ISSN: 2587-1218

Article Reviewed:

BY NIR KSHETRI, CYBERSECURITY AND INTERNATIONAL RELATIONS: THE U.S. ENGAGEMENT WITH CHINA AND RUSSIA, Buenos Aires, Argentina, 2014, Proc. FLACO-ISA Joint Conf.(FLACSO-ISA 14).

Durukan AYAN*

The article, "Cybersecurity and International Relations: The U.S. Engagement with China and Russia", by Nir Kshetri seeks to examine how formal treaties and frameworks as well as informal cooperation attempts influence the conflicts and divergences related to cybersecurity with bearing in mind organizational theory, game theory and international relations. Correspondingly, the U.S. relationships with Russia and China with regard to main cybersecurity topics, including the case of Edward Snowden, are exemplified. Following that, the article touches on different understandings and areas of disagreement about conception of the cybersecurity such as military, espionage and cybercrime dimensions. Above all, the research problem being addressed is whether informal institutions perform better than the formal ones in coping with international conflicts related to cyberspace.

Firstly, the article starts with comparison of formal treaties and ad hoc/informal mechanisms. It mainly argues that informal cooperation might be more effective than the formal treaties or frameworks in dealing with cyber conflicts. The reason behind this claim is pretty much based on the "flexibility" of informal or ad hoc cooperation methods. Following the suggestion of Lipson (1991, p. 500) as it is stated in the article "informal bargains are more flexible than treaties" since they are "willows, not oaks" and can be adapted to meet uncertain conditions and unpredictable shocks" (p. 8). Moreover this claim is supported with significant cybercrime examples to illustrate the success of informal practices on network-based cooperation.

The author includes some critical approaches on informal interactions as well. According to the critics informal networks depends on voluntary basis rather than compulsory and "engagement varies considerably across nations… informal cooperation is unlikely have a significant effect on domestic policy" (p. 8). This criticism demonstrates that informal

* Research Assist. in Department of International Relations, Afyon Kocatepe University and Graduate student in International Relations, Selçuk University Graduate School of Social Sciences, ayan.durukan@gmail.com.

cooperation is more likely to work in bilateral relations and it may accomplish a short term collaboration exclusive to the subject. However cybersecurity which is a multilateral matter requires extensive cooperation even if not at global or regional level. For this reason, formal treaties or frameworks seem more efficient to reduce the cybersecurity threats, perceptions and potential breaches. Moreover, based upon the examples which are given in the article it could be said that informal/ad hoc cooperation is quite likely to prevent cyber attacks targeting financial markets.

Secondly, the author refers to varied approaches of U.S. China and Russia regarding cooperation. With the exception of several cooperation attempts, ongoingness of the blame and counter blame circle on the cybersecurity dialogue between China and U.S. is underscored. Likewise, even though there was some uptrend in the past, the Russia-U.S. cooperation is excessively affected from the Snowden case. Having said that analysed relationships with regard to cybersecurity are mainly described on the basis of cybercrime. Furthermore, in relation to the Snowden case, the article attaches more importance to extradition concern of the U.S. rather than pointing out the distrust built by U.S. government's surveillance programs. The espionage here is evaluated as a one-sided matter and the rightful reactions and distrust of other countries are not taken into consideration decently. In respect to this, it is worth asking if cyber espionage activities are considered as legitimate acts of states in order to achieve national interests or such activities are considered legitimate as long as states act without being noticed. As a matter of fact the author specifies some worthwhile criticism about legitimacy mentioned as "strengthening" the critics' point of view: "U.S. is merely a victim and not a part of the problem, and that U.S. activities are legitimate, while those of some major economies are not" (p. 24).

Thirdly, it is being mentioned that "prior researchers have placed an emphasis on multidimensionality of security and multiple forms of security risks" (p. 18). In fact as the article gets close to conclusion, it indicates that formal treaties could be more effective rather than the informal ones. If cybersecurity should be taken as a multidimensional problem, then another question comes to mind in reference to the contributions of the aforementioned informal, ad hoc and considerably bilateral attempts. Accordingly, the most significant challenge observed from this article is addressing cybersecurity merely within the context of cybercrime.

Although cyberspace is a separate dimension, it is just another part of the reality and apart from reality it has no presence or importance. Therefore cybersecurity refers to nothing more than traditional security paradigms. Security concerns which increased with the cyberspace are directly related to national securities and the security of the international system or structure. When analyzed the existing conflicts in cyberspace, it could be seen that considerable amount of the cases are related to economic-based issues. For this reason as reported in the article, informal cooperation in suchlike security matters is more likely to be successful. Just because, as it was mentioned before, informal cooperation has more flexible practices over formal treaties.

Moreover, the game theory approach which stated in the article is worth to consider. According to this approach, interactions of the actors can be described as "infinitely repeated games" and "an outcome of such interactions is that over time, the actors are likely to expect regularities in behaviour. In this way, the bargaining processes among the game's actors lead to informal norms" (p. 24). In addition to that, "if the players' beliefs about each other's trustworthiness are confirmed by subsequent behaviour, there is a tendency of cooperative behaviour to enhance the prospects for successful further cooperation" (p. 25). Regularities in behaviour may lead to informal norms among the actors. But at the same time, it may cause deep-rooted conflicts if the behaviours regularly confront with one another. In regard to second quoted passage, it is quite true that there can be no realistic cooperation in the absence of trust-building measures. However it needs to be stated that, to be able to build mutual trust on cybersecurity undergoing economic, military, social and cultural distrusts need to be considered. The main reason for not being able to provide a realistic cooperation is that every state justifies only its own interests and preferences and disregards others' perspectives and viewpoints, as stated in the article (p. 30). Furthermore another important aspect is remarked in the article that there is a lack of ethical approach in cyberspace.

From the viewpoint of International Relations, it needs to be emphasised that while cybercrime is an important dimension, it is not the most noteworthy aspect of the cybersecurity. The foremost aspects of cybersecurity are, in my humble opinion, the threats perceived by states, cyber espionage programs, superiority of assault over defence and different types of cyberattacks mainly targeting critical infrastructures of the states such as DDoS attacks targeting governmental web resources of Estonia in 2007 and Georgia in 2008,

malware attacks just like STUXNET worm which possibly aims Iran's controversial nuclear facility in 2010, massive cyber assaults targeting electrical grid of Israel in 2016 and so on.

In brief, this article has a well written introduction and it starts with noting the failure of international formal agreements while informal cooperation is making some good progress. Later on the comparison of formal and informal cooperation is asserted fairly except that the success of informal cooperation is not clearly linked to cybercrime related conflicts. The examples, different approaches and criticism related to U.S. relations with Russia and China regarding cybersecurity matters are considerably extensive. Giving weight to the critical issues and areas of disagreement as a separate section and considering significant critical approaches makes this article valuable. Although there are some points worth to criticise on different points the article, when taken as a whole, is answering the questions which are asked above. Overall, this article is a favourable piece for the researches who wants to observe the cybersecurity issue with regard to relations between geopolitically significant economies.