Asociace
pro mezinárodní
otázky
Association
for International
Affairs

Briefing Paper 2/2015

Aiming for the stars: An ambitious Czech cybersecurity approach
–
March 2015

Aiming for the stars: An ambitious Czech cybersecurity approach
–

Tomáš Maďar

March 2015

In early February, the Government of the Czech Republic adopted updated versions of both the Security Strategy of the Czech Republic and the National Cyber Security Strategy of the Czech Republic. Can we observe a noticeable shift in approach in regards to cyber security? And how well do these strategies reflect the current developments in the field?

Cyber security in the Security Strategy of the Czech Republic 2015

The difference between the most recent Security Strategy of the Czech Republic 2015, released by the Ministry of Foreign Affairs on 4th February 2015, and its 2011 predecessor is evident at first glance. First and foremost, the Ukrainian crisis had a deep impact in terms of perceived threats – in light of the crisis, the most urgent threats as listed in the document are (1) weakening of the cooperative security mechanism and of political and international legal commitments in the area of security and (2) instability and regional conflicts in and around the Euro-Atlantic area.

Terrorism is mentioned third, with focus on lone wolves and the phenomenon of foreign fighters, clearly in relation to the so-called Islamic State, and the recent events in France. Fourth rank belongs to proliferation of WMDs and their means of delivery, as its curbing is a long-term goal of the Czech Republic. Cyber-attacks finally come into play next, followed by negative aspects of international migration, extremism, organized crime, threats to the operation of critical infrastructure, interruptions of supplies of strategic raw materials or energy, and disasters of both natural and anthropogenic origin and other emergencies.

Even though threats to cyber security are listed further below in the strategy in comparison to its previous version, this is by no means an indication that this particular issue is being given less of a priority, since cyber security is accentuated many times throughout the entire document.

The reasoning behind this is likely twofold: firstly, as experience shows, in the contemporary security environment cyber-attacks are used both in stand-alone operations and as a part of wider campaigns. Secondly, the National Cyber Security Centre[1] did achieve many on the goals set in the first national cyber security strategy, which, along with the increasing number of incidents worldwide and the growing popularization of the topic of cyber security, led to heightened awareness concerning the issue.

[1] The National Cyber Security Centre (set up within the National Security Authority) serves as a national authority on cyber security. As a part of the early warning system it also bears responsibility for both national and international cooperation in preventing and addressing cyber attacks as well as for the introduction of measures necessary to secure Czech cyberspace.

As a result, the document offers a solid analytical grasp of cyber threats[2] and their potential impact. In order to counteract these risks, a wide spectrum of measures is to be undertaken. Providing for the security of critical information infrastructure and important information systems and building flexible resilience systems belong to the top priorities. Apart from technical provisions, other – both legislative and non-legislative – measures are to be implemented in order to develop Czech information society. The objectives include promoting adherence to security standards, defining methods for protecting sensitive information or conducting activities that will help support public awareness.

The Czech Republic also aims to actively contribute to "the anti-cyber threat measures" within NATO and EU, and to support the international judicial and police cooperation in apprehending perpetrators of cyber attacks as well as the development of international legal standards on cyber security.

As a consequence, in spite of the rising number of pressing security concerns in and around the Euro-Atlantic area, the Security Strategy of the Czech Republic 2015 provides a clear manifestation that cyber security is considered one of key strategic areas.

Great ambition with many challenges ahead

Further building upon the cyber security-related findings of the Security Strategy is the National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020, which was adopted by the Bohuslav Sobotka's cabinet on 16th February 2015. In an accompanying release statement, the National Cyber Security Centre (NCSC) declared the successful completion of most of the objectives set by the previous version of the document. These included the adoption of the Cyber Security Law and associated implementing regulations or the renovation and opening of the NCSC residence (which also houses the Government CERT).

The strategy's introduction sets the tone of the entire document – it is to the point, clearly states priorities and identifies challenges, and does not sound the unnecessary alarm. The major risks listed include cyber espionage, organized crime in cyberspace, hacktivism and intentional disinformation campaigns with political or military objectives. The potential future threat of cyber terrorism is mentioned, but only in passing. Besides intentional threats, cyber incidents – both anthropogenic and natural by origin – are also being addressed.

The second part of the strategy, Visions, is in comparison to other cyber security strategies mostly nothing out of the ordinary – the objectives are to develop an information society,

[2] The only inaccuracy to point out here is that the strategy only mentions "cyber attacks", leaving out non-intentional cyber incidents.

secure the critical infrastructure and cyberspace in general, promote mutual trust with the private sector, etc.

