THE EXPERIENCE OF FOREIGN COUNTRIES IN PROTECTING THE INSTITUTION OF THE PRESIDENCY FROM INFORMATION THREATS.

Yunusov Javokhirbek Fakhriddin ugli
Master's student in Political Science at the
National University of Uzbekistan

https://doi.org/10.5281/zenodo.15581227

Abstract: This article analyzes the important role of the institution of the presidency in ensuring state sovereignty and national security in the Republic of Uzbekistan and is devoted to the issues of protecting it from information threats, in particular, from false information, insults and slander on social networks. In addition, the experience, legislative framework, technological infrastructure, and monitoring systems of the USA, Russia, China, and European countries in this area will be analyzed.

Keywords: national security, social networks, false information, insult, slander, monitoring systems, freedom of speech, cybersecurity, state sovereignty, disinformation.

In the Republic of Uzbekistan, the institution of the presidency, as the main symbol of state sovereignty, plays an important role in ensuring national security and public stability. Therefore, this institution is required to take effective measures to prevent information threats, including the dissemination of false information on the Internet, insults and slander on social networks. Approaches of foreign countries in this area, legislative frameworks, monitoring systems, as well as practical mechanisms for preventing insults and slander on social networks will be analyzed. This study will serve to create a theoretical and practical basis for the development of a national information security strategy for Uzbekistan.

The peculiarities of foreign countries in protecting the institution of the presidency, legislative aspects, technological infrastructures, and public relations strategies can serve as an important example in forming an approach adapted to the specific conditions of Uzbekistan. At the same time, the study of international experience will also address such complex issues as ensuring a balance between freedom of speech, privacy rights, and state control.

Part 3 of Article 158 of the Criminal Code "Public insult or slander of the President of the Republic of Uzbekistan, as well as insult or slander of him using the press or other mass media, telecommunication networks or the World Wide Web [1]" is considered the legislative protection of the institution of the presidency, and the experience of foreign countries in this area was studied.

The US experience in protecting the presidential institution from information threats. In the USA, the institution of the presidency, as one of the central institutions of public administration, is important not only from a political and legal point of view, but also in the information space. Against the backdrop of the global development of modern information and communication technologies and the Internet, the protection of the US presidential institution from information threats, the effective organization of online monitoring, and the prevention of insults and slander on social networks have become important components of state security and public trust.

Information threats are one of the factors that pose a serious threat to the stability of state institutions in the modern era. In the context of the USA, information threats directed at the institution of the president manifest themselves in such forms as disinformation, false messages (false information that can be disseminated by political opponents or foreign states, which undermines the president's reputation and undermines public trust), insults (insulting or directly destroying content on social networks directed against the president's personality).

These threats create complex problems in the US democratic system that must be balanced by the principles of openness and freedom of speech. The US experience reflects an approach based on cooperation between government bodies, the private sector, and civil society in ensuring this balance.

Threatening the US President is a federal crime under Article 871, Section 18 of the United States Code. This includes the intentional threat of taking the life of the U.S. President, kidnapping, or causing serious bodily harm.[2].

In 2019, 61-year-old Steven Taubert was sentenced to 4 years in prison under this article. In 2017, he called Senator El Franken's office and said he intended to "hang" former President Barack Obama. The threats were accompanied by racist words. During the court hearing, the prosecutor stated that threats of assassination of current and former civil servants based on racism are not protected within the framework of freedom of speech, which is considered a serious crime.

In the US, the protection of the presidential institution from information threats is carried out by a number of agencies, in particular, the Federal Communications Commission and the Secret Service. The Federal Communications Commission has certain powers to regulate the flow of information on the Internet and assists the President in coordinating appropriate countermeasures against disinformation[3]. The Secret Service, along with ensuring the physical security of the President, is also involved in protecting his personal information resources and identifying information risks.[4].

Organizations defending the institution of the presidency in the United States

1. White House Communications Department

2. Intelligence community

"Google," "Meta" (Facebook and Instagram), "X" (formerly Twitter)

4. PR companies

These organizations strive to protect the official position of the President and monitor negative trends on social networks, analyze posts and comments about the President on social networks in real time, identify information campaigns against the institution of the presidency, and reduce information threats. PR companies, on the other hand, serve to reduce the impact of insults or slander and strengthen the positive image of the President.

