MEST Journal
doi: 10.12709/mest.09.09.02.02

AN ANALYSIS OF SERBIA'S CYBER-POLITICAL HABITAT

Begum Burak
Independent Researcher, Istanbul, Turkey
https://orcid.org/0000-0002-0071-7330

JEL Category: **F52, H56**

Abstract

In the post-Cold War era, new strategies and approaches emerged in both political and security-related issues. Since the late 1990s, the notions such as "cyberspace" "cyberpolitics" and "cybersecurity" have taken a decisive role in the international political scene and the discourses of state elites. Today, nation-states do not only use military tools to fight terrorism. Cybersecurity instruments are also used, especially in intelligence. This study is an attempt to trace the cyberpolitics practices and cybersecurity policies in one of the Balkan states belonging to the post-communist state group, Serbia. For this attempt, this study will coin a new concept called "Cyber-political habitat". Serbia has a considerable degree of instability in internal politics. Serbia has witnessed serious protests and social media has been the primary channel through which the protesters gained support. In this regard, the cyber-political habitat of Serbia needs a particular definition and attention. The main objective of the study is to shed light on the sui generis character of Serbia in pursuing the goals related to cyberpolitics and cybersecurity. Serbia as one of the Balkan states is a unique example because despite not being a member of NATO, Serbia has taken important steps in cooperation with NATO in the cyber-security area.

Keywords: *Serbia, cyber-security, NATO, post-Cold War era, cyber-political habitat*

1 INTRODUCTION

In the post-Cold War period, world politics has witnessed major changes in both structural and security-related dimensions. In today's world, not only military measures, but also unconventional methods like the establishment of cybersecurity units in state departments and cooperation with major technology companies like Google are required for protecting both the national security and internal order and peace. The main objective of this study is to trace the cyberpolitics and cyber-security practices in Serbia. Serbia has a considerable degree of instability in internal politics. The country has witnessed social uprisings and protests and social media have been the primary channel through which the protesters gained support and got organized. In this regard, this study also aims to shed light on the sui generis character of Serbia in pursuing the goals related to ensuring cyber-security. It is known that Serbia as one of the Balkan states is a unique example because despite not being a member of NATO, Serbia has taken important steps in the cooperation with NATO in cyber-security area.

Address of the author:
Begum Burak
begumburak1984@gmail.com

The post-Cold War era refers to the end of the Cold War with the triumph of United States. In this era, the Soviet Union dissolved, and new countries emerged. As a result of the triumph of capitalism, a new concept called "post-communism" emerged. Post-communism is the period of political and economic transformation in former communist bloc states in which new governments aimed to create capitalist economies (King, 2000). Serbia is one of the post-communist states along with Bosnia and Herzegovina, Bulgaria, Croatia, North Macedonia, Montenegro, and Slovenia.

Nazli Choucri (2012) notes that in 1990 only a quarter of a million people used the Internet; today a third of the world population is connected to Internet and the number is growing day by day. In today's world, cyberspace is an important dimension of world politics along with national security dimension. The implications of this new cyberpolitical reality are not only important for technologically advanced countries such as United States, the newly independent states in 1990s also have their own concerns and methods to survive in such an international context. This study is an attempt to analyze how Serbia manages cyberpolitics and promotes security in cyberspace. Serbia is not a member of NATO, but this does not prevent the country from making cooperation with NATO in cyber-security issues.

This study argues that Serbia performs well in many areas of cybersecurity having a strong commitment to addressing the challenges of cybersecurity. The contribution of this study to the cyberpolitics literature is the concept of "*cyber-political habitat"* and the limitation of the study is the lack of enough academic research related with Serbia's cybersecurity policies. The study proceeds in three sections. The first part addresses how the concept of cyberspace changed in the aftermath of the Cold War. This part is also devoted to the definition of the concept of "*Cyber-political habitat".* The second part addresses Serbia and Serbia's relationship with NATO in general from a historical perspective. The third part analyzes Serbia's cyber-political habitat and risks and threats the country faced. Moreover, this part addresses what kind of policies and initiatives Serbia has adopted in cooperation with NATO and other international organizations in terms of cybersecurity.

