International Journal of Political Science
ISSN: 2228-6217
Vol 10, No 3, Autumn 2020, (pp.21-40)

Peace and Security in Cyberspace with a Cooperative-Based Approach in the Field of International Relations (Case Study of the Organization for Economic Cooperation and Development)

Qasem Ranjbar[1], Mohammad Abbasi[2*], Mohammadreza Dehshiri[3], Hassan Khodaverdi[4]
[1, 4]Department of Political Science and International Relations, South Tehran Branch, Islamic Azad University, Tehran, Iran
[2]Department of Political Science and International Relations, Farabi Faculty of Science and Technology, Tehran, Iran
[3]Department of Political Science and International Relations, School of International Relations, Tehran, Iran

Received: 22 Jan 2020 ; Accepted: 21 Sep 2020

Abstract:
Today, security has expanded beyond its traditional dimensions under the influence of the development of technology and information technology. Meanwhile, with the expansion of cyberspace and the globalization of cyberspace and the Internet, we are witnessing a new dimension of threats facing governments in the form of cyber threats that have affected various aspects of national security, including social, economic, military and political security. As a result, it has created a new kind of war and confrontation in the context of cyber warfare. Therefore, it has also affected international peace and security, and necessitates solutions to reduce the damage caused by this type of threat and to maintain peace and security in international relations. So, network security has highlighted some of the fundamental conflicts between international conflict and cooperation in strengthening cyber security. Thus, the present study intends to use the descriptive-analytical method to study and analyze the role of cooperation shaped in the form of international organizations and in particular the Organization for Economic Cooperation and Development, in relation to the development of security in cyberspace. The hypothesis presented in this study is that due to the widespread focus of governments on unilateral strategies and tools to ensure cyber security, international organizations can play an active role in shaping cooperation between their members in the form of approaches based on having international cooperation on cyber security and the prevention of cyber threats, as well as the creation of a shared security culture.

Keywords: Security, Cyberspace, International Organizations, Organization for Economic Cooperation and Development

Corresponding Author's Email: ma10773@gmail.com

1.Introduction

In the last two decades, governments have made significant efforts to develop strategies on cyber security and to build offensive and defensive capabilities in this regard. However, governments have tried to balance the increase in the movement of capital, people, goods and services on the one hand and the security measures taken to protect fixed assets and national assets on the other. On the other hand, it seems that these efforts will change the combination of freedom and economic control. Although maintaining this balance has long been a part of the foreign policy of governments and international relations, the importance of finding network security highlights some of the fundamental conflicts between international conflict and cooperation in strengthening cyber security. Meanwhile, in the field of international relations, some international organizations, such as the Organization for Economic Cooperation and Development (OECD), have played an active role in shaping cooperation among their members to prevent network damage and to create a "shared security culture". This study aims to examine international efforts to strengthen international cooperation on network security and cyber security. In fact, in the framework of the present research, an attempt is made to evaluate these multilateral efforts in the light of the recent actions of governments to formulate national strategies regarding network security.

In fact, various organizations have addressed their members' concerns about the issue of network security, both in telecommunications-based services and in Internet-based communications, and have taken actions in this regard. Governments have also made significant efforts over the past two decades to develop strategies for cyber security and strengthen their capabilities in this area.

However, governments have tried to balance the increase in the movement of capital, people, goods and services on the one hand and the security measures taken to protect fixed assets and national assets on the other. But it seems that these efforts will change the combination of freedom and economic control. Although maintaining this balance has long been part of foreign policy, trade policy, and international relations, the use of different ways to strengthen network security has highlighted some of the fundamental conflicts between strategies based on unilateral action and international cooperation in the field of cyber security (Keohane, 1984)

This study examines the efforts of the International Organization for Economic Cooperation and Development (OECD) to strengthen government cooperation on network security. Therefore, after introducing some of the most important features of electronic networks as well as the complexities of network security, we will discuss the views and theories that have recently been raised regarding the desirability and practicality of international cooperation in cyber security. In addition, the multilateral efforts of the Organization for Economic Cooperation and Development (OECD) in this regard will be reviewed and evaluated. The most beneficial steps to strengthen the cooperation on cyber security can be taken by concluding regional agreements in this regard or by taking action in this regard by certain sectors in cyberspace.

Network security and cyber security in the world of information

Rising concerns about cyber security over the past decade can be seen as contradicting the assertion of free trade that was widely emphasized in the 1990s, which argued that

borders were irrelevant in cyberspace and that communications based on Information technology networks are used to facilitate the free flow of goods, services, information, communications and people. Thus, it is better to examine network security with a more accurate understanding of the limitations of a view, based solely on freedom of trade and information exchange, as well as the challenges of providing a definition of security in a networked environment (Greathouse, 2015).

While governments and their relations are the cornerstone of the international system, the links of different governments to each other and the mobility and movement of information, people, goods and money have also been one of the pillars of this system. Transportation networks, communications, financial exchanges and institutions, in addition to energy infrastructure, water, etc. determine the characteristics and direction of these movements and flows. In general, some features of networks are particularly prominent when compared to the idea of government, which is to some extent characterized by being limited by national borders:

- Networks are the connection between nodes with different points;
- Networks may be the result of multiple connections between different points, not just one-way connections between two points
- Often there are links between different networks, some networks (regional and causal) are connected to other networks (such as the Internet);
- The multiple uses and applications of a network can turn that network into an infrastructure network, among these networks we can refer to financial exchange networks with transportation networks;
- Networks require shared standards and protocols to enable diverse exchanges, uses, and applications;
- Investment in infrastructure affects the direction, speed and capacity of movement and mobility of goods, services and people;
- Often in network analysis, less attention is paid to users and uses of networks and more attention is paid to communication and the status of communication points, with the general composition of the network, such as axial points or dense points;
- Open and diverse networks have multiple users communicating with others point-by-point through these networks (much like the situation with the telephone or postal system), and we are less likely to see a limited and dominant group communicate with a lot of people (almost like the model of communication through radio and television)

These network features pose fundamental challenges to many traditional security perspectives. In examining the concept of security, it should be noted that security, like positive and negative freedom (Berlin, 1958), can both mean protecting people and properties from harm and danger, and also being safe to act and behave in special ways. This can include being safe from harm, threatening, or being safe to choose certain things and actions, such as expressing an opinion, communicating, or engaging in economic activities. Perceptions and policies are very important in relation to security, in the sense that some risks and threats are part of the private sphere, but others are social risks and fall into the social and political spheres. In politics, creating security is considered as one of the main tasks of government and governance.

