Journal of Political Science: Bulletin of Yerevan University
2024, VOL. 3, NO. 2 (8), September, 122-129
https://doi.org/10.46991/JOPS/2024.3.8.122

REINHOLD, THOMAS. 2024. TOWARDS A PEACEFUL DEVELOPMENT OF CYBERSPACE: DE-ESCALATION OF STATE-LED CYBER CONFLICTS AND ARMS CONTROL OF CYBER WEAPONS. SPRINGER VIEWEG, WIESBADEN. XXVIII, 361 PP. https://doi.org/10.1007/978-3-658-43951-4.

REVIEW BY:

SVETLANA JILAVYAN[*]
Russian-Armenian University

HAYKUHI MKRTCHYAN[**]
Yerevan State University

Abstract
The book analyzes cyberspace issues and its global infrastructures, which are essential for the global political system, civiliarchy, political economy and effective administration of political processes. In the modern context, cyberspace is becoming an intelligence and military operational domain for various actors. According to the author, this is evident in the establishment of military cyber departments and the integration of cyberspace into the security and defense strategies of small and large states. Current military technologies as well as established instruments of transparency, de-escalation and arms control measures do not work for cyberspace due to its specific technical characteristics. In this context, it is important for international organizations to achieve de-escalation of state-led conflicts in cyberspace, but in reality it is simply impossible to develop arms control over cyber weapons. In this context, an effective system of classification of cyber weapons, an approach to mutual reduction of stocks of vulnerability and non-interference in cyber conflict are also important.

Keywords: cyberweapon, cyberpeace, military operational area, arms control, disarmament, peace building, peaceful development, cyberwar, confidence building measures, cyberattacks.

[*] **Svetlana Jilavyan** is a PhD candidate of the Chair of World Politics and International Relations at Russian-Armenian University. Email: svetlana.jilavyan@gmail.com. ORCID: https://orcid.org/0000-0003-2490-076X.

[**] **Haykuhi Mkrtchyan** is a PhD in Political Science, Associate Professor of the Chair of Political Science of the Faculty of International Relations at Yerevan State University. She is a Senior Officer of the International Cooperation Office at Yerevan State University. Email: h.mkrtchyan@ysu.am. ORCID: https://orcid.org/0000-0002-3825-3295.

Received: 26.05.2024
Revised: 12.07.2024
Accepted: 25.07.2024

This book analyzes the factors of peaceful development of cyberspace, various dimensions of cyber conflicts and cyber weapons that affect information and communication technologies and the transformation of international relations. A striking example of this are modern conflicts, the nature of which largely depends on the factor of cyberspace and information and communication technologies (Reinhold 2024, 3-22, 23-27). Due to the increasing role of cyberspace, an international information space was formed. With the advent of the Internet, the methods and timing of information dissemination have changed significantly. In about a second, information can be accessed almost anywhere in the world. However, modern cyberspace is characterized by a growing number of dividing lines and the introduction of information boundaries.

Cyberspace has transformed into a new field of confrontation and a new space for geopolitical competition. The boundary between the virtual and real worlds is becoming increasingly mobile, which means that confrontation in the digital environment is capable of transforming into a conventional war (Reinhold 2024, 29-36, 37-41). Cyberspace is becoming a new battlefield, just like land, sea and air. Escalation of contradictions in the digital environment can lead to escalation in the real world and conflict using not only information weapons, but also kinetic weapons, as well as weapons of mass destruction. Relations between countries in cyberspace and in the sphere of information and communication technologies are non-linear and often complex, confrontational (Reinhold 2024, 43-48, 51-72).

Earlier historical precedents show that the emergence of new technologies, such as nuclear weapons, encouraged countries to agree on confidence-building measures or create arms control systems, set limits on the development of offensive military technologies and create safeguards to prevent unintentional conflicts and their escalation. However, uniform international legally binding norms preventing cyber conflicts have not yet been adopted, let alone the creation of a system of control over cyber weapons. In this context, it seems important to maintain a dialogue between countries on the issues of the safe use of cyberspace and cyber weapons (Reinhold 2024, 73-84, 85-106). Only in this way can international security and stability be guaranteed. At the same time, states must have equal rights in this process. It is necessary to maintain channels for dialogue at both the bilateral and multilateral levels, primarily within the UN, which determines the practical relevance of the chosen research topic of this book.

