Kamil TARHAN
International Islamic University Malaysia
https://orcid.org/0000-0003-4668-7920

DOI : 10.14746/ps.2022.1.23

HISTORICAL DEVELOPMENT OF CYBERSECURITY STUDIES: A LITERATURE REVIEW AND ITS PLACE IN SECURITY STUDIES

INTRODUCTION

Today, cybersecurity is an integrated multidimensional workspace that includes individual, economic, and corporate security issues. This is because cybersecurity studies are very different from classical military security problems and traditional security fields. For example, a computer anywhere in the world could be part of an attack on the defence systems of any state or area. This situation can remove the physical boundaries drawn in time and space and gains a universal quality (Arquilla and Ronfeldt, 1993: 155). The fact that cybersecurity is not tied to any geographic area increases the importance of this area in terms of operation. The increasing importance of critical infrastructures, especially in the centre of attacks and threats, has also directly affected the work on the protection and sensitivity of these areas (Bendrath, 2001; Westrin, 2001).

Therefore, at the beginning of the 2000s, cybersecurity studies were increasingly addressed in the social sciences and has started to be discussed for political reasons, besides computer and engineering fields (Lewis, 2002). These studies especially focus on the theoretical framework within international relations (IR) and have taken care to deal with cybersecurity studies from a theoretical perspective (Eriksson and Giacomello, 2006). In general, due to the impact of critical security studies and the contribution of the Copenhagen School's securitization theory, cybersecurity studies have been analysed within the scope of security studies (Nissenbaum, 2005; Cavelty, 2008; Hansen and Nissenbaum, 2009). Undoubtedly, changes in security studies and efforts to redefine security also have been influential in evaluating cybersecurity studies within security studies. Furthermore, with the Internet and technology beginning to be included in security definitions, it has become a necessity to include certain concepts and phenomena in these studies.

On the other hand, leading from the attacks and increasing cyber threats in Estonia in 2007, cybersecurity studies have started to be examined with different approaches on a global scale. Apart from the issue of national security or international relations, it has begun to take shape through the interplay between politics, technology, and science as an international security policy. It appears as a field that needs political and social sciences as much as it needs engineering sciences (Kello, 2013: 16). According to Cavelty and Wenger, studies in cybersecurity are generally

handled in two ways. The first method is to approach cyber incidents from a more political perspective and examine the behaviour of governments in terms of governance. The second method is to address the risk situations and security vulnerabilities created by security companies in terms of information technology (IT) (Cavelty and Wenger, 2020). This fact also shows that cybersecurity studies are progressing in a multi-disciplinary manner. Cybersecurity does not have a fully agreed definition and it has not developed only as a sub-branch or field of study in an academic field. Studies have progressed as a field that benefits from many disciplines and develops its scope with each passing day. This situation has made it difficult to grasp the scope of cybersecurity studies (European Union, 2020: 13).

There is no legal binding and sanction mechanism for the anarchic structure of the cyber field, which does not consider national and international boundaries. The increasing rate of cyber weapons and attacks has rapidly caused nation-states and international actors to work in this field. Cyber threats have completely changed traditional security threats, and the resulting risks are very new. Cybersecurity has now turned into a primary security area for many governments and international actors. Therefore, over time, cybersecurity might be considered a multidisciplinary field according to international events, actors, and academic studies.

In this context of this study the development of cybersecurity studies be examined by considering historical developments. Then, it will investigate how and why cybersecurity studies are handled in security studies. Finally, the idea that cybersecurity studies should be expanded over time and expressed as a multidisciplinary field will be discussed.

THE BEGINNING OF CYBERSECURITY STUDIES (1969–2000)

Cyberspace began to form with the technological struggle that started between the USA and the Soviet Union during the cold war period (Darıcılı, 2018: 312). The first satellite was sent into space by the Soviets, followed by the USA's space studies and the creation of the Advanced Research Projects Agency (ARPA) in parallel with these studies, and then its transformation into the military-grade ARPANET which is the basis of the Internet. (Bıçakcı, 2014: 104). The technological struggle between the two superpowers has progressed by intertwining with science-technology and politics. Like the institutions created by the USA, the Soviet Union also created its own technological institutions. In contrast to institutions such as ARPANET or RAND (research and development) created by the USA, the Soviets furthered their scientific studies under The Scientific-Technological Revolution (Nauchno-Tekh Nicheskaia Revoliutsiia – NTR) (Tarhan, 2020a: 200).

