arrange international conferences, expert seminars, roundtables, public debates;
- organize educational projects;
- present critical assessment and comments on current events for local and international press;
- create vital conditions for growth of a new expert generation;
- support the interest in international relations among broad public;
- cooperate with like-minded local and international institutions.

RESEARCH CENTER

Founded in October 2003, the AMO's Research Center has been dedicated to pursuing research and raising public awareness of international affairs, security and foreign policy. The Research Center strives to identify and analyze issues crucial to Czech foreign policy and the country's position in the world. To this end, the Research Center produces independent analyses; encourages expert and public debate on international affairs; and suggests solutions to tackle problems in today's world. The Center's activities can be divided into two main areas: first, it undertakes research and analysis of foreign policy issues and comments on AMO blog; and second, it fosters dialogue with the policy-makers, expert community, and broad public.

www.amo.cz