MANAGING CRITICAL DATA FOR NATIONAL SECURITY ASSURANCE

[a]NATALIIA VARENIA, [b]OLEKSANDR ROZVADOVSKYI, [c]VITALII KHODANOVYCH, [d]TETIANA DAVYDOVA, [e]IVAN DRALIUK

[a,b,c,d]National Academy of Security Service of Ukraine, Kyiv, Ukraine.
[e]Private researcher, Ukraine.
e-mail: [a]vareniia@ukr.net, [b]rozvsa@gmail.com, [c]v.hodanovych@gmail.com, [d]Tatada2009@gmail.com, [e]ap0091994@gmail.com

Abstract: The article examines the issue of maintaining the state's information sovereignty as a necessary condition for ensuring its national security. It considers the concepts of the research apparatus and provides scientific interpretations of the terms "information security", "information warfare", "destructive propaganda", "information confrontation" and others. It is noted that protecting the country's information space from external harmful influences is a fundamental task of the state, which relates to its national interests. The use of sensitive information to ensure national security is analysed. The study and optimisation of information security as a factor in the fight against propaganda, using the experience of different countries, are explored. The subject of the study is sensitive information, which is a determining factor in the development of information security in various countries worldwide. A retrospective analysis of different strategies for optimising the use of sensitive information was conducted. The issue of overcoming propaganda through a communicative approach was studied. Historical and logical analysis methods, comparison, expert assessments, system analysis, and forecasting were used. The research materials included developments, ideas, and other intangible assets that can help humanity in the fight against propaganda. Available information in the fields of operational search, counterintelligence, and intelligence activities, operational-technical measures, protection of personal data of employees/military personnel, activities of participants in anti-terrorist operations and military actions, international cooperation, internal audit, financial reporting, civil protection, territorial defence, housing, and communal services were analysed. At the same time, a unified approach to defining the categories of information requiring restricted access in these areas is practically absent.

Keywords: Information security, classified information, confidential information, media, destructive propaganda, disinformation, ideological expansion.

1 Introduction

Digitisation and the creation of modern technologies allow for the management of vast data flows, the creation of various types of information weapons, and the execution of manipulative actions in the global media space. This makes the issue of ensuring information security in the world particularly relevant. This phenomenon is especially significant because it is inextricably linked to the fundamental concept in political science known as "national security". Protecting the country's information space and sensitive information from ideological attacks and cyber sabotage and preventing attempts by external forces to exert destructive influence on public opinion are essential tasks for the state and fall within its national interests.

The definition of "sensitive information" can vary depending on the context. However, generally, it can be characterised as information whose access is restricted due to its importance for ensuring national security, protecting privacy, or other critical interests. Sensitive information refers to data or knowledge restricted because of its critical importance in ensuring national security, protecting privacy, or other significant interests. It requires special measures for controlling access, storage, and transmission, as well as regulation at the legislative level to prevent unauthorised disclosure or use that could harm individuals, organisations, or the state. Such a definition emphasises the importance of legislative regulation and transparent criteria for categorising and protecting sensitive information. The status of sensitive information in Ukraine is not clearly defined at present.

The information security strategy is essential in Ukraine's information policy, and its legislative foundations have been established. However, the current strategy is more focused on preventing and averting threats of a technical nature. The main activities of the authorised structures are related to protecting the country's information systems and resources. At the same time, there is no mechanism for countering information-psychological wars, which can inflict material and reputational damage on the state. The lack of coordinated work in this area makes Ukraine vulnerable to modern challenges (such as military aggression from Russia), including ideological expansion. With the rapid development of the Internet and computer technologies and the virtualisation of the global information space, such favourable conditions require prompt measures to preserve the state's information sovereignty.

2 Literature Review

An attribute of social reality is communication, but there is information whose access is restricted and controlled to prevent unauthorised disclosure that could harm personal, organisational, or state interests (Mikhailova, 2023). Aristotle characterised information and communication as a higher form of human interaction, implying the interaction of individuals (as part of society) with the state (as the societal whole) (Bashuk, 2019). Later, the American researcher Lasswell referred to human communication as an "open forum for the continuous discussion of issues of mutual tolerance and access to the basic values of life" (Lasswell, 1927). The communicative approach to understanding politics is also central in the works of German researchers Arendt and Habermas, who believed that communicative activity creates and sustains a political community (Mikhailova, 2022). All contemporary communication concepts emphasise human beings' informational and communicative nature and social relations (Zaverbnyi, 2022; Turchyna et al., 2023).

