Taťána Jančárková

DOI:10.33179/BSV.99.SVI.11.CMC.24.2.4

PRIVAJANJE PSOV NA POVODEC V KIBERNETSKI VOJNI

LEASHING THE DOGS OF CYBER WAR

Povzetek Države se vse bolj ukvarjajo z razvojem kibernetskih zmogljivosti, ki lahko delujejo v celotnem spektru učinkov. Strukture, pristojne za doseganje teh učinkov, so navadno institucionalno povezane z oboroženimi silami ali obveščevalnimi službami oziroma so sestavljene iz obeh. Zaradi narave njihovih dejavnosti in možnosti vpliva na ustavne temelje demokratične države za obe vrsti organizacij navadno veljajo strogi mehanizmi nadzora in kontrole. Kljub temu je na voljo le malo raziskav o ustreznih nacionalnih okvirih, ki urejajo ofenzivne kibernetske zmogljivosti, in malo informacij o veljavnih nadzornih mehanizmih. V članku so predstavljeni pregled področij nadzora in izzivi, povezani s kibernetskimi zmogljivostmi, ter nakazane možnosti za prihodnje raziskave.

Ključne besede ***Ofenzivne kibernetske operacije, človekove pravice, pravna država, ustavni red, nadzor.***

Abstract States have increasingly been engaged in the development of cyber capabilities which can act across the full spectrum of effects. The structures competent to deliver these effects are usually institutionally tied to armed forces or intelligence services, or represent a mixture of the two. Both types of organizations are typically subject to strict oversight and control mechanisms due to the nature of their activities and their potential to impact on the constitutional foundations of a democratic state. Yet, there is limited research available on the respective national frameworks governing offensive cyber capabilities, and similarly little information on the applicable control mechanisms. This article provides an overview of the areas of oversight, explores the challenges related to cyber capabilities, and offers possible avenues for future research.

Key words ***Offensive cyber operations, human rights, rule of law, constitutional order, oversight.***

Introduction

When the US Cyber Command was established in 2009, it was a trailblazer in the field of institutionalizing cyber capabilities. Ten years later, several countries, including NATO and EU Member States, had established or were openly planning to develop cyber capabilities spanning the full spectrum of effects. In recent years »offensive cyber« has lost its somewhat negative legal and political connotations, and has been on the way to becoming a regular component of a modern state's national security and defence toolkit. Nevertheless, in spite of being a part of a broader general framework, cyber operations and cyberspace effects also have a novel character and potentially constitute a challenge from the perspective of constitutional and administrative law, including the respect and protection of fundamental rights and freedoms. This article contemplates the oversight and control mechanisms traditionally implemented in democratic states in respect of security and military elements, and assesses the applicability of executive control, parliamentary oversight and judicial review to cyber operations, with a particular focus on offensive cyber capabilities.

1 »OFFENSIVE CYBER« REVISITED

1.1 Institutionalization and frameworks

Offensive cyber capabilities can be understood as those that can deliver the full range of effects, that is, from securing to destroying or »completely and irreparably deny[ing] access to, or operation of, an asset« (NATO, 2020). They can also be understood as those that do not limit themselves to defence of one's own perimeter, but produce 'noticeable denial effects (i.e. degradation, disruption or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains' (DoD, 2018).

Unlike cyber security, which is primarily concerned with the protection of one's own information infrastructure and dependent services, cyber defence which includes offensive capabilities has the purpose of supporting multiple lines of a nation's efforts. Besides complementing the protection of critical information infrastructure, such capabilities also form part of the national defence system against terrorists, criminal and state actors, enable conventional defence operations, and help further the foreign policy agenda (UK, n.d.). While cyber security is often entrusted to civilian authorities or entities outside the military, cyber defence is an area of responsibility of structures directly belonging to or affiliated with armed forces and ministries of defence. The two concepts are, however, closely linked, feed into each other and at times overlap.

As mentioned in the introduction, there has been a clear and growing trend in openly developing offensive cyber capabilities, or active cyber defence, and institutionalizing them, including in NATO and EU countries (Pernik, 2018). According to Blessing (2021), cyber forces defined as 'active-duty military organizations with the capability and authority to direct and control strategic cyberspace operations to influence

strategic diplomatic and/or military interactions' had, by 2018, been established in as many as 61 UN Member States.