The relevance of the study from an applied point of view is determined by the practical focus on developing proposals for the effective promotion of national interests of countries in the digital environment and coordinating elements of the future international legal regime for regulating the digital environment, as well as creating a mechanism for restrictive cyber measures and cyber restrictions at the UN level, approved by the UN Security Council.

The relevance of the study from the point of view of the development of international relations is determined by the insufficient study of the problems of cyberspace in the context of interaction between countries on digital issues, especially against the background of the aggravation of political relations at the bilateral level, as well as the need for an in-depth scientific comparative analysis of the approaches of the

United States and other Western countries in the digital environment. In addition, the problem of cyber sanctions is relevant due to the fact that it is studied by a small number of experts; as a rule, the focus of researchers is sanctions in general (Reinhold 2024, 107-137, 141-172).

The theoretical and practical significance of the study of cyberspace policy and counteraction to cyber terrorism is caused by the need for a deep understanding of the theoretical, organizational and political foundations for the development and implementation of this type of policy and is determined by the following circumstances (Reinhold 2024, 173-183, 185-196).

Firstly, one of the main factors in the development of the political system is the use of cyberspace and information. In modern conditions, they play a key role in the functioning of not only public and state institutions, but also the life of each person. Computers and information and communication systems are used in all spheres of human and state activity. This is ensuring national security, providing public services in the field of health care, education, housing and communal services, air and rail transport management, trade, finance, as well as interpersonal communication, etc.

The influence of global networks on the social and political development of society is multifaceted and contradictory. On the one hand, they contribute to the development of human potential through cyberspace and computer games, educational and entertainment programs, interactive television, and electronic press (Reinhold 2024, 197-226). Global networks influence the electoral behavior of political actors, the process of organizing and conducting election campaigns, the mechanisms of communication between the authorities and society, the presentation and defense of their interests by political actors (Reinhold 2024, 227-238). By modifying the system of relationships and interactions between civil society institutions and the state, global networks contribute to the formation of a constructive dialogue between them. On the other hand, the rapid development of cyberspace and the information and communication sphere has led to the emergence of new types of computer crime and computer terrorism. Thousands of network users, not only individuals, but entire states can suffer from the activities of cyber terrorists in virtual space. The number of crimes committed in cyberspace is growing proportionally to the number of computer network users (Reinhold 2024, 241-268). Modern terrorist organizations actively use information and communication technologies, along with traditional means. At the same time, the transition time from a threat to a real act of cyberterrorists is significantly reduced.

Secondly, the relevance of studying this type of policy increases in the context of the increasing complexity of the social structure and political life of society, which radically modifies the channels of articulation and aggregation of interests of actors in socio-political interaction, creating a danger for the formation of diametrically opposed approaches to assessing political events. The danger of destructive phenomena increases in the context of a decline in the level of legitimacy of power, public trust in political institutions in general and the policies of the ruling elite in particular. These and other phenomena to some extent initiate cyber-terrorist activity, since they often lead to instability in the functioning of the social and political system, inconsistency in the actions and interactions of political institutions and individuals whose functions are associated with the development and implementation of policies to counter this phenomenon. The emergence of a new type of terrorism threatens the security of the individual, society and the state at all levels of politics, which necessitates its comprehensive study.

Thirdly, the effectiveness of the policy of countering cyber terrorism depends not only on the stability of the functioning of the social and political system, the development of state control over processes in the virtual space, compliance with legal norms in this segment of domestic and foreign policy, the development of the legal culture of the elite and the population, etc. In many ways, it is due to the presence of the ruling elite and representatives of special services of the tools for understanding the analyzed phenomenon, which is impossible without its conceptual understanding, expansion and enrichment of the methodological palette due to approaches that allow the most complete study of the essence and features of the new type of terrorism, as a political phenomenon (Reinhold 2024, 269-299).

In contrast to the position of Russia, China and Iran, the United States and other Western countries always advocate for ensuring international information security at a universal level, which is confirmed by the introduction of draft resolutions of the same name to the UN General Assembly for discussion. In many European and international legal doctrines, the prevailing view is that the powers of the United Nations as a universal international intergovernmental organization in regulating cyberspace and, in particular, international information security, should be revised.

