UDC 327.7

SOFT POWER AND CYBER POWER OF THE EUROPEAN UNION

Самархан Шұғыла Айдоскызы, Серикова Рауан Ергенкызы.
E-mail: shugyla14@gmail.com, E-mail: rauana1301s@gmail.com
Студентки 1 курса кафедры международных отношений, ЕНУ им.Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Кенжалина Г.Ж.

The EU is a unique international organization as compared to others in terms of complexity, wide range of responsibility and supranationality. Its complexity could be understood in terms of many institutions, decision-making processes and policy actors. It is involved in just about every sphere of public policy. It is a highly developed political system. The EU's soft power is related with aid, trade, investment and expertise whereas the concept of the rule of law based on respect for human rights and international treaties plays a significant role. These elements of soft power have been the magnets attracting the countries of central and eastern Europe into the EU [1, p.4].

Also, at present, the EU has begun to use its cyber power to reduce security in the world.The EU has approached the issue of cyber security in a fragmented manner, where parallel policies have sometimes been launched with different overlapping themes. Most of these initiatives have direct or indirect relevance to EU Members' preparedness to withstand serious cyber attacks, as they address the methods of cyber attacks, as well as the consequences of these attacks [2, p.29].

European Union can be reasonably reckoned among the circle of global leaders. The soft power of the European Union is implemented in the programs of assistance to reformation of economies of neighboring countries. Striving for facilitating the resolution of their social and economic problems, the European Union simultaneously aims them at European economic and trade priorities. It is possible to overcome social and economic and political difficulties only by means of gradual and soft, non-power fulfillment of reforms. And in the documents on its regional strategy the European Union it is stated that reforms may not be imposed on from outside. They must be originated by internal factors. We may structurally mark out several aspects of the potential of global leadership of Europe.

There are serious economic reasons allowing speaking on soft power of the European Union. Such international statistical indicators as population size, territory area, annual GDP per capita, economic growth rates, volume of foreign trade, foreign trade turnover and share in world trade indicatethat the European Union possesses powerful economic foundation and it is the biggest participant of international trade. On the whole the countries of the European Union cover 32 per cent of world trade. According to the analysts, economic positions of the European Union will be strengthened by transatlantic treaty on free trade between the European Union and USA, the decision on which has been taken in the summit of the European Union on 08 February 2013. According to the forecasts of European and American governmental experts in 15 years the decision will add the Europe's GDP growth by approximately 0,5%, and that of America – by 0,4%.

Cultural and political influence of the European Union that has global nature is an important element of soft power. Today the conception European values has become quite broad. It includes the notions on the necessity of resolving the disputes in amicable way through negotiations, observance of civil and political rights and liberties of human being and ethnical minorities. Such components of European values as guaranteeing economic and political stability based on the social solidarity and rise in well-being of Europeans, maintenance of safe and amicable external environment. These values exert influence on political culture of many non-European countries and

regions. On the home-policy level, these values are shared by all European states united. They are an important motif, moving the European Union to develop a common foreign policy. “The essence of Europe as the center of power, embodied by the European Union, consists in its fundamental morality”. No less important is the external aspect of the influence of European values. While the U.S. exerts its leadership influence straightforward and directly by means of force, the EU countries impact on international relations softer, giving priority to indirect tools. For example, they watch their prestige in the consideration of the facts of infringement of human values. The Council of Europe, in which the EU countries set the tone, is the most influential organization in the world for human rights protection. In fact, the Council of Europe forms a global canon of human rights protection standards, seeking to extend it to the entire international community. It is no accident that human rights activists of all countries appeal precisely to European assessments of situations prevailing in their countries with human rights and political freedoms. They are interested in the European position not less than in the Washington's opinion on relevant issues. Leadership in the field of human rights protection activity is an element of the potential of moral and political influence of the European Union. The recognition of the high authority of the European tradition of morality and the struggle for justice was the fact of deployment in Europe of internationaljudicial bodies and tribunals - the UN International Court of Justice, the UN International Tribunal for the Former Yugoslavia, the International Criminal Court, the European Court of Human Rights and other. An important tool of cultural and intellectual leadership of the European Union has become a successful EU integration experience. Now European Union can be called global intellectual center for many countries, especially those that have an interest in integration projects.

