Asociace pro mezinárodní otázky
Association for International Affairs

Conference Report 4/2014

Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge

–

May 2014

Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge

–

Tomáš Mad'ar, Tomáš Rezek

July 2014

Ministry of Foreign Affairs of the Czech Republic

US embassy

The international conference "Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge" was held in Prague, Czech Republic, on May 28-29, 2014. The conference was supported by the Ministry of Foreign Affairs of the Czech Republic and the U.S. Embassy Prague.

Conference Report 4/2014

Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge
–
May 2014

Introduction

The conference was dedicated to the current cyber challenges the transatlantic community faces. Each of its panels was revolved around a particular issue; the discussed topics consisted of Internet Regulation, Internet and Law, Safeguarding Critical Infrastructure and Virtual War and its casualties. The conference was organized by the Association for International Affairs (AMO) with kind support of the Ministry of Foreign Affairs of the Czech Republic and the U.S. Embassy Prague and in cooperation with the Embassy of the Republic of Estonia in the Czech Republic, the Representation of the European Commission in the Czech Republic, and PASOS – Policy Association for an Open Society. It was held in the premises of the Representation of the European Commission in the Czech Republic and the Ministry of Foreign Affairs of the Czech Republic on 28th and 29th May 2014.

Recommendations and conclusions

- The cyberspace needs to be open, free, secure, and interoperable. The confidentiality and resilience of the digital domain is also of major importance.

- The multi-stakeholder approach seems to be the favourable model of internet governance, provided there is ensured accountability and self-regulation, as most of the cyber infrastructure is held privately.

- The international approach to dealing with issues originating in cyberspace needs to be promoted. The larger the scale, however, the less likely the agreement because of different understanding of key terms and definitions mainly due to different values. In trying to come to terms with other key players on a global scale, a more pragmatic approach should be considered, focusing on potential economic benefits and/or losses. On a regional level, the development and harmonization of common terms and values is more probable.

- Before drafting and adopting new regulation, all of its potential consequences need to be carefully weighed and contemplated upon. An inadequate regulation, even in spite of potentially having been drafted with the best intentions, might infringe on citizens' rights or even cause damage to the local economy.

- The concept of net neutrality needs to be defined and adopted in a satisfying form that will harmonize the fragmented views of what the concept actually means. The subsequent implementation should ensure citizen rights and economic development, but also bear in mind safety precautions.

- Education of citizens is of utmost importance when approaching and dealing with the emerging cyber issues, and should be emphasized as such, while being directed at all age categories. Many individuals are so far unconscious as to how the Internet works, and do not realize the full extent of their actions and the nature of threats originating in cyberspace.

- The public-private partnerships should become one of the focal points of national approaches towards cybersecurity. Positive incentives are more likely to foster cooperation with the private sector. A respectful approach taking different perspectives into account presents a sign of good will.

- When designing new legislative measures to address current cyber challenges, a careful evaluation of the existing legislature is in order. There may already be enforceable mechanisms for the particular issue at hand, even at the international level.

- A harmonization of computer forensics among European states could reduce the legal issues the investigators face when trying to prosecute cyber offenses. A subsequent promotion of such a harmonization on the international level could further help in curbing some of the cyber offenses across the globe.

- With the ever increasing reliance on the availability and functionality of critical infrastructure, without which a modern state is difficult to imagine, states should focus on improving the resilience and preparedness for a potential crisis. Since most of the critical infrastructure is being operated via computer systems, all of it virtually becomes cyber infrastructure. Therefore, ensuring the robustness and safeguarding the infrastructure from potential threats has become a vital objective.

- Achieving cyber security will require a continuous effort of the international community. The international cooperation is absolutely vital in attempts to pursue the goal. The European Union as well as the NATO should strive to spearhead and harmonize the efforts of their member states as well as other partners across the globe.

- NATO needs to credibly define the circumstances under which the Article 5 might be invoked by a cyber-crisis.

