Cyber Diplomacy – A New Component of Foreign Policy[6]

Assistant Lecturer Dana DANCĂ, PhD. candidate
"Titu Maiorescu" University, Bucharest
dana.danca@yahoo.com

Abstract
Nowadays, the boundary between virtual and real security is diminished, organized attacks in cyberspace can cause serious consequences in physical reality. Cyber threats have a significant international component, which determines the approach of cyber security in terms of foreign policy.
This analytical approach pays particular attention to the factors determining the need for developing diplomatic instruments specific to cyber space, as a component of foreign policy. The paper focuses moreover on the operationalization of the cyber diplomacy concept and on the analysis of cyber diplomacy mechanisms developed by the European Union.
Keywords: *cyber security, cyber diplomacy, European Union, multi-stakeholders cooperation*

Introduction

Using computer and internet infrastructure, in addition to the economic, social and political benefits created for the international society actors, can cause political and military tensions, misperceptions in their relations or even conflicts between them, thus becoming a new challenge to national and international security. Along with terrorism and the non-proliferation of nuclear weapons and of weapons of mass-destruction, cyberspace represents one of the unconventional threats to international security. [1]

The specific features of cyberspace and the multinational impact of cyber attacks emphasizes the need for a public policy with a stronger international component. Due to the nature of cyberspace and its asymmetric and transnational features, the cyber threat represents a challenge for political leaders, which requires a diplomatic effort similar to the efforts in fighting terrorism.

Cybersecurity has complex valences; the cyberspace can be used as a threat from the terroristic, criminal or political – military perspective, depending on the purpose pursued by the attacker but also on the effects that a cyber attack produces. From this point of view, experts identify four dimensions of cyber insecurity, with different implications, but which may overlap in certain circumstances:

- Cyber-crime;
- Cyber-espionage;
- Cyber-terrorism;

[6] This work was supported by the strategic grant POSDRU/159/1.5/S/141699, Project ID 141699, co-financed by the European Social Fund within the Sectorial Operational Program Human Resourses Development 2007-2013.

- Cyber-warfare.

In this latter perspective, the cyberspace becomes part of the diplomatic and military conflicts between states.

With regard to the actors who use cyberspace as a military territory, attacks can be launched by government structures, either military, intelligence or of another nature, by hackers who are loyal to a government or who are sponsored by governments and by non-state actors, including terrorists. Terrorist organizations use the Internet for recruitment, fundraising, organization and propaganda.

The events of the last decade represent factors of economic, societal and political-military nature that favour the cyber security process. The cyber dependence of the economic sectors and the estimated global cost of cybercrime and cyberespionage are economic factors that have contributed to the enhancement of cyber security.

The societal impact caused by Edward Snowden's revelations on cyber espionage activities of the US government on NATO allies, but also the mass surveillance program of the population in the United States and in some European countries had a diplomatic echo at a global scale. In consequence, the Western European countries have reconsidered their position towards the US-centric model of internet governance. [2] Among the most important political-military factors favouring the enhancement of cyber diplomacy we mention the cyber attacks on IT infrastructure from Estonia in 2007, the hybrid war fought in 2008 in the conflict between Russia and Georgia, the cyber attacks on the uranium enrichment program from Iran in 2010 and the current crisis in Ukraine which has a strong cyber component. Once with the outbreak of hostilities between Russia and Ukraine, the virtual attacks aimed not only Ukraine's IT infrastructure, including the military communication system, but also the ones of Russia, European countries and NATO allies. [3]

In this context of significant increase of politically and military motivated cyber attacks, the trust between political leaders is reduced, especially with regard to control regimes (such as China or Russia), where Internet access is limited, censored or the informatics systems are surveilled. Therefore, along with appropriate defence capabilities, cyber diplomacy development and diplomatic strategies designed to outline the present security environment, are necessary.