Let’s consider the political aspect of the EU's soft power. The European Union is the largest and influential player in the field of world politics. It carries out its political activities in the framework of the mechanism of the Common Foreign Policy and Security Policy, incorporated into the structure of the working bodies of the European Union. European Union’s policy towards its neighbours is carried out on the basis of a common goal: “the establishment of EU environmental zone of stability and prosperity, consisting of friendly countries, from Morocco to Russia”. The European Union exerts tangible political influence in the world by coordinating the positions of its members within the framework of NATO. Using the resources of the alliance (NATO), European Union is building up its own potential of international influence. The political influence of the European Union allows adjusting the long-term changes in international development. It is through this resource that the European Union can influence political processes taking place in geographically proximate or remote regions.

European Union efficiently uses in international activities its organizational resource that is determined by the participation of the European Union in a number of multilateral world and regional organizations, regimes, dialogues, forums, etc. It has been developed stable practice of regular meetings between senior officials of the European Union and the governments of leading countries of the world – the U.S., Russia, China, Canada, Japan, and India. The representatives of the European Union participate in the work of the most prestigious international bodies. In addition, the European Union has an extensive network of official bilateral trade, partnership and association agreements with dozens of countries in Eurasia, Africa, the Caribbean and the Pacific, as well as South America. Adoption by the partner states of legislative norms by the European model significantly facilitates for EU firms doing business with counterpartsfrom Eastern Europe and the Mediterranean. The European Union has a huge influence in the World Trade Organization too. Actively using the procedures for resolving trade disputes within the WTO, it defends its interests in relations with the United States. Having a powerful organizational potential, and being the world's largest trading block, the European Union is based on non-coercive instruments of governing international relations. The use of organizational resource is much more consistent with the objectives of EU foreign policy than the power resource used by the United States. This is another important difference of the strategy of soft leadership characteristic to the European Union.

EU foreign policy activity increases as it moves along the path of integration. At the same time, common foreign policy has become a way for the European Union to strengthen and develop

its cohesion. European Union pursues a foreign policy through the use of instruments of "soft" power. The objectives of the European Union policy are largely designed for the long-term outlook, and less - to get a quick win. It allows the European Union to promptly correcting methods to achieve these goals. The strategy of soft leadership causes less resistance and is associated with a lower risk of trying to neutralize it. This is the advantage of the strategy of the European Union and this conditions the global leadership of the European Union [3, p.28-30].

The EU's role as a global cyber power mainly relies on its ability to shape cyber-related legislation as well as norms and standards of state behavior. This might prove challenging due to its institutional structure and civilian power characteristics [4].

The compulsory form of cyber power is the most pertinent to the traditional-realist understanding of national power. Whether by direct or indirect coercion, it focuses on modifying the behaviour and conditions of existence of one actor by another. It is understood as compulsory, as much as it is about compelling others to do what we want them to do and what they wouldn't otherwise do. One has to admit that for obvious reasons the EU does not carry much weight in this category. That is not to say that it has to stay invisible or meaningless. As a form of economic cooperation, the EU has already played an important role in coordinating national policies, which also refers to some extent to foreign security, as well as defence policies of its members. Since actors involved under a coercion paradigm no longer include states only, there is a lot of space for a number of other non-state actors like activists, hackers, criminals, terrorists, states, state proxies, military alliances, private firms, public companies etc. The EU fits perfectly in the picture as far as actions initiated on its behalf. EU bodies, that is, Commissions or particular EU members acting on their own or collectively but each time as members of the same European structure, do intend to modify the behavior and conditions of existence of other actors in the cyber realm. Just as imposing economic sanctions on Iranian or Korean entities or individuals, the EU may and should be able to operate in the realm of the cyber domain by fighting back to protect data security in the case of cyber crime or cyber espionage, especially if such an attack is directed at EU institutions. In this respect, the already established Computer Emergency Response Team for European Institutions should become a key defensive-offensive tool in future EU cyber security strategy. It is composed of IT security experts from participating EU institutions, including European Commission and others from the European Parliament, the Council, the Committee of the Regions and Economic and Social Committee and ENISA.38 The team operates under the strategic oversight of an inter-institutional Steering Board. More important than the composition of the team are its designated role and operation procedures.

