Вестник МГИМО-Университета. 2019. 12(5). С. 7-11
DOI 10.24833/2071-8160-2019-5-68-7-11

ИНТЕРВЬЮ

Talking Past Each Other: Government, Business and Civil Society Discussing Cyber Security

Martha Finnemore

George Washington University

Martha Finnemore has visited MGIMO-University this September, she gave several public lectures for students and participated in a number of roundtables. Professor Finnemore was very kind to give an interview to our journal on various issues of international information and cybersecurity. The interview was conducted by **Elena Zinovieva**, vice director of the Center for International Information Security, Science and Technology Policy at MGIMO-University.

Key words: UN Open-ended working group, UN GGE, international norms, constructivism

Elena Zinovieva: Cyber security is one of your fields of interest, you have published several articles on the matter. Could you please share your opinion on the recent events in the field of cybersecurity? In 2018 two working groups were established at the UN level dealing with the issue of ICT-related security or cyber security (in Russia we use the term "information security") – Group of Governmental experts and Open-ended working group. This is a very unusual situation, when two separate institutions were created to deal with the same matter. The creation of the Open-Ended Group was supported by Russia and its allies, while the creation of the GGE was supported by the USA and its allies. Is it a sign that international community has divergent views over how cyber norms look like? Or is it a sign that international cooperation is moving forward, and international community is interested in deepening and widening cooperation on the matter?

Martha Finnemore: I think both. There was a discussion after the last GGE collapsed in 2017 that maybe there would be nothing. Instead now we have two groups. I would not have guessed this would be the case after the collapse of the 2017 GGE,

УДК 327.3
Поступила в редакцию 15.09.2019 г.
Принята к публикации 10.10.2019 г.

which produced no recommendations, no findings. I think that both of the things you say are true. I think there continues to be this interest, but there also continues to be a deep disagreement about who should be sitting at the table, who should have a presence, who gets to have a say. The Open-Ended Working Group is founded on one set of notions about this, and the GGE is continuing the earlier set of notions about how to organize this. Whether they talk to each other is not clear to me. I know that it is a small community and that they know each other. Informally, I know they talk. Formally, I am not sure what they will do.

E.Z.: As far as I know, Russia proposed that there will be specialization of labor. Open-ended working group will focus on the applicability of international humanitarian law to the cyber warfare and Group of Governmental Experts will focus on the development of norms of responsible state behavior in the information sphere. And for me, there is another interesting question, because I have recently read your article for Carnegie Endowment "Cyber Security and the Concept of Norms" of 2017[1], where you state that it is not that much important what states discuss at the international level, it is much more important how international practice in the field of cybersecurity evolves. From that standpoint, discussions at the UN GGE and OEG are not that much important, as compared to the practice-oriented path of norms creation. What do you think about it?

M.F.: It depends on who is doing the practicing. In the meetings I go to in the United States, often there are industry people present. The way they build the technology, the decisions they make about building the hardware and the software, those shape physical reality and what you and I can do on these devices and networks. That is one set of conversations, and there is extensive cooperation going on among industry people, engineers and technologists. I do not follow that closely. Government only talks to those people sometimes, and those discussions seem to be happening on very different levels. Government people, I think, from all governments often forget that governments do not own these networks, that governments do not build these networks. More than 90% of all network infrastructure, which comprises the Internet, is owned by the private sector. As a scholar, I find this amusing. I mean that they seem to talk past each other, not to communicate very well.

E.Z.: There is another very interesting case I wanted to ask your opinion on. The United States of America proposed a multi-stakeholder approach to the international cooperation (with the participation of states, business, academia and civil society groups) for the ICT at the international level in the early 2000s, and now in 2018 they supported the creation of the GGE at the UN which is intergovernmental and with closed membership. And how you do feel, maybe, it is a sign that cyber norms are moving toward great powers discussion more than to industry and multi-stakeholder cooperation?

[1] https://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870 (accessed 12.10.2019)

M.F.: Some of my perspective on this is skewed just because I live in Washington. The policy of the United States often changes with the election processes. It is less consistent than maybe it is in Russia. A lot of people who worked on this issue for many years at the State Department are now gone. When Chris Painter[2] was there I think cyber issues were a priority. He was quite influential, and they gave him authority to do a broad range of things. The current policy seems for me to be a little different than that. But I would expect some changes with the change of administration. This does not surprise me. But over the longer term this issue will not go away. All the Western governments will have to engage with each other and also, again, with these private companies that are very important political constituencies. They are big actors in domestic politics. They contribute to campaigns; they are politically influential in all kinds of ways. What this conversation between companies and government looks like in the West will matter a lot, I think.

