VILNIUS UNIVERSITY

AGNIJA
TUMKEVIČ

Potential of International Cooperation and Conflict in Cyberspace

SUMMARY OF DOCTORAL DISSERTATION

Social sciences,
Political science 02S

VILNIUS 2019

This dissertation was written between 2014 and 2018 (Institute of International Relations and Political Science of Vilnius University). The research was supported by the Research Council of Lithuania.

Academic supervisor:

Prof. Dr. Tomas Janeliūnas (Vilnius University, Social Science, Political Science - 02S).

This doctoral dissertation will be defended in a public/closed meeting of the Dissertation Defence Panel:

Chairman – **Prof. Dr. Dovilė Jakniūnaitė** (Vilnius University, Social Science, Political Science - 02S).

Members:
Doc. Dr. Asta Maskaliūnaitė, (Baltic Defence College, Social Science, Political Science - 02S).
Prof. Dr. Arūnas Molis, (Vytautas Magnus University, Social Science, Political Science - 02S).
Doc. Dr. Margarita Šešelgytė, (Vilnius University, Social Science, Political Science - 02S).
Prof. Dr. Gediminas Vitkus, (Vilnius University, Social Science, Political Science - 02S).

The dissertation shall be defended at a public meeting of the Dissertation Defence Panel at 13.00 p. m. on 8 March, 2019 in Room 402 of the Institute of International Relations and Political Science of Vilnius University
Address: Vokiečių 10, Vilnius, Lithuania
Tel. +370 525141 30; e-mail:tspmi@tspmi.vu.lt.

The text of this dissertation can be accessed at the libraries of Vilnius University as well as on the website of Vilnius University: www.vu.lt/lt/naujienos/ivykiu-kalendorius

VILNIAUS UNIVERSITETAS

Agnija
TUMKEVIČ

Tarptautinio bendradarbiavimo ir konflikto potencialas kibernetinėje erdvėje

DAKTARO DISERTACIJOS SANTRAUKA

Socialiniai mokslai,
Politikos mokslai 02S

VILNIUS 2019

Disertacija rengta 2014 – 2018 metais Tarptautinių santykių ir politikos mokslų institute, Vilniaus universitete.
Mokslinius tyrimus rėmė Lietuvos mokslo taryba.

Mokslinis vadovas:
prof. dr. Tomas Janeliūnas (Vilniaus universitetas, socialiniai mokslai, politikos mokslai – 02S).

Gynimo taryba:
Pirmininkė – **prof. dr. Dovilė Jakniūnaitė** (Vilniaus universitetas, socialiniai mokslai, politikos mokslai – 02S).
Nariai:

Doc. dr. Asta Maskaliūnaitė (Baltijos gynybos koledžas, Estija, socialiniai mokslai, politikos mokslai – 02S);

Prof. dr. Arūnas Molis (Vytauto Didžiojo universitetas, socialiniai mokslai, politikos mokslai – 02 S);

Doc. dr. Margarita Šešelgytė (Vilniaus universitetas, socialiniai mokslai, politikos mokslai – 02S);

Prof. dr. Gediminas Vitkus (Vilniaus universitetas, socialiniai mokslai, politikos mokslai – 02S).

Disertacija ginama viešame Gynimo tarybos posėdyje 2019 m. kovo mėn. 8 d. 13.00 val. Vilniaus universiteto Tarptautinių santykių ir politikos mokslų instituto 402 auditorijoje. Adresas: Vokiečių 10, Vilnius, Lietuva, tel. +370 525141 30 ; el. paštas tspmi@tspmi.vu.lt.

Disertaciją galima peržiūrėti Vilniaus universiteto bibliotekoje ir VU interneto svetainėje adresu: *https://www.vu.lt/naujienos/ivykiu-kalendoriu*