The terms governance and security are often used interchangeably.

In many liberal theories of the state, the national sphere is considered as the realm of mobility and movement, the realm of giving citizens sufficient security to choose and enjoy civil rights, and finally the realm that is ideally free of some insecurity. The space within a nation-state allows the formation of specific social, economic and political institutions and activities. Therefore, the nation-state can be considered as the city around which a wall has been built and its border is clear and there is no guarantee of security outside of it. But in powerful networks, walls and borders are meaningless, and the nature of cross-border exchanges and movements in the international system poses challenges for security officials.

Borders have always played an important role in determining the geography and territory of a nation-state (Kahin and Nesson, 1997; Barman, 2006). Border ports or customs act as channels for allowing or not allowing the movement of people, goods and services from the outside into a nation-state or from within a nation-state to outside of it. Thus, borders determine the rules and conditions of interaction and communication with other countries. However, when we consider the role of networks and network displacements, these displacements and movements should also be added to other movements and displacements that occur in the national arena and are subject to conditions and regulations in the field. Broman (2006) states that borders are no longer purely geographical. Thus, we need to consider the different types of network communications and institutions in order to understand the importance and position of national borders and the conditions they seek to impose on the movement of people, goods, services and information.

With these considerations in mind, the conceptual and practical problems facing the strengthening of "network security" manifest themselves. In telecommunications networks that existed in the past, transnational communications were seen as an interconnection system (Zacher and Sutton, 1996). Governments and international organizations have defined the rules and conditions of communication with other parties in other countries, including technical standards, traffic exchange, network traffic costs, and sought to use these interconnection tools, namely technical and service networks to respect the borders and revive them. These efforts were reinforced by economic and strategic considerations.

Today, network security concerns include network infrastructure in its broadest sense. This can include preventing physical damage to the network, but it also includes protecting the content of the networks, as well as preventing network service outages, unwanted use, and loss of intellectual property rights and network information theft. In other words, network security concerns do not only involve the physical infrastructure of the network, but also the information stored on a computer / communication network, the software, and network assets of a particular organization or group of users, as well as issues related to civil and human rights such as freedom of expression, information retrieval, privacy and identity (Wirtz, 2017).

There is no precise and clear definition of network security and as a result, the threats made by different types of users and service providers using wired or wireless technologies in relation to all types of data (audio, video, etc.) are also included. Network security represents an attempt to strike a balance between trying to secure national assets while enjoying the benefits of free exchange, use of

networks, and freedom of networks. These benefits, in addition to economic stability and growth, include other political and cultural values too. Thus, trying to strike a balance that leads to sacrificing commitments to network freedom may have other hidden costs. More generally, efforts to strengthen network security and safety can mean the application of network technologies for monitoring and controlling measures.

Transnational cyber security

Considering cyberspace as a transnational arena requires understanding the social goals of the Internet in the post-Cold War era. Originally developed as a decentralized communications system, the Internet was designed to function in the event of a nuclear attack on the United States. Thus, the primary purpose of the Internet was to act as a communication and control system through which US policymakers could manage nuclear war operations (Kiggins, 2011: pp. 43-47), which with the end of the Cold War and US efforts to reduce the budget of its military-industrial complex, which was created during the Cold War, the Internet was separated from the military sector as a part that required a lot of funds. As a result, it was transferred from the Department of Defense to the National Science Foundation and then from there to a company in which the private and public sectors worked together and were overseen by the US Department of Commerce. The transfer of the Internet from the military to the commercial sector is interesting and well illustrates the American policymakers' view on the Internet in the post-Cold War era. The American policymakers' view on the Internet can be explained by the so-called open door interpretation of US diplomatic history. 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 (Layne, 2006).

Adas has shown that US policymakers have always used technology to expand this relationship since its foundation. Since 1996, US policymakers have pursued policies that aim to use the Internet as an arena to expand American political output and ideals (Kiggins, 2011: pp. 1961-1969). According to American policymakers, the social purpose of the Internet in the post-Cold War era is to act as an arena for the development of free trade and freedom of expression, as well as the expansion of information and economic exchanges worldwide. To ensure that the Internet serves its stated purpose, American policymakers have formed a discourse about the Internet based on the principle of freedom of exchange (McCarthy, 2011: p. 109).

In their discourse, American policymakers have advocated and defended the Internet as a free arena, with the aim of creating the favorable institutional conditions for the expansion of global information and economic exchanges that are in line with the worldview of these policymakers. Castells (1999) has shown how the Internet helps the development of Globalization, by linking governments together in a complex network of economic interdependence that characterizes this era of global capitalism created by the United States and other advanced industrial democracies. Evidence for the growth of economic activity on the Internet supports the claim that the Internet is increasingly becoming a global arena for exchange.

By 2015, the total volume of international Internet commerce, commonly referred to as global e-commerce, had reached $ 1.4 trillion and is projected to grow by 13.5% annually in the near future. This form of commerce (global e-commerce) adds more than $ 400

billion a year to US GDP. While the United States, Japan, and the United Kingdom account for 53 percent of all global e-commerce transactions, developing countries such as Brazil, China, Russia, and Mexico are projected to experience the growth of 26 percent in the near future (Enright, 2011).