The importance of social communication in governance processes called the "nervous system of public administration" is sensitive to changes and involves receiving, selecting, evaluating, and processing information, decision-making, implementation, and feedback (Hurkovskyi, 2004). In the monograph "Public Administration and Administration in the Information Society", it is noted (Usov, 2014; Zaduvailo, 2017) that management communications are a universal system that "reproduces the orderliness of the management social process, organises and actualises the management process in the complex interaction of administrative and political organisations with society" (Vasylenko & Maslak, 2010). The authors (Vasylenko & Maslak, 2019; Vyslotska, 2016; Vyslotska, 2018) described mechanisms for access control, encryption, and special conditions for data storage and processing. The article (Ihnatenko, 2022) describes norms defining sensitive information's status and establishing rules for its protection and use.

3 Aims

Analysing the use and justification of sensitive information in the context of ensuring state security. Research and optimisation of information security as a factor in the fight against propaganda, using the experience of different countries.

4 Materials and methods

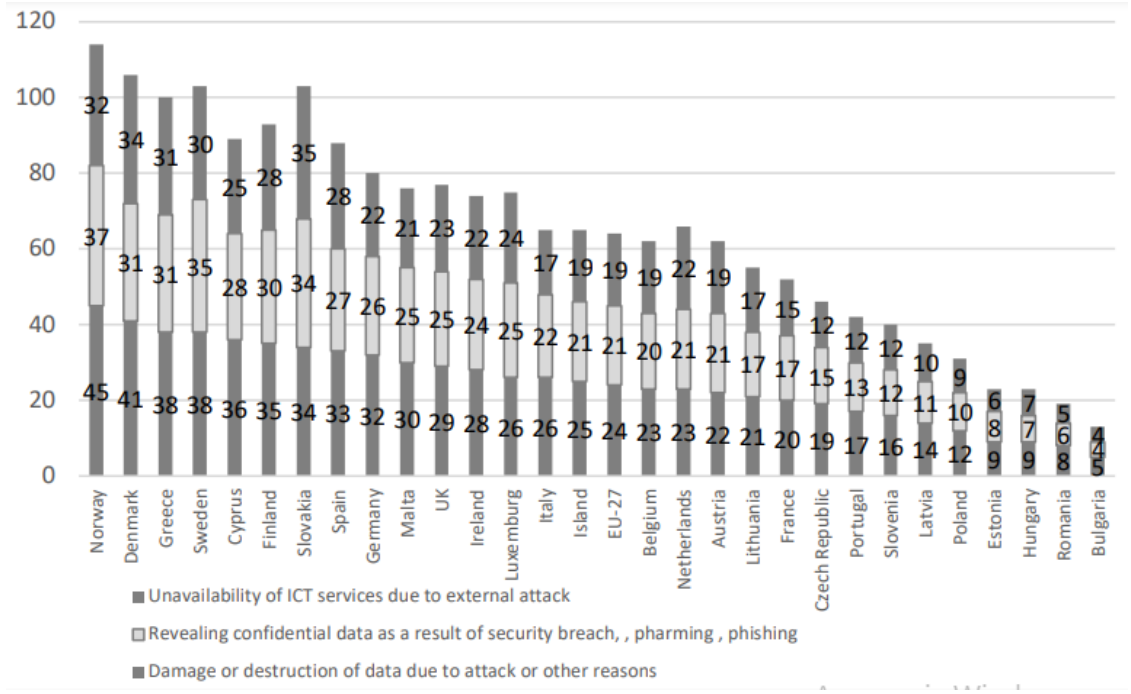
The study's subject was sensitive information, a determining factor in developing information security in various countries worldwide. It conducted a retrospective analysis of different strategies for optimising the use of sensitive information. The study addressed the issue of overcoming propaganda through a communicative approach. Historical and logical analysis and comparison methods, expert evaluations, systems analysis, and forecasting were utilised. The research materials included developments, ideas, and other intangible assets that can help humanity in the fight against propaganda.

