National Research University Higher School of Economics

As a manuscript

Aleksei Turobov

Transformation of the Sphere of Security Provision in Innovative States under the Influence of Digitalisation and Automation Technologies

SUMMARY OF THE DISSERTATION
for the purpose of obtaining academic degree
Doctor of Philosophy in Political Scince

Academic Supervisor:
Candidate of Science (PhD)
Associate Professor Mikhail Mironyuk

Moscow, 2022

Relevance of Research

Digitalisation has recently received considerable attention from representatives of states and international organisations. According to various studies, effective digital adoption plays a crucial role in achieving revenue growth and increasing user satisfaction[1]. In addition, digital technologies can give many benefits to societies by facilitating access to public services, ensuring higher employment and economic development and thus can ultimately improve the well-being of citizens[2]. Moreover, state-led digitalisation complements the traditional and formal interaction mechanisms between citizens and the government, creating additional online institutions. Moreover, successful digitalisation has significantly changed the relationship between the state and the society by increasing frequency and quality of interactions between citizens and the government[3].

These processes are changing the structure and content of state policies and governance[4]. However, the phenomenon of digitalisation is complex. On the one hand, terms such as digitisation (downloading forms online), digitalisation (filling out forms online) and digital transformation (providing a full set of services online) are used interchangeably in the literature and often focus only on the first two functions[5]. On the other hand, digitalisation itself is based on the interconnection of various types of digital technologies and a system of three elements: infrastructure/architecture, software for the interaction of technologies and users, and users with each other by means of digital technologies.

In this study, the conceptualisation proposed by Mergel, Edelmann and Haug[6], focusing on the concept of digitalisation, is used:

- digitisation – transition from analogue to digital services with a one-to-one change in content/information delivery and with the addition of a technological communication channel;

[1] Dong Q. J. Moving a Mountain with a Teaspoon: Toward a Theory of Digital Entrepreneurship in the Regulatory Environment // Technological Forecasting and Social Change. — 2019. — Sept. — Vol. 146. — P. 923– 930.
[2] Galindo-Martin M.-A., Castano-Martinez M.-S., Mendez-Picazo M.-T. Digital Transformation, Digital Dividends and Entrepreneurship: A Quantitative Analysis // Journal of Business Research. — 2019. — Vol. 101(C), no. 146. — P. 522–527.
[3] Wong, Chu. Digital Governance as Institutional Adaptation and Development: Social Media Strategies between Hong Kong and Shenzhen // China Review. — 2020. — Aug. — Vol. 20, no. 3. — P. 43–70.
[4] Bretschneider, Mergel. Technology and Public Management Information Systems : Where we have been and where we are going // The state of public administration : issues, challenges, and opportunities. — 1st ed. — London:Routledge Taylor Francis Group, 2015. — P. 187–203.
[5] Mergel, Edelmann, Haug. Defining digital transformation: Results from expert interviews // Government Information Quarterly. — 2019. — Oct. — Vol. 36, no. 4. — P. 101385.
[6] Ibid. p.12

- digitalisation – focusing on potential changes in processes (social, economic and political) beyond the mere digitisation of existing processes and forms;
- digital transformation - complete implementation of processes in the digital environment, taking into account cultural, social and organisational characteristics, using a holistic approach and obtaining mixed results.

Digitalisation encompasses technological advances and institutional changes such as reliable connectivity and quality standards, the Internet and data security, financial and legal frameworks, and scientific, innovation and human capital[7]. In this study, digitalisation is presented as a political process (rather than purely technological).

Despite high degrees of digital technologies adoption in several countries, their use does not automatically lead to increased participation of civil society in political processes. It does not provide an adequate quality of public administration (see, for example, a study on the potential impact of ICT, the Internet and e-government on transparency of governments[8]; a study on the negative impact of Internet use on political engagement[9]; a study on political participation and "failures" of tele-democracy[10]; a study on increasing political participation through technologies that do not bring results in the short term[11], etc.).

Digital technologies are also causing changes in the security domain. Digitalisation and the rapid development of ICTs have allowed new, ingenious, and aggressive ways to monitor, predict and/or mitigate potential security threats[12]. These "novel" security practices and processes (e.g., the widespread use of biometrics[13], surveillance[14], drones and targeted

[7] Specific types of technologies, as well as the concept of digitalisation in the relationship of the kinds of digital technologies with the achievement of particular goals in the example of the education sector, see: Антонова А., Туробов А. Мишени цифровых технологии через призму образования // Образовательная политика. — 2020. — т. 82, No 2. — с. 42— 55.

[8] Bertot J. C., Jaeger P. T., Grimes J. M. Using ICTs to create a culture of transparency: E-government and social media as openness and anticorruption tools for societies // Government Information Quarterly. — 2010. — Vol. 27, no. 3. — P. 264–271.

[9] Boulianne S. Does internet use affect engagement? : A meta-analysis of research // Political Communication. — 2009. — Vol. 26, no. 2. — P. 193– 211.

[10] Arterton F. C. Political Participation and «Teledemocracy» // PS: Political Science Politics. — 1988. — Vol. 21, no. 3. — P. 620–627.

[11] Arterton F. C. Teledemocracy: Can Technology Protect Democracy? — Newbury Park, CA.: SAGE Publications Ltd, 1987. — 222 p.

[12] Hendershot C., Mutimer D. Critical Security Studies // The Oxford Handbook of International Security. — Oxford University Press, 2018. — P. 1– 13.

[13] Muller B. Securing the Political Imagination: Popular Culture, the Security Dispositive and the Biometric State // Security Dialogue. — 2008. — Vol. 39, no. 2/3. — P. 199–220.

[14] Bell C. Surveillance Strategies and Populations at Risk: Biopolitical Governance in Canada's National Security Policy // Security Dialogue. — 2006. — Vol. 37, no. 2. — P. 147–6

killings[15], algorithmic security[16]) have opened up theoretical and empirical opportunities and new challenges.

One of the main functions of the modern state, regardless of the political regime type, is to ensure the security of citizens (particular groups of citizens) and itself as a whole. The quality of implementation of such a function affects citizens' perceptions of the legitimacy of the government, political institutions and actors. Security provision affects the effectiveness of the state both within its borders and beyond. The security sphere is expanding and is filled with new elements, such as cybersecurity, computer network security, information security, etc. Accordingly, due to digital technologies, the arsenal of tools to ensure security is constantly increasing.

Contemporary security research focuses on three phenomena: the sources of actors' interests, the development of national collective goals, and the state's capacity for action[17]. With the growing complexity and sophistication of digital technologies, the interconnection and interdependence of technical, information, and digital areas increase within the security sphere.

Security in political science is studied at various levels, including both at the level of the political system itself (political survival at all levels: regime, institutions, actors) and the level of society (citizens, individual social spheres, etc.). Digital technologies at every level act both as tools that strengthen and provide, and as something that creates a space (digital space) where security also needs to be ensured.

The role of digital technologies in politics is ambivalent. On the one hand, digital technologies are a tool for changing the structure of roles and responsibilities of citizens. From this point of view, digital technologies help to solve some of the problems of modern states (e.g., lower participation in elections, increasing distance between the political system and the population, and growing distrust in traditional political institutions[18]). Theoretically, the digital transformation of the political sphere corresponds with the ideals of direct democracy. It focuses on the transfer of power from traditional institutions and elites to groups of people, and collective action (using technological tools) aims to democratise governance processes. This

[15] Grayson K. Cultural Politics of Targeted Killing: On Drones, Counter-Insurgency, and Violence. — New York: Routledge, 2016. — 230 p.
[16] Amoore L., Raley R. Securing with Algorithms: Knowledge, Decision, Sovereignty // Security Dialogue. — 2017. — Vol. 48, no. 1. — P. 3– 10.
[17] Krebs R. The Politics of National Security // The Oxford Handbook of International Security. — Oxford University Press, 2018. — P. 259–273:2
[18] Susha I., Gronlund A. Context clues for the stall of the Citizens' Initiative: Lessons for opening up e-participation development practice // Government Information Quarterly. — 2014. — Vol. 31, no. 3. — P. 454–465.

transformation is gaining institutional manifestations, including electronic voting, electronic government, etc.

On the other hand, political institutions set the "rules" for individual and collective behaviour, determine information transfers and social choice[19] and can speed up or slow down social and political changes[20]. The country's technological development level also affects the degree and quality of the use of digital technologies in the political sphere. However, political institutionalisation enhances the effectiveness of such use[21]. Concerning the national security, this means that institutions and actors responsible for security provision, determining the degree of danger of specific threats, choosing measures to counter them, and assigning institutions for control and supervision of institutions and actors that provide security. are all subject to *transformations under the influence of digitalisation and automation technologies*.

The large-scale implementation of digital approaches in the absence or inaccessibility of public evidence-based analysis and assessments of the risks, challenges, benefits and threats in the security determines the agenda of academic discussions and creates uncertainty in the practical implementation of security policies. Therefore, critical reflections and evaluations of alternatives based on evidence are a significant and relevant task for the purpose of forming a proportionate, effective, evidence-based, and balanced security policy.

Development of the Research Topic

Accelerated development of digital technologies and their introduction into various spheres of life of a modern society entail fundamental changes not only of a technological and economic nature but also in the field of politics and governance. Changes in communication, collection and use of information, and digital interactions between the state and the society have led to the emergence of new concepts of governance and politics, including

[19] Plott C. R. The application of laboratory experimental methods to public choice // Collective decision making: Applications from public choice theory. — Johns Hopkins University Press, 1979. — P. 137–160:156
[20] Jackman R. W., Miller R. A. Voter turnout in the industrial democracies during the 1980s // Comparative Political Studies. — 1995. — Vol. 27. — P. 467–492.
[21] Jho W., Song K. J. Institutional and technological determinants of civil e-Participation: Solo or duet? // Government Information Quarterly. — 2015. — Vol. 32, no. 4. — P. 488–495.

"teledemocracy"[22], "e-democracy"[23][24], "virtual democracy"[25], "e-government"[26][27][28], "GovTech" and "algorithmic government"[29], etc. These concepts are evolving constantly. However, neither the academic community, nor political actors have been ready for the rapid development of modern digital technologies (e.g., complex mathematical and statistical algorithms, machine learning, neural networks, artificial intelligence, blockchain technology, 5G communication technology, big data, etc.).