SUMMARY OF DOCTORAL DISSERTATION

The cyberspace has become one of the military domains and cyber instruments are integrated into all military aspects of a modern warfare. The distinctive features of cyberspace (including difficulties of attribution, difficulties in distinguishing hostile attacks from innocent mistakes, lack of clarity about what constitutes an attack under international law, and lack of credibility of retaliatory threats) encourages countries, non-state actors and individuals to plan, initiate and conduct relatively cheap attacks with almost non-existent responsibility. On the other hand, an overwhelming dependence on cyberspace increases vulnerability to domestic and external cyber incidents, attacks and criminal activities. Cyber intrusions may target critical sectors of military, political and economic spheres and become a threat to the existence of any state. The state-sponsored weaponization of cyberspace and engagement of military structures into offensive operations in the cyberspace leads modern nations to a new level of cyber competition and heightens risks of cyber-arm race and cyber warfare. All great powers, including the US, China and Russia, have developed and integrated cyber-military branches in their military and/or secret service structures. Political and military leaders of these states focus overwhelmingly on improving their countries' cyber offensive capabilities because believe that defensive strategies are insufficient to deter enemies in cyberspace. The growing danger of cyber conflicts can destabilise the existing world order, heighten the risk of security dilemma in cyberspace and lead to inadvertent crisis escalation. This implies a patent threat of escalation from cyber conflict to kinetic warfare. The issue of increased cyber-escalation is even more important having in mind that the cyber domain still has no binding rules, while existing legal instruments to restrain cyber conflict are very modest. Lessons of history which run up to the nuclear era competition after World War II, suggest that this is a dangerous situation.

THE AIMS OF THE THESIS

The Thesis explores the motives and conditions under which the US, China, and Russia are likely to cooperate on qualitative arms control in cyberspace in order to improve both their national and international security. The analysis of causes is essential in order to *understand* which conditions are necessary for the international cooperation in cyberspace. Therefore, so-called "structural understanding" of conditions is important in order to predict whether relations are most likely to be affected by conflict or cooperation in future. It also helps to explain the key shifts in countries' relations such as massive and destructive cyber attacks or sudden decrease of them. Finally, knowing the conditions and motives leading to cooperation among potential adversaries allow to propose confidence building measures which are necessary for both cooperation and establishment of cybersecurity regime.

DEFINITION OF THE MAIN CONCEPTS AND THE NOVELTY OF THE THESIS

Concept of "negative cooperation" indicates that the collaboration between adversaries is possible. This concept is based on the arguments of defensive realists, in particular Charles Glaser, who challenges classic neo-realistic assumptions on cross-border cooperation and even terms them "unwarranted" (2014, p.157). Unlike offensive realists, who claim the costs of cooperation are too high, Glaser asserts that the costs of confrontation are much higher and offers a theory of rational security based on policies of disarmament and cooperation. The author discusses the less confrontational logic of anarchy (in which confrontation between states is seen as irrational as it forces states to use their resources inefficiently, (e.g. by engaging in an arms race), increases the possibility of military conflict, and reduces security. During and after the Cold War most realists ignored obvious displays of cooperation

among adversaries. These displays, such as the treaties on disarmament and the limitation of nuclear weapons between the US and the USSR, reveal that "negative cooperation" between competing states is not only possible, but occurs frequently. However, "negative cooperation" neither turn the adversaries into partners, nor creates the security community among them.This form of cooperation refers to voluntary restriction of exercising the offensive capabilities in order to prevent a conflict escalation. The concept of "negative cooperation" is used to explain the potential of collaboration between competing states in cyberspace. It also helps to answer the question whether or not Glaser's rational conditions, which should lead to "negative cooperation", could exist in cyberspace. If the US, China, and Russia demonstrate the ability to cooperate in cyberspace, global cyberspace conflict would be unlikely. Yet, if the states demonstrate that Glaser's theoretical conditions are unattainable in cyberspace, it would be reasonable to expect an increase in cyberspace confrontations among these three powers. Applying neorealism theory to analyze the potential of international cooperation in cyberspace is quite new theoretical approach and there is a shortage of academic researches providing further analysis and conclusions on this issue. This brings out the novelty and significance of the Thesis.

To ensure their cybersecurity, states often invoke traditional military strategies, such as deterrence or restraint. However, whether the typical rules of military strategy are valid in cyberspace is questionable. The specifics of cyberspace could pose an obstacle to cooperation. These specifics are taken into account in order to apply Ch. Glaser's approach to cooperation. As the result, Glaser's assumptions are modified. Additionally, the concept of non-cooperation *costs* is analyzed. Direct confrontation is not a necessary condition for costs in cyberspace. Non-cooperation creates the insecurity culture in cyberspace and this is a dangerous situation *per se*, since it has a debilitating impact both on cyber and national security.