2 CYBERSPACE IN POST-COLD WAR ERA AND THE CONCEPT OF "CYBER-POLITICAL HABITAT"

The concept of "Cyberspace" was first used by William Gibson in his 1984 book, Neuromancer to represent a virtual environment. The term has multiple meanings. For instance, the Oxford English Dictionary defines it as "the space of virtual reality; the notional environment within which electronic communication (esp. via the Internet) occurs". Cyberspace can be defined as the interdependent network of information technology infrastructures including the Internet, telecommunications networks, and computer systems (Olsen, 2008).

The post-Cold War era denotes to the victory of United States and the collapse of communist bloc. In this newly shaped international system, the security parameters have changed in parallel to the rapid development of digitalization. The Cold War years were characterized by the nuclear armament. The weapons of mass destruction were the main tools of fight during this period. However, in the post-Cold War era, the types of warfare changed. In contemporary world, the concept of "cyber warfare" plays a key role in the analysis of threats and risks in world political arena. According to Geers (2008), there are five main tactics used in cyber warfare: (1) espionage, (2) propaganda, (3) data modification, (4) infrastructure manipulation, (5) denial of service.

Today, cyberspace has become a war zone for ideological combats. It can be said that there is a change in security perception in the post-Cold War era. Cultural, social, and environmental security issues have gained importance in addition to economic and military security. It is known that Eastern European countries and Western European countries cooperated handling environmental problems (Laakkonen et. al, 2016: 4-8). The steps taken in the realm of cyberspace and cybersecurity are significant while addressing social, cultural and environmental problems. Cooperation on cybersecurity and environmental issues requires different types of relationships, for instance among governments and their law enforcement institutions or stakeholders. These

different types of cooperation can be in the form of bilateral cooperation or formal multilateral cooperation, such as the Council of Europe with the European Cyber Crime Convention known as the "Budapest Convention" (Cassotta & Pettersson, 2019: 622-23).

The post-Cold War era has long been characterized by a bipolar international system dominated by Russia and USA. This bipolarity shows that these two countries have been leading countries not just in military terms but also in technological and cyberspace-related terms as well. Today, international system is considered to become a mixture of a multipolar and unipolar structure. The international system of the post-Cold War era has at least five major powers, Europe, the United States, China, Japan, and Russia (Yılmaz, 2008: 46). Hence, it can be argued that, today it is not possible for a single country to manage the global Internet network and globally accessed cyberspace in an effective way. Cooperation is vital and in this context the functions of international organizations such as European Union or NATO are increasing substantially to combat cybercrimes and cyberterrorism.

The post-Cold War era brought fundamental changes in world politics. The budgets saved for military spending started to decline while Internet-related security tools started to shape the behaviors of the actors. The military command-control networks and systems have begun to be organized according to the requirements of the concept of "cyberwar" (Bıcakcı, 2012: 210). The post-Cold War era witnessed the rapid progress in information technologies. Cyberspace has never been as important as before and threats also are more challenging and complex for nation-states. Cyberspace is anarchic having no central authority. Today, it is hard to detect what kind of risks and dangers are evident in cyberspace. NATO's Cooperative Cyber Defence Centre of Excellence unit based in Estonia distinguishes between "cybercrime," and "cyber warfare." (Moss, 2013). This can be a sign showing the diversification of threats for nation-states in the post-Cold War era.

This study coins the concept of "*Cyber-political Habitat"* to better explain Serbia's unique position in cyberspace and cyberpolitics. To define Cyber-political habitat, it is important to cover the characteristics of cyberspace. Firstly, cyberspace has a trans-boundary nature. It is beyond physical border of nation-states. Secondly cyberspace enables participation as it decreases barriers to activism and expression. Thirdly, in terms of accountability, cyberspace bypasses the mechanisms of responsibility, so it is hard to control illegal actions in cyberspace (Choucri, 2012: 4).