It has been repeatedly confirmed in national statements (Cyber Law Toolkit, 2021) and academic literature that offensive cyber operations can deliver effects which qualify as use of force. Even cyber operations that do not inflict physical harm or injury, i.e. lack the effect of kinetic force, can qualify as use of force under certain circumstances (Netherlands, 2019; Schmitt, 2019). Use of force has traditionally been reserved for armed forces and subjected to stringent control nationally and internationally, given the consensus of the international community on the general prohibition of the threat or use of force, enshrined in Article 2(4) of the UN Charter.

In parallel, active cyber defence involves a number of activities usually associated with intelligence services and espionage. Reconnaissance, exploitation, infiltration and information gathering are necessary preparatory activities for offensive cyber operations, which are undertaken both abroad and on domestic soil. The entities entrusted with these activities must therefore be authorized to act internally on home territory and infrastructure. However, deployment of armed forces at home is always subject to exceptions provided by law and often limited to assistance in civilian crisis management such as cases of natural disasters or internal security (including the recent Covid-19 pandemic, for instance). It should not come as a surprise, then, if cyber defence structures including offensive capabilities are often built within military intelligence or as joint structures involving both traditional military and intelligence components (Pernik, 2018).

Given the growth in the number of countries investing in these capabilities, research interest must inevitably turn to examining the underlying regulatory frameworks. The applicable frameworks span from those governing crisis management, to intelligence services, to those regulating deployment of the military and use of force.

1.2 What are the stakes?

The activities of both military and intelligence services are subject to scrutiny and control because of their potential to interfere with fundamental rights and freedoms and the values democratic states are based on. Most states will have civilian control of the armed forces inscribed into their constitutional law, along with professed respect and promotion of human rights and fundamental freedoms. Depending on historical experience, some states apply more restrictive governance concepts to intelligence services than others; when it comes to military intelligence, the record is however, almost universally mixed (Jasutis et al., 2020).

Should we be particularly wary about oversight measures for cyber capabilities? How can they be controlled? Is it at all possible?

Cyber effects can have major negative implications for a state's performance in human rights and fundamental freedoms. The range of potential interferences is

broad, from right to privacy, freedom of speech, freedom of assembly and peaceful enjoyment of property, all the way to right to life, if we consider cyber operations that lead to destructive effects comparable to conventional acts of violence.

To some extent, cyber operations have a specific character which warrants a specific approach. Due to the borderless nature of cyberspace and the ease with which unintended effects can propagate and bleed over to other systems and infrastructure, cyberspace operations should be carefully used and well controlled. In parallel, there is need for speed, flexibility and secrecy if the desired effects are to be delivered, which might caution against too heavy a supervisory mechanism.

Considering the above, it can be expected that cyber operations will rarely be executed under declared states of emergency; most of them require quite the opposite in order to maintain the advantage of surprise over the adversary. While human rights law can be derogated under certain circumstances, in most instances of cyber operations states would be unlikely to be able to rely on such a derogation.

Admittedly, the stakes are high. Firstly, there is the constitutional principle of civilian control over armed forces, and constraints on their deployment at home and abroad. Secondly, if cyber operations can constitute use of force, states must be very careful not to trespass their commitments under international law. Thirdly, the public in NATO and EU Member States are very sensitive to interference with their rights and freedoms by excessive intelligence work. The revelations of Edward Snowden and other whistle-blowers dealt a severe blow to confidence in intelligence services in the past, and only the ensuing judicial decisions have forced states to change the applicable legislation. At the same time, armed forces usually benefit from a positive public reputation, and should strive to maintain it.

2 THREE PRONGS OF OVERSIGHT

There are three areas in which control and supervision can typically be exercised in respect of state activities: control mechanisms within the executive branch itself, parliamentary oversight, and judicial review (at the national and international levels). All three contain measures which have been applicable to intelligence activities and/or the deployment of armed forces. Can they be applied to cyber operations? What are the challenges?

The parliament and government or president are the two most important tools in restraining war or »leashing the dogs of war« (Rudesill, 2021). We might add that independent judicial review, either *ex ante* or *ex post facto*, complements the guarantees and protection against excesses of security measures. Existing case-law of the European Court of Human Rights and the European Court of Justice bears witness to that.

Nevertheless, existing research says very little on the topic of oversight of cyber operations. As a matter of fact, literature explaining the institutional and legal frameworks applicable to offensive cyber capabilities in individual states appears rather limited, and information is often scattered over various sources, while comprehensive accounts of the likes of Pernik's study (2018) are few.