The spread of digital technologies in political life is a relatively recent but recognized object of study. We may list, for example, research on global political communications and global political governance[30], the impact of the digital divide on political participation[31], the impact of Internet use and online activities on political participation[32], the impact of information and digital technologies on electoral behaviour[33], studies of institutional and non-institutional forms of political participation using information and digital technologies[34],

[22] Arterton F. C. Political Participation and «Teledemocracy» // PS: Political Science Politics. — 1988. — Vol. 21, no. 3. — P. 620–627; Idem, Teledemocracy: Can Technology Protect Democracy? — Newbury Park, CA. : SAGE Publications Ltd, 1987. — 222 p.
[23] Watson R. T., Mundy B. A strategic perspective of electronic democracy // Communications of the ACM. — 2001. — Vol. 44, no. 1. — P. 27–30.
[24] Carrizales T. Critical Factors in an Electronic Democracy: a Study of Municipal Managers // Electronic Journal of E-Government. — 2008. — Vol. 6, no. 1. — P. 23–30.
[25] Norris P. Virtual democracy // Harvard International Journal of Press/Politics. — 1998. — Vol. 3, no. 2. — P. 1–4.
[26] Brown D. Electronic government and public administration // International Review of Administrative Sciences. — 2005. — Vol. 71, no. 2. — P. 241– 254.
[27] Manoharan A., Carrizales T. J. Technological equity: An international perspective of e-government and societal divides // Electronic Government. — 2011. — Vol. 50, no. 1. — P. 56–66.
[28] Rose J., Flak L. S., Saebo O. Stakeholder theory for the E-government context: Framing a value-oriented normative core // Government Information Quarterly. — 2018. — Vol. 35, no. 3. — P. 362–374.
[29] Engin Z., Treleaven P. Algorithmic Government: Automating Public Services and Supporting Civil Servants in using Data Science Technologies // The Computer Journal. — 2019. — Vol. 62, no. 3. — P. 448–460.
[30] Castells. The new public sphere: Global civil society, communication networks, and global governance // The Annals of the American Academy of Political and Social Science. — 2008. — Vol. 616, no. 1. — P. 78–93.
[31] Sylvester D., McGlynn A. The digital divide, political participation, and place // Social Science Computer Review. — 2010. — Vol. 28, no. 1. — P. 64–74.
[32] Quintelier E., Vissers S. The effect of Internet use on political participation: An analysis of survey results for 16-year-olds in Belgium // Social Science Computer Review. — 2008. — Vol. 26, no. 4. — P. 411–427.
[33] Tolbert C., McNeal R. Unraveling the effects of the Internet on political participation? // Political Research Quarterly. — 2003. — Vol. 56, no. 2. — P. 175–185.c
[34] Hooghe M., Marien S., Quintelier E. Inequalities in non-institutionalized forms of political participation: A multi-level analysis of 25 countries // Political Studies. — 2010. — Vol. 58, no. 1. — P. 87–213.

"digital natives" and "network generation"[35], the negative impact of the Internet and the online environment on political engagement[36], e-participation[37], e-government[38], etc.

A separate aspect concerns the phenomena of "automation" and "algorithmisation". This study seeks to go beyond perception of automation as a purely technological process. The focus is on the automation of politics and governance, and for these two spheres digital technologies act as tools. We perceive automation as a more efficient use of digitalisation opportunities due to increase both in speed and scale of the introduction of digital technologies into political practice with the purpose to change the processes of simple decisions making and repetitive cognitive functions, which is accompanied by the release of staff time, allowing the staff to focus on tasks more in line with skill set[39]. In the context of this study, the fact that digital technologies (in particular, artificial intelligence technologies) are recognised as one of the critical elements of automation directly in security matters is also significant[40].

Similarly, as with automation, the conceptualisation of algorithmisation draws from a socio-technological perspective and is not limited solely to the technological domain. Algorithmisation refers to how an organisation/institution restructures its functions around the use of algorithms to make decisions and to take appropriate actions[41]. At the same time, the "reorganisation" of processes occurs through the use of algorithmic systems of varying complexity (including the use of artificial intelligence technology). The main focus of this study is on the reorganisation of work processes through the use of algorithms.

The evolutionary development of the security sphere, on the one hand, and the rapid involvement of digital technologies (and, as a result, changes) in the security sphere, on the other, allow to formulate the ***first level of problematisation of this study***. At the theoretical level of problematisation, we seek to fill gaps in the academic knowledge related to the general context of changes in the security sphere under the influence of digital technologies. Research

[35] Bennett S., Maton K., Kervin L. The digital natives debate: A critical review of the evidence // British Journal of Educational Technology. — 2008. — Vol. 39, no. 5. — P. 775–786.
[36] Boulianne S. Does internet use affect engagement?: A meta-analysis of research // Political Communication. — 2009. — Vol. 26, no. 2. — P. 193– 211.
[37] Saebo O., Rose J., Skiftenes Flak L. The shape of e-Participation: Characterizing an emerging research area // Government Information Quarterly. — 2008. — Vol. 25, no. 3. — P. 400–428.
[38] Nam T., Pardo T., Burke G. e-Government interoperability: Interaction of policy, management, and technology dimensions // Social Science Computer Review. — 2012. — Vol. 30, no. 1. — P. 7–23.
[39] Germundsson N. Promoting the digital future: the construction of digital automation in Swedish policy discourse on social assistance // Critical Policy Studies. — 2022. — P. 1–19:9
[40] Sari O., Celik S. Legal evaluation of the attacks caused by artificial intelligence-based lethal weapon systems within the context of Rome statute // Computer Law Security Review. — 2021. — Vol. 42. — P. 105564.
[41] Meijer A., Lorenz L., Wessels M. Algorithmization of Bureaucratic Organizations: Using a Practice Lens to Study How Context Shapes Predictive Policing Systems // Public Administration Review. — 2021. — Vol. 81. — Iss. 5. — P. 837–846:838

results point to specific changes (as well as concerns and uncertainty associated with these changes) in security under the influence of digital technologies. However, little research has focused on **how** technology is entering the sphere of security and **what changes** are occurring in the sphere of security of a state. Security studies operate with the concepts of threats and resources/opportunities to eliminate threats. In this vein, digital technologies can act both as security threats and as tools of security. Several questions arise: (1) How do states define and perceive security threats related to digital technologies? (2) How do states use digital technologies as tools to enhance their security? (3) What is the dynamic of the digital technologies application?

Kenneth Payne[42], drawing parallels between artificial intelligence technology (advanced algorithms for predicting and analysing data) and nuclear weapons, points out significant strategic and scientific uncertainty about the consequences of using this technology in military affairs. Moreover, ongoing changes in the military affairs require new strategic decisions: "...The rapid advances of AI that seeks to optimise human goals are beginning to *transform* military affairs, and demand new strategic thought"[43].

Accordingly, at a theoretical level, this study aims to address a specific problem - to *offer a reasonable understanding (and illustration of the dynamic) of the introduction of digital technologies into the sphere of security*.

The second level of problematisation is in the instrumental (methodological) plane. There is practically no understanding of which analytical toolkit (method/approach) makes it possible to trace such changes with the possibility of assessing the consequences for the sphere of security. Expert interviews provide some "ground" for research but attempts at an "objective" approach to the sphere of security through quantitative methodology are rare. Therefore, without downplaying the importance of expert knowledge, we strive to supplement it with more verifiable evidence.

This study seeks to provide evidence of how the dynamic of transformations in the sphere of security is formed by constructing an empirical model of transformation and evaluating the state's security system under the influence of digital technologies (using a specific type of digital technology as an example).

The empirical model aims to form the concept of evaluating the security system (not only threats but also identifying opportunities/capabilities) and offer an empirical approach to

[42] Payne K. Artificial Intelligence: A Revolution in Strategic Affairs? // Survival. — 2018. — Vol. 60. — P. 7–32.
[43] Ibid. p. 30

measuring the concept of the sphere of security of a state. Thus, at the theoretical level, the work contributes to the research into the processes of transformation of security under the influence of digital technologies. At the methodological level, it proposes an approach to measuring such transformations using an empirical model.

This study is based on the following assumptions: we consider digital technologies in the sphere of security as (1) tools used for security provision and as (2) threats defined at the national (national security) and international (international and global security) levels. The focus of the study is the national security.

Research question

What are the dynamics of the of digital technologies application by governments of different countries in the sphere of national security?

The research question is subsequent to the structural logic of the research. Transformation is a broad concept, it is understood in this study as significant changes and transformations of security policy (Chapter 1). The empirical part (Chapter 2) narrows the scope to changes in security provision. The research question aims to obtain meaningful results from the empirical part, namely, identifying the dynamics of changes in national security. Identifying such dynamics and their meaningful interpretation (based on both the theoretical part and the collected data) will allow to illustrate and explain the individual elements of the transformation (shifts and the consequences of such changes).

Additional research question:

What are the differences and similarities in the use of digital technologies in the sphere of security in different countries?

The answer to an additional research question serves as a meaningful saturation of the identified changes. Thus, the results will demonstrate actual transformations and provide qualitative content to describe best practices.

The main research question aims to identify the dynamics of changes using the developed empirical model. Additional question is to identify best practices by comparing models of different countries (directly selected country cases).

Goal and Aims of the Study

Major goal of the study is to identify features of the use of digitalisation technologies as an element (factor) of the transformation of security.

Research objectives:

1. to conceptualise and to operationalise digitalisation and automation in the sphere of security;
2. to empirically identify key types of digital technologies in the process digitalisation and the countries leading in digital transformation;
3. to create an empirical model for evaluating the process of applying digital technologies (by the example of a key digital technology) in the sphere of security (by the example of identified countries);
4. to carry out a comparative analysis of the country models of changes in the sphere of security under the influence of digital technologies;
5. to assess consequences (risks and benefits) of the introduction of digitalisation and automation technologies for states in the sphere of national security (additional task).

Research hypotheses

We offer two sets of hypotheses.