The concept of cyber conflict is controversial. Thus far, scholarship has focussed on the analysis of the potential of cyber warfare and there is still lack of a concensus whether such war is possible and how would it look like? Authors such as M. C. Libicki, T. Rid, L. Stone, G. McGraw, J. Arquilla, R. A. Clarke, B. Valeriano, R. C. Mannes, etc. have been trying to answer these questions. As the result, discussions among them have formed two academical camps, which are best identified by series of published articles. T. Rid was in total opposition with what seemed to be the mainstream assumptions about cyberwar, when he wrote in 2012 that cyber warfare is highly unlikely and that it will not occur in the future.[1] In his article "Cyberwar Will not Take Place" he states that instead of a cyberwar, the opposite is taking place: a computer-enabled assault on violence itself. Indeed, he demonstrates how sabotage, espionage and subversion mediated though cyberspace are so far mostly non-violent and only indirect (in the sense that "computer code can only directly affect computer-controlled machines, not humans").[2] An interesting critique of Rid's vision of violence has been formulated by John Stone in his article "Cyberwar Will Take Place"[3]. He underlines notably that the link between violence and lethality (stipulated by Rid in accordance with his interpretation of Clausewitz's work) is not inexorable: a military intervention, even in "minimizing loss of human life by employing advanced military technique" is still an act of war.[4] Accordingly, Stone declares that acts of war "need not to be lethal in character: they can break things, rather than kill people, and still fall under the rubric

[1] T. Rid, "Cyberwar Will Not Take Place". *Journal of Strategic Studies*, Vol 35, 2012, Is. 1. pp. 5-32.
[2] T. Rid, 5-32.
[3] J. Stone, "Cyberwar Will Take Place". *Journal of Strategic Studies*, Vol. 36, 2013, Is. 1. pp. 101-108.
[4] J. Stone, 101-108.

of war," and that consequently, "cyber war is possible [because] cyber attacks *could* constitute acts of war."[5]

Just like nuclear war, cyberwar is more theoretical than practical concept. However, when analysing the frequent trends of intersate relations some signs of cyber conflict cannot be ignored. Therefore, the concept of cyber conflict rather than cyberwar is used in this Thesis. It refers to the use of digital attacks - like computer viruses and hacking - by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction, influence public opinion on political decisions and undermine their legitimicy. Intensified confrontation is one of the necessary condition of cyber conflict which eventiually has a spillover effect on political level. Consequently, the lack of cooperation, trust and rules of engagement further deepen the conflict escalation which is expressed by increased number of cyber attacks. These factors determine the debilitating nature of cyber conflict and make it latent.

The specifics of cyberspace are discussed in the Thesis. Cyberspace is characterized by a different perception of time; cyberattacks can be carried out in the “here and now” simultaneously in many places. Moreover, there is a different perception of space. In the cyber domain, the boundaries of a state’s legal jurisdiction are extended and cyberattacks have a trans-boundary effect in that they are not bound to physical borders. Cyberspace also poses accountability and assessment problems. It is often difficult to discern who should be held liable for a cyberattack or even how much damage it has caused. However, the main accent is put on the classification of offensive and defensive weapons and capabilities in cyberspace. It is stated that traditional arms control regimes can be applicable to cyberspace and should be treated as the form of "negative cooperation".The purpose

[5] J. Stone, 101-108.

of this non-proliferation regime includes: minimizing instability, increasing predictability in relations between potentially hostile states, pre-empting the development of new cyber weapons,contributing to conflict management by establishing a framework to enable negotiations among parties, generally fostering a non-hostile atmosphere.

The Thesis follows the state-centric principle, which implies that only states can agree to common rules of conduct in cyberspace. Furthermore, the transfer of military logic to the cyber domain is justified for several reasons. First, cybersecurity is already perceived as an integral part of military security. Although cyber forces are acknowledged as a separate kind of military force, most countries' security strategies emphasize cybersecurity as a key component of their national security. Second, cybersecurity already plays a role in cross-border relations between states and bilateral agendas. Indeed cybersecurity it is as important as traditional military or economic cooperation. Third, multilateral cooperation (e.g. the UN) has led to agreements on cybersecurity and the limitations of cyber capacities.