One notable exception is the US literature and research on the US framework. This is understandable to a large extent, given that the US framework may be the most developed one, if simply on the account of their head start in institutionalizing cyber capabilities and regulating military operations abroad. The system of constitutional checks and balances applicable to cyber operations begins with the War Powers Resolution of 1973. Even in the US, however, the Title 10/Title 50 debate related to whether cyber operations should be considered, and therefore regulated, as traditional military activities or as intelligence covert actions, suggests that dilemmas accompanying the authorization and oversight of US cyber operations persist (Waxmann, 2020; West, 2021). The uncertainty became even more obvious with the signing into law of the 2019 National Defence Authorization Act by President Trump, which broadened the authorizations given to the Department of Defense and the Cyber Command (Bailey, 2020).

Admittedly, much of this regulatory framework is classified (albeit sometimes leaked) and thus difficult to analyze, beginning with the Obama administration's Presidential Policy Directive 20 (PPD-20) which laid out, in 2012, guidelines for more assertive actions of the US in cyberspace, all the way to the Trump administration's 2018 amendments to PDD-20 or new national strategic documents. Nonetheless, there is a rich body of academic literature on the Title 10/Title 50 debate and congressional oversight of US cyber operations.

When it comes to European states and offensive cyber capabilities, less information is available in the literature, and even less again when it comes to constitutional protections. There are some studies presenting the existing or envisaged national structures (Pernik, 2018; Ducheine et al. 2021); there are posts on dedicated blogs (Schulze, 2020); and there are limited explanations offered by the governments themselves (UK, n.d.).

A project currently implemented by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, aims to partially fill the gap with a comparative study providing an overview of national governance frameworks of cyber defence forces, with a particular focus on constitutional foundations and oversight provisions.[1]

[1] *NATO CCDCOE, Governing Cyber Defence Forces, Project No. 22-L2-01P (POW 2022). The outcome of the project should be publicly available in early 2023.*

2.1 Executive control – autoregulation mechanisms

The first of the areas outlined in this paper pertains to the self-regulatory mechanisms within the executive branch that deploys cyber capabilities and, more broadly, the government.

The decision-making process should be set in such a way that the decision to use offensive cyber capabilities, or the competence to effectively review and change it, should lie at the highest possible, yet reasonably practical, level of the executive, with someone with political accountability. This means a minister or even the government, not merely the head of the cyber force concerned. The minister, government and other relevant parts of the executive structures should also be informed without delay of the executed cyber operation and its effects.

There should also be the possibility within the executive branch to inspect the cyber operations. The inspection function is a well-established concept and tool of control against administrative abuses or excesses available across various areas of public activity, including the national security and defence sectors, in many countries. They serve as watchdogs within the executive branch (Gaudion, 2021), their independence being guaranteed by the manner of appointment, competences granted by law, and sources of funding.

The Czech Republic, for instance, has incorporated the position of inspector of cyber defence into its cyber defence legislation (CZ, 2021). They are appointed by the government following a hearing in the relevant parliamentary committee, and have a mandate to inspect activities of military intelligence related to cyber defence, on which they report to parliament.

Inspectors, nevertheless, can hardly have enforcement power; their main contribution is to report their findings to the leadership of a ministry and/or the parliament or specialized bodies established by the latter. On the other hand, inspectors working within or close to the structures responsible for cyber operations can alleviate some of the concerns related to the risk of leaks of information, and can develop appropriate expertise that will enable them to understand and evaluate cyber operations.

2.2 Parliamentary oversight – by the will of the people

This leads us to the second, and possibly the most important, area where oversight of state activities is exercised: parliament.

The legislature is the representative of the people as the supreme source of power and legitimacy in a state. Obligations can only be imposed by law. Parliament thus already fulfils its oversight role by adopting legislation which respects the state's constitutional commitments and protects fundamental rights and freedoms.

Parliaments also have the power to call the executive branch to accountability by way of requesting information or reporting to specialized committees or the plenary. They can establish fact-finding or investigatory bodies and, not without importance, they approve the budget.