5 Results

The preservation of the sovereignty and territorial integrity of a country is a fundamental task of the state in the current conditions. This provision is closely intertwined with another equally important aspect of state activity — the field of security. The issue of security in modern scientific discourse should primarily be considered in the political realm. This is because ensuring security requires the authorities to make

appropriate decisions and create organisational and legal mechanisms for their implementation. The report on such measures is called state policy in the security field, as shown in Figure 1, illustrating the risks of sensitive information leaks from institutions.

Figure 1: Percentage of Enterprises in EU Member States by Type of Sensitive Information Leakage Risk



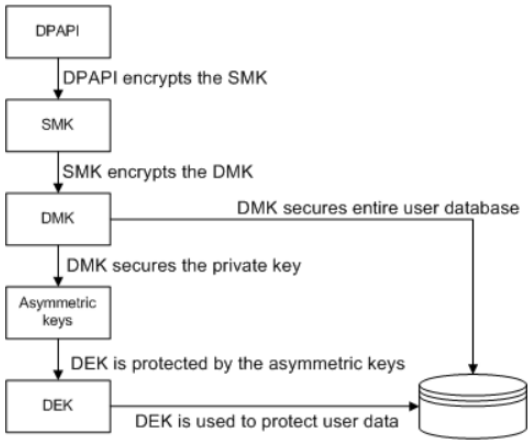
The world in the 21st century is not safe. The conflict in international relations is increasing, leading to heightened tensions across the global space. The geopolitical confrontation between significant power centres today is mainly informational. Traditional military actions, acts of aggression, and sabotage have been shifted to the media field. The endless flow of information generated by social networks on the Internet is increasingly being used as a weapon of mass destruction. Information warfare has already been recognised as an extremely dangerous type of ideological weapon, as it can affect not only human or public consciousness but also the political decision-making system. The widespread use of this modern and most effective propaganda tool has intensified the trend of information warfare on a global scale (Kovalov & Leonov, 2017).

It should be noted that thanks to the development of virtual-communicative technologies, current information wars are becoming increasingly sophisticated (Radchenko et al., 2023). Information warfare is aimed at disrupting the opposing side's information security and creating chaos at the centre of political decision-making in a country. At the same time, information warfare is a set of measures to influence mass consciousness, change people's behaviour, and impose goals that are not in their interest. This involves manipulating public opinion (Chukut, 2021).

Given Ukraine's aspiration to integrate into the Euro-Atlantic and North Atlantic space and, accordingly, into the legislative and legal framework of the EU and NATO, a series of reforms should be carried out. These reforms, particularly regarding the security situation in document circulation, are becoming increasingly relevant and should be discussed in public control institutions over the activities of state institutions in Ukraine (Verbenskyi, 2020).

A decision must be made that will consider the interests of society, individual citizens, and the state in this matter by developing and enshrining in legislation specific approaches — both the definition of sensitive information as a category of information and the preliminary classification of such information as sensitive. There is a need to systematise such a category (type) of information as sensitive (Figure 2).

Figure 2: Transparent Data and Sensitive Information Encryption Hierarchy



Currently, such information circulates (Figure 2) within the security sector (movement of military goods, logistics, temporary deployment (location, movement) of military formations, equipment, issues of securing security institutions, critical infrastructure objects), the disclosure (highlighting, posting) of which could be used to inflict significant harm on state security and, accordingly, would require the adoption of additional measures to eliminate the risks that arise (Korchenko et al., 2008).

Countering such threats and effectively managing information becomes one of the main conditions for ensuring national security (Konchuk, 2019). An encroachment on the country's information security is equivalent to a threat to its national interests. Ukraine's policy in the field of information security is outlined in Article 21 of the Law of Ukraine, "On State Secrets", and Article 9 of the Law of Ukraine, "On Access to Public Information". The approved order of the Central Administration of the Security Service of Ukraine dated 23.12.2020 No. 383 is interpreted as the state of protection of the interests of the individual, society, and the state in the information sphere. From

this, the state protects society and each citizen from destructive information (Vynohradov & Mykhailutsa, 2019).

The balanced interests of the individual, society, and the state form national interests (Shamsutdinov, 2002). This means that the issue of state information security is inextricably linked with the protection of national interests (Halushka & Tikhonov, 2021). Based on the current realities of the global political system, information security must also be considered an essential component of the national security strategy (Chernov, 2017). Destructive information campaigns, which are accompanied by the creation of fake messages, deliberate distortion of media content, and substitution of reliable information, must be addressed.

