J Arch Mil Med. 2020 December; 8(4):e114485. doi: 10.5812/jamm.114485.

Published online 2021 May 1. **Review Article**

Security in Cyberspace in the Field of International Relations

Mohammad Abbasi [1, *]

[1] Farabi College of Science and Technology, Tehran, Iran

[*] *Corresponding author*: Farabi College of Science and Technology, Tehran, Iran. Email: ma10773@gmail.com

Received 2021 March 10; **Accepted** 2021 April 18.

Abstract

As cyberspace expands and globalizes, we are experiencing a new layer of threats to governments in the form of cyber threats that have impacted various facets of national security, including social, economic, military, and political security. As a result, in the form of electronic warfare, it has developed a new kind of war and conflict. Therefore, it has impacted international security, necessitating solutions to minimize the harm caused by this form of threat and preserve international security. So, network security has brought to light some of the underlying tensions between international rivalry and cybersecurity cooperation. Thus, the current study employs a descriptive-analytical method to investigate and analyze the role of international organizations, especially the Organization for Economic Cooperation and Development, in the development of cyberspace security. The hypothesis raised in this study is that since governments are increasingly relying on unilateral policies and resources to ensure cyber protection, international organizations should play an active role in shaping cooperation among their members in the form of approaches focused on international cooperation on cybersecurity and the prevention of cyber threats, as well as the development of a global cybersecurity system.

Keywords: Security, Cyberspace, Governments, International Organizations

1. Context

Governments have made considerable efforts in the last two decades to develop cybersecurity strategies and create offensive and defensive capabilities in this region. Governments, on the other hand, have attempted to strike a balance between the increased movement of money, individuals, goods, and services on the one hand, and the security measures in place to protect fixed assets and national assets on the other hand. Besides, it seems that these attempts would alter the balance between freedom and economic control. The importance of finding network security illustrates some of the underlying contradictions between international rivalry and collaboration in improving cybersecurity, even though preserving this balance has long been part of government foreign policy and international relations. Meanwhile, some international organizations, such as the Organization for Economic Cooperation and Development (OECD), have taken an active role in shaping cooperation among their members to prevent network harm and establish a "shared security culture". This study aims to look at international efforts to improve network and cybersecurity cooperation. In reality, in the context of this study, an attempt is made to analyze these multilateral initiatives in light of recent government decisions to formulate national strategies for network security.

In reality, some organizations have expressed their members' concerns about network security, both in telecommunications and in Internet-based communications, and have taken steps to address them. Over the last two decades, governments have made considerable efforts to develop cybersecurity strategies and improve their capabilities in this region. Governments, on the other hand, have attempted to strike a balance between the increased movement of money, individuals, goods, and services and the security measures taken to protect fixed assets and national assets. However, it appears that these measures would alter the balance between freedom and economic control. While preserving this balance has long been part of foreign policy, trade policy, and international relations, the use of various methods to improve network security has highlighted some of the fundamental contradictions in the field of cybersecurity between unilateral action strategies and international cooperation (1).

This study explores the efforts of the international OECD to improve government cooperation on network security. As a result, after presenting some of the most critical features of electronic networks, as well as the complexities of network security, we will explore recent views

Copyright © 2021, Journal of Archives in Military Medicine. This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/) which permits copy and redistribute the material just in noncommercial usages, provided the original work is properly cited.

and hypotheses on the desirability and practicality of international cybersecurity cooperation. In addition, the OECD multilateral initiatives in this area will be reviewed and evaluated. The most beneficial steps to improve cybersecurity cooperation can be taken by concluding regional agreements or taking action in this area by some cyberspace sectors.

2. Evidence Acquisition

2.1. Network Security and Cybersecurity in the World of Information

The statement of free trade that was widely stressed in the 1990s, claiming that borders were irrelevant in cyberspace and communications centered on information technology networks were used to promote the free flow of products, services, information, communications, and people, can be seen as contradicting rising concerns about cybersecurity over the last decade. As a result, it is more important to look at network security with a clearer understanding of the weaknesses of a perspective focused solely on freedom of trade and information sharing, as well as the difficulties of defining security in a networked world (2).

