sciendo

Műszaki Tudományos Közlemények vol. 11. (2019) 89–92.
https://doi.org/10.33894/mtk-2019.11.18
Hungarian: https://doi.org/10.33895/mtk-2019.11.18
https://eda.eme.ro/handle/10598/31213

EME MTSZ MTK

THE ROLE AND IMPORTANCE OF THE OSCE AND THE V4 IN CYBERSECURITY

Erika HRONYECZ

National University of Public Service- Budapest, Hungary, hronyecz.erika@gmail.com

Abstract

From the mid-2000s on, new types of security challenges have emerged at a global level. Their prevention, management and recovery, given their characteristics, is a serious challenge for the countries. Cybersecurity challenges require special attention and close interaction both at national and international level. In this paper the author presents the highlights of OSCE and V4 cooperation on cyber defence.

Keywords*: cybersecurity, V4, OSCE, Central European Cyber Security, regional cooperation.*

1. Introduction

Cybersecurity is one of the most important challenges faced by developed societies throughout the modern world. The number and frequency of challenges and threats emerging in cyberspace pushes every national and international organisation, tasked with avoiding and managing such types of events, to a constant necessity for awareness.

In the past, security was divided into five sectors: military, political, economic, social and environmental. However, since the 2010-s a further information sector has evolved, becoming more and more evident within security schools. [1]

A feature of cybersecurity events is their unpredictability, frequency and their evolution within a short period, mostly spreading through more national borders and thereby reaching several countries simultaneously. Taking this into account, international cooperation has critical role. In the field of cybersecurity even a bilateral agreement can be a complicated issue due to differing national interests, values and aims, and based on this a regional cooperation seems to be increasingly problematic.

2. The role of OSCE in cybersecurity

In the last 15 years, in confronting new types of security challenges, OSCE has also had to realise the need to meet the expectations raised by the new security environment. The Organisation of Security and Cooperation in Europe is a Pan-European security organisation with a long history, comprising 57 European, North-American and Middle-Asian members and 11 partner nations. OSCE defines and manages security in a complex and cooperative way, meaning that it maintains every field of security at a similar level, and all 57 member nations bear the same rights. The most important aim of the organisation is the protection of European security and stability, early warning, conflict management and the management of post-conflict maintenance processes. OSCE constantly adapts to the expectations raised by the new security environment and fights against new types of threats, such as terrorism, human- and drug-trafficking, organised crime and cybercrime.

In order to increase personal and collective engagement in maintaining Information and Communications Technologies (ICT's) in a complex form, with its 1039 resolution of 29 April 2012, the OSCE has established the Informal Working Group (IWG). As a main task of the Group, pro-

cessing of Confidence Building Measures (CBM's) have been defined in order to maintain international cooperation, transparency, predictability and stability, and to decrease the risk of misunderstandings, escalation and conflicts connected with the use of ICT-s. Based on resolution 1202. comprising 16 CBM-s in total, the member states undertake the following tasks:

- to voluntarily share their national point of view on the different aspects of national and transnational threats and the use of ICT's.
- to voluntarily develop cooperation and information-sharing among their competent national organisations regarding ICT's.
- to voluntarily consult in order to decrease political and military friction evolving from misunderstandings stemming from the use of ICT's.
- to voluntarily share their measurements of providing an open, interoperable, secure and trustworthy internet network.
- to regard and utilise OSCE as a platform, able to maintain discussion, sharing of good practices, consulting the capacity raising of more secure ICT's, and sharing of effective answers to each threat.
- to prepare national regulations which make the bilateral cooperation between competent offices – primarily, law-enforcement.
- to voluntarily share their national strategies, directives and programs, and also their cooperation with public and private spheres within, and the security and utilisation of ICT's.
- to establish a point of contact, share the contact data for each element of the national structure, which can be utilised in an event of possible incident and they refresh these data on a yearly basis.
- in order to avoid misunderstanding evolving from the lack of common terminology, they prepare a list of terms regarding the use and security of ICT-s together with descriptions and definitions.
- they maintain consulting, voluntarily utilising OSCE platforms and mechanisms in order to ease CBM-connected communication.
- they meet at least three times each year on the level of appointed member nation experts, within IWG frames in regard of discussing, realising and developing CBM's.
- they support information sharing and information exchange among the member states through the organising of workshops, seminars and round table discussions.

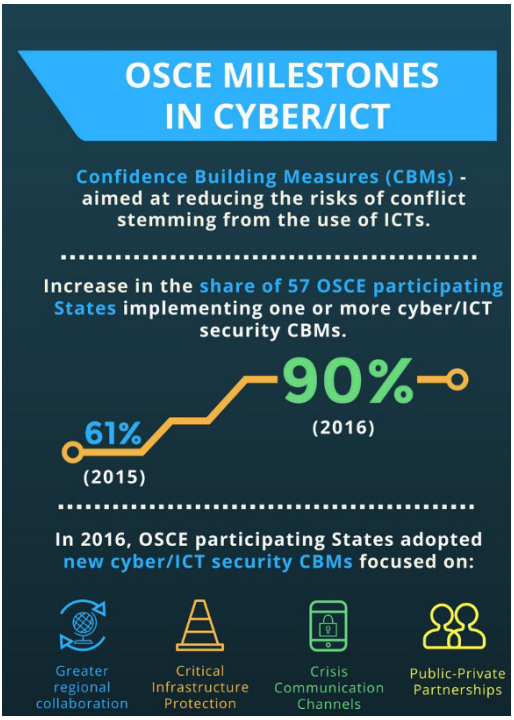

Figure 1. *OSCE milestones in Cyber/ICT* [3]

- they support that their officials and experts can communicate through protected and legal channels in order to avoid and decrease possible misunderstandings, conflicts and escalation
- they promote cooperation between the public and private sphere
- they support regional cooperation among officials responsible for the safety of critical infrastructure
- they support responsible information sharing regarding the vulnerability of ICT safety and use, since all such information and communication supports regional cooperation concerning OSCE. [2]

The work group operates under the leadership of the president, commissioned yearly by the presidency of OSCE and strives to highlight efficient and useful outcomes through the analysis of experts from countries volunteering to process proposals on utilising CBM-s.