Institutional cyber power rests on indirect control of one actor's 'manoeuvring field' through third party formal and informal institutions. In this respect, the most powerful actors are able to set norms and standards that ultimately shape the environment in which they themselves and all other actors exist and through which they try to arrive at their goals. This part of the paper will address two elementary avenues for an institution such as the EU to shape its institutional component of cyber power: international cooperation and facilitation of member states' approaches to cyber security threats.

International Cooperation. When dealing with global security threats and challenges, such as those referring to the cyber domain, it is almost a cliché to notice that the response on the part of national governments needs to cut across traditional lines of dividing organizational structures. In that respect there has been a realization within the EU Parliament, The Commission and ENISA especially that without international cooperation, including a high level of institutionalization and socialization alike, an effective EU response to cyber security threats has limited prospects. Cooperation, therefore, should not only include EU member states but other major stakeholders like China or the US. Such cooperation will definitely be easier when it comes to first of the earlier mentioned threats, cyber crime, rather than the second, cyber espionage or cyber attacks, since most states tend to treat the later as proxy to economic competition. As regards US and EU cooperation, it has been developed under the general framework of the trans-Atlantic cooperation in cyber security that allows the creation of the concurrence. In particular the EU-US Working Group on

Cyber-security and Cyber-Crime has been established.43 For the time being, focus is put on organizing events like the one on 12 June, 2012, devoted to gathering all potential intermediaries together to exchange experiences both from the EU and US sides.44 Alliance between these two is vital, as both pretend to be major shareholders in international (cyber) security (generating a huge volume of electronic trade or running critical infrastructure that is highly dependent on computer systems). Awareness raising exercises as well as sharing the pool of experience are undoubtedly important, but fundamental problems seem to limit the effectiveness. First, there seems to be a lack of clarity as regards the institutional side of the matter. As already mentioned in this paper, the NATO rapid reaction team (RRT) seems to focus more on the American side of the Atlantic. The US has signed and ratified the Council of Europe Convention on Cyber Crime (which conveys a common commitment to punish perpetrators and to deter cyber threats), but some of the EU members like Poland or Greece have not.

Public-Private Partnership. The EU's prime institution responsible for exchange of information, best practices and knowledge in the field of information security, ENISA, has been assisting EU member states in the task of developing and maintaining their own national cyber security strategies. For this purpose, ENISA has prepared a 'Good Practice Guide', 5designed as a study on national cyber security strategies in order to highlight good practices and recommendations on how to develop, implement and maintain a cyber security strategy. As such, the Good Practice Guide is meant to be a useful tool and practical advice for those responsible for and involved in cyber security strategies. It involves experts from the public sector and stakeholders from the private sector across Europe who finalized their work by the end of 2012. At the same time, The European Commission is trying to push energy, transport and financial companies operating in the EU to invest more in their cyber security and to report on any breaches that could compromise their security. Pertinent to the role and significance of 'critical infrastructure', private entities are part of the same system, and the system itself is as weak as its weakest element. Therefore the Commission plans to extend security breach notifications to new industries other than telecommunication companies and Internet firms, which in Europe are already subject to reporting obligations.

Addressing the long existing methodological conundrum of actors vs. structure, structural cyber-power is best understood as one that allows a particular actor (the most powerful) to uphold the structures of power relations in which all actors are positioned and which in turn permit or constrain their actions. It is closely related to the concept of 'information society', which rests on collecting and manipulating data, information and knowledge. The cyber domain does offer new possibilities to some previously 'underprivileged' actors. The Internet is a global electronic empowering tool through which a plethora of resistance activities takes place, changing the traditionally established balance of power within political systems. Recent examples from North Africa and the Middle East attest to the role of cyber space in creating networks of concerned citizens displaying their outrage at local governments. This is also pertinent to the idea of 'civilianization' of security, a notion relating to non-military, voluntary organizations and the business/private sector, engaged by government but acting in their own right, to prevent, protect and prepare in the context of a counterterrorism strategy. With regards to cyber security, it is a phenomenon by which ordinary civilians act as providers of their own security. Since governments and public institutions have become increasingly inefficient in providing security to citizens, especially when one takes an individual as security 'referent', it remains for private entities and non-public bodies to fill the vacuum. In fact, EU documents increasingly emphasize the potential for individuals and public/private partnership especially in the fight against cyber crime. EUROPOL for that matter is planning to get net users directly involved in catching cyber crime gangs. This would supposedly empower EU citizens not only to look out for themselves but also to report criminal activity. This 'crowd-sourcing plan', though in its embryonic stages, will depend on the functioning of the European Cybercrime Centre (mentioned earlier in this paper) that has recently started operating within the framework of EUROPOL.

