STUDIA UBB. EUROPAEA, LXII, 2, 2017, 5-15

CYBERSPACE AND THE NEW WORLD ORDER

Melania-Gabriela Ciot*

DOI:10.24193/subbeuropaea.2017.2.01
Published Online: 2017-06-30
Published Print: 2017-06-30

Abstract
The present article is trying to bring into attention the new concept of ***cyberization*** *of IR, by argumenting the importance of cyberspace and the instruments that it provides for the scholars and practitioners for a new international relations typology. The constructivist approach is used for the notion of state responsibility, for underlying the behavior of a state in cyberspace. The necessity of an international cyberspace policy is evidenced, as well as the proposed international norms for assuring the cybersecurity. The open international cyberspace will challenged national sovereignty and the state leaders will have to find ways of responding to this continuous and sophisticated threats that appeared recently.*
Key words: cyberspace, cybersecurity, digital world, international policy, world order

1. Introduction

The challenge of the process of *cyberization* of the International Relations opens a sophisticated debate that ask for an interdisciplinary approach. This debate will invite scholars and practitioners from different fields of activity to join the exploration of the relation between cyberspace and international relations.

* PhD, Associated Professor, Department of European Studies and Governance, Faculty of European Studies, Babeș-Bolyai University, Romania. Contact: Gabriela.Ciot@euro.ubbcluj.ro

The idea of this article and of coordinating this number of journal *Studia Europae* under the topic *Cybersecurity and the restructuring of the international system* came from the observation of the lack or insufficient contributions in discussions and/or debates (not mentioning the research) from scholars and experts from academic community on the topic of the influences that cyberspace exerts nowadays on the world order and the impact that it will have on restructuring of the international system or on the approaches of various subjects from the IR field, such as: decision-making, international policies, international politics, international security, peacemaking, conflict, cooperation, negotiations, diplomacy.

Our dynamic society brought into attention new challenges for our daily life, as terrorism, emotional implications of decision-making process, the increasing role of behavioral international relations, the threats of cyber-attacks and their increasing occurrence. We can say that we are living in a cyberworld and that we need cyber mechanisms to convert to this frame and tempo and to develop a sort of resilience to new threats coming from this new sort of non-state actor from international cyberspace that changes the perceptions of reality, our attitudes, and knowledge processes.

The present article will present the implications of the cyber dimension in the restructuring of the international system, the research opportunities for the scholars from academic community and some possible developments of the international relations' topology.

2. The *cyberization* of IR

Pablo A. Mazurier[1] (2015) proposes a division of the social world in four areas:

a. *international arena* – with state actors searching for power.
b. *transnational dimension* - developed after the last wave of globalization, based on multinational corporations (MNCs) searching for economic benefits.
c. *global community* – facilitated by the work of international organizations, NGOs and social networks.
d. *cyberspace* - all the actors from the other fields behave searching for cyberpower.

[1] Pablo A. Mazurier, *Facebook in Cyber Politics*, 2015, [http://www.cyberpolitics.eu/cyberpolitics_art_04_facebook.html], 4 June 2017

The author believes that cyberpowers are managed by cyber-actors depending on the knowledge and on the control of the infrastructure and of networks. Cyberspace is connected with the other three areas. The "cyber-actors exercises cyberpower in order to secure their own interests, not exclusively related with the cyberspace"[2].

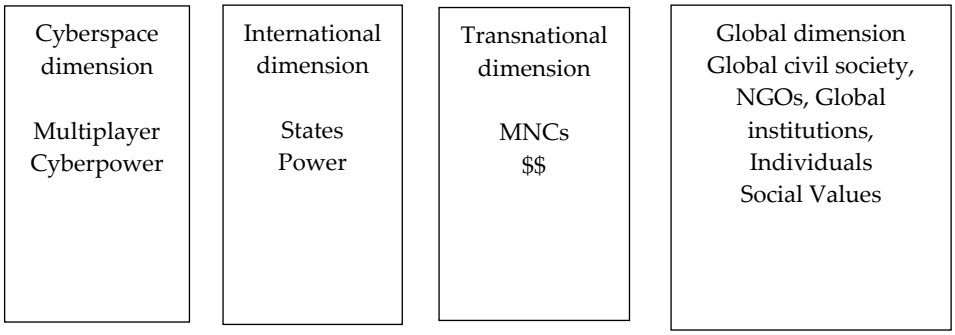

Fig. no. 1: The dimension of social world (after Mazurier, 2015, http://www.cyberpolitics.eu/cyberpolitics_art_04_facebook.html)

As we can see from above figure, the cyberspace represents one dimension of social world, characterized by multiplayers which exerts cybpowers by knowledge, infrastructure and networks[3].