It is a fact that intelligence services oversight has met with mixed results across many jurisdictions. On the one hand, the secretive nature of the work causes the legislature to adamantly insist on supervision, and leads some to a default suspicion of abuse of powers. In countries with a history of autocratic regimes, the regulation of intelligence services tends to be more restrictive, and individual services can even have their own legislation (such as in the Czech Republic, where apart from the general law on intelligence services, each of the services active on domestic soil has its own law further regulating its activities).

On the other hand, research reveals that military intelligence oversight, which is of particular importance to offensive cyber operations, specifically lags behind in many aspects in numerous states (Jasutis et al., 2020). For a long time, many states have had only a very rudimentary regulatory framework concerning military intelligence, considering it only an element of the armed forces and therefore not necessitating a specific normative approach (Jasutis et al., 2020).

In addition, parliaments are not known to be the most efficient controlling bodies. Their procedures are lengthy and formalistic. Their elected members, who form the core of the specialized bodies, lack expertise (or there is a serious imbalance in technical understanding of the controlled and the controlling) or do not have time to develop it due to the election cycle. They can also be overburdened by other agendas.

There is also a legitimate and substantiated concern about the politicization of the oversight process, and of information leaks. In intelligence operations in particular, the risk of misinterpretation taking a wrong turn is very high, leading to unwanted escalations, nationally and internationally.

Nevertheless, along with the executive branch's self-regulatory mechanisms, challenged by uncertain transparency and independence, parliamentary oversight is probably the most promising form of oversight of offensive cyber capabilities. By way of an example, Czech public and parliamentary debate led, between 2017 and 2020, to a complete overhaul of cyber defence legislation, and although the latter still leaves things to be desired, the amendments to the Act on Military Intelligence and related law adopted in early 2021 marked a substantive and substantial improvement to the original draft tabled in 2016, particularly where transparency and legal guarantees were concerned.

Last but not least, it is parliaments that control the deployment of armed forces. In some countries, parliamentary consent is already required *ex ante* (Denmark or Germany). While arguably posing administrative difficulties, the character of cyber

operations and specifically their potential effects do not automatically provide grounds for absolving the military and the executive branch of this obligation. However, more work is admittedly needed to make the process efficient and effective in respect of cyber operations.

2.3 Judicial review – powerful tool or irrelevant concept?

The third available tool of oversight, judiciary review, is potentially powerful in its impact, yet particularly challenging to resort to.

In recent years, it has been thanks to the binding decisions by the European Court of Human Rights (ECtHR) and the European Court of Justice (ECJ) that national surveillance frameworks have had to change, including bulk interception systems using similar technologies to those deployed within cyber defence capabilities.

Beginning with Klass v. Germany, courts ruled as early as the 1970s that surveillance legislation itself was susceptible to the violation of human rights, even if there was no ascertained and actual interference with the rights of the applicant (ECtHR, 1979). Rulings in cases such as Privacy International (UKSC, 2019; ECJ, 2020) or Big Brother Watch v. the UK (ECtHR, 2021) ascertained judicial review of decisions by bodies authorizing hacking, found flaws in bulk interception regimes, and brought about changes in the regulatory frameworks pertaining to the work of the same intelligence organizations that today deal with or participate in the development and deployment of offensive cyber capabilities.

At the same time, it cannot be ignored that several of those decisions hinged on procedural issues, and in principle did not oppose the legitimacy of national security concerns and the state's need to pursue it effectively. Furthermore, the courts have been criticized for not having gone all the way to establish principles more adequate for the technologies and modern digital mass surveillance systems used today, or even to declare the latter incompatible with international human rights law (O'Donoghue, 2018; Zalnieriute, 2021).

The existing case law has also shown that any change in the system is likely to have to come from within. Be that as it may, relying on the civic duty of individuals to report unconstitutional behaviour is clearly not a sustainable, systemic solution to the requirements of a democratic cyber power.

Over the past few decades, we have also seen a growing number of proceedings brought against states with regard to the conduct of their armed forces during military operations. Several court judgments by both national courts and the ECtHR are available on the application of human rights law and IHL in cases concerning the killing of foreign nationals abroad. The rulings in these cases have raised questions as to the primary source of legal authority – whether it was IHL or human rights law – and the scholarly debate on this issue is equally rich. Nevertheless, it is not disputed that states are responsible for human rights violations committed abroad.

It is also widely accepted by states that human rights apply online just as they do offline (OHCHR, n.d.). If cyber means can bring about the same effects as kinetic force, it is then easy to imagine a future case-law on the effects brought about by cyber operations.