Although governments and their ties are the foundations of the international system, other foundations include the links between governments, as well as the mobility and movement of knowledge, people, goods, and money. The characteristics and direction of these movements and flows are determined by transportation networks, communications, financial exchanges and institutions, as well as energy infrastructure, water, and other factors. When compared to the idea of government, which is to some degree determined by being restricted by national boundaries, some characteristics of networks stand out:

- Networks are the links that bind nodes at different locations;

- Multiple connections between different points, not just one-way connections between two points, may form networks;

- Some networks (regional and causal) are linked to other networks (such as the Internet), and some networks (regional and causal) are connected to other networks (such as the Internet);

- A network's various uses and applications can transform it into an infrastructure network; examples of these networks include financial exchange networks and transportation networks;

- To allow diverse exchanges, uses, and applications, networks need common standards and protocols;

- Infrastructure investment affects the course, pace, and capability of products, services, and people moving around;

- In network research, users and network uses are often overlooked in favor of communication and the status of communication points, as well as the network's overall structure, such as axial points or dense points.

- Multiple users connect with each other point-to-point via open and varied networks (much like the telephone or postal system), and we are less likely to see a small and dominant community communicates with a large number of people (almost like the model of communication through radio and television).

Many conventional security views are challenged by these network features. When considering the definition of protection, it is important to remember that, like positive and negative freedom, security can mean both protecting people and property from harm and risk and being safe to acting and behaving in specific ways. This may include protection from injury, threats, or the ability to freely choose certain items and acts, such as voicing an opinion, speaking, or participating in economic activities. In terms of protection, perceptions and policies are critical since some risks and threats come under the private sector, while others are structural risks that fall under the social and political spheres. In politics, ensuring security is regarded as one of the most important responsibilities of governments and governance. The words security and governance are often used interchangeably.

The national domain is called the realm of mobility and movement in many liberal theories of the state, the realm of providing people with adequate protection to choose and enjoy civil rights, and finally, the realm that is preferably free of any uncertainty in many liberal theories of the state. Within a nation-state, there is enough room for unique social, economic, and political structures and activities to emerge. As a result, the nation-state can be likened to a city enclosed by a wall, with a clearly defined boundary and no assurance of protection outside of it. However, walls and barriers have no significance in influential networks, and the existence of cross-border communications and movements in the international system faces security officials with challenges.

Borders have often played a significant role in deciding nation-geography states and territories. Border ports or customs serve as mechanisms for enabling or prohibiting the flow of individuals, goods, and services from outside a nation-state into it, or from inside a nation-state to the outside. As a result, the rules and conditions of con-

tact and cooperation with other countries are determined by boundaries. However, when considering the position of networks and network displacements, these movements and displacements should be considered alongside other national movements and displacements that are subject to field conditions and regulations. According to Broman (2006), boundaries are no longer solely geographical. To comprehend the importance and location of national borders, as well as the conditions they seek to place on the movement of persons, goods, services, and information, we must recognize various types of network communications and institutions.

With these concerns in mind, the philosophical and practical challenges of improving "network security" become apparent. Transnational communication was previously seen as an interconnection mechanism of telecommunications networks (3). Governments and international organizations have specified the rules and conditions of contact with other parties in other countries, such as technical standards, traffic exchange, and network traffic costs, and have tried to use interconnection tools, such as technical and service networks, to respect and revitalize borders.

Network infrastructure, in its broadest context, is now included in network security issues. This can include preventing network physical harm, as well as protecting network content, network service outages, unwanted use, loss of intellectual property rights, and network information theft. In other words, network security problems reach beyond the network's physical infrastructure to include data stored on a computer/communication network, applications, and network properties of a specific organization or group of users, as well as civil and human right issues such as freedom of speech, information retrieval, privacy, and identification (4).