Today, we are witnessing the shift of global e-commerce from the developed world to the developing world, which is partly the result of successful economic development strategies implemented in these countries, which have led to the formation of consumer classes in these countries, and is partly the result of the expansion of mobile networks in these countries. More global consumers are entering cyberspace through modern and portable communication tools such as smartphones and tablets, thus demonstrating the shift from desktop-based to cloud computing (Castells 1996, p. 1999). By changing the way of computing, global consumption patterns change, and changes in consumption patterns in turn lead to changes in global trade, economic production, employment, and political institutions (formerly). The Arab Spring can reflect these huge changes in the global political economy, which as a result of the use of cyber communication technologies has gained a simpler and faster boost. Over all, the deployment of the Stuxnet virus, the cyber-attack on Google and 33 other US companies, as well as the growing importance of the Internet in global information and business exchanges, run counter to a government-centric cyber security framework that ignores the role of the Internet on strengthening the relation between governments and non-state actors (Keohane and Nye, 2001: pp. 43-50).

Cyber security is the lack of conflict between actors in a way that creates a state of security and stability in cyberspace and allows information and economic exchanges. Looking at cyber security from this perspective better reflects the fact that cyber security is a transnational security issue and as a result, all cyberspace users are vulnerable to cyber-attacks. Given the interconnected nature of cyber security, it is better to consider cyber security as a transnational issue in which governments work together to achieve a secure cyberspace.

Existing views on the desirability and practicality of international cooperation in network security

The general characteristics of networks and the challenges faced by network security and cyber security due to the blurring of borders become more complex when considered in the context of the international system and the processes of international organizations. The desirability and practicality of government cooperation and the establishment of joint institutions to strengthen cyber security have been discussed in recent years in various circles (Fast West Institute, 2010, Schjolberg and Ghernaouti-Helie, 2011).

Challenges to network security once again highlight the classic differences between neorealist perspectives and internationalist or institutionalist neoliberal approaches in terms of understanding international politics. Often the issue of cyber security is either seen as a one-sided foreign policy issue (Goodman et al, 2007; Mathieu, 2007) or placed in a rigid neo-realist framework (Information Warfare site, 2011; Rothkopf, 1998)

However, advocates and critics of collaborative approaches to cyber security cannot be precisely placed in one of these theoretical perspectives, and proponents of different theories and perspectives have provided reasons to support or oppose the desirability and practicality of government cooperation to

ensure cyber security (i.e., institutional approaches). In the following sections, we will discuss some views on the desirability of establishing mechanisms for international cooperation, as well as on the practicality of specific mechanisms. In fact, in the continuation of this section, we will discuss the main views and claims of various authors regarding cooperation in the field of cyber security by creating an international agreement in this regard and we will try to combine these views (Goldsmith, 2011; Ford, 2010; Hughes, 2010; Koh, 2012; Nojeim, 2010; Nye, 2011; Sofaer et al, 2010; Spade, 2012).

The desirability of establishing an international treaty or a form of institutional cooperation in cyber security, has often been supported in terms of the benefits that such mechanisms have in order to reduce the costs of unilateral and technical approaches to enhancing network security as well as lowering the system risks and failures that may arise as a result of governments' unilateral and technical efforts to protect electronic communications networks or related equipment.

An international agreement or the participation of governments, in comparison with the numerous and ongoing actions of governments to advance their national interests in the absence of any international norms or commitments, can much better protect the freedom of use of the Internet and Internet communications (Wirtz, 2017).

Government cooperation is also desirable in that it can limit the actions of non-governmental actors or cybercriminals. Governments may not agree to all of the provisions of a joint cyber security agreement, but they may be able to agree on the part of the agreement that relates to specific criminal conduct.

A treaty with a common agreement on cyber security can also make government activities on the Internet subject to the law of war; in other words, specify how they should use cyber tools and technologies in times when there is no formal war between governments as well as when there is a formal war between them (Koh, 2012; Hughes, 2010). Attacks on networks, as well as attacks on network-connected control systems, can contribute to actual physical damage to individuals and facilities, and therefore, these attacks should also be considered as international conflicts by institutions that monitor inter-state warfare. State Department official, Koh (2012) argues that international law is applicable in cyberspace and it is not a lawless area.

On the other hand, a number of analysts have strongly opposed the desirability of concluding a joint international agreement on cyber security. Given the number of governments and the diversity of their political traditions, there are few common values or goals that could lead to an agreement in this regard. A joint security agreement as an intergovernmental institution should strengthen the role of government and recognize the government's sovereignty and its control over networks. These two elements have been at odds with the way the Internet and cyberspace have been managed since the 1990s, as well as by other organizations before this date, because in these organizations, instead of giving priority to the role of governments, non-governmental actors play a more prominent role.

In addition, most of the technology development and its application in network-based services are done by the private sector. Also innovation and investment in networks and their use is mostly in the hands of the private sector. Government and private actors are different in several ways. In an intergovernmental agreement, important non-

governmental actors are likely to be marginalized; these could be financial actors or NGOs and civil society groups involved in managing the Internet. On the other hand, the security policies of governments, both national and international, can be binding on non-state actors. Nojeim points out that any approach in this regard should take into account the different needs of the public and private sectors. It should be noted that policies "adopted towards government systems may have a more prescriptive aspect than policies towards private systems" (Nojeim, 2010: 119).

The distinction between public and private sector responsibilities also affects the formulation of national policy. Spade (2012) emphasizes that Americans' interest in finding ways to ensure cyber security is extremely low. In fact, they pay little attention to the need to respond to China's ability to infiltrate American networks and dismantle critical infrastructure in a matter of days or hours. From Spade's point of view, there is no uniform view of resolving this issue in the private and public sectors, and while the Department of Defense and the Department of Homeland Security have responsibilities to protect government and military websites, they do not have such responsibilities to the private sector. Thus, the private sector considers ensuring cyber security as one of the responsibilities of the government, while the government considers it as one of the responsibilities of the private sector. Nye (2011) also notes that non-state political actors have gained more influence: "Dependence on complex cyber systems for military and economic activities creates new vulnerabilities in large states which non-state actors can make use of." (McDowell et. all, 2014)

Any agreement to strengthen security can also reduce or limit the benefits of free and interconnected electronic networks in which governments have little interference. The practice of international institutions reduces the flexibility of governance and can change the hypothesis that the best way to manage the Internet is possible through more limited government intervention. One of the fundamental elements of the current order is the relative freedom of networks, and the creation of stronger security institutions is likely to lead to more government restrictions on freedom of expression and trade.