THE ARGUMENTS OF THE THESIS

1. **According to rational thinking of defensive realism, hostile states will be in favor of negotiating a limitation of cyber capabilities to reduce escalation and avoid the damage caused by a potential conflict. Respectively, while intensifying a conflict between the US and Russia, and the US and China in cyberspace, countries will be in favor of looking for the "negative cooperation".**

While explaining possible cooperation, Glaser turns to theory based on military capabilities and strategy. The balance between offensive and defensive capabilities is of great importance to strategic choice. States seeking cooperation should be able to distinguish defensive from offensive means and purposefully invest in defensive

capabilities to reduce the fears of their potential adversaries. Glaser asserts: “The defender's power multiplied by the offense-defence balance tells us much more about the defender's prospects for maintaining effective defensive capabilities than does considering power alone”[6].The chances for conflict would be highest when competing states clearly distinguish between defensive and offensive capabilities and an offensive strategy prevails in their cyber politics. Respectively, according to rational thinking, hostile states will be in favor of reducing conflict escalation and looking for cooperation possibilities.

2. **Russia is using offensive cyber instruments to gain a competitive advantage over the US. Russia’s offensive posture in cyberspace reflects the fact the country is nether interested in conflict escalation nor in cooperation with the US.**

According to Glaser, the likelihood of conflict would remain high if competing states do not distinguish between defensive and offensive capabilities and their policy is dominated by an offensive posture. Accordingly, states should seek agreements to restrict offensive cyber capabilities or, at the very least, issue retaliatory sanctions for cyber attacks. In this case, an agreement is harder to reach, because states cannot explicitly assess and compare the costs that would be incurred in choosing one of the strategies. Russia’s aggressive cyber policy is the reflection of its offensive posture. Due to prevailing offensive advantage in Russia’s cyber policy and lack of trust, cooperation efforts between the US and Russia could not have been successful.

[6] Ch. L. Glaser, C. Kaufmann, "What is the Offence-Defence Balance and Can We Measure it". *International Security*, Vol. 22, No. 4, 1998, pp. 44-82.

3. **Both the US and China prioritize defensive cyber capabilities. They can be described as the "security-seeking states" which prioritize cooperation and stability in cyberspace.**

According to defensive realism, countries which clearly distinguish between offensive and defensive cybersecurity capabilities in their strategic documents and practical arrangements establish, at least theoretically, grounds for a rational calculation of cooperative strategy. From a defensive realism perspective, the US and China's relations exhibit the necessary theoretical components to attain negative cooperation in cyberspace and avoid a large-scale cyber conflict.

METHODOLOGY

The Thesis explores the motives and conditions under which the US, China, and Russia are likely to cooperate on qualitative arms control in cyberspace in order to improve both their national and international security. The analysis focuses on the 20-year period spanning from 1998 to 2018. The premises of defensive realism serve as the theoretical background for the analysis of the countries' behaviors and motives in cyberspace. This analysis is based on Charles Glaser's theory, which explains the conditions leading to "negative cooperation" among potential adversaries.

Motives. According to Glaser, motives define a state's dominant security and foreign policy strategy. A state's foreign policy could be either revisionist or oriented toward maintaining the status quo. This corresponds to the state's typically realistic attitude regarding the

motives of states in anarchy.[7] Revisionist states seek to unilaterally strengthen their cyber capabilities, while status quo-seeking states seek cooperation and stability in cyberspace. A state's motives are often revealed in official strategic documents, such as national cybersecurity strategies and action plans and foreign security policy. Understandably, official documents do not always reveal a state's true intentions. However, to identify initial trends in how states perceive the challenges of cybersecurity,a review of the official discourse is necessary. Does the official discourse emphasize a need for cooperation or does it tend to threaten confrontation? Strategic documents not only reveal a state's perceptions of cybersecurity challenges, they also communicate messages to potential adversaries.

The distinction between defensive and offensive cyber capabilities. There is uncertainty regarding whether a distinction can be made at all between defensive and offensive capabilities in cyberspace. States seeking cooperation should be able to distinguish defensive from offensive means and purposefully invest in defensive capabilities to reduce the fears of their potential adversaries. However, if the specifics of cyberspace render this distinction difficult to make, or if states deliberately avoid distinguishing between the two means, then an offensive-defensive balance in cybersecurity is not attainable, a condition that would reduce incentive for cooperation. States that cannot differentiate between the offensive and defensive capabilities of their adversaries would not be keen to make their own offensive and defensive capabilities clearly distinguishable and would perceive the development of cyber capabilities as dual-use cyber instruments. Keeping the specificities of cyberspace in mind, identifying posture in cyberspace is important as a state's intentions and motives reveal

[7] J. Mearsheimer, "Structural Realism" in T. Dunne, M. Kurki, S. Smith (eds.), *International Relations Theories: Discipline and Diversity*, 3rd Edition, Oxford: Oxford University Press, 2013, pp. 77-93

whether the state's cyber policies are dominantly offensive or defensive.