Finally, and perhaps most importantly, productive forms of cyber-power underpin all the above mentioned. As a partly non-physical environment, cyberspace 'serves to reproduce and reinforce existing discourses, as well as to construct and disseminate new ones.' The idea is that such constructed social beings enable social relations, through which power may be exercised. This form of cyber-power is manifested by identifying certain actors as threats to national security, which in turn allows states to treat them as legitimate targets. Practicalities of cyber threats make it increasingly difficult for states or groupings of states to attribute challenges, threats or attacks, should they take place, with any particular agents. The nonphysical, transnational and imminent character of information networks best epitomizes what security experts refer to as an 'attribution problem.' Consequently this testifies to further confusion with regards to legitimate objects for states' supervision. Let us take a look at the ENISA approach to this issue. In one of its latest publications, Cyber Security: future challenges and opportunities, a document that will most likely serve as the basis for future pan-European cyber security strategy, we read: 'In the past, troops from opposing countries confronted each other on a battlefield, and "rules" for warfare were written if not always followed. The Geneva Convention, for example, describes rules for the protection of people who do not take part in the fighting. Outside these rules, terrorist organizations seek to achieve mainly political aims by operations, which, under state legislation, are assessed as criminal acts. With Internet technology it is possible for an individual, group or state to carry out remotely controlled, often covert, cyber attacks on critical infrastructures of a state. Therefore the line between soldier, terrorist and criminal becomes blurred.' Most of the communication concerning cyber security that flows from Brussels focuses on non-state actors. EU institutions as well as EU bureaucrats of various levels increasingly refer to cyber security through the lens of non-state actors. Their narratives are full of references to individuals, transnational organized crime, terrorists or simply criminals, further undermining a realistic conception of national security. Therefore it is the contention of the author of this paper that the productive power of the EU in the field of cyber security seems to be driving the conceptualization of security towards its human aspects (human security) and a social constructivist approach (a tool such as the Internet is neutral so long as it is used against the security of a particular referent object, in which case it acquires negative characteristics and can be understood as a threat) [5, p.10-18].

In conclusion, you can see that the soft power of the EU is developing in different areas to achieve leadership, as well as developing its cyber-power for the same task. The discussion of the EU's cyber-power can contribute to the discussion about EU's power in world politics more generally. Power is multifaceted and the different facets come with strengths and weaknesses that are context and issue dependent. Power discussions of all sorts make more sense if the often unspoken assumptions about what kind of power is more valuable or desirable are made explicit so that they can be questioned [6].

Literature

1. Kurtulus B. EU Soft Power in the 21st Century, Prague, 07.09.2013 // https://ecpr.eu/Filestore/PaperProposal/92de3705-9310-4278-9a71-f450d52efc73.pdf
2. Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation,Belgium,15.04.2011//http://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf
3. The EU as a model of soft power in the Eastern neighbourhood, Iasi, 2013 //http://cse.uaic.ro/eurint/proceedings/index_htm_files/EURINT_2013.pdf
4. Zabakhidze R. EU's role in shaping cyber legislation – Part Two of Three, 03.10. 2018 //http://securitydistillery.com/2018/10/03/eus-role-in-shaping-cyber-legislation-part-one/
5. Krzysztof S. European Union-Cyber Power in the Making, Hong Kong Baptist University//http://www.keusa.or.kr/korean/kor_publication/APJournal/2014_No12_1/Eu-12-1-01%20Sliwinski.pdf
6. Cavelty M.D. European Politics and Society. Europe's cyber-power, 25.01.2018// https://www.tandfonline.com/eprint/2eI6SkGwxnEra5ZTYgIQ/full