It is also not clear where the ideal scope of an international agreement or treaty on cyber security lies. Governments are likely to oppose any attempt to restrict cyber espionage and cyber-gathering activities, especially if those efforts are outside their national scope and within the scope of their financial rights and liberties. The goals and tools of cyber warfare are different from the goals and tools of cyber espionage, and each of these phenomena requires its own institutional response.

Just as there is disagreement about the desirability of adopting collaborative approaches to cyber security, there are differing views on the feasibility of implementing such approaches. Much of the work in support of the practicality of such approaches focuses on the motivation of governments to work together, and they continue their discussion by comparing cyberspace with other sectors and areas in which there are international agreements and institutions.

Proponents of the practicality of the above approaches argue that the current situation is based on the extensive interdependence of suppliers and users of electronic networks and resources, as well as governments. While all sectors or transnational issues (from abstract processes such as financial exchanges, trade and investment to specific spaces such

as seabed, extraterrestrial space or radio waves) have features that can also contribute to collaboration based approaches and also to competitive approaches to international governance. Interdependence can help develop ways to emphasize common interests and steer international conflicts toward institutional frameworks such as those responsible for resolving conflicts.

In addition to the interconnectedness and interdependence of networks, electronic communications networks are a fundamental infrastructure for all countries, and thus the protection of these resources can also provide the basis for cooperation between governments.

Also in this regard, powerful governments with the largest economies are mostly motivated to cooperate and participate, because the dangers and vulnerabilities of networks as well as cyber warfare threaten their interests more than other governments. This is an incentive for these governments to find ways for international cooperation in this regard. Bajaj (2010) argues that "no country can achieve unilateral superiority in cyberspace", similarly "no government alone will be able to fight cybercrime or ensure cyberspace security; cyber security is not a technology issue which can be resolved alone. This is a danger that must be addressed through a combination of defense technology, proper analysis and information warfare, as well as traditional diplomacy" (McDowell et. all, 2014).

Governments and private sector actors also have incentives to reduce high costs and increase technical approaches to security, while purchasing hardware, software, and security services is a form of economic consumption that requires massive investment and high costs. This also impedes the equitable distribution of economic costs and may impose other social, political, and cultural costs on network providers and users, some of which can be more difficult to measure in formal economics (Wirtz, 2017).

Governments have common interests in reducing the risks of non-state actors, and it has been proven that independent governments can work together to address cross-border challenges such as specific crimes. In some regional agreements, such as the European Commission's Convention on Cybercrime, some norms are being formed in this regard. In other areas related to electronic networks such as Internet protocols, technical standards, electronic payments, prevention of cyber fraud, common norms have been formed and institutions based on cooperation have been established by also monitoring child pornography.

Instead of designing a comprehensive framework for all challenges related to cyber security, mechanisms can be designed to identify the various challenges facing cyber security and address these challenges separately and at different levels (Bajaj, 2010: p ii). Currently, the private sector has taken many organizational and international actions in this regard, including the quick action of cyber response teams of different countries in sharing information (Choucri and Goldsmith, 2012; Sofaer et al, 2010). For example, Frantz Stephen Cordy of the East-West Institute offers a trust-building guideline to coordinate different cyber response centers (Sternstein, 2011). Another suggestion in this regard made by the Organization for Security and Cooperation in Europe (OSCE) has been to take confidence-building measures which create stability, and reduce risks" (Sternstein, 2012). Suefair, Clark, and Diffie (2010) also state that cyber security agreements will only be effective if actions that are the subject of these agreements and actions that are outside

these agreements be clear (McDowell et. all, 2014).

Critics who question the desirability of cooperating on cyber security point to the lack of common norms between governments, as well as the specific and different interests of each government (Goldsmith, 2011). If some governments do not act in good faith (Ford, 2010), an agreement to limit offensive and defensive options, could have far-reaching consequences for the signatory states.

Other problems related to the desirability of cooperating in cyber security arise from issues related to information shortages. One of these issues is the lack of mechanisms to confirm that a country has developed and not used its offensive capabilities (Ford, 2010; Nye, 2011). Nye calls this problem the lack of empirical data to shape a strategy. Identifying actors who have performed poorly or "identifying the perpetrators of cyber-attacks" is another problem in this regard (Koh, 2012). Dual or multiple uses of network capabilities makes it difficult to identify countries' offensive capabilities in cyberspace (Ford, 2010).

Ford (2010) argues that large governments may have a different understanding of cyber security strategy, and that Russia and China may see this strategy more in terms of influence and broader communication environments than in terms of US-focused technology (McDowell et al, 2014). In this context, some forms of political commentary, including foreign intelligence operations, are considered a security threat in Russia and China.

Nye (2011) notes that "interdependence and vulnerability are two realities that will persist, but we must wait for technological change to complicate early strategies" (McDowell et all, 2014). Interdependence alone is not enough for collaboration and joint institutionalization, as changing technological tools and environments complicate efforts to share information and build shared understanding.

Large governments still have incentives to pursue unilateral benefits in communication network-based activities through technical tools, and these incentives appear to be stronger than the incentives that drive governments to establish joint security institutions that may limit the independence of governments' actions. While the participation of powerful governments is essential to the creation of common multilateral institutions, these governments are fully aware of the need to use unilateral technical tools to advance their own security and interests. For example, Spade (2012) states that over the past few years, almost all major conflicts have been associated with cyber-attacks. Spade also argues that Russia and China are particularly responsible for these attacks, as the two governments have implicitly supported intellectual operations in Eastern Europe (Russia), and in Taiwan, Western Europe, and the United States. These governments do not deal with these hackers. This means that these criminals are punished and not brought before the courts. On the contrary, these governments consider the actions of these hackers to be "patriotic". Spade also points out that cyberspace is another area that can be used for war. In other words, just as land, air, sea and space are used for war, cyberspace can be used for this purpose, and just as these domains can affect each other, so can cyberspace. It can have far-reaching effects on other areas.