Information. The dissemination of information strengthens trust and confidence. At the same time, information exchange comes at a cost. By committing to exchange information with a potential adversary, the state limits its ability to cheat or bluff its opponent. This chapter seeks to identify messages the US, Russia, and China send regarding cybersecurity cooperation. An analysis of statements made by high-ranking officials reveals the official positions of states regarding possible cooperation with potential adversaries. The information variable is important in determining whether official strategies are supported in the speeches of state leaders or, conversely, contradict the state's official posture.

CONCLUSIONS

The risk of a cyberspace conflict escalating between the US, China and Russia encouraged them to seek cooperation. However, only few cooperation precedents could be described as successful. The analysis of "negative cooperation" indicates that escalation of conflict between the US and China forced these states to seek de-escalation opportunities. Following Obama and Xi's meeting in September 2015, during which the two countries agreed they would not knowingly support or conduct cybercrimes targeting trade secrets, analytical institutions reported a dramatic drop in the cyber-espionage of 72 suspected cybercrime groups in China. This improvement, even if temporary, establishes a precedent for bilateral cooperation to restrict offensive actions.

The United States and Russia also signed a landmark agreement to reduce the risk of conflict in cyberspace through real-time communications about incidents of national security concern in 2013. However, the accord didn't stop the escalation of conflict between states. On the contrary, it provoked large-scale and complex intrusions

of the US's cyberspace prior to the 2016 presidential election. This precedent shows controversy of Ch. Glaser's arguments, when saying that rational states will be in favor of negotiating a limitation of cyber capabilities to reduce escalation and avoid the damage caused by a potential conflict. One of the reason why this premise hasn't worked with the US and Russia, refers to Russia's cheating at its cyber arms control obligations under the 2013 Agreement. Consequently, the level of trust and likelihood of cooperation between states has dramatically decreased. Countries not always act rationally both in military and cyberspace.

Russia is using its cyber capabilities to provoke a political confrontation with the US and impact politics within the US. By choosing not to differentiate between its offensive and defensive capabilities and by sending confrontational messages, Russia is refusing to establish grounds for cooperation. In this respect, Russia is a revisionist state which seeks to unilaterally strengthen its cyber capabilities. This elevates the risk for the escalation of a cyber conflict between the US and Russia. According to Glaser, the likelihood of conflict would remain high if competing states do not distinguish between defensive and offensive capabilities and their policy is dominated by an offensive posture. Accordingly, states should seek agreements to restrict offensive cyber capabilities or, at the very least, issue retaliatory sanctions for cyberattacks. In this case, an agreement is harder to reach, because states cannot explicitly assess and compare the costs that would be incurred in choosing one of the strategies.

Worth mentioning, that the deterrence strategy did not work with Russia. President Obama's refusal to respond with coercive cyber measures against Russia, despite having evidence of Russia's breaches illustrates the US's cyber deterrence failure. It is too early to speak about changing US's posture and deterrence strategy toward Russia, although there are some signs that President D. Trump's administration is keen on adopting more decisive and credible policy in cyberspace toward hostile countries such as Russia.

The US and China clearly distinguish between offensive and defensive cybersecurity capabilities in their strategic documents and practical arrangements. According to Glaser, the likelihood of conflict would be low when competing states distinguish between offensive and defensive capabilities and prefer a defensive cyber policy, evidenced by voluntarily choosing to restrain their offensive capabilities. Of the three states, the US possesses the most powerful cyberspace forces, but its extensive cyber infrastructure is also the most vulnerable to cyberattacks. The US has relied on a deterrence strategy in cyberspace and has signalled clearly that it is for negative cooperation and would like to forge agreements in order to avoid offensive actions. China also officially demonstrates (frequently) a defensive posture toward its cyberspace infrastructure and toward the security of China's information space. The US and China's relations exhibit the necessary theoretical components to attain negative cooperation in cyberspace and avoid a large-scale cyber conflict. One the other hand, this precedent contradicts Glaser's argument indicating that in this case states would have less incentive to cooperate, as they would not be significantly disturbed by the possibility of a direct collision or escalation in cyberspace. The cooperation is extremely relevant even if countries demonstrate a defensive posture in their cyber policy. Therefore, Glaser's scenario for cooperation and conflict in cyberspace shall be further elaborated as following: when competing states distinguish between offensive and defensive capabilities, prefer a defensive cyber policy and are oriented toward maintaining the status quo, they still would be interested in cooperation, though an agreement is easier to reach.