Bruner[4] (2014) refers to the cyberspace as an international, special environment, in which is hard to attribute some actions to a specific actors – and this brings novelty to the world order, because we cannot establish the responsibility. In his article, the author presents different models of state responsibility and applies it to the cyberspace dimension, focusing on the behavior of a state in cyberspace.

By using a constructivist perspective for approaching the notion of state responsibility as basis for prospecting it in cyberspace, Bruner[5] identifies two models: vertical – communitarian model and horizontal – bilateral model:

[2] *Ibidem*
[3] *Ibidem*
[4] Tomáš Bruner, 2014, *States in cyber-space: perspectives of responsibility beyond attribution*, [https://ecpr.eu/.../f1874dac-6e16-4d9c-b936-723754fcc869....], 23 June 2017
[5] *Ibidem*, p. 3

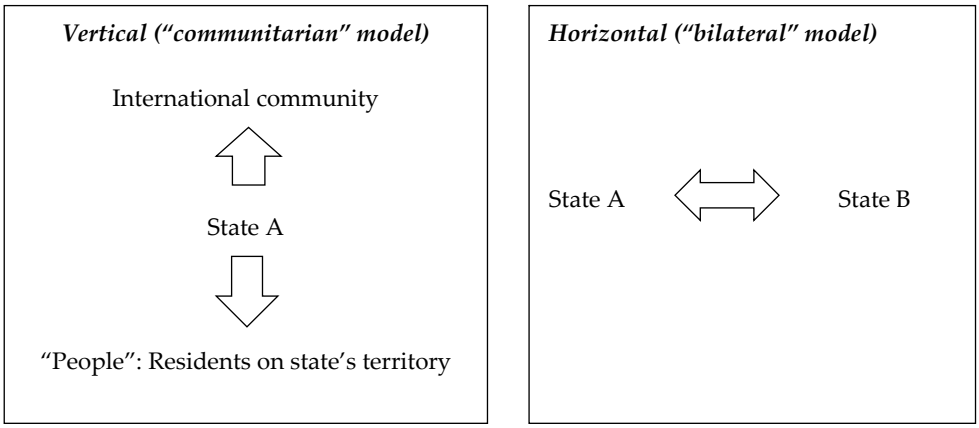

Fig. no. 2: Models of state responsibility (after Bruner, 2015, p. 4).

The vertical model states that the state responsibility toward the international community and to its citizens and demands that the state responsibility should express the interest of people, rather that the states and serves to their protection[6]. The horizontal model underlines that the state's responsibility is understood in terms of bilateral relationships of states[7].

The constructivist approach could be used by connecting these models with the constructed levels of anarchy proposed by Alexander Wendt[8], as Bruner proposed[9]. He mentioned the three cultures of this anarchy introduced by Wendt: Hobbesian (deep enmity of states, continuous war), Lockean (rivalry of states, war as acceptable optional behavior) and Kantian (friendship of states, war is prohibited)[10]. According to him, the vertical ("communitarian" model) is specific to the Kantian anarchy and the horizontal ("bilateral" model) could be correlated with the Lockean anarchy.

---

[6] *Ibidem*, p. 4
[7] *Ibidem*, p. 5
[8] Alexander Wendt, *Social Theory of International Politics*, Cambridge: Cambridge University Press, 1999, p. 246-311
[9] Tomáš Bruner, *op.cit.*, p. 6
[10] *Ibidem*

The cyberspace could be connected with the second Lockean culture of anarchy of Alexander Wendt[11]. But this construction is a process, not an outcome, without a guarantee that the state responsibility in cyberspace may forever work[12]. The limitations of this model is that it relies on territorialization and monopoly of state on coercive use of force, and in case on cyberspace cannot be applied.

But when we are speaking about the cyberspace, we haven't established the reference points. One could be the violation of international law norms, namely cyber-attacks. Without going on the legislative arguments, we could just mention the ten categories of state responsibility for cyber-attacks, relevant for policy-making [13]:

- state prohibited cyber-attacks;
- state prohibited but inadequate;
- state ignored;
- state encouraged;
- state shaped;
- state coordinated;
- state ordered;
- state rogue conducted;
- state executed;
- state integrated.

In cyberspace, the great powers will have no other choice but to cooperate and create rules, norms, and standards of new behavior and a new international order[14]. The international order in cyberspace implies the structural change, and a permanent negotiation of power and competition. The multipolarity structure of international system is the result of power distribution and power is important in international politics. And international politics are anarchic. Rules are important for international life, representing represent the fundamental normative principle of international politics[15].