At best, even if there is cooperation in some areas or sectors, governments still reserve the right to use any means more appropriate than any other to protect their funda-

mental national interests, in line with the principle of self-help. They know how to use. Spade (2012) states that cyber warfare is different from cyber warfare operations, mainly because cyber warfare is part of a planned and larger strategy that encompasses other areas. The problem is that there is no clear definition of cyber-attacks. Cyber security and cyber warfare involve a variety of activities - offensive attacks aimed at disabling and disrupting networks, defensive actions aimed at preventing possible cyber-attacks, and finally offensive attacks that only seek to steal information using the weaknesses of cyber structures - and of course each of these measures is divided into different forms.

This brief discussion of some of the claims in support of or in opposition to the desirability and practicality of cooperation on cyber security provides a conceptual and theoretical framework by which we can draw on the OECD's programs as an example in this study to evaluate in this regard.

Organization for Economic Cooperation and Development

Prior to its expansion in the 1990s, the Organization for Economic Cooperation and Development (OECD) had a limited membership and included only liberal and industrial democracies. In 2013, the organization had 36 members, mostly developed countries with market economies in Europe, North America and Asia. However, a number of Eastern European countries have recently been added to the organization. These countries have many of the most advanced communication information networks in the world, and their economies have become highly dependent on network communication infrastructure over the past decades. The Information, Computer and Communication Policy Unit (IICP) of the Organization for Economic Co-operation and Development (OECD) has been addressing the issue of international electronic information networks since the 1970s. This unit has participated in cross-border flow of information projects in 1970 and 1980 and also concluded two agreements between members of the organization on the cross-border flow of information in 1980 and 1985.

The guideline issued by the Organization for Economic Cooperation and Development (OECD) in 1992 on the security of information systems are significant in that they seek to recognize and not undermine the sovereignty of governments. This directive states: "The present directive does not interfere with the sovereign rights of national governments with regard to national security and public order, and always considers these matters to be subject to the requirements of national law. The 1992 Directive also advises member states to develop a comprehensive plan for cooperation and agreement on security measures and to take steps to implement them. This Directive recommends that Member States:

- Make arrangements, take actions, and adopt procedures that reflect principles related to information systems security Consult, coordinate and cooperate in the implementation of this guideline, including to cooperate internationally in developing standards, arrangements, actions and procedures in relation to the security of information systems;
- Agree with each other as soon as possible on specific initiatives and programs to implement this guideline;
- Promote the principles of this guideline widely;

- Review this guideline every five years to improve international cooperation on information security issues (OECD, 1992).

The Organization for Economic Cooperation and Development (OECD) published another work in the 1990s that was directly related to Internet technologies and at the same time focused more on financial and economic development. This work was the result of research and opinion exchanges conducted in the form of national information infrastructure and global information infrastructure programs (OECD, 1997). This work began as "A Framework for Global E-Commerce" (United States, 1996). The Organization for Economic Cooperation and Development (OECD) began efforts in the late 1990s to define e-commerce as well as to standardize e-commerce practices among its member states. One of the organization's documents, entitled "Operational Plan of the Organization for Economic Cooperation and Development for e-Commerce", identifies four main objectives for e-commerce: strengthening the information infrastructure, including "improving access to telecommunications and Internet services at cost, reliability and the speed needed for e-commerce", "building trust among users of e-commerce", "establishing the basic rules of digital commerce, and ultimately maximizing the benefits of e-commerce" (Tigre and O'Connor, 2002).

The Organization for Economic Cooperation and Development (OECD) has also published a document entitled Guidelines for Consumer Protection in E-Commerce (1999). This document emphasizes explicit and effective support; trade, advertising and fair economic measures; secure payment mechanisms and security level information; dispute resolution and compensation, privacy protection, and education and awareness (Donohue, 2003)

Some countries see programs such as the Global Intelligence Infrastructure Initiative, the National Intelligence Infrastructure Program, and the rise of e-commerce over the Internet as tools that will trigger the next wave of economic development and create a competitive advantage for powerful national units. This view was reinforced by the emphasis on the availability of information and communication technologies used in the infrastructure necessary to support e-commerce. For example, the Organization for Economic Cooperation and Development (OECD) published a report in 2001 which focused on issues such as Internet access costs, level of Internet use, number of Internet users per 100 people, number of secure Internet servers per 100 people in one country, the level of household use of the Internet, and the level of household use of computers (OECD, 2001).

The Organization for Economic Cooperation and Development (OECD) has also launched a series of efforts to coordinate its member states to strengthen trade. Topics covered include creating a "security culture", protecting cyberspace privacy, network security, cross-border fraud, broadband Internet access, and the importance of e-commerce for development and measurement of information economy (OECD, 2004). A report published in 2005 by the Organization for Economic Cooperation and Development (OECD) outlines the national effort to "establish a security culture for information systems and networks in its member countries" (OECD, 2005). However, other report, published in 2007, compared the development of policies to protect critical information infrastructure in Canada, South Korea, the United

Kingdom, and the United States (OECD, 2007).