If only it were not for the third point.

In a fashion completely alien to the vast majority of Czech strategic documents, the strategy states that the Czech Republic is going to aspire to play a leading role in the cyber security field within its region and in Europe. This marks a complete shift in approach, with the country transforming from one yet establishing its institutional and legislative cyber security foundations to a regional aspirant for a leadership position in this specific security field.

For the Czech Republic, the decision to focus on cyber security does however make a lot of sense. First of all, a recent Tallinn paper demonstrates – on the example of Estonia, no less – how even a small state can find its niche, and gain the respect of others. With the growing amount of nation states delving into the topic of cyber security, there might be quite some competition for the ambitious expert team of the Czech National Cyber Security Centre, on the other hand, there is still much to achieve and work on, especially in terms of developing legal norms and standards for behaviour in cyberspace.

Secondly, the recent successes in pursuing the objectives of the last version of the strategy likely mean that the self-proclaimed heart of Europe is already ahead of the rest of the V4 members, which means the country could also lead by example.

Last but not least, the Czech Republic desperately needs to show that it can be a capable and dependable ally. The military expenditures are falling closer to measly 1 % of the GDP each year, for which the past Nečas' government was in 2011 criticized even by Anders Fogh Rasmussen, then NATO Secretary General, much to no avail.

In light of the Ukraine crisis, Sobotka's cabinet promised to increase the defence budget so that it by year 2020 reaches 1.4 % of the country's GDP – a promise that the Prime Minister repeats in the introduction of the Security Strategy 2015. That still falls short of the commitment to spend at least 2 % of the GDP on defence. And even with the promise of contributing 150 soldiers to the new NATO Spearhead Force and participating in air policing and international training exercises, the country has to convince its allies that it does not neglect its security commitments.

Becoming regarded as one of the European pioneers in the field of cyber security, namely securing critical infrastructure, developing adequate norms, principles of information society and educational programmes could be a good first step.

In another chapter, Principles followed by the state in ensuring its cyber security are detailed. These include:

1. Protection of fundamental human rights and freedoms and of democratic rule of law.
2. Comprehensive approach to cyber security based on principles of subsidiarity and cooperation.
3. Trust building and cooperation among public and private sector, and civil society.
4. Cyber security capacity building.

According to the respective paragraphs, NCSC states that the Czech Republic respects the open and neutral character of the Internet, freedom of expression, personal data protection and privacy rights. The cooperative and comprehensive approach is based on the principle of indivisible security, which the Czech Republic follows in security matters. The latter two principles comprise two of the most important domestic challenges lying ahead of the NCSC.

Admittedly, due to the lack of public trust in the state, the overall domestic success or failure of the National Cyber Security Strategy might very well depend on how the confidence building measures will fare. Other listed Challenges include the low digital literacy among the increasing number of Internet and ICT end users, which is further made complicated by emerging phenomena such as the Internet of Things or mobile cybercrime.

The Czech Republic is also considered a potential test bed for adversaries considering an attack on her allies or other states with strategic importance. Other listed threats include cyber espionage, potential cyber-attacks against critical infrastructure and the states military forces, as well as security risks associated with the IPv4 to IPv6 transition or to the electronization of public administration, among others.

The chapter detailing the Main Goals mentions both rather standard objectives (such as efficient cooperation amongst relevant institutions, active international cooperation, protection of critical infrastructure, cooperation with private sector or development of legislative framework) and new incentives, including focus on research and development, support to the Czech Police in regards to fighting cybercrime and education and awareness raising along with information society development.

Especially for the focus on education, not only the tertiary programmes at raising experts, but also on modernizing the curricula for primary and secondary schools, the strategy deserves a commendation. On the other hand, the aim of modernizing the specialized departments of the Czech Police may need to be taken with a healthy dose of scepticism due to budget constraints.

The last section details that an Action Plan is expected to be adopted by the Government of the Czech Republic in the second quarter of 2015. It should detail specific steps which are to be taken in order to advance the fulfilment of the strategy. The NCSC is also expected to submit an annual "Report on the State of Cyber Security in the Czech Republic" to monitor the effectiveness of the adopted measures.

Any potential vulnerabilities in the system?

The two strategies analysed above provide a solid foundation for the Czech authorities to build upon in terms of securing critical information infrastructure and important information systems, raising the awareness of general public and contribution to securing cyberspace. But, for the sake of argument and potential for future improvements, are there any perceived weak spots to be found in the two admittedly solid strategic documents?

