IRSTI 19.01.11 https://doi.org/10.26577/HJ.2021.v61.i3.01

Y.A. Kumar[1]*, B.S. Baktybayev[2], L.R. Vaigorova[3]

[1]Institute of Diplomacy at the Academy of Public Administration
under the President of the Republic of Kazakhstan, Kazakhstan, Nur-Sultan
[2]Center for Analysis and Information of the Ministry of Information
and Social Development of the Republic of Kazakhstan, Kazakhstan, Nur-Sultan
[3]SmarTEST Prep, Kazakhstan, Nur-Sultan
*e-mail: yernazar.kumar@alumni.nu.edu.kz

HOW THE INSTALLATION OF NATIONAL SECURITY CERTIFICATE IN KAZAKHSTAN BROUGHT NEW SOCIAL MEDIA DISCUSSIONS ON CYBERSPACE REGULATIONS

In 2019, the Kazakhstani government attempted to embed the installation of a national security certificate within the country. The introduction of such a certificate was explained by the need to strengthen the cyber protection of citizens, state bodies, private companies from activities of Internet fraudsters and other types of cyber threats. However, citizens alongside local and international experts did not entirely welcome and accept this decision by voicing their dissent towards it. Criticism towards the installment of national security certificate ranged from infringements concerning personal data rights of citizens and companies towards an act of state apparatus espionage on sensitive private information. The thematic focus of the paper concerns the problem of mass communication and realm of media rights. Structurally, the paper first describes how the national security certificate was introduced and has originated in Kazakhstan. Then the paper analysis the various reasons and arguments in favor or against the introduction of a national security certificate. Here, viewpoints from different stakeholders were considered, such as by state ministries, Kcell and Activ mobile operators, ordinary citizens or local experts like Dossym Satpayev. Lastly, a thorough analysis of present and future outlooks on the development of national security certificate in Kazakhstan is discussed. A discourse analysis approach is applied as a research method with secondary sources of information used. The goal of this concise but informative article is to highlight both the development and the inter-relationship between the society and state what concerns national policies within the cyber realm. The significance of this paper is that it should help scholars in identifying new domestic issues studying in the field of journalism or public policy. In conclusion, the results and discussions of this paper showed us the practical and theoretical importance of how a national policy and its security certificate project generated both public dissatisfaction and new social movements concerning cyberspace aspects, but also a new testing ground for pilot projects in testing people's readiness for accepting new cyberspace regulations.

Key words: national security certificate, Kazakhstan, Internet blocking, mobile operators, human rights.

Е.А. Кумар[1]*, Б.С. Бақтыбаев[2], Л.Р. Вайгорова[3]

[1]Қазақстан Республикасы Президенті жанындағы
Мемлекеттік басқару академиясының Дипломатия институты, Қазақстан, Нұр-Сұлтан қ.
[2]Қазақстан Республикасы Ақпарат және әлеуметтік даму министрлігінің талдау
және ақпарат орталығы, Қазақстан, Нұр-Сұлтан қ.
[3]SmarTEST Prep, Қазақстан, Нұр-Сұлтан қ.
*e-mail: yernazar.kumar@alumni.nu.edu.kz

Қазақстанда ұлттық қауіпсіздік сертификатын орнату интернет кеңістігінің ережелері бойынша жаңа әлеуметтік медиа пікірталастарын қалай тудырды

2019 жылы Қазақстан үкіметі ұлттық қауіпсіздік сертификатын орнатуды ел ішінде енгізуге тырысты. Мұндай сертификатты енгізу азаматтардың, мемлекеттік органдардың, жеке компаниялардың интернет-алаяқтардың әрекеттерінен және киберқауіптердің басқа түрлерінен киберқауіпсіздікті күшейту қажеттілігімен түсіндірілді. Алайда, азаматтар жергілікті және халықаралық сарапшылармен бірге бұл шешімге қарсы пікірлерін білдіріп, оны толық құптамады. Ұлттық қауіпсіздік сертификатын алуға қатысты сындар азаматтар мен компаниялардың жеке мәліметтерінің құқықтарын бұзудан бастап, құпия жеке ақпаратқа мемлекеттік аппараттың шпиондық әрекетіне қатысты болды. Мақаланың тақырыбы бұқаралық ақпарат құралдары мен

БАҚ құқығы мәселесіне қатысты. Құрылымдық тұрғыда бұл мақалада алдымен ұлттық қауіпсіздік сертификаты қалай енгізілгені және Қазақстанда қалай пайда болғандығы сипатталған. Содан кейін қағазға ұлттық қауіпсіздік сертификатын енгізудің пайдасына немесе қарсы әр түрлі себептері мен дәлелдері талданады. Мұнда мемлекеттік министрліктер, Kcell және Activ ұялы байланыс операторлары, қарапайым азаматтар немесе Досым Сәтбаев сияқты жергілікті сарапшылар әр түрлі мүдделі тараптардың көзқарастары қаралды. Ақырында, Қазақстанда ұлттық қауіпсіздік сертификатын әзірлеу бойынша қазіргі және болашақ көзқарастардың толық талдауы талқыланады. Дискурстық талдау әдісі ақпараттың екінші көздері бар зерттеу әдісі ретінде қолданылады. Бұл қысқа, бірақ мазмұнды мақаланың мақсаты – қоғам мен мемлекет арасындағы кибержүйедегі ұлттық саясатқа қатысты мәселелердің дамуы мен өзара байланысын көрсету. Бұл жұмыстың маңыздылығы – журналистерге немесе мемлекеттік саясат саласында оқитын жаңа отандық мәселелерді анықтауда ғалымдарға көмектесуі. Қорытындылай келе, осы құжаттың нәтижелері мен талқылаулары бізге ұлттық саясат пен қауіпсіздік сертификаты жобасының киберкеңістіктегі аспектілеріне қатысты қоғамдық наразылық пен жаңа әлеуметтік қозғалыстардың практикалық және теориялық маңыздылығын көрсетті. Сондай-ақ тестілеу үдерісі кезінде пилоттық жобалар үшін жаңа полигон жасақталды, онда киберкеңістіктегі адамдардың жаңа ережелерді қабылдауға дайындығы айқындалды.