This shift in emphasis and approaches can also be seen in another document released by the Organization for Economic Cooperation and Development (OECD) to guide efforts to strengthen a cyber-security culture in 2002. One of the highlights of this document is that it uses the word "participants" instead of "member states". The principles mentioned in this document are:

- **Awareness**. Participants should be aware of the need for security systems and information networks and what they can do to enhance security.
- **Responsibility**. All participants are responsible for the security of information systems and networks.
- **Reaction**. All participants must take timely and participatory action to prevent security incidents and identify and resolve them in the event of such incidents.
- **Ethics**. Participants must respect the legitimate interests of others.
- **Democracy**. The security of information systems and networks must be consistent with the fundamental values of a democratic society.
- **Risk Assessment**. Participants should assess the risks and dangers.
- **Developing a security plan and implementing it**. Participants must make security an essential component of information systems and networks.
- **Security management**. Participants must take a holistic approach to security management.
- **Re-evaluation**. Participants should review and re-evaluate the security of information systems and networks and make necessary changes to security policies, actions, arrangements, and procedures.

The difference between this document and the document published in 1992 is significant. The document, published in 2002, uses the word "participants" instead of "member states." This means that the new document covers a variety of public and private organizations with different areas of national and international activity.

In the above document, apart from the principle of respect for the legitimate interests of others, there is no direct reference to international cooperation and agreement by establishing joint institutions. In fact, this document focuses more on the role of actors or participants than the activities of international organizations and agreements or mechanisms based on mutual cooperation. The principles of this document do not mention transnational activities, the importance or insignificance of borders, and respect or disrespect for borders. In fact, it seems that this document embraces or encourages the idea of a world without borders, but directly addresses the question of how governments, borders, or international cooperation come together in a framework.

Another report released by the Organization for Economic Cooperation and Development (OECD) in June 2011 entitled "A Report on Principles for Internet Policy Making" emphasizes freedom, transparency and participation of various actors in the policy making process. It also has a section on encouraging cooperation to strengthen Internet security. The report addresses security measures in the context of other goals; including innovation, economic growth, and social progress, and it highlights the importance of "market-based security standards":

Developing policies to address security threats and reduce vulnerabilities is important for the continued functioning of the Internet. The implementation of internationally approved market-based standards and guidelines on Internet security should be encouraged. In addition, research programs on new security systems which can adapt themselves to the vast complexity of ICT networks and information systems, should be encouraged. Policies which are made to strengthen the Internet security should not be a barrier to the conditions that enable the Internet to act as a free global arena for innovation, economic growth and social progress. Nor should these policies be used as an excuse to restrict Internet freedom. These policies should also seek to strengthen individual and collective efforts to protect themselves and increase trust and confidence. Before adopting and implementing these policies, their compatibility with, and their potential impact on, the other social and economic dimensions of the Internet must be carefully assessed through the process in which the various actors are involved (OECD, 2011).

Another report released in July 2016 by the Organization for Economic Cooperation and Development (OECD) entitled "Council Recommendations on Guidelines for the Security of Information Systems and Networks: Towards a Common Security Culture" was the result of a five-year review of the 2002 report. It included the principles of this report (OECD, 2012).
The report assesses the changing situation and notes that governments have given greater importance and priority to cyber security policies in recent years. The report also notes that the proposed directive is "voluntary and does not intend to interfere with the sovereignty of governments", and that the report does not propose a single solution to cyber security. However, it is now recommended to the member countries of the organization that:

- Modify existing policies, measures, arrangements and procedures or establish new policies, measures, arrangements and procedures to reflect or take into account the guidelines proposed in this report on the security of networks and information systems. To move towards creating a common security culture by accepting and strengthening the security culture outlined in the guidelines;
- Consult, cooperate and coordinate at national and international levels to implement the proposed guidelines;
- Promote the proposed guidelines in the public and private sectors, including government agencies, the business sector, other organizations and private users, to create a common security culture and hold all individuals and entities involved accountable and take the necessary steps to implement the suggested instructions in a way that suits their roles;
- Appropriately make the proposed guidelines available to non-member countries.

The report emphasizes the desirability of collective action and cooperation in security policies. However, the proposed cyber security guidelines also highlight the benefits of free trade and also emphasize that security measures should not impede the free flow of information, trade and capital. Instead of inviting member states to conclude a formal agreement as the main solution, the 2012 report provides guidance and urges member states and other participating parties to act accordingly. The report goes a little further than previous reports and calls on member states to

work together. This is because of the concerns raised about cyber security and the possibility that unilateral actions by governments could harm the free flow of information.

Since the Organization for Economic Co-operation and Development (OECD) comprises a small number of countries in the world, these countries have common approaches to economic growth and governance, resulting in the development of a set of guidelines on cyber security and cooperation and exchange of ideas on this issue. Under these circumstances, it seems that this organization can be better than other international organizations in institutionalizing the cooperation of member countries in this regard. At the same time, the guidelines developed by the Organization provide more norms for harmonizing the national policies of the Organization's member countries than inviting them to conclude a formal agreement. Although the Organization for Economic Cooperation and Development (OECD) consists of a small group of countries, the general principles and standards that this organization has provided regarding cyber security can be applied to other international forums as well. In fact, the principle of creating a common security culture has also been considered in UN resolutions (2003).

The Organization for Economic Cooperation and Development (OECD) has also concluded a number of formal agreements or memoranda in this area, the most prominent of which are the Transnational Data Flow Agreements, adopted in 1980 and 1985, with the aim of keeping borders open for the free flow of digital data. However, given the need for more comprehensive agreements on network security by the Organization, as well as the fact that many of the Organization's member states, are also the members in the Council of Europe, NATO and the Security and Cooperation Council, the lack of such agreements is interesting.

Conclusion

This study examined the efforts made by the International Organization for Economic Co-operation and Development (OECD) to strengthen international cooperation on network security. Although these efforts have received little attention in recent years due to unilateral actions by governments to defend ICT-related resources and strengthen their defense capabilities, the challenges ahead as well as the importance of strengthening collaboration and multilateral Internet management remains strong.