The cooperation between Russia and China shall be considered as rational behaviour, though this partnership neither ensures cybersecurity, nor reflects tendencies of conflict and cooperation in cyberspace. Cyber-espionage attacks by Chinese groups against Russian targets have increased significantly.Therefore, it seems that the cybersecurity agreements between two countries has actually

brought little development to ensure their safety in cyberspace. Nevertheless, cyber-espionage is not the core of Sino-Russian cybersecurity cooperation. Much like Russia and China's combined effort to oppose a US-dominated world order, the insistence on "cyber-sovereignty" is a shared strategic interest that contrasts with the US advocacy for "cyber freedom."The closeness of China and Russia's cybersecurity relationship is not dependent on their ties with each other, but is defined in relation to the US.The fear for and the opposition to US dominance over the Internet brings China and Russia together.

The research has shown that Ch. Glaser's theoretical model serves as the appropriate starting point to analyse "negative cooperation" in cyberspace. Though some of the Glaser's assumptions are not confirmed (i.e. cooperation between China and the USA, China and Russia), they provide understanding of conflict and cooperation dynamics and enable to assess future cooperation scenarios between the states. Presuming that the strategic posture of the US does not change and is based on unreliable cyber deterrence, Russia will keep up with its aggressive cyber policy, testing American "red lines" in cyberspace. Since, Russia's cyber attacks are becoming more sophisticated, the threat of devastating cyber assault on critical U.S. infrastructure is growing.

The relationship between the US and China in cyberspace is based on cyber agreement negotiated in 2015. However, the accord does not guarantee the long-term stability and a higher level of trust between the states. Though this precedent shows that a potential for bilateral cooperation restricting offensive actions exists, the success of further cooperation will depend on China's determination not to fraud and comply with its commitments under the agreement. Looking from the perspective of defensive realisms, if the offensive advantage dominated China's cyber policy, the relations with the US would become confrontational.

Non-cooperation in cyberspace has *per se* a negative impact on cybersecurity. Due to the problems of assigning responsibility and anonymity in cyberspace countries with the prevailing offensive cyber-posture, such as Russia, will keep exploiting adversary's cyber vulnerabilities and applying the so-call exhaustion strategy in cyberspace. The exhaustion strategy in cyberspace does not seek the gradual erosion of an enemy nation's will or means to resist. When applied in cyberspace, the strategy reminds the acts of extremely expensive hooliganism based on testing and exploiting security gaps, for example for cyber spying purposes. The main risk of the exhaustion strategy relies on the fact that it could be applied both by the aggressor and defender. As the result, the potential of a further confrontation increases which is even more dangerous in cyberspace, since it blurs the line between the attacker and the target. Therefore, the cost of non-cooperation in cyberspace can incur even when there is no obvious signs of direct political or military conflict between the adversaries. On the other hand, continuous cyber attacks could lead to important spill over impacts on political agenda between states, as the example of the Russia and the USA relations shows.

Worth mentioning that the exhaustion strategy is used partially due to the lack of the effective regulation and control of cyberspace. This legal gap can be prevented or counteracted by the adoption of international agreements on cybersecurity principles, such as the agreement on not conduct or knowingly support cyber-enabled theft of business secrets reached between the US and China's leaders in 2015. This precedent shows that adversaries acting rationally can make "negative cooperation" efforts, in order to de-escalate tensions in cyberspace and avoid high-scale cyber conflict.

The Thesis shows that the same principles and conditions are valid for both cyber and military disarmament regimes. Two types of conditions necessary for effective cyber disarmament are identified.