Given the fact that in the 21st century a new branch of international law has emerged, namely cyberlaw, the law of the Internet, fundamental issues affecting the practical aspect of regulating the use of cyberspace remain unresolved. Is it possible in the current circumstances to agree on and adopt a universal convention devoted to the obligations of states? What is the U.S. approach to cyberspace at the international and national levels? Are there prerequisites for finding a compromise in international legal relations on this issue? What influence does U.S. legislation have on the formation of the agenda in the field of international information security at the UN level? Resolving these fundamental issues will help ensure the use of cyberspace for peaceful purposes, in the interests of all its users and avoid its use for military purposes. In connection with the above, there is no doubt about the relevance of studying the essence of the modern international legal regime of cyberspace from the point of view of the United States of America. Is this space still the so-called ‘gray zone’ in which each actor of international law, possessing the appropriate technological advantages, develops legal regulation not only in national but also in international legal systems? In modern realities, the issue of maintaining the decisive role of the UN in considering issues of legal regulation of cyberspace as a leading platform is recognized as particularly controversial.

Based on the analysis of approaches used in the United States to define the cyberspace regime, the following features can be identified: 1) the technical component of most terms (e.g., cybernetic operation, cybernetic attack, etc.); 2) the presence of conditional boundaries when conducting ‘preventive protection’ of the state; 3) expansion of the list of actors endowed with powers in cyberspace; 4) the use of not only the framework of international law, but also legal structures characteristic of the American legal system.

The history of the formation of arms control systems demonstrates that the arms race is better regulated by binding agreements that help reduce tensions and increase the transparency of state actions. The emergence of new types of cyber weapons, the development of new military technologies inevitably led to decisions on the need to control and limit their use (Reinhold 2024, 301-317).

Modern military cyber activities in the war of Russia against Ukraine and the efforts of the United States and Western countries to contain cyber wars demonstrate the need for arms control and its applicability to cyberspace. Experts note a number of difficulties in creating a cyber weapons control system. *Firstly*, the problem of establishing the person responsible for committing cyber attacks, the so-called 'problem of attribution of cyber attacks', is noted. These problems have been successfully resolved for the most part thanks to strict prohibitions, their strict observance, strict reporting requirements, as well as thanks to international monitoring systems and high fines for fraud. *Secondly*, it is noted that a cyber treaty may quickly become obsolete. However, arms control systems, as a rule, face the problem of the speed of technological progress, therefore, states include in most international normative legal documents on arms control provisions for holding periodic review conferences, within the framework of which the possibility of updating the terms of previously concluded agreements is laid down. Thus, states parties to the Biological Weapons Convention (BWC) have held more than 7 review conferences since the BWC entered into force in 1975, most of which focused on strengthening verification and review of the BWC, taking into account new scientific and technological developments. The cyber agreement will most likely require revision to adapt to technological changes. If it includes clauses prohibiting specific actions, such as first use of cyber weapons or the use of cyber weapons against civilian targets, the problem of adapting to technological change may be less serious than critics claim. *Third*, it is argued that it is too early to conclude an international cyber treaty, since digital technologies have not yet been used for a long time and states do not yet know all the intricacies, capabilities and limitations of their use. However, historically, states have acted far-sightedly, for example, concluding the Outer Space Treaty in 1967, which prohibits the placement of weapons of mass destruction in space. It seems that a similarly far-sighted agreement is possible for cyberspace.

Modern cyber weapons are available to a wide range of actors and are easy to conceal. However, we can draw on the experience of weapons control systems such as chemical and biological weapons, which set strict and unambiguous rules against their use in principle. It is important that the use of such weapons is completely prohibited, which is also true for cyber weapons. States must be sure that cyber attacks will lead to serious and inevitable consequences, such as sanctions. To this end, it is necessary to conclude a legally binding cyber treaty containing the relevant rules of conduct for states in the digital environment and liability for violating them. Confidence-building measures, which are currently used by states, contribute to the development of interstate dialogue and represent a first step towards mitigating destabilizing effects in the digital environment. It seems that the UN, NATO, the Council of Europe, the