Cyberpolitics can broadly be defined as the intersection of political sphere and cyberspace. The arena of cyberpolitics is located at the intersection of "*innovation in information and communication technology and applications to the discourse of political analysis and political inquiry*" (Chouri, 2000: 246).Cyberspace makes political participation easier as computer networks enable masses to interact and communicate freely. The intersection of politics and cyberspace has reinforced some of the fundamental precepts of politics. It has not just enhanced the potential for political participation, but also created new possibilities for expressing views. It is difficult to identify an area of politics that is devoid of cyber-related manifestations (Choucri, 2012: 10). In the post-Cold War era, the traditional political tools and methods are not sufficient for the states to guarantee sovereignty or retain control over instruments of force. In this regard, cyber-political instruments play a key role in world politics. International agreements protecting cyberspace and combating cybercrimes can be seen as examples of cyber-political instruments.

Based on the above-noted explanations, this study defines the concept of "*Cyber-political habitat*" as an arena consisting of the interactive and dynamic relationship between political space and cyberspace. Political space can be defined as the space shaped by governmental dynamics. Cyberspace refers to all the virtual and computer-related environments. The *Cyber-political habitat* is unique and distinct for every country depending on their economic, technological, and political conditions. It can be argued that the technologically- advanced, politically stable, and financially well-developed countries like USA has a convenient *Cyber-political habitat* for fighting against cybercrimes and ensuring cybersecurity while countries having internal instability and economic problems like that of Serbia does not

have a convenient *Cyber-political habitat* for ensuring cybersecurity. Thus, Serbia and similar countries need international cooperation for ensuring cybersecurity more and Serbia's cooperation with NATO can be seen as an example of this.

3 A SNAPSHOT OF SERBIA'S HISTORY AND SERBIA'S RELATIONSHIP WITH NATO

The Federal Republic of Yugoslavia was established in 1992 as a federation. In 2003, it was reconstituted as a political union called the State Union of Serbia and Montenegro. Serbia became a sovereign republic in 2006 after Montenegro voted in a referendum for independence (Recknagel, 2006). Serbia was part of two South Slavic states, including the interwar Kingdom of Serbs, Croats, and Slovenes and the Socialist Federal Republic of Yugoslavia from 1945 to 1992. Belgrade was the capital of both Yugoslav states, and Serbia was widely regarded as the dominant force in political, and military affairs. Serbia used to be at the center of the Balkan conflicts during the 1990s (The US Congressional Research Service Report, 2018). After the wars in the Balkans in the 1990s Serbia became one of the main destinations for refugees from Bosnia and Herzegovina and Croatia.

Regarding Serbia's relationship with international organizations, it is known that Serbia officially applied for European Union membership on 22 December 2009. Serbia is expected to complete its negotiations by the end of 2024, allowing it to join the EU in 2025 (Rettman, 2018). In terms of relations with United Nations, it is known that Serbia is a member of United Nations. Serbia joined the UN in 2000, as the Federal Republic of Yugoslavia. After gaining full independence in 2006 the President of Serbia informed the United Nations Secretary-General that the membership of Serbia and Montenegro in the UN was being continued by Serbia (Schneider, 2006).

Serbia's relationship with NATO can be considered as a very dynamic relationship. It is known that unlike other Western Balkan states, Serbia does not aspire to join NATO. As a result of NATO's intervention in Yugoslavia in 1999, Serbia today enjoys exceptionality in its relations with NATO that is being acknowledged by both Serbia and NATO. According to Radoman (2012: 4) this exceptionality implies "*being the only Balkan state that has not either already achieved NATO membership, as is the case with Croatia and Albania, or declared that ambition, as Montenegro, Macedonia and Bosnia and Herzegovina have done.*" Serbia is known as the only Western Balkan country that is least interested in joining NATO, despite recent improvements in relations. It is noteworthy to state that, despite having a turbulent past with NATO, Serbia's security policies are tailored in accordance with the security concepts of NATO from the end of the Cold War onwards (Radoman, 2012: 18).

Before becoming a sovereign Republic in 2006 NATO had suffered from cyber-crimes committed by the Serbians. The Serbian computer hackers denied public access to the web server supporting the public affairs apparatus of the NATO operation in Kosovo, rendering the server virtually inoperable for several days in 1999 (Verton, 1999).