---

[11] *Ibidem*, p. 11
[12] *Ibidem*
[13] *Ibidem*, p. 8
[14] James Wood Forsyth Jr., Maj Billy E. Pope, "Structural Causes and Cyber Effects Why International Order is Inevitable in Cyberspace", in *Strategic Studies Quarterly*, Winter 2014, p. 113
[15] *Ibidem*, p. 116

The global players have to cooperate to create rules to shape the international order, but it is difficult to do so in cyberspace. Why is that so difficult? Because it concerns sovereignty, freedom of speech, and democracy and it is almost impossible to govern cyberspace. No state alone could do all, only by cooperation. A good example are the USA which proposed an International Strategy for Cyberspace.

In May, 2011, former President Obama has launched the *International Strategy for Cyberspace*, with three important keywords: prosperity, security and openness in a networked world[16]. That was the signaled for international actors that a new dimension of international system was framed and that a new international policy - cyberspace policy – will designed the global governance.

The prosperity is visible by using the means of new technologies, which brought advantages in different spheres of daily lives, as:

- e-business, which supports jobs creations and economic development opportunities for companies;
- learning (with videoconferences facilities) and field-changing research;
- e-administration, by empowering people by using of new technologies, and by making public administrations more open, transparent and responsive.

The international security is challenged for a few years to re-design its priorities, strategies, mechanisms and means (technological, laws, diplomacy) in order to response to this new forms of crime and aggression - cyberattacks, in order to protect our innovations, that intend improve lives and drive markets. Cybersecurity is a new field of international security, without which we cannot conceive any initiative of security policy and international or national level.

Nevertheless, the digital world is not a privileged space, but a dimension of international environment with specific laws, conduct for state and non-state actors, for individuals and public or private entities, as well as one of the best examples for an interconnected community, where public administrations, academia, private sector and other non-state actors work together for a common goal.[17]

---

[16] *International Strategy for Cyberspace. Prosperity, Security and Openness in a networked world*, 2011, [https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyber], 1 June 2017

[17] *Ibidem*.

The proposed international cyberspace policy is based on three principles: fundamental freedoms, privacy, and the free flow of information[18]. Besides the freedom of expression and association, is relevant for this policy, for the first principle to mention ability "to seek, receive and impart information and ideas through any medium and regardless of frontiers"[19]. It is about the freedom of speech in cyberspace, but taking into account the laws that the use of Internet implies (referring here also to the inciting to the acts of violence and terrorism, etc). The protection of citizens and of our interests comes with the commitment to the privacy, in terms of using the personal data. Regarding the free flow of information, cybersecurity should be the instrument that assure the adaptability, without affecting the network performance.

The information and communications technologies brought benefits for states and their citizens, but they are also used by a variety of actors with differing motivations and means. That is why the cybersecurity community has consistently warned about the increasing number of cyber -attacks. So, the cyberspace is operationalized by nation states as a domain for conflict, and permanent threats[20].

The Internet dependence and the increasing interdependence within the online environment will become a fact of life and will continue to challenge our ability to manage the consequences of cyber-attacks, at national and international levels.[21] A strong supports for the development of cybersecurity norms should be seen from actors from state and private entities. The cybersecurity norms will have to increase the security of cyberspace and also the preservation of a globally connected society.

The above mentioned authors believe that these norms should take into account acceptable and unacceptable state behaviors, fostering greater predictability, and limiting the potential for the most problematic impacts. They conceptualize two types of norms:

- norms for improving defenses, which reduce the risk by providing a foundation for national cybersecurity capacity and for domestic, regional, and international organizational structures and approaches that increase understanding between states;

[18] *Ibidem,* p. 5

[19] *Ibidem*

[20] Angela McKay, Jan Neutze, Paul Nicholas, Kevin Sullivan (eds.), *International Cybersecurity Norms, Reducing conflicts in an Internet-depending world*, 2015, Microsoft, p. 2

[21] *Ibidem*

- norms for limiting conflict or offensive operations, which will serve to reduce conflict, avoid escalations, and limit the potential for catastrophic impacts in, through, or even to cyberspace[22].

They proposed six cybersecurity norms to limit conflicts:

- states should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.
- states should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
- states should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.
- states should commit to nonproliferation activities related to cyber weapons.
- states should limit their engagement in cyber offensive operations to avoid creating a mass event.
- states should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace[23].