- The issue of trust needs to be resolved by building specific confidence building measures among members of transnational and international organizations as well as during bilateral and multilateral negotiations.

- On the national level, the main challenge lies in efficiently dividing responsibilities among respective national authorities and in the incorporation of cyber security into crisis management and defense planning.

- With the increasing level of cyber capabilities being developed, the talks for a regime limiting the proliferation of cyber weapons to the non-state actors might be advisable. With the propensity of some nation states to outsource the capabilities to non-state actors, the potential for escalation of future conflicts and crises (as well as the potential impact caused by these actors, whose rationality is difficult to estimate) is on the rise.

Internet regulation

The importance of the Internet and the impact of the network on our everyday lives have grown immensely in the past couple of decades. With this growing importance, many political challenges and questions arise as well. Among the focal points of discussion were the questions of whether or not the Internet should be regulated and by whom it should be governed. Tomáš Rezek, who chaired the first panel, brought up the issue of regulation potentially jeopardizing the development on which the network was based in the first place.

Martin Drtina argued that development is a bottom-up process. According to him, the current system works well in transparently resolving disputes. The Internet Corporation for Assigned Names and Numbers (ICANN) is generally respected as a neutral and transparent body that supports technical innovations. Mr. Drtina stressed the importance of the privatization of the internet: the multi-governmental approach to Internet governance is not the answer. He sees the future of the Internet as not under governmental control, but also not in anarchy. An emphasis was put on self-regulation through the multi-stakeholder governance model.

Václav Mach was pleasantly surprised to agree with Mr. Drtina. He then stated that there are key rules that need to be established – these involve no restrictions for the infrastructure and clear rules of how to behave as well as an antimonopoly regulation. Due to the perceived propensity of the mobile industry and the Internet service providers to exploit the users, regulation promoting strong competition and consumer rights protection. Mr. Mach pointed out that the concept of net neutrality is viewed differently from the point of view of respective parties involved – the industry is allegedly fragmented in its opinions as to what neutrality means. Some of these issues might be resolved provided the existing EU draft of regulation is adopted in its current form.

The state of cyber security affairs in the Netherlands was introduced by Gerben Klein Baltink. The presented Dutch view stressed the need for a free, open and available cyberspace, which is also secure and able to rely on its infrastructure. Mr. Klein Baltink

stated that while cyberspace has to be open for everyone, importantly it also needs to be confidential and resilient. Cyber awareness, education and being able to learn from past mistakes are seen as key in order to face the current and future cyber challenges. Several dilemmas in of the digital domain were touched upon, including governance, privacy, awareness, "The Internet of Things", and international cooperation. The Dutch approach builds upon the public-private partnerships (PPP) – these offer real benefits, particularly when applied to specific conditions of each country. The future challenge revolves around putting the PPP in the international context. Dutch authorities also support the multi stakeholder model in regards to the Internet governance.

A certain contrast between the often expressed need for Europe to stay competitive and many regulations that limit the economies of the EU in comparison to the US or China was pointed out by Michal Feix. Mr. Feix stated that the only efficient way to regulate the Internet would be to censor it, which would result in damage being done to both local economy and citizens' liberties. Many of the phenomena perceived as needing regulation can actually be addressed by existing laws; however, there is much room for improvement in terms of enforcement and international cooperation. Mr. Feix emphasized the importance of education and called for a significant effort to be made in this area.

Denis Gibadulin also stressed the need for an open, stable, interoperable and secure Internet, which has been the reason behind our incredible economic and social growth in the recent past. The importance of the availability of the network was the focal point of Mr. Gibadulin's speech: the Internet has to be open to businesses, individuals and academia as well as the civil society as a whole. A certain dichotomy was also mentioned: while in some countries the access to the Internet is already understood as a basic human right, only 2.5 billion individuals actually have access to it.