Түйін сөздер: қауіпсіздік сертификаты, интернетті бұғаттау, ұялы байланыс операторлары, адам құқықтары.

Е.А. Кумар[1*], Б.С. Бақтыбаев[2], Л.Р. Вайгорова[3]

[1]Институт дипломатии Академии государственного управления
при Президенте Республики Казахстан, Казахстан, г. Нур-Султан
[2]Центр анализа и информации Министерства информации
и социального развития Республики Казахстан, Казахстан, г. Нур-Султан
[3]SmarTEST Prep, Казахстан, г. Нур-Султан
*e-mail: yernazar.kumar@alumni.nu.edu.kz

Введение сертификата национальной безопасности в Казахстане для защиты от киберугроз и новые дискуссии в социальных сетях по этому поводу

В 2019 году правительство страны попыталось внедрить установку сертификата национальной безопасности в Казахстане. Введение такого сертификата было объяснено необходимостью усиления защиты граждан, государственных органов, частных компаний от противоправных действий интернет-мошенников и других видов кибератак. Однако граждане наряду с местными и международными экспертами не полностью приняли это решение, объяснив свои резоны. Критика в отношении установки сертификата национальной безопасности варьировалась от нарушений прав граждан и компаний на личные данные до шпионажа государственного аппарата в отношении конфиденциальной частной информации. Тематическая направленность статьи касается проблемы массовой коммуникации и прав СМИ. В данной работе описывается, как сертификат национальной безопасности вводился в Казахстане, анализируются различные причины и аргументы за и против такой инициативы. Авторами были учтены точки зрения заинтересованных сторон: государственных министерств, мобильных операторов Kcell и Activ, рядовых граждан и местных экспертов, в частности мнение политолога Досыма Сатпаева. Представлен тщательный анализ нынешних и будущих перспектив развития сертификата национальной безопасности в Казахстане. Подход дискурсивного анализа применяется как метод исследования с использованием вторичных источников информации. Цель статьи – осветить как развитие национальной политики в киберсфере, так и взаимосвязь между обществом и властью. Статья может быть полезной ученым в выявлении новых внутренних проблем, изучаемых в области журналистики и государственной политики. Результаты и обсуждения этого документа показали практическую и теоретическую важность национальной политики и проекта сертификата безопасности, которые вызвали как общественное недовольство, так и новые социальные действия, касающиеся аспектов киберпространства. Был создан новый полигон для пилотных проектов в процессе тестирования, где отражалась готовность людей принять новые правила киберпространства.

Ключевые слова: сертификат безопасности, блокировка интернета, мобильные операторы, права человека.

Introduction

Kazakhstan is a post-soviet developing democratic state characterized by a strong state apparatus, which often is criticized for limiting the freedom of mass media activities. In recent years, Kazakhstan had introduced several laws that were directed to further restrict the cyber space activities in the country. One of these laws included the Kazakhstani law on banning anonymous comments was criticized as it had restricted the principle of freedom of expression inside the country (Baytukenov, 2018: para. 3). A more nationwide debatable government-initiated security certificate installation issue had emerged, which became a hot boiling spot for criticism to be directed towards the government. Such criticisms included the infringement of personal data protection, an increased state monitoring process of citizen's cyber space activities and possible restriction of Internet content via censorship or blockage of web traffic. However, this law met societal resistance and was later cancelled by President Kassym-Jomart Tokayev due to the active public discourse and public outcry. In this paper, this case will be discussed in greater detail in both mass media as well as cyberspace aspect in the context of Kazakhstan.

Material & Research Methodology

In this paper, we will use a discourse analysis approach concerning the national security certificate matter in Kazakhstan. For that, we will mostly use secondary sources as information reference for analyzing the issue. Firstly, the paper introduces the history and origin of national security certificate initiatives in Kazakhstan and how it became a widely discussed societal issue. Then, the paper will further analyze the explanations for the need to install security certificate as well as their different reactions by different stakeholders. Here, we will consider the viewpoints provided by the Ministry of Digital Development, Innovation and Aerospace Industry, Kcell and Activ mobile operators, ordinary citizens as well as international and local experts like Netblocks, Mikhail Pozdniak or Dossym Satpayev. Lastly, the paper discusses current and future outlooks concerning the national security certificate development in the country. The paper serves as an informational-analytical paper outlining the problem of security certificate in Kazakhstan with new and great insights. The very fact that such a paper on the topic of national certificate has not yet been published among the academia in Kazakhstan, makes the paper a unique case study. Moreover, in terms of mass media aspect, this paper will highlight the impact of government-driven initiatives on the perception of Kazakhstani people regarding cyberspace rights and how a government project has led to catalyze social and social media movements on a specific matter.