When it comes to *ex ante* judicial control, in most countries intelligence services are obliged to seek a court's permission, an independent authorization, if their operations are to interfere with fundamental rights. While cyber defence structures may not be entirely equated with intelligence services, and the threat scanning will usually not touch upon individuals, it does appear plausible that the execution of a cyber operation should be vetted by an independent authority, be that a secret tribunal or another independent body. Yet at present there is no indication that any European or other country would incorporate a court's permission into the decision-making process applicable to offensive cyber operations, be it for any partial component of the operation.

Conclusion

Our modern values-based society model dictates mostly a defensive posture. However, the dilemma of whether to build offensive cyber capabilities appears to have been largely solved in the affirmative, and the states have been moving from advocating strictly passive defence in cyberspace to openly admitting offensive capabilities and building corresponding institutional frameworks.

Yet, resorting to 'active cyber defence' brings implicit regulatory challenges that democratic, rule-of-law abiding societies cannot ignore. Offensive cyber operations oscillate on the borderline of intelligence and military actions and are usually executed by either one, or by another type of structure within a state's security/defence apparatus. Some states have created capabilities combining the two.

Both types of structures are subject to cautious national regulation given the potential impact of their actions on rights and freedoms, on political stability and on the state's international standing.

The challenge therefore lies in crafting a democratic and responsible cyber power. Respect for the constitution, protection of fundamental rights and freedoms, and effective oversight of cyber capabilities should be an integral part of the solution. In fact, the new regulatory frameworks should address these concerns by design, learning from and avoiding the mistakes of their predecessors in cyber security or other avenues of national security business.

While there are differences between states in regulatory approaches, as well as varying levels of sensitization towards potential human rights violations, the 'right to security' advocated by states and to a growing extent accepted by courts and international organizations should be approached with caution, lest we risk its over-securitization and compromise the values we profess to defend.

Future research should therefore take a closer interest in states' approaches to national cyber defence and their constitutional foundations, and should be able to alert states should they get too close to falling into a chasm of 'unconstitutionalism', in these turbulent times of 'unpeace'.[2]

Bibliography

1. *Bailey, C. E., 2020. Offensive Cyber Operations: A Gray Area in Congressional Oversight, Boston University International Law Journal, 38-2, pp 240-85.*
2. *Big Brother Watch and Others v. the United Kingdom (2021), European Court of Human Rights, Applications Nos. 58170/13, 62322/14 and 24960/15. https://hudoc.echr.coe.int/eng?i=001-210077.*
3. *Blessing, J., 2021. The Global Spread of Cyber Forces, 2000-2018, 14th International Conference on Cyber Conflict: Going Viral, T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.), NATO CCDCOE Publications, Tallinn, Estonia, pp 233-55.*
4. *Czech Republic, 2021. Act No. 289/2005 Coll, on Military Intelligence, as amended by Act No. 150/2021 Coll, Article 16k. https://www.zakonyprolidi.cz/cs/2005-289, [CZ, 2021].*
5. *Ducheine, P. A. L., Arnold, K. L., Pijpers, B. M. J., 2021. Decision-Making and Parliamentary Control for International Military Cyber Operations by the Netherlands Armed Forces, in Military Operations and the Notion of Control under International Law. https://doi.org/10.2139/ssrn.3540732.*
6. *Gaudion, A. C., 2021. Answering the Cyber Oversight Call, work in progress. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3904732.*
7. *Jasutis, G., Fuior, T., Vashakmadze, M., 2020. Parliamentary Oversight of Military Intelligence, DCAF – Geneva Centre for Security Sector Governance, Geneva. https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf.*
8. *Klass and Other v. Germany, 1979. European Court of Human Rights, No. 5029/71. https://hudoc.echr.coe.int/fre?i=001-57510.*
9. *Ministry of Foreign Affairs, 2019. Letter to Parliament on the International Legal Order in Cyberspace, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace. [Netherlands, 2019]. Not available online.*
10. *NATO, 2020. AJP-3.20: Allied Joint Doctrine of Cyberspace Operations, Allied Joint Publication, January 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.*
11. *O'Donoghue C., Keyhani N., 2018. ECtHR Rules on UK Mass Surveillance under RIPA, Technology Law Dispatch, 25 October 2018. https://www.technologylawdispatch.com/2018/10/in-the-courts/ecthr-rules-on-uk-mass-surveillance-under-ripa/.*
12. *OHCHR (n. d.) International Standards. OHCHR and Privacy in the Digital Age. https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards.*
13. *Pernik P., 2018. Preparing for Cyber Conflict: Case Studies of Cyber Command, ICDS, Tallinn. https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018.pdf.*
14. *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (2020), European Court of Justice, C-623/17. https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-623/17 [ECJ, 2020].*