The subsequent discussion mostly revolved around the issue of regulation and censorship – while Mr. Gibadulin and Mr. Feix disagreed with the notion of any more rules being adopted and implemented, Mr. Klein Baltink deemed some hypothetical regulations aimed at education potentially positive. On the contrary, Mr. Mach advocated further regulations from the standpoint of safeguarding the Internet from dynamically evolving threats – he considers a flat out refusal of any regulation unfeasible. Michal Feix disagreed, claiming these phenomena have been around since 1980s and have only spread in scale and impact. Denis Gibadulin expanded on Mr. Feix statements, claiming that less than 2% of online activities are not being regulated by a law. All panellists have agreed that more effort concerning education needs to be made.

Internet and law

Ilési Zsolt explained the need for forensic services when identifying and prosecuting the perpetrators of cyber offenses. He mentioned that while a successful attack on an unpatched system can only take a few seconds, the average time for a thorough forensic analysis requires months or even years. The analysis is also made more difficult due to a plethora of existing concepts with no clear definition, cryptography and anonymization tools that protect the culprits, slow approach of the investigative authorities to cyber forensics and insecure software and hardware environment. Mr. Zsolt calls for an adoption of a due diligence regulation that would clearly identify the author and/or the responsible person behind a given code. He also perceives a need for European harmonization of a European cyber forensics standard to avoid some of the legal issues that are present at the moment.

A more sceptical view concerning the definitions of terms associated with cyber security was offered by Radim Polčák, who declared himself "an enemy of definitions". Mr. Polčák expressed his concerns about our ability to foresee the future development of cyberspace and to create efficient laws in the cyber domain. It was also argued that in most cases, the existing legislature is applicable, thus there is little need to create a new one solely for the needs of the cyber domain. There are certain concepts that, however, must be agreed upon, the information sovereignty of the states being one of them. In conclusion, Mr. Polčák described two core elements in factual applicability of law concerning the Internet: the international cooperation concerning cyber security and the cooperation of the providers with the public sector.

Tomáš Flídr introduced one of the currently much discussed issues concerning cyber space: the concept of net neutrality. Mr. Flídr sees net neutrality as an ideal principle not dissimilar to the concept of democracy; however, it is also being limited in its implementations. According to him, the reasons to limit net neutrality vary – they include security concerns, commercial reasons, technical reasons, law enforcement and even user requirements. On the other hand, a strong rationale as to why net neutrality is important was also presented: to protect the freedom of speech, to shield us from censorship, to protect the privacy of users and to prevent the internet service providers' (ISP) "dictatorship". Mr. Flídr described the European Union's, the British and the American stance on the issue.

Russian internet legislation and the changes the network has undergone in the recent years were described by Kevin Rothrock. According to him, the Russians see the Internet as an instrument of their foreign policy. Unlike the West, Russia does not share the sentiment that internet freedom should be regarded as a human right. On the contrary, the Internet is seen as a potential threat, and is therefore being monitored and censored. The data has to be stored by the ISPs for 6 months. Successful content creators even have to register to the authorities and will be held liable for their content. Mr. Rothrock highlighted the presence of a potential

for misuse: the law might serve as a pressure point for the government. On the other hand, Russia acknowledges the economic value of the Internet.

The subsequent discussion of the panellists was centred on the implementation of human rights in the cyberspace across the globe. Mr. Polčák identified the main issue of sharing common values among different cultures, and proposed that for the time being, financial motives should be the key to promote international cooperation regarding the cyberspace. The discussion also involved the ins and outs of law enforcement in cyberspace and the issue of attribution as well as questions regarding data protection and the implementation of the right to be forgotten.

Safeguarding critical infrastructure

After a brief examination of the Prague Transatlantic Talks' history by Vít Dostál, the Ministry of Foreign Affairs of the Czech Republic was introduced by Petr Kypr as "one of the groups of people preparing the cyber security of the Czech Republic". Since the life of the society relies on a working internet, it can be considered a part of the critical infrastructure as a whole. The trouble lies with efficiently dividing responsibilities. Mr. Kypr also expressed his view that, while in the long run, the notion of freedom of the Internet is a great idea, so many obstacles need to be overcome that some regulation is in order. He also stated that the impact of cyber-attacks against the society would be comparable to the effects of WMDs.