Introduction of the security certificate in Kazakhstan

The first serious initiatives of introducing new restrictive amendments into the legislation regarding the cyber space in Kazakhstan began back in 2011 with the relocation of all domains that contained the names "*.kz*" to be held within the country (CABAR, 2019: para. 11). During that year, according to Freedom House, Kazakhstan started its first move towards online censorship activities (CABAR, 2019: para. 9). Such restrictive measures had its roots from the 2010 established national policy of gradual strengthening of digital space control in Kazakhstan (CABAR, 2019: para. 8). Four years after, Kazakhstan attempted to introduce its first steps to regulate the idea of national certificates within the country, which led eventually in 2015 and then in 2017 for a new law to be created that prescribed citizens and their usage of phones and SIM cards to become deanonymized and registered (CABAR, 2019: para. 19) (Plakhina, 2019: para. 1 of section on "History repeats itself").

The Ministry of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan (MDIA) first-mentioned about the installation of security certificates in the country on June 2019 (Shamsutdinov, 2019: para. 5). MDIA reported carrying out technical works aimed at strengthening the protection of citizens, state bodies and private companies from hacker attacks, Internet fraudsters and other types of cyber threats (Shamsutdinov, 2019: para. 7 and 8). Other Kazakhstani scholars have also backed up this argument (Symbat & Yesseniyazova, 2019: p. 1 and 2) (Aben, D. & . Makhanov, K., 2019: p.1) (Gussarova, A., 2020: p 6). In case of problems with access to certain Internet resources, MDIA recommended checking the registration of mobile devices (mobile phones and tablets), to install a security certificate (available on the websites of telecom operators) or to contact the call center of telecom operators (Shamsutdinov, 2019). Prior to that, back in November 30 of the year 2015 an announcement of installation of security certificates were made to the public via the publishing of articles on this matter in various mass media outlets (Shamsutdinov, 2019: para. 4). However, these articles a few days later have been quickly removed, as the certificate system has not yet been entirely prepared to be embedded as a nationwide policy initiative and at that time not yet ready for a successful implementation phase (Shamsutdinov, 2019: para. 4).

After MDIA's announcement in 2019, several mobile operators sent a message to their subscribers about the need to install a security certificate on each device that had Internet access (Kursiv.kz, 2019b: para. 2). Mobile operators were obliged to skip traffic by using a security certificate according to Article 26 of the Law "On Communications" (Kursiv.kz, 2019b: para. 2). Mobile operators claimed that subscribers could face difficulties with access to the network if they did not install a security certificate (Kursiv.kz, 2019b: para. 2) (Shamsutdinov, 2019: para. 14). According to Emil Shamsutdinov, since the law "On Communications'' did not oblige citizens to install security certificates but mobile operators, the access to the Internet could be limited and certain websites were still blocked as outlined by the deputy director of the Committee for Informational Security of MDIA Mr. Ruslan Abdikalikov (Shamsutdinov, 2019: para. 14). This statement did suggest that users' rights and access to the Internet were to a certain degree negatively affected by it.

Discussion & Results Section

Explanation of the need to install security certificates

MDIA's recommendation to install a security certificate seems reasonable at the beginning alongside with the launch of the Cyber Shield Kazakhstan program back in 2017, since the number of cyber-attacks in Central Asia has increased in recent years if we look at the statistics (Woollacott, 2019: para. 12). According to Kaspersky, an Internet Security Suite, Kazakhstan is in the list of top ten countries in terms of users being attacked by mobile ransomware trojans, man-in-the-middle threats, XSS attacks and miners (Woollacott, 2019: para. 7). Ministry of Defense and Aerospace Industry found that 1 billion cyber-attacks happened in Kazakhstan alone during 2016 (Woollacott, 2019: para. 8). 20 billion attacks against state bodies were fixed in 2018 alone (Woollacott, 2019: para. 9). Apart from this staggering number, one of the hacking groups stole 600,000 US dollars from Kazakhstani banks (Woollacott, 2019: para. 13). Kaspersky Company argued that these attacks have a political agenda to some degree and might have originated from China and Russia, and the number of such attacks is not going to decrease in the future (Woollacott, 2019: para. 14 and 17).

Minister of Digital Development, Innovation and Aerospace Industry Askar Zhumagaliev, argued that the installation of a security certificate ensured protection from the Internet materials related to terrorism, extremism, and pornography (24.kz, 2019: para. 2). He also added that security certificates will help to deal with information security problems and do not violate citizen's rights, since the safety of personal data of Kazakhstani citizens is guaranteed by the Constitution (24.kz, 2019: para. 5 and 6). The same viewpoint also shared the deputy director of the Committee for Informational Security of MDIA Mr. Ruslan Abdikalikov (Shamsutdinov, 2019). According to Arman Abdrasilov, the director of the Centre for Analysis and Investigation of Cyber Attacks in Kazakhstan, the centralization of traffic management system controlled by national providers would make traffic management convenient and safe, but also in exchange has to receive by any means public backlash as this is unavoidable (CABAR, 2019: para. 30 and 31).