[2] *The notion of 'unpeace' has been borrowed from Lucas Kello and his keynote speech delivered at the 2022 US Cyber Command Legal Conference, on 10 March 2022.*

15. *R (Privacy International) v Investigatory Powers Tribunal, 2019. United Kingdom Supreme Court, UKSC 22, Judgment of 15 May 2019. https://www.supremecourt.uk/cases/uksc-2018-0004.html [UKSC, 2019].*
16. *Rudesill, D. S., 2021. Cyber Operations, Legal Secrecy, and Civil-Military Relations, in Beehner L., Brooks R., Maurer D., Reconsidering American Civil-Military Relations: The Military, Society, Politics, and Modern War, Oxford University Press, as published on 16 December 2020 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3745263.*
17. *Schmitt, M., 2019. The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis, Just Security, 14 October 2019. https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/.*
18. *Schulze, M., 2020. German Military Cyber Operations are in a Legal Gray Zone, Lawfare Blog, 8 April 2020. https://www.lawfareblog.com/german-military-cyber-operations-are-legal-gray-zone.*
19. *United Kingdom Government (n.d.), National Cyber Force Explainer, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1041113/Force_Explainer_20211213_FINAL__1_.pdf [UK, n. d.].*
20. *US Department of Defense, Joint Chiefs of Staff 2018, JOINT PUB. 3-12, CYBERSPACE OPERATIONS II-7 (2018). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.*
21. *Use of Force. National Positions, 2021. International Cyber Law in Practice – Interactive Toolkit, NATO CCDCOE, viewed 2 April 2022. https://cyberlaw.ccdcoe.org/wiki/Use_of_force.*
22. *Waxmann, M. C., 2020. Cyberattacks and the Constitution, The Hoover Institution Working Group on National Security, Technology and Law, Aegis Series Paper No. 2007, Columbia Public Law Research Paper No. 14-675. https://scholarship.law.columbia.edu/faculty_scholarship/2725.*
23. *West, L.B., 2021. The Rise of the »Fifth Fight« in Cyberspace: A New Legal Framework and Implications for Great Power Competition, Military Law Review, 229-3, pp 273-347.*
24. *Zalnieriute, M., 2021. Procedural Fetishism and Mass Surveillance under the ECHR: Big Brother Watch v. UK, Verfassungs Blog on Matters Constitutional, 2 June 2021, https://verfassungsblog.de/big-b-v-uk/, DOI: 10.17176/20210602-123858-0.*

e-mail: tatana.jancarkova@ccdcoe.org

e-mail: tatana.jancarkova@ccdcoe.org

Taťána Jančárková je magistrirala iz prava in ruskih ter vzhodnoevropskih študij na Karlovi univerzi v Pragi in iz mednarodnega javnega prava na Univerzi Leiden. Je raziskovalka v Sektorju za pravne zadeve Natovega Centra odličnosti za kibernetsko obrambo v Talinu v Estoniji. Kot raziskovalko jo trenutno zanimajo uporaba mednarodnega prava v kibernetskih operacijah (projekt Interactive Cyber Law Toolkit), regulativni vidiki zaščite kritične informacijske infrastrukture in nacionalni okviri kibernetske obrambe. Pred tem je bila pravna svetovalka in vodja Oddelka za mednarodne organizacije in pravo pri Nacionalni agenciji za kibernetsko in informacijsko varnost Češke republike.

Taťána Jančárková holds master's degrees in law and in Russian and East European studies from Charles University in Prague and an LL.M. in public international law from Leiden University. She is a researcher at the Law Branch of NATO CCDCOE in Tallinn, Estonia. Her current research interests include application of international law to cyberspace operations (Interactive Cyber Law Toolkit project), regulatory aspects of critical information infrastructure protection and national cyber defence frameworks. She has previously served as legal adviser and led the International Organisations and Law Unit at the National Cyber and Information Security Agency of the Czech Republic.