The first set of hypotheses is formulated regarding the modelling of the process of applying digital technologies in security. Based on the logic of the empirical model (the ratio of the threat evaluation indicator and the digital capabilities of responding to threats), it can be assumed that the threat indicator will exceed the capability indicator in country models. The justification is the specificity of digital technologies, the ambiguity of their application and their rapid development. The analysis and evaluation of digital threats (and assessment of "traditional" threats using digital technologies) will outpace existing threat countermeasures. Testing the hypothesis will reveal official "attitudes" toward transformations in the sphere of security initiated by digital technologies. The explanatory mechanism will allow to understand how states determine the role and place of technologies (threat evaluation will show the fears of states and the potential of capabilities - how states can respond to threats). If the hypothesis is confirmed, we will see an increase in security concerns since governments are paying more attention to the potential of threats (both directly from digital technologies and in issues where technology should serve as a tool for eliminating threats). Conversely, if the hypothesis is refuted, governments successfully integrate technologies by a balanced assessment of threats. In this case, we demonstrate that states have adapted to modern changes and designed their security systems so that the response capabilities exceed the evaluated threats. More specifically, the hypothesis is formulated as follows:

H1: *Threat evaluation will exceed the capabilities of threat response*

The temporal coverage of the empirical model makes it possible to formulate hypotheses in terms of the dynamics of change. The organisational principle of contemporary national security is expressed in the following maxim "maximisation of military power through the use of technology"[44]. Accordingly, it is logical to assume that the use of digital technologies in the sphere of security occurs before there is a meaningful discussion in society about these digital technologies. If they are genuinely committed to maximising opportunity, governments must start making policy decisions and adopting technologies faster and earlier than societies are included in these discussions. The primary public debate about applying artificial intelligence technology in security began around 2010 in the form of a discussion of concerns associated with an "artificial intelligence arms race"[45]. Hypothesis testing will provide an understanding of the immediate dynamics and will allow us to assess the "inclusion" of governments in harnessing of the potential of technological changes in security systems. In other words, we can reveal how proactive governments are. Do we see the intention of the state to apply technologies (given the duration of the technological cycle from the moment of decision-making to direct practical implementation) at a faster pace before society pays attention to the significant risks and opportunities associated with digital technologies. If the hypothesis is confirmed, we can argue that states do indeed seek to maximise power and security by means of new technologies. Thus, observed changes (and, more broadly, transformations) are supported and even initiated by governments. However, there may be several explanatory mechanisms if the hypothesis is refuted. The primary mechanism will be that states fear threats and risks more than they perceive the potential for technologies' applications. Therefore, the authorities will seek first to obtain an evidence base of contingent benefits and only then begin to introduce and apply technologies. An alternative explanation would be a redistribution of government's focus, i.e. maximisation can and does occur, but by means of other technologies or other strategies and tactics. Thus, the second hypothesis of the study is formulated as follows:

> **H2**: *The dynamic of the use of digital technologies in the sphere of security will manifest itself in the period of 2008-2010.*

[44] Farrell T. Constructivist Security Studies: Portrait of a Research Program // International Studies Review. — 2002. — Vol. 4, no. 1. — P. 49– 72:67

[45] Artificial Intelligence arms race. For example, see the article on the popular Wikipedia resource: https://en.wikipedia.org/wiki/Artificial_intelligence_arms_race (accessed: 11.09.2021)

The second set of hypotheses is formulated regarding the comparative analysis of country models. There is a consensus in security studies that different states (governments) do not assess threats similarly. The same threat can be evaluated and interpreted differently by states[46]. Although one of the leading papers on this topic (the study of Wolfers) refers to "traditional" approaches to security and can be considered "outdated", the issue of uncertainty of threats is very relevant. Despite existing discussions about the correct and proper understanding of security, the perception of threats (and their content) is both a scientific and a practical problem. In other words, in this hypothesis, we rely on the substantive component of the argument that states define and evaluate threats differently. The empirical model of this study allows us to analyse the evaluation and perception of threats by each state separately and evaluate such perceptions. However, despite differences in threat assessment, there is security ambiguity regarding digital technologies which creates unnecessary fears. Therefore, we assume that the evaluations of threats will be homogeneous in the analysed countries, and heightened concerns will characterise them. By testing this hypothesis, we seek to identify the existence of uncertainty in the assessment of threats, complicated by the specifics of digital technologies. On the one hand, identifying differences in threat assessment will confirm the empirically grounded theoretical assumption about differences among states in the evaluation and perception of threats. On the other hand, we will be able to demonstrate whether there is (or is not) a certain specificity related to digital technologies. If the hypothesis is confirmed, we will refute the theoretical notion of uncertainty in threat assessment and, in doing so, demonstrate the unique attitude of states towards digital technologies. This will significantly expand the discussion about the transformational effect of digital technologies. If the hypothesis is refuted, we will confirm the existing theory about the uncertainty of threat evaluation and demonstrate that governments' perceptions of digital technologies do not differ significantly from other tools, etc. More specifically, the third hypothesis is formulated as follows:

> **H3**: *The perception of threats and the type of threats will reach maximum values in all analysed countries.*

Our comparative analysis will also allow to test the assumption that states are highly alerted to risks and challenges from digital technologies. We assume that by 2018-2019 in all

[46] Wolfers A. «National Security» as an Ambiguous Symbol // Political Science Quarterly. — 1952. — Vol. 67, no. 4. — P. 481–502:151

analysed countries as leaders in the field of technology, high values of the indicators of the empirical model will be observed. These will indicate that states (1) are on high alert to risks and threats arising from digital technologies and also (2) are rapidly introducing digital technologies into the sphere security to meet current challenges. When testing this hypothesis, we will be able to assert the existence of changes (and, more broadly, transformations) and to find out the directions of these changes. The fast pace of technology adoption and a high assessment of risks and challenges will demonstrate the adaptability and readiness of governments to contemporary security challenges associated with digitalisation. More specifically, the fourth hypothesis is formulated as follows:

> **H4**: *By 2018-2019, the indicators of the empirical model of all analysed countries will approach the maximum values, which indicates a high readiness of states for the risks and challenges from digital technologies.*

Theoretical and Methodological Foundations and Limits of the Research

This research faces two theoretical and methodological challenges. First, it is widely believed that security is studied primarily within the domain of international studies. Secondly, the design of a unified research program for this study will face a discussion about the possibility of implementing quantitative empirical research in the theoretical logic of the Copenhagen School of security studies, where the vast majority of research is of a qualitative nature.

The first challenge can be countered by Ronald Krebs's argument on the need to bring politics (and political science) back into national security studies ("returning politics to security studies")[47]. Krebs argues that not all security preferences are equally accounted for in the definition of "national interest", as political institutions empower actors and direct preference aggregation in different ways[48]. Political institutions also influence which resources are available to decision-makers and which policy tools they find attractive. As a result, leaders gravitate toward the policy instruments over which they have more control.

A security policy is *political* on two levels. The first delas with questions of insecurity, which are necessarily products of political action[49] since neither security nor insecurity are a

[47] Krebs R. The Politics of National Security // The Oxford Handbook of International Security. — Oxford University Press, 2018. — P. 259–273:2 - «...bringing politics back into the study of national security...»
[48] Ibid.
[49] Cultures of Insecurity: States, Communities, and the Production of Danger / J. Weldes [et al.]. — Minneapolis, MN : University of Minnesota Press, 1999. — 452 p.

"natural" state of affairs. Political actors promote discourses of security or insecurity and feed the corresponding public emotions through rhetorical "speech acts" (asserting vulnerability, promising security) and thereby shape the political landscape[50]. The second level is directly the development and implementation of security policies (policy)[51].

For this study, institutionalism will serve as a foundation, which, on the one hand, allows us to cover the above mentioned levels of the political for security studies and, on the other hand, provides an opportunity for empirical analysis.

Responding to the second challenge, we are faced with a "warp" in approaches taking shape of discussions about security research programs[5253]. For a long time, realist thinking has heavily influenced the study of security. Many security studies have "focused on the four S's: states, strategy, science, and the status quo."[54]. This approach to the study of security is based on the understanding of actors as instrumentally rational and dealing with an external reality, which does not depend on their values and ideas. Similarly, the concept of a state action as an instrumentally rational pursuit of its interests is at the heart of the structural-realist analysis of international security[55]. On the one hand, we establish a methodological framework for security research in the concepts of rational choice theory[56]. On the other hand, we directly appeal to the Critical security studies (CSS). Substantiation of the subject field and limits of our research and a description of the existing discussions about contradictions in approaches to the study of security are presented in Section 1.1 of the Dissertation.

The methodological framework of rational choice theory (RCT) is based on the assumption that all social phenomena, including political ones, can be derived from the behaviour of individuals. Political actors (voters, politicians, bureaucrats, etc.) pursue the goal of maximising their material interests by means of votes, positions, power, etc. Considering the criticism of RCT by the academic community[57], this study introduced institutional

[50] Wirls D. Buildup: The Politics of Defense in the Reagan Era. — Ithaca, NY: Cornell University Press, 1992. — 247 p.
[51] Krebs R. The Politics of National Security // The Oxford Handbook of International Security. — Oxford University Press, 2018. — P. 259–273:9
[52] Farrell T. Constructivist Security Studies: Portrait of a Research Program // International Studies Review. — 2002. — Vol. 4, no. 1. — P. 49– 72.
[53] Gheciu A., Wohlforth W. The Oxford Handbook of International Security. — Oxford, UK: Oxford University Press, 2018. — 784 p.
[54] Williams P. D. Security Studies: An Introduction. — 2-nd. — London, UK: Routledge, 2013. — 656:3
[55] Krause K., Williams M. C. Critical Security Studies: Concepts and Cases. — 1-nd. — London, UK: Routledge, 1997. — 404:40
[56] Wittek R., Snijders A., Nee V. The handbook of rational choice social research. — Stanford, California: Stanford University Press, 2013. — 624 p.
[57] Грин Д., Шапиро И. Объяснение политики с позиции теории рационального выбора: почему так мало удалось узнать? // Полис. Политические исследования. — 1994. — No 3. — с. 59.

restrictions to study the optimal behaviour of actors and obtain a more objective result of changes in both the political agenda and political institutions.

We are restricting "rationality" to political actors. Thus, we exclude rational institutionalism from the scope of this study. The theory of rational institutionalism suggests that states are rational, unitary actors whose actions aim to maximise certain benefits[58]. However, this approach has several significant drawbacks for security research. First, many observable national and international institutions have proven ineffective in identifying problems and responding to new challenges. Secondly, rational institutionalism does not have explanatory power when "weaker" actors begin to suppress "stronger" institutions (for example, when Iran or North Korea try to challenge international non-proliferation regimes, etc.). Thirdly, rational institutionalism demonstrates limitations in understanding interconnection and interactions among the authorities and the institutions themselves. We will not use the framework of rational institutionalism in this study. Moreover, substantively, rational institutionalism strongly contradicts the approaches of critical security studies.