The Finnish approach towards cyber security was presented by Aapo Cederberg. Without a robust and secure cyberspace, a competitive welfare state is unimaginable. The digital domain presents both an opportunity and a threat. States have responsibility to protect the critical infrastructure of a nation, but the challenge has to be tackled coherently and comprehensively on the international level. Modern crises will incorporate the cyber components. In order to promote the will, the knowledge, the tools and the understanding in the society so that it is resilient in times of crisis, it needs to be involved as a whole. Education and public-private partnerships play a key role in the endeavour.

Neil Mitchison stressed the need to understand the critical infrastructure before we start efficiently protecting it. According to him virtually all critical infrastructure (CI) is now a cyber-infrastructure with potential cyber vulnerabilities. To effectively protect it, partnerships between the operators and the authorities need to be made. Since the systems are very complex and hard to understand, being able to model them via simulation and emulation of the cyber-physical systems such as smart grids can produce desired results. The modelling could also serve to expand the necessary knowledge as well as test whether or not a particular facility can withstand a certain type of cyber-attack.

The Czech approach to cyber security of the CI was presented by Roman Pačka, who sees the critical infrastructure as the backbone of the country's national and economic security. The Czech approach revolves around shared responsibility of the public and private sector. Mr. Pačka stressed the need for incentives to promote collaboration of the operators with the public sector and to motivate them to invest in protection against cyber-attacks. The inexistence of critical information infrastructure database and direct communication channels among entities is also perceived as an issue. The public entities seem to be adapting well to the standards that will be required by the coming law based on the risk-analysis of the Czech National Security Authority (NSA). In the future, a model for efficient mutual information exchange and effective international cooperation will play a key role in securing Czech critical infrastructure.

Joanna Świątkowska focused on the CI protection in the European Union, which undergone changes after 9/11. Protection of the CI has become a very important topic of the modern security of states. Prior to 2004, this protection was the sole task of respective EU member states. EU aims to overcome the problems of the different approaches and to take steps to secure the entire European CI. In doing so, it not only sees the CI as a whole, but also studies its respective elements. The EU still needs to become more involved in the protection of CI, especially in the context of potential cyber warfare and terrorism. The issue of trust between the private and public sector needs to be resolved: research conducted by the Kosciuzsko Institute shows that private companies are more likely to cooperate when given positive incentives the companies might benefit from; actions limited only to sanctions are considered less effective. The parties also need to respect the different perceptions of risks of one another.

The discussion further expanded on the issue of trust – Mr. Mitchison pointed out that governments and legislatures set the legislative framework, which affects operational decisions, and that it is important to be aware of, and respect, the different roles of legislators, regulators and operators. . Mrs. Świątkowska stressed that private partners often perceive restrictive measures unnecessary and are then less inclined to cooperate. Mr. Pačka explained how the Czech approach incorporates both sanctions and positive incentives for cooperation with private entities. Mr. Cederberg then emphasized the importance of constantly evolving our understanding and approach towards cyber security. The panellists then discussed the role of transnational bodies, such as the EU, in protecting the CI.

The U.S. approach towards cybersecurity

The U.S. approach towards cybersecurity was presented in a keynote speech by Christopher Painter, who agreed with the notion of Internet being both an opportunity and a potential threat. Mr. Painter remarked that president Obama has called the challenges we now face "the great irony of our Information Age – the very technologies that empower us to create and build empower those who would disrupt and destroy." Accordingly, cyber challenges such as government-sponsored economic theft, threats to critical infrastructure and cybercrime have recently risen to the top of the policy agenda.

Mr. Painter then again stressed the need for an open, interoperable and secure cyberspace. The importance of diplomacy in addressing the issue was also accentuated, as cyber security is not only a technical endeavour. The overall vision of the United States is rooted in the International Strategy for Cyberspace, which was released by the White House in May 2011. The Strategy's focal point is the international collaboration, which is seen as more than just a best practice: as the very first principle.