The emergence of the Internet and the connections initially created with certain computers began to increase in the 1980s. In this period the first evidence of malicious software was formed and some cyber events occurred. The Siberian Natural Gas Explosion (Logic Bomb) that occurred in 1982 is a prime example (Yılmaz, 2017: 34). In this period, studies on cyberspace began to form gradually. During this evolution phase, we started to see examples of actions taken by presidents of

the United States of America (USA), leading to their increasing role in the development of cyberspace and the internet. Because, as actor US presidents and the USA has an important actor position in the development processes of cyberspace and the internet environment. Both the statements made and the action decisions are taken prove this situation. For example, during the John F. Kennedy era, national telecommunications systems were dealt with, starting to be heavily involved. During the Jimmy Carter era, the document titled 'Continuity of the State' covering information processing and communication systems was signed in June 1980. In addition, Ronald Reagan was the first US President to address the problem of cyber-threats in today's sense. Reagan was also a main actor on the global scale, directly referring to these threats and evaluating them in terms of national security (Cavelty, 2008: 44). However, the importance of cyberspace for critical infrastructures in today's sense was first started when the Clinton administration recognized cybersecurity as a problem in the 1990s (Buzan and Hansen, 2009: 248; Boys, 2018: 760). This process can be expressed as the securitization of non-traditional security threats by securitizing actors. The USA and its political elites have formed an international discourse with securitizing discourses on cyberspace and cybersecurity.

The matter of cybersecurity also became a high-priority agenda for many other countries in the 1990s. The USA continued to direct its cybersecurity policies as an active actor in the early periods when it started to form serious studies and discourses. In the 1990s, the USA National Academy of Sciences started its report on computer security by saying, "…we are at risk." It was remarked that the USA is becoming more dependent on computer systems every day. According to the National Research Council report, it was noted that hackers would cause more damage to the state's security via computers than bombs in the following years (National Research Council, 1991: 7). In essence, it can be indicated that there was an early prediction of all security vulnerabilities related to cybersecurity and the Internet, or an important international actor securitized this area in the early periods. With this report, the USA became the first country to focus on national critical infrastructures related to cyber security. By defining possible scenarios as an Electronic Pearl Harbour, the USA tried to predict what the new threats might be (Bendrath, 2001: 82). Therefore, the USA expressed in the early periods that this area was significant, and with the Pearl Harbour analogy, it indirectly influenced other countries to work on this area. Furthermore, cybersecurity studies started in the USA as a discourse (Lawson and Middleton, 2019), opening opportunities for its implementation on a practical level and discussing information and computer security.

With the increasing threats in cyberspace that have targeted critical infrastructures and caused direct damage to economic sectors, the security policies that need to be made have also taken shape. For example, in 1994, with the Rome Laboratory incident, high-level computer systems in the USA were infiltrated. In the same year, $10 million was transferred from Citibank to accounts in other parts of the world. In 1998, the Solar Sunrise and Moonlight Maze incidents were recorded as early cybercrime and cyber espionage incidents. In the same year, the Dutch Hacking was recorded as an incident in which confidential information was leaked by accessing computers in the Pentagon (Cavelty, 2017).

There were also attacks that directly targeted countries and international organizations. The first of these is the First Gulf War in 1991. Cyber incidents that occurred mainly in the form of conflict, are cited as the methods used by the U.S. air force and military to control information from intelligence, surveillance, and reconnaissance (ISR) (Krepinevich, 2012: 15). Another important event is the interruption of communication between member states with attacks on the information systems of the North Atlantic Treaty Organization (NATO) during the Kosovo war. It has been reported that these attacks were organized by anonymous Serbian hackers (Verton, 1999). On the other hand, as a result of the accidental bombing of the Chinese Embassy in Belgrade, cyber-attacks were also announced by China (Messmer, 1999). The most important feature of this attack is that it was the first time that a cyber-attack targeting NATO took place.

These attacks have brought into account the risks posed by the internet environment in general for many nation-states, international organizations, multinational companies, private companies, and individuals. Progress has been made with some studies on the security of computers and networks and the protection of personal data. Parallel to these studies, terminology has been tried to be formed regarding the possible threats that may occur in cyberspace. The concept of cyber warfare is an example of the terminology used as a new type of warfare (Arquilla and Ronfeldt, 1993). In addition to the concept of cyber warfare, some authors have also used the concept of information warfare in their studies on cyberspace (Anderson and Hearn, 1996). These concepts coincide with the mid-1990s spread of the internet on a global scale. It has been observed that the concepts produced against the types of attacks are renewed and developed day by day. The risk situations and vulnerabilities that these concepts want to emphasize have changed conceptually over time and have been evaluated as computer security and network security (Arquilla and Ronfeldt, 2001). The terminological ground that is tried to be formed conceptually is generally called the information age (Gompert, 1998). Towards the 2000s, studies in this field have progressed conceptually and analyses the unique features of cyberspace and concepts related to cyber security (Johnson and Post, 1996; Lessing, 1996).