We also pay attention to the "bounded rationality"[59] assumption, which highlights the inability of decision-makers to follow a strict utility maximisation strategy in a highly complex environment and under conditions of limited time and information. Instead of choosing the best possible outcome from all available outcomes, actors use strategies to find the most affordable outcome that is more satisfying than the status quo. Within this framework of bounded rationality, we analyse actors.

Concerning institutions, we do not simply rely on the classical "institutions matter" but consider them broadly as rules and as normative representations of the political will. Remaining in the subject field of political science, we approach institutions as meaningful manifestations of politics.

Critical security studies (CSS) examine the process of framing security as a political phenomenon[60]. Critical security studies are concerned with analysing the politics underlying the construction of security knowledge: ideas about security have come to be seen as political because they are the product of interpretation, debate and struggle among various political actors. In addition, CSS also seek to shed light on the relationship between the security theory

[58] Peters, G.B. Institutional Theory in Political Science. The «New Institutionalism» - London: Continuum - 2005 - P. 232: 14, 19

[59] Simon, H. A. Bounded rationality. In Utility and probability // Palgrave Macmillan, London - 1990 - pp. 15-18

[60] Nunes J. Reclaiming the Political: Emancipation and critique in security studies // Security Dialogue. — 2012. — Vol. 43, no. 4. — P. 345–61.

and the broader political order by examining ways in which specific concepts of security cannot be separated from more comprehensive ideas about how politics works or should work[61]. Scholars who adhere to this approach seek to draw attention to the influence of security ideas and practices on creating a particular political regime/political system, thereby *conceptualising the theorisation of security as an independent political activity*. Moreover, CSS aim to develop an understanding of the dynamics and implications of building security practices in a particular historical and social context[62].

The expansion of security domains has required to rethink *who* and *what* can become a security issue. Thus, CSS approach can serve as an optimal theoretical and methodological framework for this study.

This study is implemented in the theoretical and methodological framework of CSS, taking into account the concepts of institutionalism and rational choice theory. This sets the logic of the study, which is subject to the conceptual framework and sectoral approach to security analysis developed by Barry Buzan[63], with a particular focus on the political aspect of the administration and functioning of the security sector. Like the Copenhagen School, Barry Buzan is among the earliest and most influential exponents of the CSS[64].

At the methodological level, this study is based on the concept of logical models by Rein Taagepera[65] in search of a methodological balance in security studies. Without intending to criticise or challenge both expert opinion (the most common approach in security studies) and current statistical methods, this study seeks to use Taagepera's logic modelling framework to propose an alternative and more objective approach to security analysis.

Now we have to make a statement on what is **not** in this study. First, this study does not create and (or) rethink any security theory. The purpose of the work is to study the changes and their potential impact triggered by digitalisation and automation technologies in the sphere of security. An additional (but optional) task is to trace and evaluate both the positive potential (benefits) of these changes and the negative one (threats and risks). The specified is realised

[61] Ibid. p. 347
[62] Gheciu A., Wohlforth W. The Future of Security Studies // The Oxford Handbook of International Security. — Oxford University Press, 2018. — P. 1–12.
[63] Buzan B., Waever O., Wilde J. Security: a new framework for analysis. — London: Lynne Rienner, 1998. — 239 p.
[64] Hendershot C., Mutimer D. Critical Security Studies // The Oxford Handbook of International Security. — Oxford University Press, 2018. – P.1-2: «To consider a future for Critical Security Studies (CSS) it bears reiterating that CSS should not be considered a subdiscipline of Security Studies or International Relations….Some of the most influential works produced in the early years include:… and Security: A New Framework for Analysis (Buzan et al. 1998).»
[65] Taagepera R. Making Social Sciences More Scientific: The Need for Predictive Models. — Oxford, UK: Oxford University Press, 2008. — 232 p.

within the framework of existing theories and approaches. Secondly, the study does not contain recommendations on which decisions need to be made, how to implement them, etc. In other words, this study is "above the phenomena" and evaluates, analyses, and substantiates the actual aspects of the interaction of digital technologies with the sphere of security without providing methodological recommendations for building a digital "Leviathan" in the national security domain. Thirdly, this is not a study of singular events (cases). Implementation of structural approach with the "reconstruction" of a comprehensive picture of security transformations in the sphere of security requires a systematic analysis of the policies of each country (taking into account variations in political conditions, internal conflicts, clashes of the technological determinism and the political will, etc.). In this regard, instead of relying on specific cases of using digital technology as units of analysis, we focus on the relationship and structure of the country's political institutions producing the national security policy.

Research Design and Empirical Basis

The structure of this study is determined by the goals and research problem. To reveal the effects of the "transformation", a meaningful analysis of the digitalisation policy and security policy changes is given in the theoretical part of the work (Chapter 1). We analyse various changes and their effects making up “transformation”. In this context, transformation is understood as significant changes improving quality, etc.

We first present transformations in security studies. Then, a theoretical analysis of the digitalisation policy reflects significant changes and the accompanying effects of digitalisation and its impact on politics and public administration. Thus, at the theoretical level, we reveal the ongoing transformation meaningfully. Despite the controversial nature of the term "transformation", its use in the work is not accidental. The very "the notion of security expanded greatly as a consequence of *transformations in policy*"[66] under the influence of various factors, including the technological ones. Moreover, the environment can lead to a "…*transformation of what it means to secure*"[67]. At the same time, there is "…a link between the transformation of security policies and the development of security studies"[68]. Thus, **awareness of the expansion of the content of "security" and the presence of significant changes - "transformations" - in politics serve as the starting point of this study**.

[66] Schlag G., Junk J., Daase C. Transformations of security studies: dialogues, diversity and discipline. - Routledge. 2015. - P.250:12 -
[67] Ibid. p. 152
[68] Ibid. p. 233

The empirical part of the study (Chapter 2) narrows down the transformation to its elements - the dynamic of change and its consequences. This is due to both the theoretical framework and methodological limitations. At this stage the research question is narrowed down to an evaluation of the dynamic (subordinate to the empirical part of the study). This separation of the theoretical and empirical parts is not accidental. *Demonstration of the dynamic of changes will make it possible to highlight the substantive elements of how such a transformation has affected the sphere of national security*. Thus, a uniform structural logic of the study is observed, and though the transformation is presented as a broader concept, measurable elements of changes and effects are suggested.

The empirical design consists of several stages. **At the first stage**, a preliminary study is carried out, it consists of two independent network analyses, and as a result a pool of countries on which the study focuses have been determined. Separately, a "key" digital technology (and the focus of the study) has been identified - artificial intelligence (AI) technology. For the study, the countries that demonstrate leading positions (according to two network analyses) have been identified - *the United States, Sweden, Germany, Finland, and France*.

For the purposes of this research, artificial intelligence technology is understood as *algorithmic and computer systems (including software and/or hardware) that, while learning, can solve complex problems, make predictions, or perform tasks requiring human perception, learn, plan, communicate or perform a physical act, necessarily in the security domain or, directly, in the military sphere*.

At the second stage, an empirical model has been designed. In developing an empirical model, our choice of indicators and parameters is determined by what is measurable[69]. Working with indicators, in turn, depends on the need to strike a balance between the completeness and availability of data[70].

The security consistency index is developed by the difference in threat indicators (threats) and AI capability to respond to such threats. Methodologically, the influence of algorithms (AI as a particular type of the digital technology) in national security is presented as a decision-making process in security using flowcharts with the definition of mathematical parameters. The security consistency index reflects how a state can evaluate threats (an indicator of threats) and whether a state has the necessary level of capabilities to repel them (an indicator of capabilities).

[69] Fioramonti L., Kononykhina O. Measuring the Enabling Environment of Civil Society: A Global Capability Index // Voluntas. — 2015. — Vol. 26. — P. 466–487.
[70] Ibid. p. 467

The AI capability indicator is calculated in the logic of composite indexes. Based on the conceptual framework for understanding artificial intelligence and the goals of creating the indicator, four areas have been identified (technological area; economic area; governance; social area) with the distribution of weights.

The design of the threat evaluation indicator is based on the approaches of a highly specialised subject field of research on weapons and military threats - Threat Evaluation and Weapon Assignment (TEWA)[71][72][73][74][75]. This study's logic requires evaluation of threats and search of balance between these threats and the defended objects and security sectors.

Additionally, **the model has been verified and tested** using simulation analysis[76]. Simulation analysis is aimed at checking the model's sensitivity[77]. What if some data do not correspond to reality, are false, or are completely missing? To what extent does this circumstance affect the results? Testing the model through simulation aims to answer these questions.

As a result of simulations and testing, the model demonstrates stability to most indicators. However, special attention should be paid to data sources for Threat factors (TF) from the Threat evaluation indicator and the Technological and Social indicators from the AI Capability indicator. In addition to these indicators, overestimation in the available sources' data is also checked.

The next step has been to apply the empirical model for each country case and compare the resulting models. The direct implementation of the empirical model for each selected country has been carried out according to a uniform protocol. The first step is to determine the temporal coverage relevant for each country in focus. The temporal coverage is to take into account the following:

---

[71] Cocelli M., Arkin E. A threat evaluation model for small-scale naval platforms with limited capability // EEE Symposium Series on Computational Intelligence. — 2017. — P. 1–8.

[72] Johansson F., Falkman G. Comparison between two approaches to threat evaluation in an air defense scenario // Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). — 2008. — Vol. 5285. — P. 110–121.

[73] Naeem H., Masood A. An optimal dynamic threat evaluation and weapon scheduling technique // Knowledge-Based Systems. — 2010. — Vol. 23, no. 1. — P. 337–342.

[74] Decision support system for optimum decision making process in threat evaluation and weapon assignment: Current status, challenges and future directions / A. Naseem [et al.] // Annual Reviews in Control. — 2017. — Vol. 43. — P. 169–187.

[75] Kumar S., Tripathi B. Modelling of Threat Evaluation for Dynamic Targets Using Bayesian Network Approach // Procedia Technology. — 2016. — Vol. 24. — P. 1268–1275.