Several systems are used to protect the institution of the presidency from information threats. These systems operate within the framework of general national security and cybersecurity, but play an important role in protecting the official communications and image of the president. The National Security Agency and the Federal Bureau of Investigation are the governing bodies of such systems.

PRISM is a classified electronic surveillance program launched by the National Security Agency in 2007 aimed at collecting Internet communications (email, social networks, cloud services). It collects data from major technology companies such as Google, Apple, Meta, and

Microsoft. PRISM is based on Section 702 of the "FISA Amendments Act (2008) " (the Law Amending the Foreign Intelligence Surveillance Act) and allows for the analysis of encrypted data. The system filters and stores data in real time. It is used to identify foreign threats against the institution of the presidency. For example, in the 2016-2020 elections, the interference of Russia and other foreign states was observed through PRISM.

"NarusInsight" is a system used by the National Security Agency for deep packet inspection (DPI). It collects and analyzes large amounts of data in real time. The system is capable of monitoring telephone communications, social networks, and website activity. Used to detect cyberattacks or disinformation against official resources of the Presidential Administration.

"XKeyscore" - a system for searching and analyzing global Internet data of the National Security Agency. Disclosed by Edward Snovden, this system tracks users' internet activities (websites, email, social networks) on a large scale. The system allows monitoring the online activities of any person without a court order. Helps identify potential threats to the president (e.g., from external states or internal groups).

The experience of the Russian Federation in protecting the institution of the presidency from information threats. In the Russian Federation, the institution of the presidency, as the highest body of state power, is considered not only a key element of the political and legal system, but also an important object in the information space. The development of modern information and communication technologies and the widespread use of social networks have further complicated the information threats directed at the institution of the president. These threats directly affect the stability of the state, the public image of the president, and national security. Russia's experience in this area is based on a synthesis of strict control mechanisms, legislative measures, and technological approaches.

The institution of the presidency, as the central symbol of the state, is subject to internal and external information threats. As seen in the US experience, information threats in Russia are carried out through the dissemination of disinformation, insults, and slander. These include information campaigns conducted by Western countries against President Vladimir Putin during the 2014 Ukrainian crisis, the 2022 Russian-Ukrainian war, and content on social networks that is insulting or defamatory towards the President. These negative materials not only exacerbate the political climate but also damage the image of the head of state. In Russia, such incidents are often incited by opposition activists or bloggers.

This type of threat is balanced by the policy of strengthening state control in Russia. The experience of Russia, unlike democratic states such as the USA, demonstrates an approach aimed at protecting the presidential institution through strict regulation of the information space and repressive measures.

In the Russian Federation, the protection of the institution of the presidency from information threats is provided by a number of laws, in particular, the Law "On Information, Information Technologies and Protection of Information," which is the main legal framework for regulating information flows on the Internet. This document, revised in 2019, will allow the isolation of the Russian Internet from external threats and strengthen internal monitoring. Also, according to Article 319 of the Criminal Code, public insult of a representative of the authorities in the performance of official duties or in connection with them is punishable by a fine of up to 40 thousand rubles (5.636,000 soums) or a fine equal to the defendant's salary for up to three months, other income, compulsory labor for up to 360 hours, or correctional labor for up to 1 year. This article also applies to offensive messages on the internet. In 2019, blogger Vladislav Sinica was sentenced to 5 years in prison for an insulting post against the president on Twitter.

In the Russian Federation, information policy is carried out by Roskomnadzor (Federal Service for Control of Communications, Information Technologies and Mass Media). This federal service plays a central role in monitoring content on the Internet, tracking materials against the head of state on social networks using automated algorithms and special programs, blocking and regulating prohibited information.

The Federal Security Service also acts as the main executive body in identifying and combating information threats against the institution of the President[7]. The Service has extensive authority to monitor negative content on the Internet. The restrictions on the protection of the presidential institution established in Russian legislation differ sharply from democratic standards, such as in the USA or the countries of the European Union. In Russia, information threats are considered a matter of national security.