On the other hand, in recent years, Serbia has begun to deepen its cooperation with NATO on issues of common interest. Cooperation has deepened since 2015, when the country agreed its first two-year Individual Partnership Action Plan-IPAP. In July 2021, Serbia will complete its most recent IPAP, at which point it will either be renewed or transition to the new Individually Tailored Partnership Programme (NATO Analysis, 2021). NATO and Serbia make cooperation in various fields and cybersecurity is one of these fields. It is known that, in 2016, NATO recognized cyberspace as a domain of operations.

4 SERBIA'S CYBER-POLITICAL HABITAT: STRUCTURE, ACTORS, RISKS AND PRECAUTIONS

"Cyber-political habitat" as noted earlier can be defined as an arena consisting of the interactive and dynamic relationship between political space and cyberspace. The *Cyber-political habitat* of Serbia is dependent on the economic, technological, and political parameters. There were 6.89 million internet users in Serbia in January 2021 and Internet penetration in Serbia stood at 79.0% in January 2021. (Kemp, 2021).

In Serbia social media is used effectively during mass protests. One of these protests broke out in 2018. The "One of Five Million" protests lasted over a year. These protests represented the widest outbreak of popular discontent since the collapse of the Milosevic regime in 2000 and especially the left-wing groups used social media to increase their visibility (Pesi& Petrovic, 2020)

Serbian National Internet Domain Registry (RNIDS)[1] states that criminal offences against computer data security according to the Republic of Serbia Criminal Code are as follows: (1) damage to computer data; (2) computer sabotage; (3) computer viruses; (4) unauthorized access to personal computers; (5) electronic data processing denial; and (6) unauthorized use of computer networks. In the legislation of Serbia different dimensions of the right to personal privacy in digital platforms are guaranteed by the Constitution of the Republic of Serbia. Also, the Law on Personal Data Protection provides the conditions for collection and processing of personal data (cited in Vilic, 2018: 126).

Academic literature published in English on Serbia's cybersecurity is quite limited. One of the significant studies addressing Serbia's cybersecurity issue is a report published in 2016 by Diplo Foundation with the support of the Federal Department of Foreign Affairs of Switzerland. According to this report titled "Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities" Serbia's legal and institutional framework in cybersecurity is based on the Law on Information Security, which was adopted in early 2016. The Diplo Report (2016: 22) notes the following about Serbia's fight against cybercrimes:

Like other countries in the region, the legal mechanisms to fight cybercrime are in place. The Criminal Code provides norms on criminal offences in accordance with legal frameworks of the CoE and the EU. The Criminal Code does not regulate cyber terrorism as an offence, although cyber terrorism can be prosecuted based on existing offences on terrorism and computer data."

In terms of cybersecurity challenges in Serbia, it is documented that listening or control of the flow of information of nearly 400.000 people occurs on daily basis, of which only 15.000 legal, while others are under unauthorized supervision. In Serbia, the monitoring of communications has reached major proportions and that it is vital to establish a serious control system (cited in Sinteza Report, 2014). Apart from that, in 2014 Serbia witnessed another major cyber threat. Personal data of millions of citizens were leaked from the database of the Serbian Business Register Agency (Milatovic, 2015).

The World Bank Press Release (2020) notes that to combat threats and risks in cyberspace, Serbia has undertaken major steps. Serbia has a substantial commitment to addressing the challenges of cybersecurity providing a legal foundation and protection mechanisms. For example, in 2019, Serbia ratified and implemented the Council of Europe Convention on Cybercrime (Budapest Convention), including its additional protocol on xenophobia committed through digital platforms (Council of Europe iPROCEEDS, 2019). Despite not being a member of NATO, Serbia has made various cooperations with the Alliance in cybersecurity area. It is known that in 2007, Serbia joined NATO Science for Peace and Security Programme and it has become increasingly active over time (Andjelkovic, 2017). Also, in 2017, the civil servants from the Office of the National Security Council and Classified Information Protection of Serbia were trained to deal with information systems security. The training took place as part of NATO's Science for Peace and Security Programme (NATO News Release, 2017).