[76] Marquardt K. L. How and how much does expert error matter? Implications for quantitative peace research // Journal of Peace Research. — 2020. — Vol. 57, no. 6. — P. 692–700.

[77] Gelman A., Hill J., Vehtari A. Regression and Other Stories (Analytical Methods for Social Research). — Cambridge University Press, 2020. — 552 p

1. major regulatory legal acts in security (national security strategies, laws, decrees, doctrines, etc.);
2. primary regulatory documents of the information technology sector with a special focus on digitalisation, algorithmisation, automation of politics and governance (taking into account the concept of e-government, up to the regulation of specific types of digital technologies);
3. several governments/administrations to catch dynamics of changes.

An obligatory condition for data collection is to consider both national legal acts and official statistics and international reports, databases, etc., for every country of interest to us. As a result, a data set is formed for each country. The data are available in the open GitHub repository via a stable link in separate files for each country[78].

More extensive work has been carried out with national legal acts and official statistics when building a data set for each country. Fundamental national legal acts set time frames for analysis. However, the data for the model have resulted from analysis of all relevant public documents. Therefore, in the absence of data at the national level or the existence of a uniform database for all countries, data from international organisations have been used.

The specified distinction between processing legal acts and extended work with national acts is subject to a uniform research logic: we strive to identify and trace the changes taking place directly at the national level.

Contribution to the Field of Research

Security studies today are heavily influenced by the paradigms of international relations and often rely on the qualitative methodology and expert interviews. Though we do not underestimate the value of existing approaches, this study seeks to overcome both limitations: firstly, the study "returns" the institutional foundations of political science regarding security studies and, secondly, it offers a quantitative approach to evaluating dynamics in this sphere by developing an empirical model that allows to evaluate the transformational effects of digital technologies in the national security systems of the leading innovative countries.

At the theoretical level, the study describes the process of introduction of digital technologies (by the example of the AI technology) into the sphere of security. The results demonstrate how national security systems are being adapted by introducing advanced digital technologies. Indirectly, the results indicate that states actively apply the developments of

[78] Repository with data for each country: https://github.com/AlTurobov/PhD_SecurityConsistency (stable link). A separate file corresponds to each country, and an additional link with comments and descriptions of sources is provided for each country.

significant (in the context of national and international markets) tech companies for security purposes. Thus, the trend of subordination and securitisation of development to security purposes continues. States' evaluations and perceptions of threats in the context of digital technologies are non-linear and have a wave-like characteristics. The dynamics of changes in all analysed countries' models are not uniform, although they have several similar stages.

Statements to be Defended

1. Security studies, like the "security" construct itself, develop evolutionarily. They expand in terms of understanding of threats (and the capabilities to react to threats) and are filled with new phenomena. We propose to consider the evolution of the subject area of security studies as a coherent process. We propose to consider substantive changes in security studies going beyond the discussions about (as well as among) security studies schools, but with an analysis of the contents of concepts, the expansion of security sectors, etc. Digital technologies permeate all security sectors and transform them dramatically.
2. The phenomenon of digitalisation is political and is dependent on the functioning of institutions. The quality of digitalisation depends on the joint actions of political institutions and technology companies. The process of digitalisation is subject to decisions of policymakers. At the same time, the process itself is directly related and depends on the use of specific types of digital technologies.
3. Network analysis[79] of countries' trade (ICT and digital goods and services) highlights the leading countries (for example, Finland, Germany, and Sweden) and demonstrates international competition in digitalisation. In the network structure, one can observe countries that are critical links in the connectivity of international trade. Countries of this types act as "bridges" for the global exchange of experience, technology diffusion and, potentially, key actors in the global institutionalisation of digitalisation.
4. For this study we propose an "umbrella" concept of artificial intelligence technology. This allows us to cover a set of approaches, tools, and algorithms. Artificial intelligence technology refers to algorithmic and computer systems (including software and/or hardware) that, through learning, can solve complex problems, make predictions or perform

[79] The results of the second network analysis (as part of the preliminary study, two network analyses were carried out to identify the countries to be included in the research and to identify a specific type of digital technology as the focus of the empirical part of the study) are presented in the publication: Туробов А.В. Возможности трансплантации политических институтов при торговле технологиями: результаты сетевого анализа в сравнительной перспективе // Вестник Томского государственного университета. Философия. Социология. Политология – 2022–№65 - С. 310-327.

tasks requiring human perception, plan, learn, communicate, or perform physical actions (required for security purposes and (or) directly in the military domain).

5. An empirical model for examining changes and evaluating a national security system under the influence of digital technologies has been developed, tested, and validated. The impact of technology on national security is presented through a security decision-making process. The security consistency index reflects how a state evaluates threats (the indicator of threats) and whether a state has the necessary capabilities to repel them (the indicator of capabilities). The proposed approach is an addition to the existing ones and allows to evaluate the dynamic of security system's development of a particular state under the influence of artificial intelligence technology.
6. A comparative analysis of country models suggests that (1) governments have a uniform approach to determining the capabilities of AI technology in the sphere of security; (2) there is a constant accumulation of knowledge and experience about the potential of the technology; therefore, in all models, there is a constant increase in the indicator of capabilities; (3) internationally, there are both uniformity and competition, as countries at approximately the same time are beginning to pay attention to the impact of digital technologies in the sphere of security; (4) the regulation of artificial intelligence technology takes place uniformly and at the similar time intervals (all analysed countries adopted relevant strategies in the period of two years - 2017-2019).
7. The dynamics of changes of national security systems are not linear. The non-linear (wave-like) features of the dynamics reflect differences in the adaptability of political institutions and the diversity of political decisions in the application of technologies in the sphere security. While all analysed countries are maximising their capabilities of digital technologies application in the sphere of security, threat evaluations are not uniform and may vary. On the one hand, this finding illustrates the specifics of digital technologies: there are difficulties in evaluating threats, technological challenges, etc. On the other hand, this finding allows to argue that the very understanding of threats from country to country can change significantly. Also, a specific threat can be reconceptualised even within the same country over time.
8. States determine roles and significance of technologies in proportion to their capabilities. In other words, governments are adapting to challenges and are transforming national security by introducing new technologies. States have designed the security system so that the ability to respond outweighs the evaluated threats. A broader interpretation of our results suggests that states are in full control of changes and transformations in their security systems.

Approbation of Results

List of publications

1. Turobov A.V., Mironyuk M.G. (2021) Empirical Model for Analysis of the Dynamics of Algorithmization (Artificial Intelligence Technology) in the Field of Security by the Example of the USA // Political Science (RU). No 3. p.72-111.

   Туробов А.В., Миронюк М.Г. Эмпирическая модель анализа динамики алгоритмизации (технологии искусственного интеллекта) в сфере обеспечения безопасности на примере США // Политическая наука. 2021. No 3. С. 72-111.
2. Turobov A. Opportunities for Transplantation of Political Institutions in Technology Trade: Results of Network Analysis in a Comparative Perspective // Vestnik TGU. Filosofiya. Sotsiologiya. Politologiya (RU). Tomsk State University Journal of Philosophy, Sociology and Political Science. 2022. V. 65. p.310-327

   Туробов А.В. Возможности трансплантации политических институтов при торговле технологиями: результаты сетевого анализа в сравнительной перспективе // Вестник Томского государственного университета. Философия. Социология. Политология. 2022. №65. С. 310-327.
3. Turobov A., Chumakova M., Vecherin A. (2019) World Best Practices in Applying Mathematical and Statistical Crime Prediction Algorithms // Journal of International Relations Theory and World Politics "Mezhdunarodnyye protsessy"(RU). V. 17. No 4. p.153-177

   Туробов А.В., Чумакова М.А., Вечерин А.В. Международный опыт применения математико-статистических алгоритмов прогнозирования преступности // Международные процессы. 2019. Т. 17. № 4. С. 153-177.
4. Antonova A. , Turobov A. (2020) Aims of Digital Technologies Through the Prism of Education // Education Policy (RU). No 2 (82). p. 42-55

   Антонова А.В., Туробов А.В. Мишени цифровых технологий через призму образования // Образовательная политика. 2020. № 2 (82). С. 42-55.

Conferences

1. 9th International Conference on Information Law and Ethics. Psychological and socio-political dynamics within the Web: New and old challenges to Information Law and Ethics. 11-13 July 2019 Rome, Italy. Report: Data for Public Policy in the Web Era: A Call for Systemic and Ethical View.

2. 11th Russian Internet Governance Forum. Youth Seminar on Internet Governance. April 4-8, 2020, Moscow, Russia. Speaker invited expert. Report: State, Ethics and Artificial Intelligence: Humanitarian and Legislative Problems of Development and Implementation of Algorithms in Everyday Life // 11-й Российский форум по управлению Интернетом. Молодежный семинар по управлению интернетом. 4-8 апреля 2020, Москва, Россия. Выступающий, приглашенный эксперт. Доклад: Государство, этика и искусственный интеллект: гуманитарные и законодательные проблемы разработки и внедрения алгоритмов в повседневную жизнь.

Presentation of Research Results in Study Disciplines

1. From Big Data to Political Decision Making // «От больших данных к принятию политических решений», ОП «Прикладная политология» (2019/2020 - ongoing);
2. Government and Public Policy in the Age of Digital Technology // «Правительство и государственная политика в эпоху цифровых технологий», ОП «Прикладная политология» (2019/2020 - ongoing);
3. Topical Problems of Modern Politics // «Актуальные проблемы современной политики», Майнор (2019/2020 - ongoing).

Aprobation of Research Results on a Grant Basis

As part of the PhD research, RFBR grant No. 20-011-31658 “Analysis of the Dynamics of Algorithmization (Artificial Intelligence Systems) in the Field of National Security: An Empirical Model of Security Stability on the Example of the United States” («Анализ динамики алгоритмизации (технологии искус- ственного интеллекта) в сфере национальной безопасности: эмпирическая модель стабильности безопасности на примере США») was won and successfully implemented (Head - M. Mironyuk, Executor - A. Turobov)

Main Contents of the Work

The theoretical part of this research is devoted to establishing and justifying the interface between the subject area of security and the digitalisation policy. A broad understanding of the concept of transformation has been offered. The *first level of theoretical analysis* aims to identify the evolutionary development of understanding of the concept of "security" and the subject field of security studies. The theoretical analysis aims to demarcate the field of security studies, to identify critical transformations in the understanding and approaches to security,

and to construct an approach to changes in the sphere of security associated with digital technologies. This section simultaneously performs the function of conceptualising security and demonstrating the development of approaches to such an understanding. As a result, it is proposed to consider the penetration of digital technologies into security issues not as the formation of an independent security sector (in the logic of the Copenhagen School) but as a process, which permeates all sectors (similar to the specifics of information security). The proposed theoretical framework aims to study the relations of digital technologies in the sphere of security.