As a result of the lack of a precise and consistent description of network protection, risks posed by various types of users and service providers using wired or wireless technology in relation to all types of data (audio, video, etc.) are included. Network security is an effort to strike a balance between protecting national assets and taking advantage of free trade, network use, and network independence. Other political and cultural values are included in these benefits, in addition to economic stability and development. As a result, attempting to strike a compromise that involves compromising commitments to network independence could have unintended consequences. Efforts to improve network security and safety, in general, will include the use of network technology for monitoring and regulating steps.

2.2. Transnational Cybersecurity

Understanding the social priorities of the Internet in the post-Cold War period is essential for considering cyberspace as a transnational arena. The Internet was intended to operate in the event of a nuclear attack on the United States when it was first created as a decentralized communications system. As a result, the Internet's primary function was to serve as a contact and control mechanism for US politicians to coordinate nuclear war operations (5). The Internet was segregated from the military sector as a part that needed a lot of funds with the end of the Cold War and US efforts to reduce the budget of its military-industrial complex, which was established during the Cold War. Therefore, it was moved from the Department of Defense to the National Science Foundation, and then to a corporation in which the private and public sectors collaborated, with the US Department of Commerce overseeing the process. The transition of the Internet from the military to the commercial sector is fascinating, and it exemplifies American policymakers' attitudes toward the Internet in the post-Cold War era. The so-called open-door interpretation of US diplomatic history can explain American policymakers' views on the Internet. In open doors interpretation, it is believed that US policymakers believe in a worldview in which US security depends on expanding political and economic relations with the outside world (6). Since its inception, US policymakers have used technology to extend this partnership, as Adas has shown. Since 1996, US politicians have adopted policies aiming at expanding American political production and values across the Internet (5). The social aim of the Internet in the post-Cold War period, according to American policymakers, is to serve as a platform for the promotion of free trade and freedom of speech, as well as the expansion of global knowledge and economic exchanges. To ensure that the Internet fulfills its stated objective, politicians in the United States have established an Internet dialogue focused on the concept of free trade (7).

American politicians have promoted and defended the Internet as a free forum in their debate, with the goal of establishing favorable institutional conditions for the expansion of global knowledge and economic transactions that are consistent with their worldview. Castells (1999) illustrated how the Internet contributes to the growth of globalization by connecting governments in a dynamic network of economic interdependence that characterizes the age of global capitalism generated by the United States and

other advanced industrial democracies. The assertion that the Internet is gradually becoming a global arena for trade is backed by evidence of the growth of economic activity on the Internet.

The overall volume of international Internet trade, also known as global e-commerce, had reached $ 1.4 trillion by 2015, and is expected to rise at a rate of 13.5 percent per year in the near future. Global e-commerce contributes more than $400 billion to the US economy per year. Although the United States, Japan, and the United Kingdom account for 53% of all global e-commerce transactions, developing countries such as Brazil, China, Russia, and Mexico are expected to rise by 26% in the coming years (8).

Today, we are seeing a change in global e-commerce from developed to developing countries, which is partly due to effective economic growth policies implemented in these countries, which has resulted in the formation of market groups in these countries, and is partly due to the expansion of mobile networks in them. More people around the world are accessing the Internet via modern and portable communication devices like smartphones and tablets, demonstrating the change from desktop to cloud computing (9). Global consumption patterns change as a result of changes in computing, and changes in consumption patterns lead to changes in global trade, economic activity, jobs, and political institutions (formerly). The Arab Spring can be seen as a reflection of these massive shifts in the global political economy, which have been aided by the use of cyber communication technologies. Overall, the Stuxnet virus's deployment, the cyber-attack on Google and 33 other US firms, and the increasing importance of the Internet in global information and business exchanges run counter to a government-centric cybersecurity system that ignores the Internet's role in improving the relationship between governments and non-state actors (10)

Cybersecurity is described as the absence of conflict between actors in a way that promotes security and stability in cyberspace while allowing for information and economic exchanges. Looking at cybersecurity from this angle better reflects the fact that it is a global security problem, and as a result, all users of cyberspace are vulnerable to cyber-attacks. Because of the integrated existence of cybersecurity, it is more appropriate to think of it as a transnational problem in which governments collaborate to create stable cyberspace. Here, we have also examined the indicators of cyber power and security of governments published by reputable institutions, which are ranked in Table 1.