Mr. Painter then identified the following 6 areas of focus that should be further addressed, the first of which is international security in cyberspace, which incorporates developing a shared understanding about norms of acceptable state behaviour in cyberspace and establishing practical cyber risk reduction and confidence building measures. The second area revolves around internet governance, which is considered the emerging front in the struggle for openness in cyberspace.

The third area is promoting internet freedom and human rights online, since the United States' Government perceive a growing threat to internet freedom in the past several years and feel the need to ensure the ability of individuals worldwide to exercise their fundamental freedoms online. Mr. Painter also summed up the US accomplishments in this area in the recent past.

The fourth area is focused on fighting cybercrime, which is deemed "a transnational scourge that has cost the global economy, by some estimates, billions of dollars, and has reduced public trust in the Internet". Mr. Painter here stressed the importance of the 2001 Budapest Convention on Cybercrime, which the United States is a party to, and which they intend to keep promoting as a key diplomatic priority. The United States is also willing to support capacity building efforts to enhance states' ability to fight cybercrime.

The fifth area revolves around ensuring that countries perform due diligence in their cyber security approach. The measures the U.S. intend to take involve efforts to strengthen relationships with other countries, enhancing mutual collaboration and supporting development of required capabilities as well as enhanced participation in existing regional

and global cybersecurity fora. The sixth and last area is the Department of State's work to promote the Internet (or cyberspace as a whole) as an engine for economic growth.

According to Mr. Painter, the multi-stakeholder approach is deemed favourable by the U.S., provided there is accountability, and will probably be preferable over the intergovernmental solution, which could potentially be exploited by repressive regimes to undermine human rights online, "as they see the open Internet as a threat to their stability."

Virtual war and casualties

The ambiguity and complexity of the concepts regarding cyber warfare were stressed by Alexander Klimburg. Mr. Klimburg touched upon the issue of defining roles, the pervasiveness of cyber phenomena, and the attribution problem. He also accentuated that cyberspace consists of more than just the Internet – there is the physical layer, the logical layer, the content itself and the social layer, which is allegedly the most important one, as all attacks eventually target people. Mr. Klimburg differentiates between 4 military tasks in using the cyberspace and capabilities within cyberspace to pursue national goals: Protection, Battlefield Cyber (supporting conventional military activities at a tactical/operational level), Strategic Strike and Cyber-Espionage and Counterespionage. Attribution is likely to stay circumstantial at best, but intelligence means might provide an alternative.

The context of lack of rules governing the Internet was highlighted by Karsten D. Geier, who also mentioned the loss of trust within the transatlantic community in light of practices revealed by Edward Snowden. On the other hand, letting this affect all areas of cooperation would not be wise. According to the most recent Cyber Index published by the UN Institute for Disarmament Research, 114 states are developing cyber capabilities. These capabilities, however, are not limited to states – criminals, terrorists and activist can also obtain them. While an all-out cyber-war has not happened yet, cyber capabilities have been used in conflicts in Estonia or Georgia. Some of the capabilities are even able to transcend or cross domains and inflict physical damage, such as the Stuxnet virus. Unlike during the Cold War, deterrence and denial might not be adequate security strategies, given the multitude of potential actors, the possibility of "false flag" attacks, and the problem of attribution. There is a risk of conflict escalating from the use of offensive cyber capabilities. Increasing cyber resilience, applying existing international law to cyberspace, cooperating with partners on an international level and confidence building are some of the measures to be taken when trying to address the issues in question.