The Organization for Security and Cooperation in Europe adopted a set of confidence-building measures to increase trust in cyber security (CBMS). OSCE aims to be a platform for dialogue between Member States in the cyber security field. [4]

General considerations on the concept of cyber diplomacy

At a state level, the activity in cyberspace can create diplomatic disagreements, as national interests and positions of the states can be divergent. Cyberspace becomes a component of foreign policy in the situation where states intensively debate in international fora the issues of the applicability of existing public international law to cyber attacks, the rules of acceptable behaviour in the virtual environment or the respect of human rights in cyberspace. [5]

Cyber diplomacy mechanisms are at an early stage of development. The difficulties in approaching the issue globally arise primarily from the differences in terminology and the different legislation on punishment for the acts committed in cyberspace, both in the stage of investigation and conviction. We consider important to agree upon an international agreement that contains definitions of specific concepts such as global cyber security, aggression in cyberspace and cyber weapons. For example, the Romanian and American legislation use the term cyber security, in the European Union the term is network and information security, while Russia uses the concept of information security.

One of the confidence-building measures stated in OSCE Decision No. 1106/2013 is developing a glossary of terms specific to the security of information and communications technology. The wording of this document will be made in collaboration with all participating states, which voluntarily submit a national list of specific terms with explanations or definitions. This exchange process is being facilitated by the OSCE bodies, including the Conflict Prevention Centre, through its Secretariat.

The concept of cyber diplomacy summarize a series of behaviours and attitudes of the international actors, among which we highlight the availability for dialogue with international partners, the identification of multilateral consultation mechanisms, the acceptance of compromises in order to overcome misunderstandings, the creation of a global culture regarding cyber security, the confidence building between states, the encouragement of transparency in communication, the identification of common advantages offered by cyberspace, the

attention for internal vulnerabilities rather than external threats and the awareness of stakeholders about the cyber risks, threats and vulnerabilities.

Political decisions regarding the cyberspace have strong international implications that require international commitment and collaboration. Therefore, the diplomatic activity in the cyber domain has an important dimension of cooperation, of concluding diplomatic engagements and multi-level agreements, including with the private sector stakeholders. Concluding bilateral and multilateral agreements on cyber security, aims at coordinating policy and harmonizing the legal framework at national level, in areas such as data protection or police and judicial cooperation in cybercrime matters (for instance, extradition and mutual legal assistance agreements). The only international legally-binding instrument in force is the Budapest Convention on Cybercrime adopted by the Council of Europe in 2001. Because of the fact that there are differences between states regarding the punishment of the acts committed in cyberspace, as some states considers a certain act an offense, some sees it as a misbehaviour or even a legal fact, the Budapest Convention is an instrument designed to harmonize the national legislations through its provisions on the activities and practices considered illegal in cyberspace. [6]

Pan-European or transatlantic trainings and multinational joint exercises, represent an important way of establishing common response procedures to cyber incidents. Throughout these trainings and exercises, governments cooperate with representatives from the specialized private sector.

Another way of cooperation consists of information exchange and the exchange of good practices between computer emergency response teams (CERTs), but also between law enforcement bodies and government departments responsible for cyber security.

Investing in innovation, research and development projects, providing technical support to enhance cyber resilience capabilities (technological resources and human resources with specific skills) are also ways of cooperation in the cyber field.

Cyber diplomacy mechanisms at European Union level

At the state and international level, cyber security has been identified as a threat to international security. The European Union considers that transnational

threats to EU security include cyber security, along with nuclear proliferation, international terrorism and organized crime.

According to the EU Security Strategy, cyber security is almost exclusively a national prerogative. Given the functional EU interdependence, the level of national cyber security could strengthen or weaken the collective security of the EU as a whole. [7] However, the EU's role is to coordinate, supplement or establish a minimum legislative level or in the matter of technical capabilities.

The European Union aims to become a strong global player in foreign policy issues with regard to cyber security, identifying six pillars of union cyber diplomacy that reflects the EU values, interests and objectives. [8]

1. Applicability of rule of law and human rights law in cyberspace

The protection and promotion of the human rights is a principle applicable also in cyberspace. Moreover, increasing cyber security must not cause an impairment of fundamental human rights, especially the right to privacy, protection of personal data and freedom of speech.

2. Norms of behaviour in cyberspace

The European Union reiterates the elements set out in the United Nations Report [9], which established the applicability of public international law, including the UN Charter provisions for cyber attacks. It is also noted the need to adapt the existing legislation or to create new rules to reflect the particularities of cyberspace.