2.3. Existing Views on Desirability and Practicality of International Cooperation in Network Security

When considered in the light of the international environment and the structures of international organizations, the general characteristics of networks and the problems posed by network security and cybersecurity as a result of the blurring of boundaries become more nuanced. The desirability and practicality of government cooperation and the establishment of joint institutions to strengthen cybersecurity have been discussed in recent years in various circles.

In terms of understanding international politics, threats to network protection illustrate the classic contradictions between neo-realist viewpoints and internationalist or institutionalist neoliberal approaches once again. Cybersecurity is often perceived as either a one-sided foreign policy problem (12, 13) or a static neo-realist paradigm (14). Advocates and opponents of collective approaches to cybersecurity, on the other hand, cannot be specifically put in either of these theoretical viewpoints, and supporters of various theories and perspectives have given reasons to support or oppose the desirability and practicality of government collaboration to ensure cybersecurity (i.e., institutional approaches). In the following sections, we will address several perspectives on the necessity of developing frameworks for international cooperation, as well as the practicality of specific mechanisms. In addition, we will address the key views and claims of various authors regarding cooperation in the field of cybersecurity by establishing an international agreement in this regard in the continuation of this section, and we will attempt to combine these views (15-21).

The benefits of creating an international treaty or other forms of institutional cooperation in cybersecurity have been frequently argued in terms of lowering the costs of unilateral and technological approaches to improving network security, as well as lowering the device risks and failures that may occur as a result of governments' unilateral actions, and taking technical measures to safeguard electronic communication networks or associated equipment. In contrast to the various and continuing activities of governments to further their national interests in the absence of any international standards or agreements, an international agreement or government involvement would much better secure the freedom of access to the Internet and Internet communications (4).

Cooperation between governments is also desirable because it can restrict the activities of non-governmental actors and cybercriminals. Governments may not be able

Table 1. Top 10 Cyber Powers and Security (11)

	Belfer Center: National Cyber Power Index 2020	International Telecommunications Union: Global Cybersecurity Index 2018	Economist Intelligence Unit & Booz Allen Hamilton: Cyber Power Index 2011
1	United States	United Kingdom	United Kingdom
2	China	United States	United States
3	United Kingdom	France	Australia
4	Russia	Lithuania	Germany
5	Netherlands	Estonia	Canada
6	France	Singapore	France
7	Germany	Spain	South Korea
8	Canada	Malaysia	Japan
9	Japan	Canada	Italy
10	Australia	Norway	Brazil

to agree on all of the terms of a joint cybersecurity agreement, but they may be able to agree on the section of the agreement that deals with particular criminal behaviors. A treaty with a common agreement on cybersecurity can also subject government operations on the Internet to the law of war; in other words, it can define how governments can use cyber resources and technology both when there is no formal war between them and when there is (17, 18). Attacks on networks, as well as on network-connected control systems, can result in direct physical harm to individuals and facilities, and as a result, organizations that track inter-state warfare should regard these attacks as foreign conflicts (18). A state department official claims that international law applies in cyberspace and that it is not a lawless place.

Some experts, on the other hand, have voiced clear opposition to the conclusion of a joint international agreement on cybersecurity. Given a large number of governments and the diversity of their political traditions, there are few shared principles or priorities that could lead to a consensus in this field. As an intergovernmental organization, a joint security agreement should reinforce the position of the government and acknowledge the government's sovereignty and control over networks. These two things have been at odds with how the Internet and cyberspace have been handled since the 1990s, as well as by other organizations prior to that time, because in these organizations, non-governmental actors take precedence over government actors.