Representatives of Kcell and Activ, both one of the largest Kazakhstani mobile operators, also argued that a security certificate is going to be an effective tool in dealing with hackers, Internet fraudsters and other types of cyber threats (Kursiv.kz, 2019b: para. 5 and 6). According to them both, a security certificate will protect information systems and data as well as the banking sector before any damage is going to be made (Kursiv.kz, 2019b: para. 5).

It is important to note that this was the third attempt by the Kazakhstani authorities to enforce the use of a national security certificates (Plakhina, 2019: para. 1 of section on "History repeats itself"). The first certificate-related amendments on the law on communications were introduced to oblige telecom operators to install a security certificate to encrypted traffic already back in 2016 (Plakhina, 2019: para. 3 of section on "History repeats itself"). However, the national security certificate did not come into force during that year (Plakhina, 2019: para. 3 of section on "History repeats itself"). The next announcement regarding the security certificate was in March 2019 (Plakhina, 2019: para. 3 of section on "History repeats itself"). However, the public did not notice this announcement until July when they started to receive messages from mobile operators (Plakhina, 2019: para. 3 of section on "History repeats itself").

Citizens' and subscribers' reactions

In general, citizens criticized the state's decision to introduce a security certificate (Plakhina, 2019) (Shamsutdinov, 2019). For example, a civic activist who goes by the name Yelena Shvetsova questioned the necessity of such a certificate and asked others what to do in such a case (Plakhina, 2019: para. 6). She described those measures as an attempt to gain access so to say into personal information or data (Plakhina, 2019: para. 6). According to her, interception made by the government would spy on correspondence messages and total access to phones (Plakhina, 2019: para. 6).

The same viewpoint was also shared by Emil Shamsutdinov, who additionally referred to another similar problem that occurred in July 2019 with the leak of passport information from 11 million Kazakhstani citizens (Shamsutdinov, 2019: para. 20). In this case, third party stakeholders having access to personal data such as that of passport-related or financial information and tampering or misusing information will jeopardize not only the citizen's data protection but also the private company's reputation. This is especially risky if a proper system of security certificates installations was not introduced, well-thought-out and effectively implemented.

Another journalist named Irina Sevostyanova and IT expert Daniil Vartanov called the initiatives as a role constituting that of a "big brother", an instrument that would allow to access personal information by state security services or the Ministry of Internal Affairs (Plakhina, 2019: para. 7). Other comments were similar to the aforementioned comments. Many citizens were not willing to install a certificate since this certificate could not guarantee the full protection of personal data guaranteed as stipulated in the constitution of Kazakhstan (Plakhina, 2019).

The reaction of civil activists and mobile operators

A group of lawyers filed lawsuits against four Kazakhstani mobile operators: Beeline, Tele2, Altel, and Kcell companies after receiving numerous SMS with the request to install a certificate (Ramazanov, 2019: para. 1 and 2). Lawyers argued that they could go to court to investigate this issue since they believe that citizens cannot be disconnected from the Internet even though they didn't install a security certificate (Ramazanov, 2019: para. 3).

Altel and Tele2 PR Director Olzhas Bibanov commented the lawyer's lawsuits as following: "This kind of lawsuits are populist. Apparently, these lawyers want to be recognized among potential clients" (Ramazanov, 2019: para. 8). He also added that it is not the mobile operators' decision to enforce citizens to install a security certificate (Ramazanov, 2019: para. 9). Bibanov argued, that it is a legal requirement, and this is a collaboration with authorized bodies, where mobile operators help subscribers to comply with legal requirements regarding the installation of a security certificate (Ramazanov, 2019: para. 10).

The reaction of international and local experts

It is important to note that citizens had problems with access to the Internet before the introduction of the security certificate. There were numerous cases of intermittent social media blockings. According to the Netblocks team that monitors Internet freedom in the world, there was an unprecedented total blocking of social media for Kazakhstan during victory day (Netblocks, 2019). Netblocks team argued that Kazakhstani authorities undertook this measure as a response to the planned demonstrations by the dissident groups (Netblocks, 2019). Media platforms Facebook, Instagram and YouTube, and some independent news media websites were completely disabled, while Telegram was partially available (Netblocks, 2019). Netblocks team found that the one hour of the shutdown of Facebook, Instagram and YouTube for Kazakhstan costs approximately if calculated $318,923 or KZT 122,750,767 thanks to the COST (The Netblocks Cost of Shutdown Tool) service that was created this year to assess the economic losses due to Internet blocking measures in different countries (Netblocks, n.d.).

The introduction of a security certificate also attracted international attention. Google, Mozilla, and Apple have responded to the introduction of a national security certificate in Kazakhstan by blocking it (bne IntelliNews, 2019: para. 1). Their reason for doing that was because these companies did not trust this certificate that can be used to monitor citizens' use of the Internet (bne IntelliNews, 2019: para. 1). Mozilla's representatives expressed their negative attitude towards such "lightly actions", while Apple said that they are going to undertake measures to protect users of its Safari browser from negative consequences of Kaznet related initiatives (bne IntelliNews, 2019: para. 5 and 7). Google browser chief was also against any attempt that can compromise Chrome users' data (bne IntelliNews, 2019: para. 6).

