From discourse to policy change in cybersecurity: US-Russian rivalry for cyber rules, cyberpower and practices of norm-making

The lack of constructivist perspective on cyber conflicts between nations leaves a significant gap in modern academic scholarship. Constructivism and liberalism nominally have more to say about security in the digital age because of the diversity of actors and a wide range of topics including information society and networked economies (Ericksson and Giacomello, 2006). Yet, the realist paradigm has been dominating political literature on cybersecurity and warfare for the last two decades, by focusing on strategic studies and the military dimension.

In a realist perspective, a state develops its cybersecurity policy to achieve national interests. The underlying premises of cyber policy were thus transferred from classical and neorealist works about the struggle for power (Morgenthau, 1948) and balance of power (Waltz, 1979), or maximization of power to ensure survival in anarchy (Mearsheimer, 2001). Reardon and Choucri (2012) noted this transfer to cyberspace and identified the tendencies in academic and policy literature.

In the past decade, a variety of works have described the essence of cyberconflict with evolving narratives. Firstly, there were two competing views on the probability of a cyberwar – while Clarke and Knake (2012) claimed that cyberwar is a very real and pressing threat to national security, Rid (2013) argued that cyber war does not represent true violence in the Clausewitzian sense and is unlikely to be in the future. Segal (2016) seemed to support this view and emphasized that cyberattacks pose less of a threat of bodily harm but more to infrastructures such as financial institutions, power grids, and networks. Secondly, authors covered specific features of cyberconflict dynamics using terminology of strategic studies, to mention a few of them. Cyber offense was claimed by Libicki (2009) more cost-effective than cyber defense. Gratzke (2013) suggested the security dilemma for cyberspace has a reverse effect, - arguing that cyberweapons loose their capability after their usage because exploited vulnerabilities in adversarial networks are patched and secured. Then Gartzke and Lindsay (2014) put forward the idea of cross domain deterrence including cyber. Nye (2017) developed the cyber deterrence concept and highlighted its main components: punishment and denial (coercive options), and entanglement and norms (restraining options). Coercion in cyberspace was studied and theorized by Borghard and Lonergan (2017), Sharp (2017). Valeriano and Maness (2015) introduced the theory of cyber restraint saying that adversaries are unlikely to engage in cyber conflict because of normative restrictions, the ease of proliferation of cyber weapons, and other unknown risks.

The constructivist approach to cyber conflict has been underappreciated. The Copenhagen school and securitization theory got its second birth with studies on new cyber threats and new referent objects by Dunn-Cavelty (2008, 2013) and Hansen and Nissenbaum (2009). Paletta et al. (2015) drew attention to the media coverage of an unseen cyber arms race. Craig and Valeriano (2016) demonstrated a relationship between build-up of cyber capabilities and mutual perceptions of threat and competition between states in a select number of cases. Also, they defined militarization of cyberspace by a particular discourse expressed in new military organizations, cyber-military doctrines, cybersecurity budgets.

However, constructivist view on developments in cyber policy doesn't confine itself to empirical and methodological issues of research as it may seem first. In contrast, it can explain developments in cybersecurity policy through changes in discourse, in other words, conceptions of what is secure mean in cyberspace. Recent history of US-Russian relations in cybersecurity provides a fresh set of facts for analysis and opens new perspectives for theoretical research. The power of discourse has influenced formulation of foreign policy. Since discourse emanates from domestic actors and processes it is necessary to track the evolution of cybersecurity discourse in both countries. Globally, there are two prevailing discourses for security in cyberspace: cybersecurity and infosecurity. The former deals predominantly with the technical dimension of network security while the latter incorporates issues of content regulation – how information affects national security and social order in addition to network security. As a result, there is a tacit distribution of countries belonging to the two global discourses: the more a country is authoritarian the stronger is information security discourse and vice versa. Such a split became entrenched during the work of the first UN group of governmental experts (GGE) in 2004 that examined the existing and potential threats from cyberspace and possible cooperative measures to address them. Group members, the US and Russia in particular, couldn't agree whether to address issues of information content, or only network infrastructure. Thereafter, UN GGE groups began to use the neutral wording of "ICT use" to facilitate consensus in their reports. The failure of the last UN GGE in 2017 to reach the consensus on applicability of international humanitarian law, was partly due to political tensions between countries, but also because the format has exhausted itself. However, Russia claimed to continue this