In Russia, monitoring the information space on the Internet is an important part of protecting the institution of the presidency. This process is carried out through the following systems:

"SORM" (System of Operational Search Activities) is a technological infrastructure that forces Russian internet providers to make all user data public for the Federal Security Service. This system allows real-time detection of information attacks or insults against the president.

"Oculus" is a system that recognizes images and symbols, illegal scenes and actions, and analyzes texts in photo and video materials. A Roskomnadzor representative stated that Oculus automatically detects violations such as extremist topics, calls for mass illegal activities, suicide, drug propaganda, LGBT propaganda, and other prohibited activities. The system is also programmed to detect negative images against the President.

Representatives of the industry informed the media that "Oculus" is a system that performs the functions of classifying images and videos in accordance with established requirements, which includes the main types of prohibited content. According to them, "Oculus" operates as a classifier that works with a predetermined set of information sources, in which the content is analyzed in terms of compliance with legal requirements. This system can analyze specific pages of websites or groups and profiles on social networks, but does not collect data, but only classifies them.

In addition, state-controlled media, such as the media group "Russia Today" and the TV channel "Russia Today," are actively involved in protecting the image of the president and disseminating information against disinformation. These agencies conduct counter-propaganda on social networks to neutralize negative anti-presidential tendencies. Russian local social networks, such as "VKontakte," work closely with the government to control content in accordance with government requirements.

The experience of the People's Republic of China (PRC) in protecting the institution of the presidency from information threats. In the PRC, the National People's Congress is the supreme body of state power and elects the Chairman of the People's Republic of China. As head of state, the Chairman of the PRC represents the highest level of state administration. This institution plays a central role in the one-party political system of China, ensuring not only internal political stability, but also protecting the strategic interests of the state in the global information space. China's experience in this area is characterized by a state model based on enhanced control, advanced technological infrastructure, and strict legislative measures.

In China, the head of state is highly sensitive to internal and external threats as a symbol of the political legitimacy of the Chinese Communist Party and state stability. Misinformation disseminated by foreign states or dissident groups within China undermines the authority of the head of state and creates distrust in the leadership of the CCP.

Content on social networks, in particular on platforms such as "Weibo" or "WeChat," which is offensive or slanderous against the head of state, damages the image of the party and causes discontent among the public. China's political system views these threats as actions against state stability and relies on the use of absolute control measures to combat them. This approach, unlike the experience of the USA or Russia, is based on the complete isolation of China's information space and reliance on the local technological ecosystem.

In China, the protection of the head of state from information threats is carried out through strict legislative and institutional frameworks. In particular, the Law "On National Security," adopted in 2015, considers information attacks against the head of state as a threat to national security. This law allows for the assessment of insult or slander as a crime against the state[9]. Also, according to the Law "On Cybersecurity" of 2017, all activities on the Internet are under state control and create a legal basis for eliminating information threats against the head of state. According to the law, internet providers and social media platforms must comply with state requirements[10].

Furthermore, the PRC's Criminal Code does not specify direct threats to the head of state, but Article 105 stipulates that attempting to overthrow state power or a socialist regime with physical or informational threats will result in at least 10 years or life imprisonment.[11].

The Central Commission for Cybersecurity and Informatization of the Communist Party of China, headed by the Chairman of the PRC, plays a central role in monitoring the Internet and coordinating strategies against information threats. The State Internet News Agency is the main body responsible for controlling content on the Internet, blocking prohibited materials, and regulating social media platforms. The agency demands that foreign and local platforms promptly remove anti-government content.

Unlike the principles of freedom of speech in the USA or the partially flexible approach in Russia, Chinese legislation is aimed at bringing the information space under full state control. This system ensures high effectiveness in protecting the head of state.

In China, monitoring information flows on the internet is the most important part of protecting the head of state. This process is carried out through the following mechanisms:

The Great Wall of China (Great Firewall) - China's Internet security system blocks foreign platforms and resources such as Google, Twitter, Facebook, and isolates information flows against the head of state. This system allows for full control of the information space within the state. The government uses advanced AI algorithms to detect insults or slander against the head of state on local platforms such as Weibo, WeChat, and Douyin. These technologies are capable of analyzing billions of posts in real time. These companies also work closely with the state and filter and delete anti-government content in advance. Foreign platforms cannot operate in China.