E.Z.: Speaking about the norm promotion. You use the concept of "norm entrepreneurs" in your articles meaning the actors who promote a certain set of norms. Who do you believe are norm entrepreneurs in the cyber realm: states, business or, maybe, civil society or NGOs on the global scale?

M.F.: Can I say "all"? I can see norm promotion activity from all states, and from civil servants, like Chris Painter. I would call him a norm entrepreneur. He was very interested in developing this. But "Microsoft" also has this initiative on a Geneva Convention for cyber space and has been interested in this area for a long time. And there is a whole array of NGOs and civil society groups who are interested in promoting privacy and human rights norms. They lobby both the businesses and governments. They want the businesses to change their technology to make sure that people's privacy is not compromised. And they want the governments to be conscious and aware about this issue. So, if I can say "all", then all.

E.Z.: In what area do you believe there is the highest possibility that such norms will emerge? In some narrow areas like financial information infrastructure? Or may be broader issues can be solved at international level, the global cybersecurity regime, covering a broad range of cybersecurity issues?

M.F.: I do not know. I am not good at predicting. If I were good at predicting, I would be much more interesting and famous than I am. Historically, when I watched the norms evolving in other kinds of issues, there were exactly what you say: two paths of norm emergence. Sometimes the norms start very narrow and then people build out. For example, I could imagine the Carnegie corporation has been very interested in specific financial sector norms and has been very active in pushing this. Others share their concern. Banks are very worried about criminals compromising their networks. So, I can imagine a set of norms which can start narrow, focused on finance. Other business sectors would see this and say, "Oh! This is a good thing. I want that too. I

[2] Christopher Painter was the world's first cyber diplomat at the U.S. Department of State.

want to build this out norms for my sector". I can also imagine agreement on some broad norms and that people will elaborate and make more detailed. The current climate makes me worried about the broad norms. I do not know how easy it will be. But maybe, life is long, things will change, and agreement will come. It is hard to predict these things.

E.Z.: Thank you and the last question concerning the international relations theory. Alexander Wendt have just recently published a book on the quantum theory and its applicability to the international relations analysis. So maybe you can share your ideas on the matter because this is very new theoretical approach for Russia. And the application of the quantum analysis and physics to the international relations analysis is starting to be popular here in Russia.

M.F.: I am going to dodge this question. I read this book when it came out. And I have not read it recently. So I do not think I have a short answer. I have enormous respect for Alex. I also do a different type of scholarship than Alex. He is a theorist at the very high level of abstraction. I am still most interested in the problems on the ground in the real world that policy people have to deal with. I always need to be able to take abstract ideas and to figure out how to frame empirical research questions with this. And I have not yet tried with the quantum theory. This is a challenge for my own scholarship. I have not done it yet.

E.Z.: I have recently read a paper by Cornellu Bjola. He applied the quantum theory to the digital diplomacy analysis.

M.F.: This would be interesting. Was it good?

E.Z.: Yes, it was interesting. He is concerned with the way of measuring an impact of public diplomacy. There are some areas of digital diplomacy which are prone to quantification (the number of likes, shares etc.), and there are some areas which are not prone to quantification (like the emphasis of digital diplomacy on the soft power of a given state). Drawing heuristically on quantum theory, he argues that the nature of the impact and the method of measuring it are two facets of the same ontological construct. The very act of measuring shapes the type of impact we may seek to capture. These are the general ideas.

M.F.: There has also been an effort to apply complexity theory to some of these kinds of problems (norm evolution, for example). Complexity theory has a different set of assumptions about relationships, about agents. To go back to Alexander Wendt, they see agents and structures who are interacting to build out these complex systems. People have also done some creative things in quantitative analysis trying to count the number of treaty signatories. They have data on hundreds of years. This is very interesting though this is not the way I do my research.

E.Z.: Thank you very much for your time and your interesting answers!

M.F.: Thank you!

About the author:

Martha Finnemore – Professor of Political Science and International Affairs at George Washington University. 2115 G Street NW, Washington, DC 20052. E-mail: finnemor@gwu.edu.