Furthermore, the private sector is responsible for the majority of technology growth and application in network-based services. In addition, the private sector controls much of the innovation and expenditure in networks, as well as their uses. The government and private actors vary in some respects. Significant non-governmental actors, such as financial actors, NGOs, and civil society organizations active in Internet management, are likely to be marginalized in an intergovernmental agreement. Governments' security policies, both domestic and foreign, can, on the other hand, bind non-state actors. Any strategy in this regard, according to Nojeim, should take into account the disparities in needs between the public and private sectors. Policies "adopted for government systems will have a more prescriptive nature than policies for private systems," it should be noted.

The distinction between public and private sector obligations affects national policy formulation. According to (21), Americans' interest in ensuring cybersecurity is extremely poor. In reality, they are oblivious to the need to react to China's ability to penetrate American networks and destroy critical infrastructure in a matter of days or hours. According to Spade, there is no shared understanding about how to resolve this problem in the private and public sectors, and although the Departments of Defense and Homeland Security are responsible for protecting government and military websites, they are not responsible for the private sector. Therefore, the private sector views maintaining cybersecurity as one of the government's obligations, while the government views it as one of the private sectors. Non-state political actors have also grown in power; according to (19): "Dependence on complex cyber structures for military and economic activities generates new weaknesses in large states that non-state actors can exploit"

Any agreement to strengthen security risks reducing or limiting the advantages of open and interconnected

electronic networks with little government intervention. International institutions' practices decrease governance stability and could alter the hypothesis that the best way to handle the Internet is made by less government interference. The relative freedom of networks is one of the basic elements of the existing order, and the establishment of stronger security agencies is likely to result in further government restrictions on freedom of speech and trade.

It is still unclear what the desired scope of a cybersecurity international agreement or treaty will be. Governments are likely to resist any attempt to limit cyber espionage and cyber-gathering activities, especially if the efforts fall outside of their national scope and affect their financial rights and liberties. The aims and tools of cyber warfare vary from those of cyber espionage, and each of these phenomena necessitates a distinct institutional response. There are differing views on the viability of applying collaborative approaches to cybersecurity, just as there are differing views on the desirability of pursuing such approaches. Most of the research into the practicality of such interventions focuses on policymakers' motivation to collaborate, and they continue their debate by contrasting cyberspace to other fields and areas where international agreements and organizations exist.

The current situation, according to proponents of the above methods, is focused on the widespread interdependence of suppliers and consumers of electronic networks and services, as well as governments. This is while all sectors or transnational problems (ranging from abstract processes like financial markets, commerce, and investment to concrete spaces like the seabed, extraterrestrial space, or radio waves) have characteristics that can lead to collaborative and competitive approaches to international governance. Interdependence will aid in the development of methods for emphasizing shared interests and directing international conflicts against institutional structures such as those in charge of conflict resolution.

Electronic communication networks, in addition to their interconnectedness and interdependence, are critical infrastructure for all countries, and thus their security will serve as a foundation for government cooperation. In this regard, dominant governments with the largest economies are most driven to collaborate and engage because the risks and weaknesses of networks, as well as cyber warfare, pose a greater threat to their interests than to the interests of other governments. This serves as a motivator for these governments to seek international cooperation in this region. "No country can achieve unilateral hegemony in cyberspace," according to (22), and "no government will be able to combat cybercrime or ensure cyberspace stability; cybersecurity is not a technology problem that can be resolved alone." This is a threat that requires a mix of defense technology, proper research, and information warfare, as well as conventional diplomacy to address.

Although buying hardware, software, and security services is a type of economic consumption that involves substantial investment and high costs, governments and private sector actors have incentives to minimize high costs and increase technological approaches to security. This also makes it more difficult to distribute economic costs fairly, as well as impose other social, political, and cultural costs on network operators and consumers, some of which are more difficult to quantify in formal economics (4).

Governments have a shared interest in mitigating the threats posed by non-state actors, and it has been shown that autonomous governments can collaborate to resolve cross-border issues like specific crimes. Some norms are being established in this regard in some regional agreements, such as the European Commission's Convention on Cybercrime. General norms and institutions based on collaboration have been established in other areas related to electronic networks, such as Internet protocols, technological standards, electronic payments, and the prevention of cyber fraud, by also monitoring child pornography.