5 CONCLUSIONS

This article has aimed to address Serbia's cyberspace and cybersecurity policies through coining the concept of "cyber-political habitat". Following this aim, first the changing nature of international system and the emerging tactics and strategies used in the post-Cold War era have been put under scrutiny. The international system of the post-Cold War era has multiple actors

[1] The official web page of Serbian National Internet Domain Registry retrieved from https://www.rnids.rs/en/about-us/cyber-security(15.05.2021)

shaping world politics. This makes it impossible for a single country to manage the global Internet network and protect cyberspace in an efficient way. Cooperation is vital and, in this regard, international organizations such as European Union or NATO have become more significant to combat cybercrimes and cyberterrorism. The concept of Cyber-political habitat can be defined as an arena consisting of the interactive and dynamic relationship between political space and cyberspace. The *Cyber-political habitat* of Serbia is dependent on the economic, technological, and political parameters of the country.

The emergence of cyber warfare and the increasing importance of information technologies for ensuring national security have been two significant factors shaping today's world order. Serbia is not an exception in the post-Cold War order. The rising importance of cyberpolitics led Serbia to build partnerships with NATO despite not being a part of the organization. Serbia has established a substantial commitment to addressing the challenges of cybersecurity providing the legal foundation and protection mechanisms. It can be argued that Serbia performs well in many areas of cybersecurity having a strong commitment to addressing the challenges of cybersecurity. However, it should also be noted that the country has serious online data privacy problems, so a more robust protection mechanism is an urgent need for protecting online privacy.

WORKS CITED

Andjelkovic, K. (December 25, 2017). Cyber security: New area of cooperation between Serbia and NATO?, retrieved from https://europeanwesternbalkans.com/2017/12/25/cyber-security-new-area-cooperation-serbia-nato/ (14.05.2021).

Bıcakcı, S. (2012). Yeni Savas ve Siber Juvenile Arasında NATO'nun Yeniden Dogusu, Uluslararası Iliskiler, 9/ 34, 205-226

Cassotta, S., & Pettersson, M. (2019). Climate Change, Environmental Threats and Cyber-Threats to Critical Infrastructures in Multi-Regulatory Sustainable Global Approach with Sweden as an Example. Beijing Law Review, 10, 616-642.

Chouri N. (2000). Introduction: CyberPolitics in International Relations,International Political Science Review, Vol 21(3), 243-263

Choucri N. (2012). Cyberpolitics in International Relations, The MIT Press.

Council of Europe iPROCEEDS, (March 11-12, 2019). iPROCEEDS: Assessment of legislation on cybercrime and e-evidence in Serbia, retrieved from https://www.coe.int/en/web/cybercrime/-/iproceeds-assessment-of-legislation-on-cybercrime-and-e-evidence-in-serbia (14.05.2021).

Diplo Foundation Report, (2016). Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities, retrieved from https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf (11.05.2021)

Geers, K. (2008). Cyberspace and the changing nature of warfare, SC Magazine, retrieved from https://ccdcoe.org/library/publications/cyberspace-and-the-changing-nature-of-warfare/ (16.05.2021).

Gibson, W. (1982). Neuromancer, New York, Ace Publishing

Kemp, S. (February 11, 2021). Digital 2021: Serbia, retrieved from https://datareportal.com/reports/digital-2021-serbia (14.05.2021)

King, C. (2000). Post-Postcommunism: Transition, Comparison, and the End of "Eastern Europe". World Politics, 53(1), 143-172.

Laakkonen et.al (2016). The Cold War and environmental history: complementary fields, Cold War History, 4, 377-394.

Milatovic, I. (July 8, 2015). Serbia's efforts to respond to cyber security threats, retrieved from https://www.osce.org/mission-to-serbia/170361 (12.05.2021).

Moss, T. (April 19, 2013). Is Cyber War the New Cold War?. retrieved from https://thediplomat.com/2013/04/is-cyber-war-the-new-cold-war/ (9.5.2021)

NATO Analysis (April 6, 2021). Relations with Serbia, retrieved from https://www.nato.int/cps/en/natohq/topics_50100.htm (10.05.2021).