work by preparing a draft resolution for the 73rd UN session creating a new group based on an open-ended principle in contrast to previous 25 members selected by geographically equal representation. Interestingly, the US also introduced their own resolution seeking to continue the GGE format without any changes. Finally, the General Assembly voted and passed both resolutions by the end of 2018, so this opens up a competition between the two newly established groups GGE and OEWG on cybernorms. The voting records show the traditional international split between countries on the principle of adhering to the one of the dominating cybersecurity discourses.

A critical change in US cybersecurity discourse subsequent to the alleged information operations and hacks associated with the 2016 presidential elections politically attributed to Russia serve as a key case study for this study. "Hacked" elections became a milestone for changes in the US cybersecurity discourse. The new National Cyber Strategy signed by President D. Trump in 2018 cemented the change in discourse to infosecurity. In the introduction, the strategy lists, among other threats, cyber tools that adversaries use to "sow discord in our democratic process." Moreover, the document has a separate section devoted to malign cyber influence and information operations. It claims that the US will "counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation <…> and prevent the use of digital platforms for malign foreign influence operations while respecting civil rights and liberties". Thus, infosecurity has been communicated in the discourse on the highest official level.

Constructivism can also provide new explanations for the question of power in cyberspace. Power is a key concept for political realism, and it already has several interpretations for the cyber domain from a realist materialistic perspective. Nye (2011), Valeriano and Maness (2015), Segal (2016). Segal seemed to start conceptualizing cyberpower including not only the material but also using an idealist base. However, this is not enough for filling the gap in constructivist theory for cybersecurity. Cyber capacities are more difficult to be counted than nuclear warheads and missiles, yet some countries are still identified as cyberpowers. This means that the perception of a particular country comes from rumors and hard-proven intelligence about its offensive cyber capabilities, as well as from attacks and campaigns it had (allegedly) committed. The last part is a big puzzle for international cybersecurity, since there is no reliable attribution mechanism for cyber incidents, and international law needs to be developed to establish responsibility of states for acts of aggression committed in cyberspace. Thus, a new trend for political attribution of cyber incidents has emerged (Schulzke, 2018, Kaushik, 2018).

This case study of US-Russian cyber relations seeks to answer two critical questions. Firstly, can one country change the discourse of cybersecurity in another country even without committing malign activity? Secondly, whether shifts in the state of discourse will lead to changes in foreign policy toward cybernorms? The answers will help to fill gaps in the constructivist literature on cybersecurity, providing theoretical ground for the concept of cyberpower through adding to its materialist understanding. Also, this research contributes to discourse studies explaining how a change in the conception of what is secure in cyberspace has led to cyber policy change.

Obviously, the trend for shifting cybersecurity discourse towards infosecurity in the US is backed by the release of new strategic documents by the new administration. However, the impact of perceived Russian influence on American discourse still needs to be proven. Without a doubt, meddling in the election process has triggered the changes, but the findings of the Mueller commission have yet to be released. Whether or not evidence of Russian interference is proven, its perception has already confirmed the hypothesis of the research. A country can change the discourse of another country by either conducting or being perceived to be conducting malign activity against it.

However, the second part of the research question still remains unanswered. Recent developments in the UN GGE process signals that the fight for cybernorms is continuing. While Russia is pushing an infosecurity agenda, the US tries to keep its cybersecurity policy on a separate track. Since the composition of working groups is as yet unknown, we have to watch whether there will be a joint collaboration between them and wait for the final reports due in 2020 and 2021.