3. V4 and the Central-European Cybersecurity Platform

Visegrád Cooperation – based on medieval fundamentals – was formed on 15. February 1991. Initially with the involvement of three countries:

Czechoslovakia, Poland and Hungary. Among the aims of the declaration were the vanishing of the remnants of the socialist block in Middle-Europe, protection of democracy, and the support of quick joining of the member states to the Euro-Atlantic Community. After a successful integration, new aims have been declared, since from the middle of the 2000's, new types of security threats were being met by the member states globally. [3]

AAs a result of the above mentioned security threats the member states started to maintain cyber defence more actively at the beginning of the 2010-s. They prepared their own cyber defence strategy and beyond that they felt the necessity of a regional cooperation within the EU in this field. They began to build up their cooperation system. In 2013 the Central European CyberSecurity Platform (CECSP) was founded as an initiative of Austria and the Czech Republic, with Hungary, Slovakia and Poland also joining, and with the aim of increasing regional cyber security. In order to fulfil that goal, they defined the following five points:

- **Introducing information, knowhow and the best, most effective practice**:
  In order to strengthen their survivability and enhance preparedness against cyber threats, the member states volunteered to strengthen their capabilities and share information and best practice regarding cybersecurity. Also, common education and training are part of the agreement.
- **Planning and realising secure channels of communication**:
  In order to share data and information regarding future, recent and already solved cyber threats, the member states strive to shape such channels that cannot be accessed by unauthorised people.
- **Definition and agreement on category system**:
  In order to share information, the member states have to agree in a category system regarding sensitive data. It is proposed to define such regulations that ease the understanding and analysis of a given cybersecurity incident.
- **Coordination of own perspectives within international forums**:
  According to the agreement the member states have to consult on national aspects in order to harmonise transregional approaches before every larger international cooperation – like EU, NATO, UN, OSCE and ENISA meeting.
- **Developing of practical work groups**:
  With the aim of discussing special topics, there is a possibility to bring temporary groups to life. The form of these groups, working with a minimum of two members, is depending on what exact aim they have been founded for (technical, control, operational, political). Common topics can regard patterns and actual development, hardware and software verification and acquiring transnational cooperation, etc.

The activity and success of the CECSP since the beginning of 2013 can be summarised in not more than the mutual sharing of experience and organising of common training regarding the above principles. The reason stems from the different strategies, the shifting of focus in foreign policy, and the decreasing willingness to share information and experience. While Hungary was among the first EU members to create national a cybersecurity strategy in 2013, The Czech Republic and Poland have taken the role of more innovative and engaging partners [4] All in all, there is a chance to coordinate the cyber defence of the Visegrád nations, but there is still a long way to go in order to achieve this goal, and for the member states to build mutual trust and find a compromise in the differing interests.[5]

4. Conclusion

In order to reach national and regional cybersecurity interests and goals, the development of strong cooperation within the region and an efficient and fast sharing of information is necessary. An effective engagement against cybersecurity threats and challenges makes collective and cooperative work of the member states inevitable. Priority is of course prevention, but fast and effective response to cybersecurity events and crises, crisis management and the process of rebuilding is also of the same importance. Giving a priority to the national interests builds up an obstacle during international cooperation, thus creating a more or less long stagnation in the work and attainment of goals for the given cooperation. Also in the case of OSCE and V4 there are examples of the above reasons causing a fall back in the cooperation, but it is also clear that regarding present and future times, regional cooperation is inevitable to address and solve the new, transnational types of security challenges

Acknowledgement

„Supported by the ÚNKP-18-3-IV-NKE-77 New National Excellence Program of the Ministry of Human Capacities"

References

[1] Gazdag F., Remek É.: A biztonsági tanulmányok alapjai. Dialóg Campus Kiadó, Budapest, 2018.

[2] Decision No.1202 OSCE Confidence-building measures toreduce the risks of conflict stemming from the use of information and communication technologies https://www.osce.org/pc/227281?download=true (accessed on: 2019. febr. 27.).

[3] V4 connects, *Hungarian presidency 2017/2018 of the Visegrad Group* http://v4.gov.hu/a-visegradi-egyuttmukodesrol (accessed on: 2019. febr. 27.).

[4] Rajnai Z., Fregán B.: *Új alapokon a magyarországi kibervédelmi stratégia*. In: A XXII. Fiatal műszakiak tudományos ülésszak előadásai. Proceedings of the 22th international scientific conference of youngth engineers, Kolozsvár/Cluj, Románia, Műszaki Tudományos Közlemények 7. (2017) 351–354. https://eda.eme.ro/handle/10598/29842

[5] Antal József Tudásközpont, *Kutatás- Kutatói Blog* http://www.ajtk.hu/kutatoi-blog/219/a-visegradi-negyek-helyzete-a-kibervedelem-tekintetében-/ (accessed on: 2019. febr. 26.).