Kazakhstani expert-analyst of Ak Kamal Security Mikhail Pozdniak said that every state is interested in finding effective measures to fight with criminal elements on the Internet (Kursiv, 2019a: para. 3). According to him, Kazakhstani authorities were likely going to intercept all data between each user and the websites, which the user is using thanks to this certificate (Kursiv, 2019a: para. 5 and 6). Pozdniak argued that the state attempts to spy on its citizens (Kursiv, 2019a: para. 5). He found the state's arguments regarding installing a security certificate as not convincing, as he was curious to know how state bodies are going to protect citizens with such kind of certificate from various types of cyber-attacks (Kursiv, 2019a: para. 10 and 11). Similarly to that of the ideas of Pozdniak, Radio Azattyq Organization claimed that the state is going to strengthen control over the Internet in the country (Radio Azattyq, 2019).

The decision to cancel the national security certificate

After numerous public backlashes, President Kassym-Zhomart Tokayev decided to cancel a security certificate (Kim, 2019). This decision was sudden and Tokayev argued that the quick completion of testing the security certificate under the Cyber Shield Program showed a high level of technical equipment in case of external cyber-attacks that have frequently happened (Kim, 2019: para. 4). He explained that testing was carried out on his behalf and thanked the KNB (Committee for National Security) for testing the security certificate (Kim, 2019: para. 1). President Tokayev also added saying that: "The security of the information space of the Republic of Kazakhstan and the possibility of using the certificate only in cases of intrusion from the outside are proved. There is no inconvenience to Internet users. Thanks to the KNB." (Kim, 2019: para. 2).

Dossym Satpayev's opinion regarding Kazakhstani "cyber shield"

One of the popular independent Kazakhstani political and public figures Dossym Satpayev said that the state's initiative about a national security certificate had two main reasons. The first reason is the testing of the system (Giperborey, 2019). The second reason was to see citizens' reactions towards it and so understand the societies readiness or unreadiness towards new law amendments (Giperborey, 2019). Satpayev noted that the national security certificate was postponed, but was not completely thrown away (Giperborey, 2019). Satpayev argued that the same testing was made with the Internet (Giperborey, 2019). Initially, live broadcasts were blocked, and then state authorities experimented by blocking a gigantic segment of the Internet in a certain political period (Giperborey, 2019). All this should boil down to the idea that the field of Kazakhstani cyber field is a new area for experimentation, tests and opportunities for both the government and the society to understand its level of mutual acceptance for new regulations and changes.

The current and future outlooks of cyber space regulations in Kazakhstan

Freedom House has published a report on Internet Freedom on November 4, 2019 (Freedom House, 2019). According to this report, Kazakhstan and Sudan have shown the biggest score decline alongside Brazil, Bangladesh, and Zimbabwe in terms of Internet freedom (Freedom House, 2019: para. 1 of section on "key findings"). Kazakhstan was in the list of states with frequently blocked Internet and limited political, social or religious content (Shahbaz & Funk, 2019). This was especially the case when it came down to usage of government-backed informational tactics (Shahbaz & Funk, 2019: chapter on "key tactics of digital election interference"). Kazakhstan has been enlisted as one of the countries alongside Egypt and Turkey, who systematically used bots and strong government apparatus informational tactics to disseminate information directed towards non-mainstream trajectories (Shahbaz & Funk, 2019: chapter on "key tactics of digital election interference"). Such tactics included propagandistic news, dissemination of fake news or automated bot accounts (Shahbaz & Funk, 2019: para. 3 of chapter on "politicians and hyper-partisans use digital means to manipulate elections"). Of course, this is not to say that the actions by the government are wrong, but something to be aware of. Here it is crucial to understand that Kazakhstan is a semi-democratic state with a legacy containing elements of a post-soviet era. Moreover, contextually wise, it is obvious that a newly independent state like Kazakhstan can not afford to have "completely" loose and uncontrolled cyberspace regulations (Aben, D. & Makhanov, K., 2019: p. 1). In this regard, limited Internet access accompanied by unregulated cyberspace regulations disfavor both the government and the society (Aben, D. & Makhanov, K., 2019: p. 1) . It is better for a state to be aware of its problems rather than ignoring them. And the national security certificate installation in fact does try to fill in this gap of unregulated cyberspace matter (Aben, D. & Makhanov, K., 2019: p. 1).

According to Sarkis Darbinyan, a lawyer in cyber rights in Russia, he claims that Kazakhstan path towards the introduction of national certificate in their country resembles the trajectory that of Russia for the last eight years (CABAR, 2019: para. 20). For instance, while Russia raised the introduction of regulations into the national cryptography and SSL certificates a few years back, Kazakhstan on the other hand had started it a bit earlier (CABAR, 2019: para. 20). Another viewpoint to look at this trajectory is also by understanding the developmental aspect of it. Similarly to Russia and China, Kazakhstan tries to preserve its independent path alongside the control of the cyber space to establish its own system of governance model. If we for example look at how China introduced its new idea of cyber superpower idea of a new governance model of cyberspace and big data management systems (CABAR, 2019: para. 25 and 26), this would also mean that geopolitically this would tempt Kazakhstan to become more independent and re-conceptualize its approach towards cyberspace management. No other country has ever tried to embed a security certificate on a nationwide basis, but Kazakhstan itself does not really have the capability to launch a Chinese-style independent cyberspace since for that it would need more than just resources (Plakhina, 2019: para. 4 of section on "What's next?"). This would require moral backup by the domestic societal community and guaranteed protection for the people that accept it.