In order to be effective, these norms should meet four key criteria:

- they must be practicable.
- they also need to reduce risks of complex cyber events and disruptions that could lead to conflict.
- they need to drive behavioral change that is observable and that makes a demonstrable difference in the security of cyberspace for states, enterprises, civil society, and individual stakeholders and users.
- effective norms should leverage existing risk-management concepts to help mitigate against escalation, and, if escalation is unavoidable, they should provide useful insight into the potential actions of involved parties[24].

[22] *Ibidem*
[23] *Ibidem*, p. 11-13
[24] *Ibidem*, p. 11

The cybersecurity norms are needed by different actors from international arena, such as states, the private sector, and citizens. Without them, there is a genuine risk that threats in cyberspace could grow and undermine economic growth and technical innovation[25].

We are living in a world of *cybered conflicts* and we will need cyber mechanisms to limit the negative actions of different actors. The open international cyberspace will challenged national sovereignty and the state leaders will have to find ways of responding to this continuous and sophisticated threats.

There is an evolution of conflicts and competitive relations among states in a changing international system. That is why policymakers, representative of military, academic and business communities have to react to the global spread of a cyberspace and its changes to the international environment[26]. The Policymakers in have issued or are writing national cyber security policies and laws. The scholars of international relations seem to be bound to their theories. But they will have to capture the emerging world and to explain major events such as the unprecedented rise of China in a single decade given the enormous scale of its poverty[27].

The international system is now shaped by international state and non-state actors and the new world order has assume the "systemic effects of the depth and rapidity of the global and largely unmonitored spread of the cyberspace"[28], which will modernize the nations. This could be a call for more research among scholars in this field of study. *Cyberizing the thinking of international relations scholars* requires "published works that challenge them to think beyond state–state conflicts of the past, beyond game or power theories that rest largely on isolating events from the new reality of a host of interrelated and ever more deeply integrated substate systems"[29].

[25] *Ibidem*, p. 19

[26] Jan-Federick Kremer, Bendict Müller, "Preface", in J.-F. Kremer, B. Müller (eds.) *Cyberspace and International Relations. Theories, Prospects and Challenges*, Berlin Heidelberg: Springer- Verlag, 2014, p. vi

[27] *Ibidem*

[28] *Ibidem*

[29] *Ibidem*

Now it is the moment to pay attention to the c*yberization* of IR, which refers to "the ongoing penetration of all different fields of activity of international relations by different mediums of the cyberspace on the one hand, and the growing dependence of actors in IR on infrastructure, instruments, and means offered by the cyberspace on the other hand[30]".

The new world order is now created!

3. Conclusion

The cyberspace represent a challenge, which not new in international politics. The international system is a continuing reconfiguration of a world order.

We can build now a future in which universities and companies are free to research and develop new concepts and products because they know their intellectual property and valuable data are safe and shared by networks. Also, individuals are aware and know the threats to their personal computers, and they can take easy-to-use measures to protect their systems. Private companies can take a responsibility for their network hygiene, and protect their investments.

The technological means of cybersecurity can detect threats early and share data in real-time to mitigate the spread of malware or minimize the impact of a major disruption. The laws that we created, limit the actions of cyberterrorists and try to create a protected space.

We have to create and develop instruments that will assure the international security and a more sustainable peace. The state actors will act as responsible parties in cyberspace and collaborate at bilateral, multilateral, and international level to negotiate and bring consensus in seeking to preserve the Internet, our innovations and the continuing configuration of the world order.

[30] *Ibidem*, p.xi

Bibliography

Bruner, Tomáš (2014), *States in cyber-space: perspectives of responsibility beyond attribution*, [https://ecpr.eu/.../f1874dac-6e16-4d9c-b936-723754fcc869....], 23 June 2017.

Forsyth Jr., James Wood; Pope, Maj Billy E. (2014), "Structural Causes and Cyber Effects Why International Order is Inevitable in Cyberspace", in *Strategic Studies Quarterly*, Winter 2014, 113 – 130.

Kremer, Jan-Federick; Müller, Bendict (eds.) (2014), Cyberspace and International Relations. Theories, Prospects and Challenges, Berlin Heidelberg: Springer- Verlag, 2014.

International Strategy for Cyberspace. Prosperity, Security and Openness in a networked world, (2011), [https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyber], 1 June 2017.

Mazurier, Pablo A., (2015), *Facebook in Cyber Politics*, 2015, [http://www.cyberpolitics.eu/cyberpolitics_art_04_facebook.html], 4 June 2017.

McKay, Angela; Neutze, Jan; Nicholas, Paul; Sullivan, Kevin (eds.), (2015) *International Cybersecurity Norms, Reducing conflicts in an Internet-depending world*, Microsoft.

Wendt, Alexander (1999), *Social Theory of International Politics*, Cambridge: Cambridge University Press.