The "Social Credit System" is also used to monitor citizens' online activities and identify negative behavior against the head of state. Individuals who write offensive posts will lose their social rating, and penalties will be applied for the committed offense.

The experience of European countries in protecting the institution of the presidency from information threats. European countries, mainly in the context of EU member states, use approaches based on democratic principles, transparent legislation, and civil society participation in protecting the institution of the presidency from information threats. The development of modern information and communication technologies and social networks has made information threats to heads of state even more urgent. The experience of European countries, unlike Russia and China, emphasizes the balance of freedom of speech and personal rights, while striving to protect the stability of state institutions.

In European countries, information threats to the institution of the presidency are carried out through disinformation, insults, and slander on the Internet, as in the above-mentioned countries. Such threats are carried out through false information from political opponents, foreign countries, or populist groups, and content on social networks that is insulting and defamatory against the head of state, aimed at undermining the president's political decisions, public trust, and disrupting political stability.

In European countries, the protection of the institution of the presidency from information threats is carried out through a synthesis of common legislation and national laws at the EU level. The General Data Protection Regulation, adopted in 2016, plays an important role in ensuring the information security of public figures, such as the president, along with protecting personal data. According to national legislation, the Law on the Use of the Network in the Federal Republic of Germany (Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken-NetzDG, 2017) officially aims to combat fake news, offensive language, and misinformation on the Internet[13]. This law obliges social media platforms with more than 2 million users to remove "clearly illegal" content within 24 hours and all illegal content within 7 days after posting, otherwise resulting in a fine of up to 50 million euros. Also, in France, the "Avia Law 2020" is aimed at combating disinformation and insults and serves to limit insults against the president.

In addition, the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz) in Germany and the Directorate General for Internal Security (Direction générale de la Sécurité intérieure) in France are actively involved in identifying and countering information threats against the institution of the presidency.

In European countries, monitoring information flows on the Internet is used as an important tool in protecting the institution of the president, but it is carried out within strict legal boundaries. At the EU level, initiatives such as the EU vs Disinfo project monitor foreign disinformation campaigns and help identify information attacks against the presidential institution. Platforms such as Meta, X (Twitter), and Google cooperate with the government to remove illegal content against the president in compliance with EU law. Fact-checking organizations such as Correctiv and EU DisinfoLab play an important role in identifying disinformation against the presidential institution.

In conclusion, it can be said that the institution of the presidency, as an important symbol of state sovereignty and public stability, plays a central role in ensuring national security. Article 158 of the Criminal Code of Uzbekistan serves to protect this institution by law. The experience of foreign countries - the balanced approach of the USA, the experience of

Russia, the isolation model of China, and the democratic principles of Europe - serve as a theoretical and practical basis for Uzbekistan in the formation of national information security.

References:

1.Criminal Code of the Republic of Uzbekistan. https://lex.uz/docs/111453.
2.United States Code of Laws. https://www.law.cornell.edu/uscode/text/18/871.
3.Official website of the Federal Communications Commission. https://www.fcc.gov/.
4.Official website of the United States Secret Service. https://www.secretservice.gov/.
5.Federal Law of the Russian Federation "On Information, Information Technologies and Information Protection." https://www.consultant.ru/document/cons_doc_LAW_61798/.
6.Criminal Code of the Russian Federation. https://www.consultant.ru/document/cons_doc_LAW_10699/.
7.Official website of the Federal Security Service of the Russian Federation. http://www.fsb.ru/fsb.htm.
8."Media: Roskomnadzor launched the intelligent online content tracking system Okulus." https://habr.com/ru/news/716464/.
9.Law on National Security of the People's Republic of China. https://www.wipo.int/wipolex/ru/legislation/details/15752.
10.Law on Cybersecurity of the People's Republic of China. https://itp.cdn.icann.org/ru/files/government-engagement-ge/ge-010-31jan22-en.pdf.
11.Criminal Law of the People's Republic of China. https://www.cecc.gov/resources/legal-provisions/criminal-law-of-the-peoples-republic-of-china.
12.General Data Protection Regulation data. https://gdpr.eu.org/full/.
13.Law on Improving Law Enforcement on Social Networks. https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html