Piret Pernik brought up the pervasiveness of cyber threats: many companies are being attacked daily, 84% of corporations have been infected by malware. While militaries, governments and non-state actors all play a role, cyberspace is primarily safeguarded by the

private actors. Mrs. Pernik emphasized the need for a comprehensive approach and to incorporate cyber security into crisis management and defense planning. Offensive cyber capabilities are likely to be an element of almost any future crisis and/or geopolitical conflict. Attribution may therefore pose less of an issue, since most of the offensive cyber actions seem to be regional and connected to foreign policy issues. While offensive cyber capabilities are considered niche with limited effects, they should not be underestimated. Mrs. Pernik claimed that as of now, states seem to be unwilling to cross the threshold of an armed cyber-attack and mostly focus on cyber espionage. They are also tempted to outsource offensive cyber capabilities to non-state actors. NATO should work on its interoperability concerning cyber defense and clear out which attacks might invoke Article 5 of the Washington Treaty.

A sceptical approach to the issue of cyber warfare was presented by Jozef Vyskoč, who emphasized the problems in finding definitions. Mr. Vyskoč considers the language often used with cyber issues as "great for attracting attention and inciting emotions, but unsuitable for scholarly discussions." A wrong selection of a concept in the beginning, he added, may cause further problems in the future. By building something on shaky grounds we might be wasting resources by missing what is really important. Mr. Vyskoč disputed the need to find a solution to the attribution problem and called for explicit statements of priorities and the development of a common basis for discussion.

The discussion revolved around the potential for terrorists to use offensive cyber capabilities, which Mr. Klimburg considered potentially likely, but for the moment limited in their impact. The cyber capabilities of NATO and the potential to invoke the Article 5 were also put to question. Mr. Vyskoč and Mr. Klimburg then discussed attribution and its importance on different levels of analysis. Nikola Schmidt also mentioned the need to develop routines in how to react to potential cyber crisis situations, but also warned that such routines might be exploited and have to deal with ever changing and dynamic situation in cyberspace.

Speakers

Gerben Klein Baltink, Secretary, Dutch National Cyber Security Council, Ministry of Security and Justice of the Netherlands, The Hague
Aapo Cederberg, Senior Programme Advisor, Geneva Centre for Security Policy, Geneva
Vít Dostál, Director of the Research Center, Association for International Affairs – AMO, Prague
Martin Drtina, Senior Press Officer, Czech Telecommunication Office, Prague
Michal Feix, Business Development Director, Seznam.cz, Prague
Tomáš Flídr, Owner, Information server Cyber Security Info, Brno
Karsten D. Geier, Head of Division, Dialogue and Communication; New Threats, Federal Foreign Office, Berlin
Denis Gibadulin, Public Policy & Gov't Relations Analyst, Google Czech Republic, Prague
Alexander Klimburg, Research Fellow, Belfer Center for Science and International Affairs, Cambridge/US
Petr Kypr, Director of Strategic Group, Ministry of Foreign Affairs of the Czech Republic, Prague
Václav Mach, Legal and Corporate Affairs Lead, Microsoft Czech Republic; Member of the Board of Directors, ICT Unie, Prague
Neil Mitchison, Head of the "Security and Technology" Assessment Unit, Institute for the Protection and Security of the Citizen (European Commission's Joint Research Centre), Ispra
Roman Pačka, National Security Authority, National Cyber Security Centre, Prague
Christopher Painter, Coordinator for Cyber Issues, U.S. Department of State, Washington D.C.
Piret Pernik, Research Fellow, International Centre for Defense Studies, Tallinn
Radim Polčák, Head of the Department, Institute of Law and Technology, Masaryk University, Brno
Tomáš Rezek, Research Fellow, Association for International Affairs – AMO, Prague
Kevin Rothrock, Project Editor, Global Voices, Fairfield/US
Nikola Schmidt, Researcher, Institute of Political Studies, Charles University in Prague, Prague
Joanna Świątkowska, Expert, The Kosciuszko Institute, Krakow
Jozef Vyskoč, Associate Fellow, Central European Policy Institute, Bratislava
Ilési Zsolt, Associate Professor, College of Danaújváros, Danaújváros

ASSOCIATION FOR INTERNATIONAL AFFAIRS (AMO)

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.

FOLLOW US!