OSCE, the EU and other intergovernmental organizations can agree on confidence-building measures in the digital environment, since their goal is to exchange information, not to change the balance of power. Confidence-building measures in the digital environment are important because they help ensure stability and transparency in an area characterized by secrecy and uncertainty. However, it is important to note that the cyber arms race is best contained through legally binding normative legal documents. Thus, both during the Cold War and in the full-scale war of Russia against Ukraine since 2022, strategic nuclear deterrence based on the principle of mutually assured destruction and the arms control system neutralized the risk of a nuclear conflict, which is also true in the digital environment. Negotiations on concluding a cyber agreement between Russia and the United States will be associated with a number of difficulties, including due to differences in interests and the geopolitical situation. However, as history shows, its conclusion is not impossible. At present, the main obstacle is Russia's war against Ukraine and the continuation of this aggressive full-scale war, as well as the counteraction of Russia due to their intention to use their current strategic advantages in the digital environment and maintain maximum freedom of action in this area.

Funding statement

This research was funded through a Social Sciences internal scientific grant from Yerevan State University, and the opinions, findings and conclusions or recommendations expressed herein are those of the authors and do not necessarily reflect those of Yerevan State University.

Conflict of interests

The authors declare no ethical issues or conflicts of interest in this research.

Ethical standards

The authors affirm this research did not involve human subjects.

References

Reinhold, Thomas. 2024. Introduction. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 3-22. https://doi.org/10.1007/978-3-658-43951-4_1.

Reinhold, Thomas. 2024. Findings Part A: Concepts and Challenges of Peace in Cyberspace. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 23-27. https://doi.org/10.1007/978-3-658-43951-4_2.

Reinhold, Thomas. 2024. Findings Part B: Threats From Malicious Activities in Cyberspace and Technological Trends. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 29-36. https://doi.org/10.1007/978-3-658-43951-4_3.

Reinhold, Thomas. 2024. Findings Part C: Approaches for the Peaceful Development of Cyberspace. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 37-41. https://doi.org/10.1007/978-3-658-43951-4_4.

Reinhold, Thomas. 2024. Discussion and Conclusions. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 43-48. https://doi.org/10.1007/978-3-658-43951-4_5.

Reinhold, Thomas. 2024. From Cyberwar to Cyberpeace. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 51-72. https://doi.org/10.1007/978-3-658-43951-4_6.

Reinhold, Thomas. 2024. Military Cyber Activities in Russia’s War Against Ukraine and Their Significance for the Debates on the Containment of a Cyberwar. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 73-84. https://doi.org/10.1007/978-3-658-43951-4_7.

Reinhold, Thomas. 2024. Arms Control and its Applicability to Cyberspace. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 85-106. https://doi.org/10.1007/978-3-658-43951-4_8.

Reinhold, Thomas. 2024. Challenges for Cyber Arms Control: A Qualitative Expert Interview Study. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 107-137. https://doi.org/10.1007/978-3-658-43951-4_9.

Reinhold, Thomas. 2024. Towards a Cyberweapons Assessment Model—Assessment of the Technical Features of Malicious Software. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 141-172. https://doi.org/10.1007/978-3-658-43951-4_10.

Reinhold, Thomas. 2024. Spotting the Bear: Credible Attribution and Russian Operations in Cyberspace. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 173-183. https://doi.org/10.1007/978-3-658-43951-4_11.

Reinhold, Thomas. 2024. Wannacry About the Tragedy of the Commons? Game-theory and the Failure of Global Vulnerability Disclosure. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 185-196. https://doi.org/10.1007/978-3-658-43951-4_12.

Reinhold, Thomas. 2024. The Digital Divide in State Vulnerability to Submarine Communications Cable Failure. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of

Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 197-226. https://doi.org/10.1007/978-3-658-43951-4_13.

Reinhold, Thomas. 2024. Cyberweapons and Artificial Intelligence—Impact, Influence and the Challenges for Arms Control. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 227-238. https://doi.org/10.1007/978-3-658-43951-4_14.

Reinhold, Thomas. 2024. Preventing the Escalation of Cyberconflicts: Towards an Approach to Plausibly Assure the Non-Involvement in a Cyberattack. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 241-268. https://doi.org/10.1007/978-3-658-43951-4_15.

Reinhold, Thomas. 2024. ExTRUST: Reducing Exploit Stockpiles with a Privacy-Preserving Depletion System for Inter-State Relationship. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 269-299. https://doi.org/10.1007/978-3-658-43951-4_16.

Reinhold, Thomas. 2024. Verification in Cyberspace. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 301-317. https://doi.org/10.1007/978-3-658-43951-4_17.