3. Cyber capacity building of technological and institutional nature, but also with regard to the human resources skills. At EU level, bodies have been created to manage incidents of various natures that can occur in cyberspace, such as the European Network and Information Security Agency (ENISA) in 2004. The EU uses the existing institutions and mechanisms and structures them in order to respond to the cyber threat - for example, creating the European Cybercrime Centre (EC3) within Europol or the preparatory body of the Council the Friends of the Presidency Group on Cyber Issues.

4. Internet Governance

The European Union promotes the enhancement of the multi-stakeholders Internet governance model, which involves cooperation and coordination between

stakeholders: governments of Member states (law enforcement bodies, cyber incident response agencies, intelligence services), private companies from the information and communications technology and defence industry, international intergovernmental organizations, NGOs, civil society, the academia, technical experts, think tanks.

5. Enhancing the competitiveness and promoting EU economic interests, due to the fact that information and communications technology plays a key role in strengthening the EU Single Market.

6. Strategic engagement with key partners and international organizations

Cyber security cooperation between the EU and third states or international intergovernmental organization, in order to achieve global effects, but also between the Member States, as the EU encourages a general legal framework for bilateral agreements.

A special role in the diplomatic activity of the EU plays the strategic partnerships with the ten states (USA, Canada, Mexico, Brazil, South Africa, India, China, Japan, South Korea and Russia). The EU-US partnership is the most developed in cyber security, especially within the Working Group on Cybersecurity and Cybercrime – WGCC, established in 2010.

Russia is not considered by the EU a strategic collaborator in the cyber security field, the situation being similar with China; both states are considered sources of cyber insecurity due to espionage activities and politically motivated attacks that they perform. [10] The EU's relationship with Russia has deteriorated since the beginning of the conflict with Ukraine. Russia and China cooperate in the cyber security field especially in the Shanghai Cooperation Organization, founded in 2001.

Within the United Nations, in the ‘90s, Russia was the initiator of a cybersecurity regulation process. In 1999, the diplomatic efforts resulted in the adoption of the General Assembly Resolution on the Developments in the Field of Technology and Telecommunication in the Context of International Security. [11]

Conclusions

From a regional point of view, the diplomatic activity has increased due to the significant contributions of international intergovernmental organizations; unlike the global perspective that is not very well developed. Therefore, we consider necessary

the promotion of an international cyberspace policy involving all multi-stakeholders, in order to obtain social development and economic and political progress at a global level.

The Budapest Convention is one of the most appreciated instruments of diplomatic effort at a global level. However, the peculiarities of cyberspace can cause controversy about the extent to which cyber security international conventions respect human rights and state sovereignty.

We moreover highlight the opportunity for cyber security to be the central theme of regional and international summits, since the field is currently mostly addressed in correlation with transnational crime or terrorism.

References:

[1] The National Defence Strategy of Romania, Bucharest, 2010.
[2] T. Renard *(2014), The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security*. The European Strategic Partnership Observatory, Working Paper 7, June, p. 21.
[3] *Ibidem*, p. 8.
[4] Decision No. 1106. Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. The Permanent Council of the Organization for Security and Cooperation in Europe, 3 December 2013.
[5] Council of the European Union. Outcome of Proceedings 6122/15. *Council Conclusions on Cyber Diplomacy.* Brussels, 11 February 2015.
[6] Council of Europe. *The Budapest Convention on Cybercrime*. Budapest, 23 November 2001.
[7] European Commission, High Representative of the European Union for Foreign Affairs and Security Policy. Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* JOIN(2013) 1 final, Brussels, 7.2.2013.
[8] Council of the European Union. *An Outline for European Cyber Diplomacy Engagement.* 9967/4/14, Brussels, 23.09.2014.
[9] United Nation General Assembly, Sixty-eight Session, Document A/68/98. The Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013.
[10] Thomas Renard *(2014), The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security*. The European Strategic Partnership Observatory, Working Paper 7, June, p. 21.
[11] F.-S. Gady, G. Austin (2010), Russia, The United States and Cyber Diplomacy: Opening the Doors. East West Institute. New York, p.10.