According to Viktor Pyagai, in the future the cyberspace (Internet) alongside the introduction of new regulations in Kazakhstan will change but not drastically, even with the full introduction of national certificates (CABAR, 2019: para. 35). This is due to the fact that local streaming services and local social media platforms will not become as popular as Instagram or YouTube that are today (CABAR, 2019: para. 35 and 36). He claims that people will always look out for international content and further restrictions would rather lead to social tensions (CABAR, 2019: para. 37). So, one may ask how lawful the introduction of national certificates are in Kazakhstan as well as how the government could find a golden middle to regulate the cyberspace in order to guarantee data protection and well-controlled traffic management, while on the other side of the coin to achieve the goal in minimizing public backlash towards such measures. Such matters in a post-soviet space are delicate and quite a new phenomenon, as within the context of a country like that of Kazakhstan, new measures can be associated with a new change. And whether this change is good or bad decides both the government and the society, since the society is the first actor that will feel, understand, accept or rebuke changes and new measures, while the government will guide and introduce changes if necessary. This dual harmonic cooperation is immensely crucial for the healthy coexistence of the state and its people. Without it, any change introduced can be rejected from either side at any time.

In terms of the discussions surrounding the mass and social media aspect, the reactions by various stakeholders against the installation of a national security certificate showed on the one hand the reactive approach by the citizens towards government initiatives while also being cautious about every government initiative. This is argued to be a good aspect of a democratic society that is ready to reflect on the actions of others as well as on their impact on the society (Symbat & Yesseniyazova, 2019: p. 2). Another scholar Gussarova A. argued that digital development and cyber security matters and their interrelated progress would spur sustainable development in the cyber realm (Gussarova, 2020: p. 2). Moreover, since national cyber security is intertwined with the process of digital development progresses and aspects of national security, it is an important aspect for developing countries like Kazakhstan if the country wants to move on in terms of cyber space development (Symbat & Yesseniyazova, 2019: p. 2) (Gussarova, 2020: p. 6) (De Haas, 2015: p. 1). However, in terms of social and mass media movement, here there is an interrelationship. Any public backlash causes social media movements, which in return cause the mass media to take up on that. The same analogy can be brought up with the matter on domestic violence or sexual abuse on women in Kazakhstan and its subsequent social media movements like NeMolchiKz. In another example, the Talgo train rape case also stirred huge societal discussions and brought new internal matters to the forefront. Of course, one may argue that such problems are picked up by the mass and social media in order to feed the society with temporary "sensational news" rather than bringing problems to the forefront for productive discussions. This though is of course the job of a journalist, who should be able to choose the right topic for mass and social media discussions and stir at the right angle without any predetermined propaganda and misleading misconceptions. Thus, in conclusion, one may argue that the activities of the social and mass media alongside its role are intertwined in Kazakhstan, but this may not always be the case for every problem or matter that is brought up.

Conclusion

In conclusion, the national security state initiative in mid-2019 showed us the active reaction and interest by the public society to respond to policy initiatives and cyber security issues. On the one hand, the state was interested in strengthening control on the Internet, while on the other also to ensure the protection of citizen's web data and information. However, the attempt to enforce the public society in installing the national security certificate was not entirely welcomed in a positive manner by the citizens as well as local and international experts. The state was forced to step back because of public dissatisfaction with the way how the national security certificate was presented to the public, since they had many questions about this policy initiative ranging from accusations from spying and third-party access to data to limiting or blocking access to certain websites. As a result, President Tokayev cancelled the entire policy initiative. However, one may argue that, as Dossym Satpayev said, the given certificate was not completely thrown away and it may just be an experiment to test out the societal reaction and level of readiness for such changes. Thus, a security certificate may remain open for the government to implement it in the future in a probably similar or different fashion.

Besides that, the paper also showed us how a new aspect of cyberspace security and its regulations can generate strong social media reactions, causing new social media movements and new mass media discussions. On top of that, the national security certificate installations also highlighted the necessity for the government to find a golden middle between regulating cyberspace properly while at the same time ensuring and guaranteeing protection of cyberspace users. Of course, here comes the question of the timely necessity and lawfulness of the installation itself in Kazakhstan. Having also discussed the reasons by the government to introduce such measures, it would also be interesting for journalists to tap into this area by investigating the issue on how such installations have been introduced in other countries of Europe or Asia. This should help the society in bringing new informational content to read and digest in order to understand better why such installations are crucial and necessary. And, as a result, this would help the society to reach better analytical conclusions by weighing out various informational sources and arguments, and for the government better societal outreach for their government-led projects. After all, most of the societal issues occur not only due to government ineffectiveness or policy failures, but also due to the existence of society's informational asymmetry and level of understanding and readiness for new changes.

Литература

Aben, D. & . Makhanov, K. (2019). Ensuring Cybersecurity in Kazakhstan: Problems and Solutions. Eurasian Research Institute. URL: https://eurasian-research.org/wp-content/uploads/2020/07/Weekly-e-bulletin-22-04-2019-28-04-2019-No-208.pdf

De Haas, M. (2015). Kazakhstan's security policy: steady as she goes?. The Journal of Slavic Military Studies, 28(4), 621-645.