Rather than creating a holistic structure to solve all cybersecurity issues, frameworks can be created to recognize the numerous challenges that face cybersecurity and address them separately and at different levels (22). Currently, the private sector has taken several operational and international steps in this regard, including the rapid exchange of information by cyber response teams from various countries (20, 23). For example, the East-West Institute's Frantz Stephen Cordy provides a trust-building guideline for coordinating various cyber response centers (24). The Organization for Security and Cooperation in Europe (OSCE) has made another recommendation in this regard: "Take confidence-building steps that establish stability and minimize risks" (25). According to Suefair, (20), cybersecurity agreements can be successful only if the activities that are the focus of the agreements and those that are not will be transparent.

Critics who challenge the value of government cooperation on cybersecurity point to the lack of shared standards, as well as each government's unique and competing interests (15). An agreement to restrict offensive and defensive options could have far-reaching implications for the signatory states if certain governments do not behave in

good faith (16).

Other concerns that occur when it comes to the desirability of cooperating in cybersecurity are linked to information shortages. One of these problems is the lack of mechanisms to verify that a nation has built but not used offensive capabilities (16, 19). The lack of empirical evidence to form a plan is what Nye refers to as the issue. Another issue in this regard is recognizing actors who have performed poorly or "identifying the perpetrators of cyber-attacks" (18). It is difficult to classify countries' offensive cyber capabilities due to their dual or multiple uses of network capabilities (16).

According to (16), large governments may have different perspectives on cybersecurity policy, with Russia and China seeing it more in terms of leverage and wider connectivity environments than in terms of US-centric technology. Some types of political criticism, such as foreign intelligence operations, are viewed as a security threat in Russia and China in this context.

"Interdependence and weakness can remain," (19) writes, "but we must wait for technical progress to complicate early strategies". Changes in technical tools and environments hinder attempts to exchange knowledge and create mutual understanding, but interdependence alone is not enough for cooperation and joint institutionalization. Large governments continue to have incentives to seek unilateral benefits through technological tools in communication network-based operations, and these incentives tend to be greater than the incentives that push governments to create joint security agencies, which may restrict the independence of governments' behaviors. Although powerful governments' participation is essential for the establishment of common multilateral institutions, these governments are well aware of the need to use unilateral technological resources to advance their own security and interests. According to (21), almost all major conflicts over the last few years have been linked to cyber-attacks. Spade also claims that Russia and China are specially to blame for the attacks, stating that the two governments have sponsored intellectual operations in Eastern Europe (Russia), Taiwan, Western Europe, and the United States. These governments are unconcerned about the hackers. On the contrary, these governments regard these hackers' activities as "patriotic." Cyberspace, according to Spade, is another field where the battle can be waged. To put it another way, just as land, air, sea, and space are used for combat, cyberspace can be used for war, and just as these realms can influence each other, cyberspace can as well. It has the potential to have far-reaching consequences in other regions.

Even if there is cooperation in certain areas or industries, governments retain the right, in accordance with the principle of self-help, to use some means more suitable than any other to defend their fundamental national interests. They know how to put it to good use. According to (21), electronic warfare differs from cyber warfare operations because cyber warfare is part of a broader strategy that includes other fields. The issue is that cyber-attacks have no specific meaning. Offensive attacks aimed at disabling and disrupting networks, defensive acts aimed at stopping potential cyber-attacks, and finally offensive attacks that only attempt to steal information using the vulnerabilities of cyber systems are categorized into various forms of cybersecurity and cyber warfare.

This brief discussion of some of the arguments for and against the desirability and practicality of cybersecurity cooperation offers a conceptual and theoretical context through which we can analyze the OECD's programs as an example in this report.

3. Conclusions

The efforts of the International OECD to improve international cooperation on network security were explored in this report. Even though these initiatives have gained little attention in recent years due to governments' unilateral measures to protect ICT-related resources and improve their security capabilities, the challenges ahead, as well as the value of improving cooperation and multilateral Internet management, remain.