While accepting the contradictions among different approaches, we strive to demonstrate the coherence of the development of the sphere of security. Threats are being filled with new content. They are expanding, and their conceptualisation is changing. However, previous ideas and concepts are to be taken into account. Thus, we propose to consider substantive changes in security studies without engaging in the discussion about schools in security studies. Instead, focus on substantive aspects of concepts, recognition of the expansion of security sectors are offered. This approach to security is not novel or unique. Noteworthy, a similar perception of the coherence of existing approaches can be found in the book "Transformations of Security Studies: Dialogues, Diversity, and Discipline", which aims to "...build bridges of communication between different 'camps' by initiating a dialogue...of security studies"[80].

A brief introduction to the security studies' evolution is necessary to substantiate a particular understanding of security. We do not equate military security (absence of military threats and challenges) with security of a state *per se*. Accordingly, this study is in the field of security studies.

The second theoretical level is aimed at analysing the policy of digitalisation. We start with conceptualisation of digitalisation and demonstrate a significant role of political institutions in this process. Moreover, the conceptualisation of digitalisation allows us to consider this phenomenon as a distinctly political process. Understanding that digitalisation is not a "process in a vacuum" but is directly implemented through digital technologies, various typologies of digital technologies are proposed. Identifying and analysing types of digital technologies is not subject to the logic of technological determinism but is inextricably linked with the institutional basis. By demonstrating the implications of digitalisation and the accompanying transformations, we are presenting direct "procedural" political changes. These

[80] Schlag G., Junk J., Daase C. Transformations of security studies: dialogues, diversity and discipline. - Routledge. 2015. - P.250:2

features of our approach allow us to consider the transformation more broadly. By combining theoretical levels, we formulate and demonstrate how security and digitalisation are linked.

The empirical part of the study narrows the theoretical framework of transformation to its measurable elements of change and consequences. A preliminary study is carried out using the network analysis methodology in order to identify the leading countries to be analysed further. We are striving to analyse countries both with high "innovative potential" and with leading positions in digitalisation. Also, a preliminary analysis allows the focus of the study on one specific type of digital technologies, i.e. artificial intelligence technology.

An empirical model with substantiation is proposed. Also, the model verification results are demonstrated in order to check the model for stability using simulation analysis. Based on the results, we assert with confidence that the model makes it possible to measure and analyse the dynamics of digital technologies' implementation into modern states' security systems.

Building an empirical model for five countries - the United States of America, Sweden, Germany, Finland, and France - allows us to demonstrate the introduction of the technology into national security and identify the dynamic properties of this process. For the abovementioned countries, data collection and model building have been carried out according to a uniform protocol. Finally, results of modelling are presented with a qualitative description and interpretation of specific cases.

Comparative analysis of country models on three indicators (AI capabilities, threat evaluation and security consistency index) reveals differences in approaches to applying digital technologies in the sphere of security and provides a basis for identifying the best practices (additional research question).

Comparing country models in terms of artificial intelligence technology capabilities allows to understand the dynamics of official evaluations of technological capabilities in the sphere of security. Graphically, the comparison of the models is presented in Figure 1.

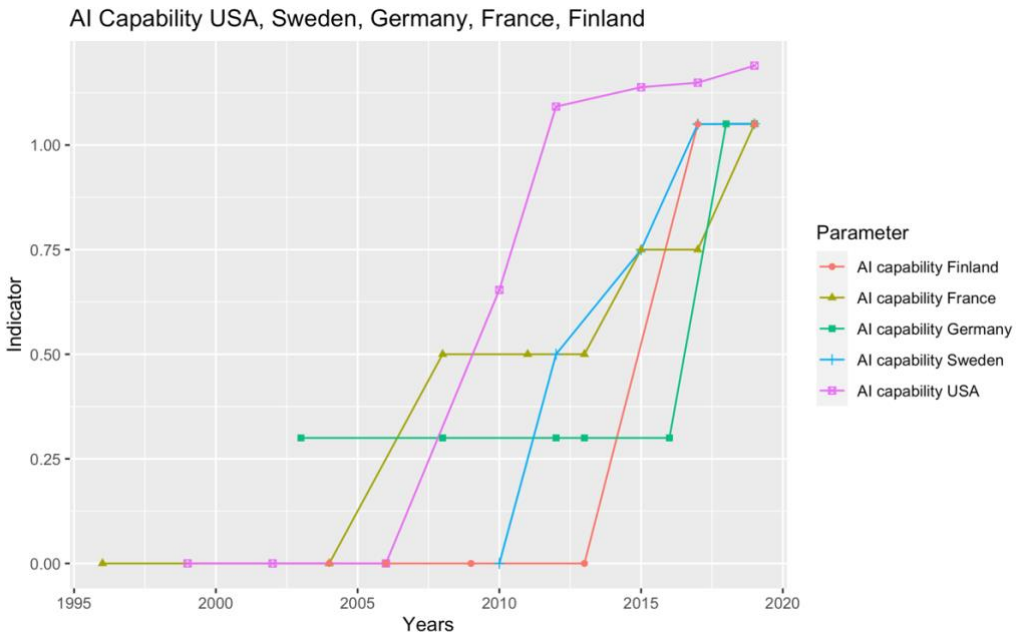

Figure 1. Graph Comparing Country Models in Terms of AI Capabilities

A comparative analysis of country models in terms of threat evaluation allows to track how governments define threats associated with a technological factor in the sphere of security. Graphically, the comparison of the models is presented below in Figure 2.

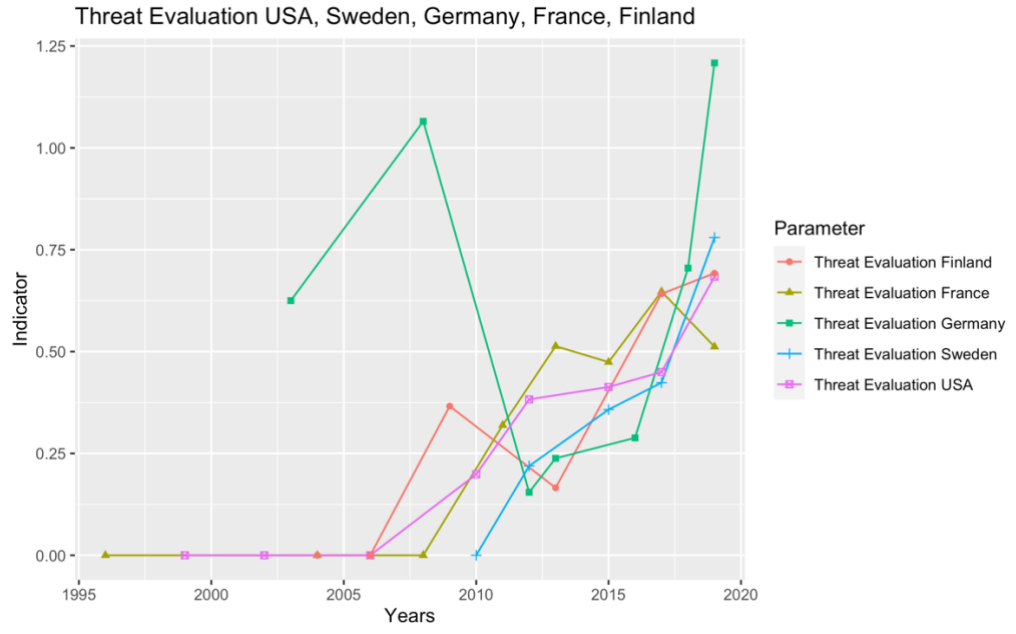

Figure 2. Graph Comparing Country Models in Terms of Threat Evaluation

The logic of the security consistency index reflects readiness of a state to respond to threats. Readiness is measured by considering how the state evaluates threats and determines

the ability to respond to threats (AI capability indicator). This indicator focuses on a particular type of digital technologies, namely artificial intelligence technology. Thus, a higher score of the security consistency index means that the state's security system is ready to adequately respond to the threats identified by a government.

Comparative analysis of country models in terms of the index of security consistency is presented below in Figure 3.

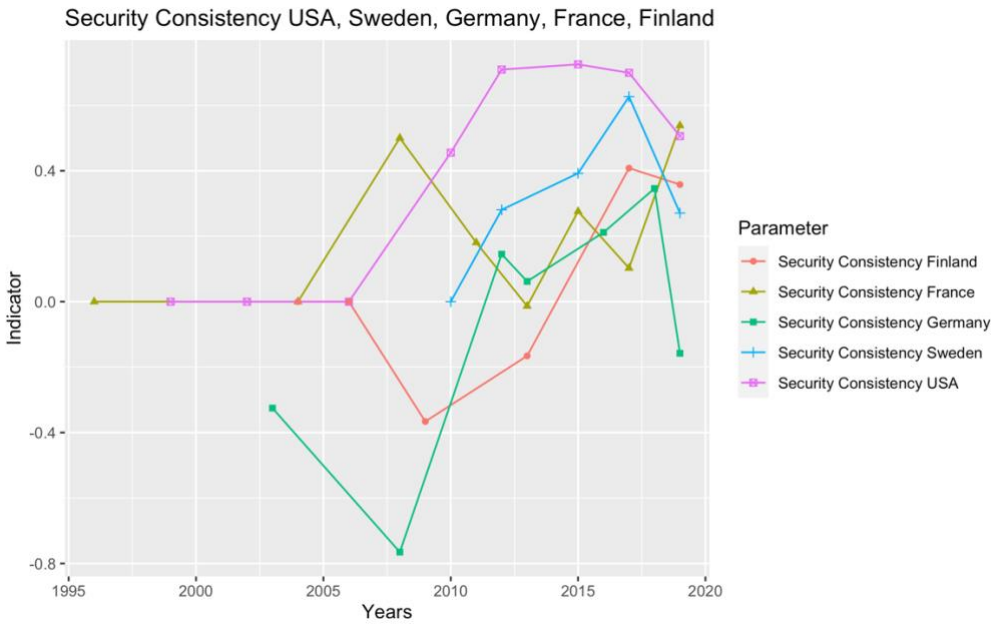

Figure 3. Graph Comparing Country Models in Terms of Security Consistency Index

The models reveal similar trends. Firstly, there is a uniform approach of governments to the definition of technology capabilities; it manifests itself in the constant growth of this indicator. There has not been a single case of this indicator showing a negative trend. Secondly, the models demonstrate more or less similar dynamics. Attention to the assessment of technological threats is manifested in the period of 2006-2008, and the maximum values for all indicators are achieved in 2017-2019. In other words, we can observe a certain uniformity (or competition) when countries in approximately the same period of time begin to pay attention to digital technologies in the sphere of security. Thirdly, the uniformity in terms of the regulation of artificial intelligence technology is puzzling. In 2017, Finland and France adopted national strategies to develop this technology. In 2018, Sweden and Germany followed, and 2019 it was the United States to do the same. This circumstance can also be explained by both the technological competition among countries and by a certain degree of uniformity of in development of technological innovations in the leading countries.