The first refers to external conditions such as the increased confrontation in cyberspace, the use of offensive cyber capabilities and applying of exhaustion strategy. The second type refers to internal condition which could be described in a more intersubjective manner – this is a lack of trust between states which deepens the security dilemma in cyberspace. While evaluating the potential of cyber disarmament regime, worth mentioning that conditions which lead to "negative cooperation" between potential adversaries create the ground for the disarmament regime in cyberspace. Therefore, the cooperation efforts between the US and China can be treated as the example of such regime. The main characteristics of the regime is the self-restriction of offensive cyber capabilities, commitment to the agreements, sharing the information, in order to strengthen the trust between states. The specifics of cyber weapons complicates the creation of cyber security regime. However, countries' determination and will to pursue a policy of peaceful coexistence in cyberspace are the crucial conditions for the "negative cooperation" and establishment of cyber regime.

PUBLIKACIJŲ SĄRAŠAS

1. Agnija Tumkevič, „Cybersecurity in the Central Eastern Europe: from Risks to the Security Threats“. *Baltic Journal of Political Science* 2016 (5), 73-88.
2. Agnija Tumkevič, „Uncertain Security Community: Building Western Cybersecurity Order“. *Journal of Information Warfare* 2017,Vol 17, Issue 1.
3. Tomas Janeliūnas, Agnija Tumkevič, „Rational Motives to Seek for a Negative Cooperation between the US, China and Russia“, V. Benson, J. McAlaney (sud.), *Emerging Cyber Threats and Cognitive Vulnerabilities*. Elsevier (*straipsnis priimtas spausdinimui, knygą planuojama išleisti 2019 m.*)

TRUMPOS ŽINIOS APIE DISERTANTĄ

Agnija Tumkevič gimė 1987 metais Vilniuje. 2006 m. ji baigė Jono Pauliaus II gimnaziją ir įstojo į Vilniaus universiteto Tarptautinių santykių ir politikos mokslų institutą (TSPMI). Baigusi politikos mokslų bakalauro studijas, 2010 m. ji tęsė magistro studijas TSPMI (Tarptautinių santykių ir diplomatijos programoje). 2014 m. ji baigė magistro studijas ir gavo diplomą už geriausią magistro darbą.

2014 m. Agnija Tumkevič įstojo į doktorantūros studijas TSPMI. Jos moksliniai interesai apima kibernetinio saugumo sritį, ypatingai didžiųjų valstybių vaidmenį tarptautinio kibernetinio saugumo režimo kūrime.

2011-2017 m. A. Tumkevič dirbo Lietuvos Respublikos užsienio reikalų ministerijoje. Nuo 2017 m. Agnija užima patarėjos pareigas Lietuvos Respublikos Seimo Nacionalinio saugumo ir gynybos komiteto biure.

LIST OF PUBLICATIONS

1. Agnija Tumkevič, „Cybersecurity in the Central Eastern Europe: from Risks to the Security Threats“. *Baltic Journal of Political Science* 2016 (5), 73-88.
2. Agnija Tumkevič, „Uncertain Security Community: Building Western Cybersecurity Order“. *Journal of Information Warfare* 2017,Vol 17, Issue 1.
3. Tomas Janeliūnas, Agnija Tumkevič, „Rational Motives to Seek for a Negative Cooperation between the US, China and Russia“, V. Benson, J. McAlaney (sud.), Emerging Cyber Threats and Cognitive Vulnerabilities. Elsevier (straipsnis priimtas spausdinimui, knygą planuojama išleisti 2019 m.)

INFORMATION ABOUT THE PhD CANDIDATE

Agnija Tumkevič was born in 1987. In 2006 she finished the Gymnasium of John Paul II in Vilnius. In the same year she began bachelor studies of political sciences at Institute of International Relations and Political Science (IIRPS) of Vilnius University.

In 2010 she accomplished her bachelor studies and continued her studies at the IIRPS, Vilnius University (master programme of International Relations and Diplomacy). She finished her master studies by receiving diploma for the best Master Thesis. In 2014 she began her PhD studies of political sciences at Vilnius University. Her main research interest centres on cybersecurity issues and the role the great powers such as the US, China, Russia, the UK etc. in creating international cybersecurity regime(s).

In 2011-2017 Agnija Tumkevič worked at the Ministry of Foreign Affairs of Lithuania. From 2017 she works as the Adviser for the Office of National Security and Defence Committee of the Lithuanian Parliam

Vilniaus universiteto leidykla
Universiteto g. 1, LT-01513 Vilnius
El. p. info@leidykla.vu.lt,
www.leidykla.vu.lt
Tiražas 40 egz.