The OECD's multilateral initiatives contrast with large governments' efforts to ensure network security through national and technological approaches. Although it has aided in the strengthening of international cooperation on network protection, it has refrained from explicitly addressing the problem of cyber militarization, perhaps because powerful governments are hesitant to see unilateral action against their interests, while weaker governments with less capacity have shown little willingness to help stop their self-assist systems. Or, if they did have this tendency, they lacked the courage to interrupt the machine. Even though collective security and arms control have been enforced in other ways, whether by small parties, multilateral arrangements, or the United Nations, cybersecurity is still not as effective as it should be. It has failed miserably. Given policymakers' reliance on unilateral policies and resources for maintaining cyber protection, approaches focused on international collaboration and the

development of stronger international frameworks to protect the freedom and security of information flow in cyberspace continue to face significant challenges.

The OECD has a long history of developing collaborative network management methods, demonstrating the utility of these processes in general. One of the system's fundamental principles has been to enhance the advantages of using electronic networks, as well as to improve and preserve the freedom of communication and use of these networks. The group supports efforts to fight cybercrime and the unauthorized use of networks, but it has not yet gotten involved in government-to-government cyberwars.

In several respects, the organization's activities run contrary to arguments that international collaboration approaches to cybersecurity are undesirable. Although governments can disagree, no doubt leveraging the benefits of increased trade, investment, technological change, and other policies in member countries will lead to cooperation on network security within the context of the OECD. Non-governmental advisory bodies are included in the OECD. The word "participant" rather than "member state" is used by the OECD in its guideline on establishing a shared security culture, suggesting the importance of private sector actors in developing approaches focused on cooperation on network security, as well as efforts to minimize the separation between the public and private sectors. While the focus has changed over time, the aim of international cooperation-based interventions in the OECD has been to reduce the costs of security activities while also strengthening economic development.

In terms of the viability of using collaborative-based methods to ensure cybersecurity, the organization stresses the interdependence of all countries in interconnected electronic networks, as well as the fact that these networks are a critical part of all countries' internal infrastructure. The OECD is a group of influential governments in the developing world that have a market economy. While member states can disagree with some of the organization's policies, the organization has mechanisms for negotiation. In reality, the OECD takes a multi-sectoral approach to identify various types of cybersecurity problems and finding the best solutions.

The actions of the OECD in some fields, but not in all, contradict the claim that it is impractical to use collaborative-based approaches to cybersecurity. The member countries of this organization, on the other hand, share similar norms that are expressed in their histories and objectives. The company has several research and knowledge-sharing projects that can be used to solve the problems caused by a lack of information protection in network security. However, the continued focus on governments' wide position in Internet management has hampered the ability to produce and exchange data to address concerns such as user authentication, tracking cyberattackers, and dual-use of network technologies. Technical advances, on the other hand, have complicated any effort to implement collaborative and interactive-based approaches; however, the company is aware of these changes and is taking measures to manage them. This organization's members have a variety of interests. Even though all members agree to comply in some way with international agreements requiring governments to follow specific policies and procedures in various sectors, considering the existence and scope of the OECD's activities, governments are unlikely to be deterred from using one-sided tactics and any instruments they find more suitable as a result of these practices.

In general, the actions of this organization seem to demonstrate that implementing more comprehensive approaches to international cooperation, rather than global approaches, is successful in enhancing network security. One of these minor approaches is the conclusion of regional agreements among a group of governments, such as the OECD's, which can help establish common norms and practices. Long-term dialogue between middle-level policymakers in these countries will contribute to the development of a shared understanding of a variety of issues and topics.

In general, the goals and expectations set for collaboratively oriented approaches to network security have been far too ambitious and far out of control to be realized in the international arena. These far-reaching ideas and ambitions have often expressed themselves in the form of treaties and agreements. This problem appears to be solved by concluding regional agreements and agreements that deal only with specific sectors, and current opinions on the challenges and solutions to these challenges in this sector seem to have been redirected. Another problem is the historical and incomplete existence of institutionalization in this area. In certain cases, the number of decisions and agreements is smaller, which aids in the development of awareness, action, and common institutions over time. Even when an institutional structure is relatively stable and well-developed, full cooperation and involvement of governments within that framework (such as trade and investment or dispute resolution) do not always occur. As some of the studies discussed in this study

have shown, a historical and more detailed understanding of these processes will aid in identifying the next important steps.