Major Results of the Study

On the theoretical level this study presents a description of **how** digital technologies (by the example of the AI technology) find their way into the sphere of security and **which** changes are taking place in the security system of a state. The results show a maximisation of national security capabilities by means of advanced digital technologies (however, this process does not take place evenlydue to institutional features of states). Indirectly, the results demonstrate that states actively apply the achievements of big (in the context of national and international markets) technology companies in the sphere of security. Thus, the trend of subordination and securitisation of development to security is apparent.

The dynamics of changes in all analysed countries' models are not uniform but have several similar stages. By 2018-2019 the indicator of AI capabilities is stabilising, while the indicator of threat evaluation by this period shows rapid growth. The security consistency index demonstrates differences among states regarding the beginning of the infiltration of digital technologies into the sphere of security (an increase from 2003 to 2006). While some countries are actively building up potentials for transforming their national security systems (for example, the United States and Sweden), other countries are demonstrating the opposite trend of increased fears and risks of changes (for example, Germany and Finland).

At the second level of problematisation - in the instrumental (methodological) plane - an empirical model of changes and evaluation of the state security system under the influence of digital technologies has been developed, tested, and validated (by the example of the AI technology). The model aims to offer means of assessing the security system (it does not only evaluate threats but also identifies capabilities) and to create an empirical approach to measuring the sphere of security of a state.

An attempt at an "objective" analysis of dynamics demonstrates some advantages:

1. We can observe changes both in the official threat evaluation (how a state defines threats, what is perceived as a threat), as well as in the definition of technology capabilities (in the context of public perception of ongoing research, testing, and implementation of various algorithmic systems covered by the concept of artificial intelligence).
2. We can analyse, taking into account time periods, how the technology has been developing, and how its "infiltrates" the security system. For example, the rapid development of the AI technology between 2006 and 2012 in the United States allowed this country to initiate and lead a technological race, the consequences of which go far beyond the scientific research and technological frameworks.

3. Our focus on threat evaluation allows to analyse public attention to the technology. This expands the existing discussion in the subject field of technology politicisation and securitisation.
4. The model has interpretative flexibility, given that the collected data represent different areas (social, economic, political) and with broad temporal coverage.
5. The model can be helpful for comparative studies.

Future research will strengthen cross-country comparative analysis on a security consistency index and individual indicators of AI capabilities and related threat evaluation.

Of particular note is the model's scalability: it is potentially possible to replace AI technology with any other digital technology (for example, cloud computing, fifth-generation communications technologies, etc.) and build an empirical model of security consistency, taking into account a specific technology. Presume that spheres, weights, and coefficients will be preserved for another type of digital technology. However, this will be verified in subsequent studies. As a result, it is possible to trace the dynamics of changes in the state security system concerning a specific type of technology and conduct a comparative analysis of countries. Future research will focus on testing the model's capabilities and verifying its interpretative abilities (especially from a comparative perspective).

Results of hypothesis testing

The first hypothesis has been **partially refuted**. Despite the specificity, ambiguity, and rapid development of digital technologies, in particular the artificial intelligence technology, most states have time, at least at the institutional level, to determine and consolidate the ability to respond to such threats. In other words, we observe that states for the purposes of security provision at the initial stage assess capabilities of responding to threats in a more capacious manner (in comparison with the threat evaluation). However, this state of affairs does not apply to all states uniformly. Germany’s model is the only one where, by 2019, threat evaluation scores exceed its AI Capability scores. This is the reason why we can only partially refute the first hypothesis.

A meaningful interpretation of the results of the first hypothesis testing allows to determine official “attitudes” toward changes in the sphere of security initiated by digital technologies. States define roles and significance of technologies in proportion to their potential capabilities. Governments are successful in integrating technology when assess threats in a balanced manner. We demonstrate that states have adapted to changes and designed security systems in such a way that capabilities exceed the perceived threats. With a broader

interpretation of the results, it can be assumed that states are in complete control (or try to be in complete control) of changes and transformations in the sphere of security. In other words, this is not a “spontaneous transformation”, not a one-dimensional reaction to emerging challenges. Successful transformations are made possible by systematic and strategic political activities to assess capabilities vis-à-vis threats. This approach is not taken by every state. In some states (for example, Germany), there is an increase in security concerns because governments are paying more attention to the potential for threats associated with the AI technology.

The second hypothesis is inspired by the organisational principle of modern security forces of "maximising military power through the use of technology". The results of the models **partly refute** the assumption that the use of digital technologies by states in the sphere of security occur before there is a public discussion about these types of digital technologies. Despite similar dynamics, the German model shows the proofs of application of digital technologies only by 2016, and the models of France and Finland - by 2013. Thus, we cannot state that in all countries proofs of application of digital technologies in the sphere of security precede relevant public discussions. Although the US and Swedish models support the hypothesis, these results do not apply evenly to all countries. A possible explanatory mechanism for such an unexpected result lies in the specifics of artificial intelligence technology, which is not originally a military/security technology. It has first been developed for commercial (civilian) purposes.

Ambiguous results do not allow us to unequivocally conclude that states strive to maximise power and security through introduction of the technology. A potential explanation for the variation in country models may be that some states fear threats and risks associated with the technology more than they see benefits from technology application. Therefore, they will first try to obtain a solid evidence base of benefits and only after that governments begin to introduce and apply technologies. Also, variation can be explained by the existing opportunities for technological development and the human capital (presence or absence of highly qualified personnel to develop and implement technologies).

The third hypothesis is constructed around the consensus that states can perceive the same threat differently. We wanted to test whether there is substantial uncertainty about digital technologies creating unnecessary fears. Therefore, the perception of threats will reach maximum values in all analysed countries. The results of the analysis demonstrate that the hypothesis **is confirmed**. However, *from the standpoint of empirical accuracy, this hypothesis is confirmed partially*. This indicator may fluctuate in different periods, even within the same

country. Thus, the perception of threats by states is not linear. Nevertheless, maximum scores for this indicator are observed in the mid-2010s with a subsequent decrease. This finding confirms that states define and assess threats differently. We have not only confirmed the existing consensus on the differences in the definition and evaluation of threats among states but have also clarified it directly regarding digital technologies. Moreover, we observe that same threats are defined and evaluated differently in different time periods. This does not mean that the perception of the same threat should "decrease" over time.

We find significant specifics concerning digital technologies and expand the discussion about the transformational effects of technologies. Moreover, we demonstrate that such transformations are not linear. Instead, states are adapting to threats and try to assess the emerging potential for reacting to them proportionately. In turn, digital technologies act both as a tool (reinforcing change) and as a factor, that raises fears. This is a significant result, which allows, with an extended interpretation, to argue that the transformation can be associated with positive changes and the emergence of reasonable fears.

The fourth hypothesis has been formulated in the logic of states' readiness for risks and challenges associated with digital technologies. The hypothesis has been **partially confirmed**. We expected to observe a roughly uniform trend in all models of the analysed countries by 2018-2019. The indicator of AI capabilities levels off and remains stable at the same level over several years. States begin to apply the technology with an adequate understanding of the capabilities and limitations of applicability of the technology. In turn, we expected the threat evaluation indicator to grow rapidly by 2018-2019, which should have indicated a high assessment of risks and threats by states in recent years as more knowledge on the impact of technologies and associated risks became available. We expected the security consistency index to increase from 2006 up to 2010 with approximately similar dynamic and to increase sharply from 2016 up to 2017 because during this time period, firstly, the states could observe, in fact, the first real consequences of the use of technologies. Secondly, there was an increase in the politicisation and securitisation of digital technologies.

However, our findings have met these expectations in cases of the USA and Sweden. For these countries, the logic described above can be found in the official approach to changes in the national security systems under the influence of digital technologies. Still, it does not fully apply to Germany, France and Finland. Indeed, in all countries analysed, the indicator of the capabilities of artificial intelligence technology reaches a similar maximum value by 2019. Still, for other indicators and their dynamics, the differences between countries' models are significant. Firstly, the threat assessment in all country models is not linear with the

achievement of high values by 2019. The French model on the contrary, shows a decline in threat assessment from 2017 to 2019. Secondly, the security consistency index does not necessarily show gradual growth. Its dynamics are undulating and unique to each country except for the US and Sweden. This reinforces existing discussions about national security systems' heterogeneity and demonstrates new findings on the diversity of government responses to technological security challenges. Thirdly, contrary to theoretical expectations, a sharp increase in the security consistency index in 2016-2017 was observed only in the model of France, while in other models, there is a decline. It can be explained by the complexity of artificial intelligence technology development, as earlier there were a lot of expectations of the benefits and potential of this technology. Over time, optimistic expectations were replaced by a pragmatic understanding of the limitations of the technology and increasing risks. An alternative explanation may lie in the growing securitisation of the technology and the shift in attitudes towards AI from public discussion to information restrictions.