There might be one imperfection – the somewhat neglected potential threat posed by potential hostile information operations, which could arguably be troubling, since both the armed conflict in Ukraine and the activities of the Islamic State show the potential of propaganda, psychological warfare and disinformation. To be more precise, both strategic documents in question do mention the use of propaganda and disinformation in pursuing political and military agenda as a threat (the Security Strategy 2015 in a rather obvious jab at the Russian Federation), but neither expands on the issue in any way (apart from statements of striving to build a strong information society).

One could pose the question of: "How exactly are information operations relevant to cyber security in this specific context?" First of all, cyber operations are often categorized as being within the broader set of information operations (or the so-called information warfare). Secondly, most of the contemporary information operations are being conveyed by information and communication technologies, the same systems that can be considered as some of the referential objects of cyber security. Last but not least, the recent National Cyber Security Strategy openly considers "intentional disinformation campaigns with political or military objectives" as a major risk, essentially redefining them as a threat associated with cyber security.

This is mostly a competences issue – while the information assurance in terms of propaganda and disinformation should mostly be addressed by the diligence of media, the non-governmental organizations, the academia, etc., a platform for dialogue coordinated by an entrusted authority could go a long way in building the necessary mental resilience of the population.

Most of the criticism here is directed at the somewhat lacking coordination and imperfect division of competences within the Czech security system. The omission of information warfare is especially baffling due to how much accent the Security Strategy 2015 put on the threat of instability and regional conflicts in and around the Euro-Atlantic area, and how securitised hybrid warfare has become in the past few months due to its successful utilization in the Ukrainian armed conflict.

Despite this particular question, both strategic documents offer a solid analytical grasp of the contemporary cyber security environment and provide the Czech authorities with a solid foundation and directions on which to build upon. Whether and how well will the National Cyber Security Centre fulfil all of the objectives set by the strategies is yet difficult to predict.

On one hand, it certainly did a great job in establishing the cyber security framework necessary for addressing the current security issues in the field. On the other, we must take into account the high ambitions of the new cyber security strategy and the objective of growing into a leadership role. It is worth mentioning that last year, the National Cyber Security Centre only employed 22 experts. While this number is expected to rise up to 34 by 2016, can such manpower suffice for all the tasks the Centre took upon itself?

If the Czech Republic is to succeed in its attempts to play a leadership role in cyber security in its region and beyond will depend on the amount of means and support available to the NCSC, the successful efforts of the Centre in its task to help secure Czech computer systems and networks as well as the ability of the Czech Republic to come to terms with the neighbouring states as well as the rest of the EU and NATO member states, and other parties in the international arena, in developing common norms and platforms for cooperation with the aim of promoting international information and cyber security.

In terms of domestic goals within the Czech Republic, the NCSC has so far proven itself. Notwithstanding the objectives of promoting public-private partnerships, information sharing with businesses and building information society, which without a doubt are demanding long-term challenges, but given enough enthusiasm and hard work, by no means impossible.

Conclusions

The adoption of the new Security Strategy of the Czech Republic 2015 and the National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020 marks a significant step. Having successfully established the essential groundwork on which to build upon in the recent years, the Czech authorities responsible for cyber security have now accepted new challenges and objectives with the aim of not only securing Czech computer systems and networks, but also of attaining a leadership role within the Central European region and potentially beyond in the future.

The observed overhaul of the National Cyber Security Strategy as well as the rising ambition of the Czech authorities cannot be considered unexpected, due to the reached milestone and the successes of the recent past.

Both the documents offer strong analytical insights and seem to focus on the right priorities, which – apart from securing critical infrastructure and important information systems – include international cooperation and education of both prospective cyber security experts and the broad public. The exception here might be the lacking semblance of countermeasures to neutralize the impact of potential hostile information operations. As a whole, however, the strategies are well-written and provide the necessary directions for the impending period.

The ambition of growing into a leading position in terms of European security is a welcome feature of the National Cyber Security Strategy for the period from 2015 to 2020. However, in order to succeed, the Czech Republic will have to provide tangible results in providing a platform for cooperation and engaging in successful efforts to develop international norms and standards. Being able to find and set a relevant agenda might be the key.

The Czech authorities are also likely to face stark competition in this regard, such as Estonia – a long-established cyber security leader within both the European Union and NATO – as well as other EU and NATO member states, including the small ones, for which the field of network security is a chance to shine.

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