NATO News Release (November 23, 2017). NATO trains Serbian civil servants in cyber defence, retrieved from https://www.nato.int/cps/en/natolive/news_149194.htm?selectedLocale=en (14.05.2021)

Olsen, Kelly L. (2008). Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative. Research paper, Carlisle Barracks, PA: U.S. Army War College.

Pesic J. and Petrovic J. (2020). The Role and the Positioning of the Left in Serbia's "One of Five Million" Protests. *Balkanologie*, *15*(2), 1-21.

Recknagel, C. (May 22, 2006). Montenegro: Independence Referendum Turns into Cliffhanger, retrieved from https://www.globalsecurity.org/military/library/news/2006/05/mil-060522-rferl03.htm (10.05.2021)

Rettman, A. (June 28, 2018). Macedonia to join next wave of EU enlargement, retrieved from https://euobserver.com/enlargement/142220 (9.5.2021)

Radoman, J. (2012). Serbia and NATO: From Enemies to (almost) partners, retrieved from https://www.files.ethz.ch/isn/144512/nato_and_serbia_(2).pdf (10.05.2021)

Scheneider, D. B. (June 29, 2006), World Briefing | Europe: Montenegro: U.N. Makes It Official, retrieved from https://www.nytimes.com/2006/06/29/world/world-briefing-europe-montenegro-un-makes-it-official.html (10.05.2021)

Sinteza Report, (2014). Impact of Internet on Business in Serbia and Worldwide, published by Singidunum University, retrieved from http://eprints.ugd.edu.mk/10076/1/Sinteza-2014.pdf#page=705 (11.05.2021)

The official web page of Serbian National Internet Domain Registry retrieved from https://www.rnids.rs/en/about-us/cyber-security (15.05.2021)

The Oxford English Dictionary, retrieved from https://www.oed.com/ (9.5.2021)

The US Congressional Research Service Report, (2018). retrieved from https://fas.org/sgp/crs/row/R44955.pdf (10.05.2021)

The World Bank Press Release (December 21, 2020). Serbia Has Undertaken Critical Steps in Cybersecurity, Says First Cybersecurity Capacity Maturity Model Assessment, retrieved from https://www.worldbank.org/en/news/press-release/2020/12/21/serbia-has-undertaken-critical-steps-in-cybersecurity-says-first-cybersecurity-capacity-maturity-model-assessment (12.05.2021)

Verton, D. (April 4, 1999). Serbs launch cyberattack on NATO, retrieved from https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx (16.05.2021)

Vilic, V. (2018). International and Serbian legal framework of the right to privacy in cyberspace, MEST Journal, 6(1), 119-131

Yılmaz, M. E. (2008), Alternatives: Turkish Journal of International Relations, Vol. 7, No. 4, 44-58.

Received for publication: 17.05.2021
Revision received: 09.06.2021
Accepted for publication: 06.07.2021

How to cite this article?

Style – **APA** *Sixth Edition:*

Burak, B. (2021, July 15). An analysis of Serbia's cyber-political habitat. (Z. Cekerevac, Ed.) *MEST Journal, 9*(2), 7-14. doi:10.12709/mest.09.09.02.02

Style – **Chicago** *Sixteenth Edition:*

Burak, Begum. 2021. "An analysis of Serbia's cyber-political habitat." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 9 (2): 7-14. doi:10.12709/mest.09.09.02.02.

Style – **GOST** *Name Sort:*

Burak Begum An analysis of Serbia's cyber-political habitat [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, July 15, 2021. - 2 : Vol. 9. - pp. 7-14.

Style – **Harvard** *Anglia:*

Burak, B., 2021. An analysis of Serbia's cyber-political habitat. *MEST Journal,* 15 July, 9(2), pp. 7-14.

Style – **ISO 690** *Numerical Reference:*

An analysis of Serbia's cyber-political habitat. **Burak, Begum.** [ed.] Zoran Cekerevac. 2, Belgrade – Toronto : MESTE, July 15, 2021, MEST Journal, Vol. 9, pp. 7-14.