Now we can answer the primary research question of this study. Firstly, the dynamics of AI technology application in the sphere of security are non-linear and wave-like. This is due to differences in how nations conceptualise national security and in how they approach this type of digital technologies. Despite theoretical concerns, governments have time to assess the risks and benefits of technologies and, based on this assessment, to implement them. In other words, the results demonstrate that countries may be free from both "alarmist" and exaggerated fears and leniency towards issues of technological changes in national security. Secondly, there are general trends in the countries both in terms of time (for example, similar terms for the adoption of national strategies and programs on artificial intelligence) and in the dynamics of determining the capabilities of artificial intelligence technology (they all approached the maximum values by 2019). Curiously, this may indicate either existence of a system of international cooperation in the sphere of security and development of digital technologies or the development and intensification of competition among countries in the area of artificial intelligence technology development and its applications. Understanding the actual mechanism may require combining these competing explanations: countries continue to engage in international cooperation, but at the same time, competition between them is intensifying.

Comparative analysis, in turn, reveals both application similarities and similarities over time, as well as unique country differences to answer the additional research question of this study.

Conclusion

Security studies today reflect practical and theoretical concerns about development and application of digital technologies in the sphere of security. Yet, despite the increase in academic interest and the public interest in the issues of technological changes in national security systems, there is little understanding of how these changes occur.

This study focuses on the transformation of the sphere of security initiated by the digitalisation policy. This study also offers an empirical evaluation of the elements of this transformation and assesses the dynamics of changes and their consequences.

On the theoretical level this study offers:

1. An analysis of the transformations of the digitalisation policies and the field of security. We present an in-depth and broad analysis of the changes and effects shaping this transformation. The concept of security and practices of security provision account for new phenomena (including specific areas, for example, cybersecurity, and various processes that permeate the entire security system, for example, digitalisation). As a result, the sphere of security and the conceptualisation of threats are expanding.
2. Security issues are essentially political for two major reasons. First of all, the very conceptualisation of threats is a product of political actors' activities. The concept of security and actual security provision practices are experiencing similar influences. Secondly, security is provided through political institutions, and the quality and results of security provision depend on the quality and interactions of institutions.
3. The phenomenon of digitalisation is a political process. Such a process is subject to political decisions. However, it also involves (and depends on) the use of specific types of digital technologies.
4. In social and political research, it is acceptable to use "umbrella" concepts that embrace various approaches to a phenomenon, tools, factors, and functions. This research is based on the understanding of artificial intelligence technology as algorithmic and computer systems (including software and / or hardware) that, while learning, can solve complex problems, make predictions, or perform tasks that require human perception, learn, plan, communicate or perform physical acts in the sphere of security or directly in the military domain.

At the empirical level this study has accomplished the following:

1. The countries leading in the process of digitalisation have been identified (for example, Finland, Germany and Sweden). Using the network analysis, we have studied international competition in the area of digitalisation. The network structure makes it possible to single

out countries that are critical links in the international trade in ICT and digital technologies and services.

2. A validated empirical model is proposed for studying changes and evaluating security systems of states under the influence of digital technologies. The impact of technology on national security is understood as a security decision-making process. The security consistency index reflects how the state evaluates threats (the indicator of threats) and whether the state has the necessary capabilities to react to them (the indicator of capabilities). The proposed approach is meant as an addition to the existing ones. It allows to evaluate the dynamic of development of the security system of a particular state under the influence of a particular type of digital technologies.
3. Comparative analysis of country models indicates that:

   3.1 Governments generally display a uniform approach to defining the capabilities of AI technology in the sphere of security (both at the level of the political process and decision-making and the level of institutional fixation);

   3.2 Constant accumulation of knowledge and experience with the potential of technology leads to a systematic increase in the capabilities of technologies in the sphere of security;

   3.3 Competition among countries is increasing; there is a uniformity of approaches to political control and regulatory consolidation of technologies in the sphere of security (in the sample of five leading countries);

   3.4 Political decisions on the regulation of the AI technology occur uniformly and at similar time periods (all countries of the sample adopted appropriate strategies in the period of 2017-2019). The above may indicate uniformity in the politicisation and securitisation of the AI technology (and, possibly, other digital technologies).
4. The dynamics of changes in national security systems are non-linear. The wave-like dynamics reflect the differences in the adaptability of political institutions and the diversity of political decisions in applying technologies in the sphere of security. Although all the countries analysed are maximising the capabilities to apply digital technologies in national security systems, the assessments of threats are heterogeneous and may vary in each country (and among countries). On the one hand, the above illustrates the specifics of the digital technologies themselves, including difficulties in assessing the potential of threats and opportunities, technical challenges, etc. On the other hand, it allows us to argue that the very understanding of threats from country to country can vary greatly. as Also, a specific threat can be reconceptualised even within a country over time.

5. States (governments) are adapting to technological challenges in the sphere of security. States determine significance of technologies proportionately to their potential capabilities. In other words, states adjust to current challenges and transform national security systems by integrating technologies. National security systems possess abilities to respond to threats that outweigh the assessed threats. A broader interpretation of the results suggests that states completely control changes in their security systems.

In our study, we have demonstrated the dynamics of changes in the sphere of security under the influence of digitalisation and automation technologies using the example of a specific type of digital technologies, namely the artificial intelligence technology. From a methodological standpoint, we have attempted to build a systematic research based on the methodological foundations of rational choice theory (regarding political actors), institutionalism[81], modern approaches of the critical security studies and R. Taagepera's general approaches to logical modelling. We do not deny the value of expert knowledge on the subject and attempt to enrich it with a quantitative approach.

This study demonstrates the dynamics of changes in the security sphere under the influence of digitalisation and automation technology using the tested empirical model. Our findings reinforce the existing literature on the politicisation and securitisation of technology in the security sector, heterogeneous perception of threats by governments of different countries, partially confirm the thesis on the militarisation of technology, and indirectly illustrate the subordination of development to security purposes. Also, among our findings are the non-linear dynamics of development of national security systems and the identification of specific features of national security policies as well as the relationship of political will with the technological change.

Comparative analysis reveals the best practices of adaptation to digitally-driven changes in the sphere of security.

1. Countries with more mature public-private partnerships perform better. Political and institutional opportunities to attract technological developments from private companies and start-ups allow to better adapt to change and achieve more consistency in the sphere of security. This finding is confirmed by positive examples from different countries of applying dual-use technologies: initially, technological developments are oriented towards

[81] Again, we do not just rely on the classic "institutions matter" but consider them broadly as rules and normative representations of political will. Remaining in the subject field of political science, we approach institutions as meaningful manifestations of politics. At the same time, without rationalising the institution itself, it gives an "opportunity" to the existence of informal forms of institutional presentation and identification of power in security matters.

civilian use and have been developed by private companies; later, these developments are introduced in the sphere of security.

2. A balanced approach to purchases of technologies from abroad and their national development leads to better security outcomes. For example, Sweden's adaptation of best practices and technological processes through a network of trade relations and stimulation and support for national R&D efforts allow this country to demonstrate leading positions (in the results of network analysis) as well as high scores in the empirical model. Thus, an emphasis only on import substitution policies or an assertive reliance on acquisition of technologies abroad do not allow to produce a balanced and adaptive national security system (regarding its digital transformation).
3. Countries actively involved in international interactions (at the level of trade as demonstrated by the network analysis, as well as at the level of alliances and supranational organisations, and a wide network of involved experts) and capable of the political will for the institutional and political streamlining of rules and norms perform better.

Cooperation within the alliances (NATO, EU) allows for a more systematic and broader consideration of technologies' opportunities and potential risks. In turn, involvement of experts and strong trade ties make it possible to evaluate the effects of digitalisation on security issues practically. If the quality and interaction of institutions in a state make it possible to adapt to such changes, national security system is changing proportionately and in a balanced way using digital technologies.

At the instrumental level, our empirical model of changes and evaluation of a state security system under digital technologies have been developed, tested, and validated (by the example of the artificial intelligence technology). The model allows to assess security in terms of threats (how governments define and evaluate threats) and technology capabilities (how governments determine the technology’s potential and its applications).

Our model helps to expand the existing discussions and fill in some gaps. For example, the analysis of dynamics of changes suggests that governments are more pragmatic when dealing with new technologies technology. In this respect, many concerns of the academic community are somewhat exaggerated. Despite differences among states in the understanding and implementation of technologies and the wave-like dynamics of changes, this does not entail significant problems for countries' national security systems. Another important result reflects the emergence and active development of competition among states in matters of the artificial intelligence technology. Moreover, such competition manifests not just in the "usual" areas of international trade, etc., but also in security issues. In turn, the scalability of the proposed model

allows to evaluate effects produced by any other type of digital technologies for national security systems of countries.

Further research developing theoretical and instrumental (methodological) findings of this study may be data-driven (with an eye on adding new data on various types of digital technologies in the subject area of security studies as well as comparative.

1. It is possible to expand the study's boundaries and explore the links between the dynamics of national security systems initiated by digital technologies and regime variations. In other words, one of the possible directions of further research may involve a comparative analysis of models of countries with various regime characteristics. Instead of contrasting "autocracies" with "democracies", it may be optimal to study distinct regime variations (for example, according to the V-Dem typology, which includes the types of liberal democracy, electoral democracy, electoral autocracy, and closed autocracy.
2. Addition of other types of digital technologies into the model will require its systemic upgrade to evaluate the security through the interrelation of different types of technologies. Such a model will allow to assess the dynamic in the sphere of security in a more comprehensive manner.
3. Over time, additional model building will be required to track the changes after 2019.

Design of predictive models based on the current model may also be an interesting direction of further research. Predictive models will expand our understanding of the transformational impact of technologies and enable a more informed approach to both the planning of technology effects and the improvement of relevant policies.

For future research, it is possible to expand the conceptualisation of the AI technology. This task will require a systematic analysis of scientific publications (using keywords relevant to the subject of AI) with the extraction of abstracts and keywords from each article. will be A quantitative thematic analysis (topic modelling) of an array of texts with a focus on the country affiliation of authors may be carried out. Such an analysis will make it possible to identify specific trends in the modern understanding of the technology and to identify countries (through authors' affiliations) that have the most significant intellectual and scientific potential for developing the AI technology. This will allow to test our earlier findings and to clarify the pool of countries with leading positions in the AI technology development. Moreover, the modelling results will allow to compare "positions" of countries with the results of the network analysis carried out for this study. will be A broader conceptualisation of the artificial intelligence technology may be an independent result of such research.