Gussarova, A. (2020). Kazakhstan Adapting to the Cyber Space. Marshall Center Organization. URL: https://www.marshallcenter.org/sites/default/files/files/2020-09/pC_V7N2_en-2_Gussarova.pdf

Shahbaz, A. & Funk, A. (2019). Freedom on the Net. The Crisis of Social Media. / Freedom House Organization. – November 04, 2019. – URL: https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdfSymbat, I. & Yesseniyazova, B.M. (2019). Cyber Security Issues in Digital Kazakhstan. NISPA Organization. URL: https://www.nispa.org/files/conferences/2019/e-proceedings/system_files/papers/cyber-security-issues-issabaeva.pdf

Электронные ресурсы

Bne IntelliNews. (2019). Google, Mozilla and Apple block Kazakhstan "trust" certificate that spies on citizens' internet use. (2019, August 23). URL: https://www.intellinews.com/google-mozilla-and-apple-block-kazakhstan-trust-certificate-that-spies-on-citizens-internet-use-166588/

Байтукенов Т. (2018). Бес комментариев. (2018, февраль 21). Режим доступа: https://time.kz/articles/tulegennaya-inzheneriya/2018/02/21/bes-kommentariev

Гиперборей (2019). Досым Сатпаев про митинги, Аблязова и транзит власти. (2019, август 29). Режим доступа: https://www.youtube.com/watch?v=keaom9QJUp8

Ким С. (2019). Президент Токаев: тестирование сертификата безопасности проводилось по моему поручению. (2019, август 07). Режим доступа: https://factcheck.kz/dajdzhest/prezident-tokaev-testirovanie-sertifikata-bezopasnosti-provodilos-po-moemu-porucheniyu/

Курсив. (2019b). Жители Нур-Султана негативно восприняли сообщение от сотовых операторов. (2019, июль 19). Режим доступа: https://kursiv.kz/news/obschestvo/2019-07/zhiteli-nur-sultana-negativno-vosprinyali-soobschenie-ot-sotovykh

Курсив. (2019a). Эксперт прокомментировал внедрение сертификата безопасности. (2019, июль 19). Режим доступа: https://kursiv.kz/news/obschestvo/2019-07/ekspert-prokommentiroval-vnedrenie-sertifikata-bezopasnosti

Радио Азаттык. (2019). Токаев заявил, что сертификат Qaznet вводил КНБ по его поручению. (2019, август 07). Режим доступа: https://rus.azattyq.org/a/30096331.html

Рамазанов О. (2019). На Tele2, Beeline и Kcell подали в суд из-за сертификата безопасности. (2019, август 06). Режим доступа: https://tengrinews.kz/internet/tele2-beeline-kcell-podali-sud-iz-za-sertifikata-375763/

24 Хабар. Зачем нужен сертификат безопасности, рассказал Аскар Жумагалиев. (2019, июль 23). Режим доступа: https://24.kz/ru/news/social/item/329888-zachem-nuzhen-sertifikat-bezopasnosti-rasskazal-askar-zhumagaliev

CABAR (2019). Kazakhstan: Google and Mozilla will block national security certificate. (2019, August 22). URL: https://cabar.asia/en/kazakhstan-google-and-mozilla-will-block-national-security-certificate

Freedom House Organization (2019). Social media are a growing conduit for electoral manipulation and mass surveillance. (2019, November 04). URL: https://freedomhouse.org/article/social-media-are-growing-conduit-electoral-manipulation-and-mass-surveillance

Netblocks Organization. (n.d.). Netblocks Organization, Cost of Shutdown Tool (COST). URL: https://netblocks.org/cost/

Netblocks Organization (2019). Social media blocked in Kazakhstan on Victory Day. (2019, May 09). URL: https://netblocks.org/reports/social-media-blocked-in-kazakhstan-on-victory-day-eBOg47BZ

Plakhina, Y. (2019). Kazakhstan pauses interception of encrypted traffic, but for how long? (2019, August 30). – URL: https://advox.globalvoices.org/2019/08/30/kazakhstan-pauses-interception-of-encrypted-traffic-but-for-how-long/

Woollacott, E. (2019). Rising levels of cybercrime renews focus on cybersecurity in Central Asia. (2019, September 17). URL: https://portswigger.net/daily-swig/rising-levels-of-cybercrime-renews-focus-on-cybersecurity-in-central-asia

Шамсутдинов Э. (2019). Национальный сертификат безопасности как очередная «попытка контролировать интернет». Что не так? (2019, июль 23). Режим доступа: https://informburo.kz/stati/nacionalnyy-sertifikat-bezopasnosti-kak-ocherednaya-popytka-kontrolirovat-internet-chto-ne-tak-.html

References

Aben, D. & . Makhanov, K. (2019). Ensuring Cybersecurity in Kazakhstan: Problems and Solutions. Eurasian Research Institute. URL: https://eurasian-research.org/wp-content/uploads/2020/07/Weekly-e-bulletin-22-04-2019-28-04-2019-No-208.pdf

De Haas, M. (2015). Kazakhstan's security policy: steady as she goes?. The Journal of Slavic Military Studies, 28(4), 621-645.