The multilateral efforts of the Organization for Economic Cooperation and Development (OECD) contrast with the efforts of large governments to ensure network security through national and technical approaches. However, while it has helped strengthen international cooperation on network security, it has refrained from directly addressing the issue of cyber militarization, perhaps because powerful governments are reluctant to see unilateral measures to their interest to stop, and at the same time weaker governments with less capability have shown little inclination to help stop their self-assistant systems. Or if they have shown this inclination, they did not have the ability to stop this system. Collective security and arms control have been implemented in some other areas, whether in small groups, multilateral agreements or in the form of the United Nations, yet in the area of cyber security it isn't still as successful as it should be. It has not been successful. Given the broad focus of governments on unilateral strategies and tools for ensuring cyber security, there appear to be major challenges to approaches based on international cooperation and the creation of

stronger international institutions to protect the freedom and security of information flow in cyberspace.

The Organization for Economic Cooperation and Development (OECD) has a long history of developing collaborative approaches to network management, indicating the general desirability of these mechanisms. One of the basic principles of this system has been to strengthen the benefits of using electronic networks, as well as to strengthen and protect the freedom of communication and use of these networks. The organization encourages efforts to combat cybercrime and illegal use of networks, but has not yet entered into cyber-wars between governments.

In many ways, the organization's actions run counter to arguments that criticize the desirability of adopting international cooperation approaches to cyber security. While governments themselves may disagree, there is no doubt that within the framework of the Organization for Economic Cooperation and Development (OECD), maximizing the benefits of increased trade, investment, technical change and similar policies in member countries can lead them to cooperate on providing network security. The Organization for Economic Cooperation and Development (OECD) also includes non-governmental advisory groups. The guideline issued by the Organization for Economic Cooperation and Development (OECD) on creating a common security culture uses the term "participant" instead of "member states", indicating the importance of the private sector actors in developing approaches based on cooperation on network security as well as efforts to minimize the separation between the public and private sectors. The goal of international cooperation based measures in the Organization for Economic Cooperation and Development (OECD) has been to minimize the costs of security efforts and to strengthen economic development, although the emphasis has shifted over time.

Regarding the feasibility of applying collaborative based approaches in the field of ensuring cyber security, the organization emphasizes the interdependence of all countries in interconnected electronic networks and that these networks are part of the vital internal infrastructure of all countries. The Organization for Economic Cooperation and Development (OECD) consists of powerful governments that have a market economy and are part of the developed world. The organization has mechanisms for negotiation, although member states may disagree with some of the organization's policies. In fact, the approach of the Organization for Economic Cooperation and Development (OECD) is to work in several sectors to identify different modes of cyber security and resolve these challenges optimally.

The actions of the Organization for Economic Cooperation and Development (OECD) in some sectors, but not in all, contradict the claim that it is impractical to use collaborative based approaches to cyber security. However, the member countries of this organization have common norms that are reflected in their history and goals. The organization has extensive research and information sharing programs that can be used to address the challenges posed by poor information security in network security. However, the ongoing emphasis on the broad role of governments in managing the Internet has limited the ability to generate and share information to resolve issues related to user authentication, identifying perpetrators of cyber-attacks, and dual use of network technologies. On the other hand, while technical changes have complicated any attempt to develop collaborative and interactive based ap-

proaches, the organization is taking technical changes into account and is taking steps to manage them. The members of this organization have different interests. Although all members in some way commit themselves to complying with international agreements that require governments to adopt certain policies and procedures in different sectors, given the nature and scope of the OECD's activities, it is unlikely that these activities will deter governments from using one-sided approaches and using any tools they deem more appropriate.

In general, the activities of this organization seem to show that adopting more detailed approaches, instead of global approaches, regarding international cooperation are effective to strengthen network security. One form of these minor approaches is the conclusion of regional agreements, such as the Organization for Economic Cooperation and Developments', among a group of governments that can help develop common norms and practices. The interaction of middle-level policymakers in these countries with each other in the long run can lead to the formation of a common understanding on various issues and topics among them.

In general, the goals and aspirations set for collaborative based approaches to network security have been too ambitious and out of reach that they are unlikely to be achieved in the international arena. These ambitious proposals and aspirations have often manifested themselves in the form of far-reaching treaties and agreements. It seems that by concluding regional agreements and agreements that deal only with certain sectors, this problem can be solved and the existing views on the challenges and resolving these challenges in this sector can be given direction again. Another issue in this regard is the historical and incomplete nature of institutionalization in this area. In many cases, the set of decisions and agreements is more limited, which over time helps to build understanding, action and common institutions. Even when an institutional framework is relatively stable and well developed, full cooperation and participation of governments within that institutional framework (such as trade and investment or dispute resolution) will not always occur. A historical and more accurate understanding of these processes, as we have seen in some of the analyses mentioned in this study, can help identify the next important steps.

References

Bajaj, K. (2010). The cybersecurity agenda: Mobilizing for international action. Available via The East West Institute. http://www.ewi.info/system/files/Bajaj Web.pdf

Barman, S. (2006). Change of state: Information, policy, and power. Cambridge MIT Press.

Berlin, I. (1958). Two concepts of liberty. In Isaiah Berlin (1969), Four essays on liberty. Oxford: Oxford University Press.

Castells, M., & United Nations Research Institute for Social Development. (1999) Information technology, globalization and social development. Geneva United Nations Research Institute for Social Development

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the internet, international relations, and global security. Bulletin of the Atomic Scientists, 68(2). 70-77.

Donohue, M. (2003). Consumer protection across borders: OECD work to build consumer trust in the digital economy. Presentation at the OECD/UN/World Bank Global Forum: Integrating ICT in Development Programmes, Paris, 5 March 2003.

East West Institute. (2010). Protecting the digital economy: The first worldwide cybersecurity summit in Dallas. Dallas, 2010.

Enright, A. (2011). Global e-Commerce to Reach $1.4 Trillion in 2015. International marketing http://www.internetretailer.com/2011/06/07/global-e-commerce-reach-14 trillion-2015. Accessed 30 Oct 2012

Ford, C. A. (2010). The trouble with cyber arms control. The New Atlantis Fall. 29. 52-67.

global information infrastructure. Cambridge: MIT Press.