Ukraine often becomes a target of information attacks by Russia, which destabilise the socio-political situation in the country, incite national hatred, and divide society (Chmyr et al., 2023). To counteract destructive actions promptly, the state must organise its information security. In science, this is referred to as the policy of information counteraction, which is one of the critical elements of information warfare, along with information influence (Primush et al., 2023).

6 Discussion

In Ukraine and worldwide, specific experience has been accumulated in ensuring information security, and this process's legislative, organisational, and institutional foundations have been established. However, the activities of authorised structures are more focused on protecting information systems and networks of strategic importance. At the same time, the issue of countering ideological expansion remains on the periphery of their attention. The authorities of most of the countries discussed in the article do not carry out comprehensive, coordinated work to combat fake news and destructive propaganda, which poses a real threat to national interests. The article examines specific cases of promoting Russian propaganda narratives in the media segment. It highlights the vulnerability of Ukraine's information security system. It provides practical recommendations for addressing them, including creating an early warning system for information attacks, cyber sabotage, and external manipulative actions, with a built-in mechanism for promptly responding to such threats. The article also discusses and examines the improvement of the relevant legislative framework and the adoption of a comprehensive concept of information security for Ukraine, as well as for global leaders China and the USA, which involves enhancing the capacity of domestic media to counter destructive propaganda.

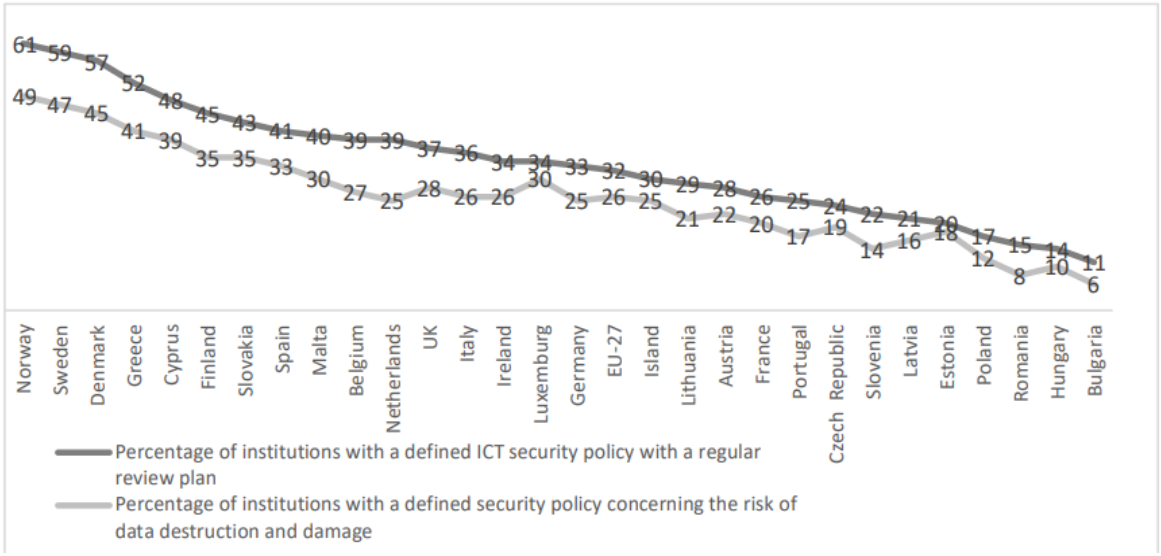
Analysing the described results, the following classification of confidential information can be proposed based on the following criteria (Hren et al., 2023).

1. By ownership rights:
   a) State;
   b) Private;
2. By access rights:
   a) During the performance of official duties by officials;
   b) By the owner and persons to whom this right has been granted;
3. By field of application:
   a) Commercial;
   b) Banking;
   c) Taxation;
   d) Legal;
   e) Judicial.

The processing of sensitive information requires caution. Sometimes, the law prohibits processing such data, even when consent has been given. In other cases, the law requires special measures during processing (for example, it requires encryption before transmission over open networks or mandates its concealment).

Let us analyse the international experience of leading countries (Figure 3). We can see that state secrets in China currently cover various areas—from decision-making by the government and the Communist Party to military and diplomatic activities, as well as economic development, science, and technology. The updated law, which was lobbied for, requires state institutions and working units to protect information "that is not a state secret but may cause certain adverse consequences if leaked".