Gussarova, A. (2020). Kazakhstan Adapting to the Cyber Space. Marshall Center Organization. URL: https://www.marshallcenter.org/sites/default/files/files/2020-09/pC_V7N2_en-2_Gussarova.pdf

Shahbaz, A. & Funk, A. (2019). Freedom on the Net. The Crisis of Social Media. / Freedom House Organization. – November 04, 2019. – URL: https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf

Symbat, I. & Yesseniyazova, B.M. (2019). Cyber Security Issues in Digital Kazakhstan. NISPA Organization. URL: https://www.nispa.org/files/conferences/2019/e-proceedings/system_files/papers/cyber-security-issues-issabaeva.pdf

Electronic resources

Bne IntelliNews. (2019). Google, Mozilla and Apple block Kazakhstan "trust" certificate that spies on citizens' internet use. (2019, August 23). URL: https://www.intellinews.com/google-mozilla-and-apple-block-kazakhstan-trust-certificate-that-spies-on-citizens-internet-use-166588/

Baytukenov, T. (2018). Bes kommentariyev. [No comments.]. (2018, February 21). URL: https://time.kz/articles/tulegennaya-inzheneriya/2018/02/21/bes-kommentariev

Giperborey. (2019). Dossym Satpayev pro mitingi, Ablyazova i tranzit vlasti – GIPERBOREY. Vypusk #1. [Dosym Satpayev is talking about meetings, Ablyazov, and power transit – Giperborey. Issue #1]. (2019, August 29). URL: https://www.youtube.com/watch?v=keaom9QJUp8

Kim, S. (2019). Prezident Tokayev: testirovaniye sertifikata bezopasnosti provodilos' po moyemu porucheniyu. [President Tokayev: testing of the safety certificate was carried out on my behalf.] (2019, August 07). URL: https://factcheck.kz/dajdzhest/prezident-tokaev-testirovanie-sertifikata-bezopasnosti-provodilos-po-moemu-porucheniyu/

Kursiv.kz. (2019b). Zhiteli Nur-Sultana negativno vosprinyali soobshcheniye ot sotovykh operatorov. [Residents of Nur-Sultan negatively perceived the message from mobile operators.] (2019, July 19). URL: https://kursiv.kz/news/obschestvo/2019-07/zhiteli-nur-sultana-negativno-vosprinyali-soobschenie-ot-sotovykh

Kursiv.kz. (2019a). Ekspert prokommentiroval vnedreniye sertifikata bezopasnosti. [The expert commented on the implementation of the security certificate.] (2019, July 19). URL: https://kursiv.kz/news/obschestvo/2019-07/ekspert-prokommentiroval-vnedrenie-sertifikata-bezopasnosti

Radio Azattyq. (2019). Tokayev zayavil, chto sertifikat Qaznet vvodil KNB po yego porucheniyu. [Tokayev said that the Qaznet certificate was introduced by the KNB on his behalf.] (2019, August 07). URL: https://rus.azattyq.org/a/30096331.html

Ramazanov, O. (2019). Na Tele2, Beeline i Kcell podali v sud iz-za sertifikata bezopasnosti. [Tele2, Beeline and Kcell sued over security certificate.] (2019, August 06). URL: https://tengrinews.kz/internet/tele2-beeline-kcell-podali-sud-iz-za-sertifikata-375763/

24kz. (2019). Zachem nuzhen sertifikat bezopasnosti, rasskazal Askar Zhumagaliyev. [Askar Zhumagaliyev talked about the necessity of the security certificate.] Khabar 24 News, 23 July 2019. URL: https://24.kz/ru/news/social/item/329888-zachem-nuzhen-sertifikat-bezopasnosti-rasskazal-askar-zhumagaliev

CABAR (2019). Kazakhstan: Google and Mozilla will block national security certificate. (2019, August 22). URL: https://cabar.asia/en/kazakhstan-google-and-mozilla-will-block-national-security-certificate

Freedom House. (2019). Social media are a growing conduit for electoral manipulation and mass surveillance. (2019, November 04). URL: https://freedomhouse.org/article/social-media-are-growing-conduit-electoral-manipulation-and-mass-surveillance

Netblocks. (n.d.). Netblocks Organization, Cost of Shutdown Tool (COST). URL: https://netblocks.org/cost/

Netblocks. (2019). Social media blocked in Kazakhstan on Victory Day. (2019, May 09). URL: https://netblocks.org/reports/social-media-blocked-in-kazakhstan-on-victory-day-eBOg47BZ

Plakhina, Y. (2019). Kazakhstan pauses interception of encrypted traffic, but for how long? (2019, August 30) URL: https://advox.globalvoices.org/2019/08/30/kazakhstan-pauses-interception-of-encrypted-traffic-but-for-how-long/

Woollacott, E. (2019). Rising levels of cybercrime renews focus on cybersecurity in Central Asia. (2019, September 17). URL: https://portswigger.net/daily-swig/rising-levels-of-cybercrime-renews-focus-on-cybersecurity-in-central-asi

Shamsutdinov, E. (2019). Nacional'nyj sertifikat bezopasnosti kak ocherednaja "popytka kontrolirovat' internet". Chto ne tak? [National security certificate as another "attempt to control the Internet." What's wrong?] (2019, July 23). URL: https://informburo.kz/stati/nacionalnyy-sertifikat-bezopasnosti-kak-ocherednaya-popytka-kontrolirovat-internet-chto-ne-tak-.html