Goldsmith, J. (2011). Cybersecurity treaties: a skeptical view. In: Future challenges in national security and law. http://media.hoover.org/sites/default/files/documents/Future Challenges Goldsmith.pdf

Goodman. S. E. Kirk, J. C., & Kirk, M. H. (2007). Cyberspace as a medium for terrorists. Technological Forecasting and Social Change, 74(2), 193-210.

Greathouse, B. Craig (2015). Cyber War and Strategic Thought: Do The Classic Theories Still Matter? In Jan-Fredrik Kremer and Benedict Muller, Cyberspace and International Relations (PP. 21-40), Springer.

http://www.carlisle.army.mil/dime/documents/China's%20Cyber%20Power%20and%20America's%20National%20Security%20eb%20Version.pdf.

http://www.nextgov.com/cybersecurity/2011/01/internationalcybersecurity treaty-might-not-be-achievable-report-says/48282/

Hughes. R. (2010). A treaty for cyberspace. International Affairs, 86(2), 523-541.

Kahin, B. & Nesson, C. (1997). Borders in cyberspace: Information policy and the

Keohane, R. O. (1984). After hegemony: Cooperation and discord in the world political economy. Princeton, NJ: Princeton University Press.

Keohane, R. O., & Nye, J. S. (2001). Power and interdependence (3rd ed.). New York: Longman

Kiggins, R. D. (2011). Wired world: US policy and the open door intemet, Dissertation, University

Koh, HH. (2012). International law in cyberspace. Remarks at USCYBERCOM Interagency Legal conference. Ft. Meade, MD. Retrieved September 18. 2012. from http://www.state.gov/s/l/releases/remarks/197924.htm.

Layne, C. (2006). The peace of illusions: American grand strategy from 1940 to the present. Ithaca: Cornell University Press

Mathieu, G. (2007). Cyberterrorism: Hype or reality? Computer Fraud & Security. 2007(2), 9-12.

McCarthy, D. R. (2011). Open networks and the open door: American foreign policy and the narration of the internet. Foreign Policy Analysis, 7(1). 88-111

Noieim. G. T. (2010). Cybersecurity and freedom on the internet. Journal of National Security law and Policy, 4, 119-137.

Nye. J. S. (2011). Nuclear lessons for cyber security. Strategies Studies Quarterly

Organization for Economic Cooperation and Development. (2001). Business to consumer electronic commerce: An update on the statistics. Paris: OECD.

Organization for Economic Cooperation and Development. (2002). OECD guidelines for the security of information systems and networks: Towards a culture of security. http://www.oecd.org/dataoecd/16/22/15582260.pdf.

Organization for Economic Cooperation and Development. (2004). Electronic commerce. http://www.oecd.org/development/electroniccommerce.htm.

Organization for Economic Cooperation and Development. (2005). The promotion of a culture of security for information systems and networks: Towards a culture of security. http://oe.cd/2002sg.

Organization for Economic Cooperation and Development. (2007). Development of policies for the protection of critical information infrastructures. In: Report on OECD ministerial meeting on the future of the internet economy. Seoul. 17-18 June 2008. Retrieved from http://www.oecd.org/sti/40761118.pdf.

Organization for Economic Cooperation and Development. (2011). Communique on principles for internet policy-making. In: OECD high level meeting on the internet economy. Paris, 28-29 June 2011. Retrieved from http://www.oecd.org/internet/innovation/48289796.pdf.

Organization for Economic Cooperation and Development. (2012). Cybersecurity policy making at a turning point: Analyzing a new generation of national cybersecurity strategies for the internet economy. OECD Digital Economy Papers. doi:10.1787/5k8zq92 vdgtl-en.

Organization for Economic Cooperation and Development. (2012). The role of the 2002 security guidelines: Towards cybersecurity for an open and interconnected economy. OECD Digital Economy Papers. doi: 10.1787/5k8zq930xr5j-en. Tanner. E. (2012). US rejects telecommunications trendy, In: The New York Times Retrieved December 13 from http://www.nytimes.com/2012/12/14/technology/14ihttreaty

14.html?r0&adxnnl_1&pagewanted-1 & adxnnx=1363493660 ngCpGplj9 LwTJSızmwbxg,

Organization for Economic Cooperation and Development. (2012a). Recommendation of the council concerning guidelines for the security of information systems and networks: Towards a culture of security. acts.oecd.org/instruments/Show Instrument View. aspx? Instrument ID=116&La

Rothkopf, D.J (1998). Cyberpolitik: The changing nature of power in the information age. Journal of International Affairs, 51, 325-360

Schjolberg, S., & Ghernaouti-Helie, S. (2011). A global treaty on cybersecurity and cybercrime. (2nd ed.). http://www.cybercrimelaw.net/documents/A Global Treaty on Cybersecurity and Cybercrime, Second edition_2011.pdf

Sofaer, A. D. Clark, D, Diffie, W. (2010). Cybersecurity and international agreements in: Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. Policy, Committee on Deterring Cyberattacks: Informing Strategies and Developing Options: National Research Council. Available: https://download.nap.edu/catalog.php ?record id=12997.

Spade, J. M. (2012). Information as power: China's cyber power and America's national security. Carlisle Barracks, PA, US Army War College

Sternstein, A. (2011). International cybersecurity treaty might not be achievable, Report says. Available via Next gov.

Sternstein. A. (2012). U.S., Russia, other nations near agreement on cyber early warning pact. Available via Next gov. http://www.nextgov.com/cybersecurity/2012/12/us-russia-other-nations-near

Tigre. PB and O'Connor. D. (2002). Policies and institutions for e-commerce readiness: What can be developing countries learn from OECD experience? In: OECD. Development Centre. Technical Papers No. 189. Paris: OECD Publishing

Wirtz, James J. (2017), Intelligence and National Security, The Cyber Pearl Harbor, 32;6, 758-767

Zacher, M., & Sutton, B. (1996). Governing global networks: International regimes for transportation and communications. Cambridge: Cambridge University Press