Figure 3: Percentage of Institutions in EU Member States with a Formal ICT Security Policy (Eurostat, 2020)



Uzbekistan's policy in the field of information security is outlined in the law "On Principles and Guarantees of Freedom of Information" dated 12 December 2002. In this document, the concept of "information security" is interpreted as the state of protection of the interests of the individual, society, and the state in the information sphere. This implies that the state must protect itself and society from destructive information and each citizen separately. It is worth noting that in US legislation, there is no single normative legal act on state secrets similar to that in the legislation of other countries, including the corresponding legal system. Executive Order No. 13526, issued by the President of the USA in 2009, established the classification system for classified information currently in force in the USA.

Table 1: Laws or Regulations of Countries Regulating the Use of Sensitive Information for State Security

Country	Laws and regulations
France	The classification of secret and sensitive information is defined in Article 413-9 of the Constitution. In particular, three levels of military classification (secrecy marks) are declared.
Germany	Section 97 contains the concept of a 'criminal offence' for disclosure of sensitive information.
Japan	The country's Constitution, section 13, part 2 of the Code, contains a provision that defines criminal liability for disclosure of secrets, including sensitive information.
China	The Law of the People's Republic of China on the Protection of State Secrets.
EU	In the European Union, there is a Recommendation No. 2 (2002) on access to official documents held by public authorities public authorities.
Ukraine	Articles 328, 329, and 422 of the country's Constitution regulate the use and unlawful dissemination of classified information.
USA	Executive Order 13526 by US President Barack Obama.

Thus, in every sphere of social relations, appropriate procedural requirements for the circulation of information containing personal data must be developed based on the basic legal requirements defined in the particular law and regulations. The identified features of the legislation of the studied countries, as described, will help improve Ukraine's legislation in the field of information protection (Table 1).

7 Conclusion

The available information in the fields of operational search, counterintelligence, and intelligence activities, operational-technical measures, protection of personal data of employees/military personnel, activities of participants in anti-terrorist operations and military actions, international cooperation, internal audit, financial reporting, civil protection, territorial defence, and housing and communal services has been analysed. At the same time, a unified approach to defining categories of information that require access restrictions is practically absent in these areas. The lack of a unified approach to defining categories of information that meet the requirements of Article 6 of the Law of Ukraine "On Access to Public Information" and require access restrictions may lead to situations where the same information has different statuses in different agencies.

In the current conditions of resisting armed aggression by Russia, considering that many of the aggressor's actions take place in the information sphere, the provisions of the Law of Ukraine "On Access to Public Information" do not fully reflect the need to establish restrictions on sensitive information. At the same time, there is an apparent discrepancy between specific departmental lists of information that constitute official information and the current legislation in the information field.

Literature:

1. Mikhailova, O.: Communication strategies in public management and administration: state and problems in implementation. *International Science Journal of Management, Economics & Finance*, 2023. 2(2), 93-99. https://doi.org/10.46299/j.isjmef.20230202.10
2. Bashuk, A. I.: *Communication strategies of state power in the conditions of the information society: a monograph.* Kamianets-Podilskyi: Ruta Printing House LLC, 2019.
3. Lasswell H.: *Propaganda Technique in the World War*. USA: MIT Press Classic, 1927.
4. Chernov, S. (Ed.).: Public management and administration in the conditions of the information society. Domestic and foreign experience: monograph. Zaporizhzhia: ZDIA, 2017.
5. Mikhailova, O. G.: Modern communication strategies in public management and administration under conditions of uncertainty. *Problems of modern transformations. Series: law, public administration and management*, 2022. 5. https://doi .org/10.54929/2786-5746-2022-5-02-03
6. Zaverbnyi, A.: Communication strategies: problems and prospects of formation and implementation in the context of European integration. *Innovation and Sustainability*, 2022. 1, 13-19. https://doi.org/10.31649/ins.2022.1.13.19
7. Turchyna, M. P., Boyko, I. A. and Tur, O. V.: The choice of communication strategy at different stages of brand development as a component of the information flow of the enterprise. *Market economy: modern theory and practice of management*, 2023. 213(52), 249-263. https://doi.org/10.18524/2413-9998.2022.3 (52).275808
8. Chukut, S. A.: Communication strategies in public management and administration: foreign and Ukrainian experience. *Investments: practice and experience*, 2021. 12, 72-79. http://nbuv.gov.ua/UJRN/ipd_2021_12_14
9. Usov, D.: Criminal law characteristics of disclosure of state secrets. *Criminal law and criminology, criminal enforcement law*, 2014. 18.
11. Zaduvailo, O.: The problem of defining the concept of "Sensitive information" in the context of ensuring the information security of the state. *Scientific Bulletin*, 2017. 116, 280-285.
http://nbuv.gov.ua/UJRN/gileya_2017_116%281%29_70
12. Shamsutdinov, O. V.: Liability for disclosure of state secrets under the criminal legislation of Ukraine. Kyiv, 2002. p. 245.
13. Vasylenko, D. P. and Maslak, V. I.: Legislation of the world's leading countries in the field of information protection. *Visnyk KDU im. M. Ostrovskoho*, 2010. 2(61), 1, 128−132.
14. Verbenskyi, M. H., Kulyk, O. H. and Naumova I. V.: *Criminal situation in Ukraine: main trends. Monograph*. Kyiv: Yurinkom Inter, 2020.
15. Vynohradov A. K. and Mykhailutsa M. I.: Political and legal analysis of criminal liability for the disclosure of state secrets and for the disclosure of information of a high nature, constituting a state secret, or the loss of documents or materials containing such information. *South Ukrainian legal journal*, 2019. 46–49. https://doi.org/10.32850/sulj.2019.3-11
16. Vyslotska, T.: Protection of secrecy in the history of criminal legislation of Ukraine. *Jurnalul juridic naţional: teorie şi practică,* 2016. 2(1), 108−112.
17. Vyslotska ,T. Yu.: *Criminal law protection of secrets in Ukraine*. Lviv, 2018.
18. Perepelytsia, H.: *Ukraine's military security is on the verge of millennia. Monograph*. Kuiv: Stylos, 2002.
19. Halushka, V. and Tikhonov, H.: Peculiarities of legal regulation of protection of state secrets in Ukraine and abroad. *Enterprise, economy and law*, 2021. 1, 205–209. https://doi.org/10.32849/2663-5313/2021.1.36
20. Hurkovskyi, V. I. *Organizational and legal issues of interaction of state authorities in the field of national information security*. Kyiv, 2004. p 205.
21. Ihnatenko, I. V.: *The right to freedom of speech: information as a weapon in the fight against the aggressor. Legal means of combating crimes against the foundations of national security in conditions of military aggression: materials of the round table*. KPI by I. Sikorskyi, Kyiv, 2022. 107–111.
22. Kovalov, K. Ye. and Leonov, B. D.: Ensuring the protection of state and official secrets in the field of operational and search activity according to the legislation of individual states: a comparative analysis. *Information and law*, 2017. 1(20), 112–122.
23. Konchuk, N. S.: Criminal liability for treason. Abstract. *Criminal law and criminology; criminal executive law*, 2019. 18.
24. Korchenko O. H., Arkhypov O. Ye. and Dreis Yu. O.: *Assessment of damage to the national security of Ukraine in case of leakage of state secrets: monograph*. Kyiv: NASB Ukrainy, 2014. p 332.
25. Primush, R., Chmyr, Y. and Kravtsov, M.: Information Wars: Historical and Comparative Analysis, Specifics and Factors of Actualization in the Modern World. *Contributions to Political Science*, 2023. 1367, 259-272.
26. Hren, L., Karpeko, N., Kopanchuk, O.: Substantive Essence and Components of the Societal Phenomenon "Information Security" in the Age of Information Society. *Contributions to Political Science*, 2023. 1367, 75-91.

27. Chmyr, Y., Deineha, M. and Shchepanskiy, E.: Tools for Counteracting Information Aggression Use of Elements of Information War in Ukraine. *Contributions to Political Science,* 2023. 1367, 285-299.
28. Radchenko, O., Nepomniashchij, O. and Shkurat, I.: Information Weapons: Forms and Technologies of Modern Information Wars. *Contributions to Political Science,* 2023. 1367, 273-284.
29. Eurostat. *ICT security in enterprises 2018 – 2019,* 2020.

Primary Paper Section: A

Secondary Paper Section: AG