Footnotes

Conflict of Interests: There was no conflict of interest.

Funding/Support: There was no funding/support.

References

1. Keohane RO. *After hegemony: Cooperation and discord in the world political economy*. Princeton, New Jersey: Princeton University Press; 1984.
2. Greathouse CB. *Cyber war and strategic thought: Do the classic theorists still matter?* Berlin, Heidelberg: Springer; 2014.
3. Zacher MW, Sutton BA. *Governing global networks: International regimes for transportation and communications*. Cambridge University Press; 1995.
4. Wirtz JJ. The Cyber Pearl Harbor. *Intell Natl Secur*. 2017;**32**(6):758–67. doi: 10.1080/02684527.2017.1294379.
5. Kiggins RD. *Wired world: United States policy and the Open Door Internet [Dissertation]*. University of Florida; 2011.
6. Layne C. *The peace of illusions: American grand strategy from 1940 to the present*. Ithaca, London: Cornell University Press; 2006.
7. McCarthy DR. Open networks and the open door: American foreign policy and the narration of the Internet. *Foreign Policy Anal*. 2011;**7**(1):89–111.
8. Enright A. *Internet retailer*. 2011. Available from: http://www.internetretailer.com/2011/06/07/global-e-commerce-reach-14-trillion-2015.
9. Castells M. *Information technology, globalization and social development*. Geneva: UNRISD; 1999.
10. Keohane RO, Nye Jr JS. Power and interdependence. *Survival*. 1973;**15**(4):158–65.
11. Voo J, Hemani I, Jones S, DeSombre W, Cassidy D, Schwarzenbach A. *National Cyber Power Index 2020*. Harvard Kennedy School: Belfer Center for Science and International Affairs; 2020.
12. Goodman SE, Kirk JC, Kirk MH. Cyberspace as a medium for terrorists. *Technol Forecast Soc Change*. 2007;**74**(2):193–210. doi: 10.1016/j.techfore.2006.07.007.
13. Gorge M. Cyberterrorism: hype or reality? *Comput Fraud Secur*. 2007;**2007**(2):9–12. doi: 10.1016/s1361-3723(07)70021-0.
14. Rothkopf DJ. Cyberpolitik: The changing nature of power in the information age. *J Int Aff*. 1998;**51**(2):325–59.
15. Goldsmith J. *Cybersecurity treaties: A skeptical view*. Hoover; 2011. Available from: https://www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf..
16. Ford CA. *The trouble with cyber arms control*. Cambridge: MIT Press; 2010.
17. Hughes REX. A treaty for cyberspace. *Int Aff*. 2010;**86**(2):523–41. doi: 10.1111/j.1468-2346.2010.00894.x.
18. Hongju Koh H. International law in cyberspace. *Harv Int Law J*. 2012;**54**.
19. Joseph S, Nye ,J. Nuclear lessons for cybersecurity. *J Strateg Stud*. 2011;**5**(4):18–38. doi: 10.21236/ada553620.
20. Sofaer A, Clark D, Diffie W. Cybersecurity and international agreements. *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for us policy*. National Academies Press; 2010.
21. Spade JM, Caton JL. *Information as power: China's cyber power and America's national security*. US Army War College; 2012.
22. Bajaj K. *Expert Witness Institute*. 2010. Available from: http://www.ewi.info/system/files/Bajaj.
23. Choucri N, Goldsmith D. Lost in cyberspace: Harnessing the internet, international relations, and global security. *Bull At Sci*. 2012;**68**(2):70–7. doi: 10.1177/0096340212438696.
24. Sternstein A. International cybersecurity treaty might not be achievable, Report says. *Available via Next gov*. 2011.
25. Sternstein A. US, Russia, other nations near agreement on cyber early-warning pact. *Nextgov*. 2012.