The works produced in the 1990s paid special attention to the importance of cybersecurity to the world. Arquilla and Ronfeldt presented road maps that showed how vital this field would be in the coming years. One of the most prominent of these was "Cyber War Is Coming." This study briefly argued that the information revolution has taken place and that wars will be formed around information and technology in the next period. The importance of cyber activities has been referred to as the extent of its reach. For example, in the thirteenth century, the Mongols succeeded due to the enormous communication and information transfer between the command centre and the soldiers in the field. In this context, the concept of cyber warfare was used for the first time (Arquilla and Ronfeldt, 1993: 142). The concept involves the technological and cyberspace situations that may occur in the military field. In the authors' study, some determinations were made on the concept of netwar, and its difference from cyber warfare was explained. This study predicts information and computer security, conflicts and attacks that may occur in the military field over time. Information has become one of the most important factors of security at the end of the twentieth century.

Studies carried out until the 2000s focused on the nature of cyberspace, the threats that may occur and the legal norms required in this field in terms of content. In addition to states' national security, studies have been carried out on the protection mechanism against individual rights violations and how any legal rule will be applied. By defending the idea that cyberspace should be taken seriously, some have argued that this area will create its own rules and legal norms over time (Johnson and Post, 1996: 1387). However, there have been debates as to whether the social norms to be created in this area will function, as states begin to regulate them in the real world. It is indicated that it is challenging to foresee how much society will internalize the established rules in this abstract area (Lessig, 1996: 1407). Such studies advocated that individuals should be protected against violations of rights in this abstract area outside of the state. The necessity of legal regulations in this field has been mentioned.

Even though the debates began with an orientation toward different fields, various institutes and writers have continued to address the security threats raised by cyberspace. In other words, the institutions managed by the USA have created studies on the securitization of the area. Supported by RAND Corporation, the authors remarked that crimes related to network warfare are increasing, and they are different from cyber warfare and information war concepts. The authors tried to reveal the differences by defining the network war. The term netwar "connotes that the information revolution is as much about organizational design as about technological prowess and that this revolution favours whoever masters the network form" (Arquilla and Ronfeldt, 1996: 7). Several works, including the studies of Arquilla and Ronfeldt, have shown how to bring concepts of cybersecurity, cyber warfare and network war into literature and shape them according to the interests of the USA. In another work published by RAND, Anderson and Hearn discussed the second of the "The Day after…" project (the first is "Nuclear Proliferation in the Post-Cold War World Volume I, Summary Report") and ARPANET employees. After RAND built the Internet, the researchers discussed the projects and actions that should be done to solve the problems that started in this area (1996: 1). Although RAND put forward ideas in the interests of the USA, it also made a significant contribution to the development of cybersecurity studies. For many authors, RAND has been an overlooked institution in cybersecurity studies. However, it represented the critical stage of benefitting all humanity that RAND remarked while defining itself.

In the international arena, the IT and information revolution took place in the 2000s. In the information age period, optimistic ideas and discussions have occurred about how knowledge will develop nations. Some authors focused heavily on how the information revolution can liberate nations and develop them in both economy and knowledge. This will strengthen nations, individuals, and governments to the point of freedom. According to Gompert, 'the information revolution has strengthened the relationship between freedom and knowledge and that between knowledge and power, it links power to freedom' (Gompert, 1998: 23). Gompert also describes how the democratization movement is progressing positively around the world due to technology. The development of Japan and Germany, the dissolution of the Union of Soviet Socialist Republics, and the importance of underdevel-

oped third-world countries in world politics have been realized due to democratization of knowledge. Information is at the heart of many cybersecurity issues that occur every day. Since the 1990s, information has been increasingly secured and has been a priority area. The common features of these regions, such as cyberspace and the Internet, focus attention on the controlling of information and ensuring information security. Therefore, information is a priority for all events derived from the concept of cyberspace.

Ralf Bendrath, on the other hand, has reused the concept of risk society which was first employed by Ulrich Beck. According to Bendrath, the information society shows the most important signs of being a risk society in the current conditions. Using early periods of cyber warfare, the author discussed this concept from the perspective of protecting critical infrastructures. Bendrath indicated that cyber warfare threats had changed traditional security threats, and the risks that now occur are very new and challenging to define (Bendrath, 2001: 80–81). Some nation-states, such as the USA, have started to form statements regarding the protection of critical infrastructures. However, this development began to be an element of security at a late time. In connection with the space created by cyberspace, all cases have gradually taken place in the literature.

The concept of cybersecurity was not used directly in the early periods of the works that dealt with cyberspace. Some have observed that studies on the security of critical infrastructures or security in the information age have only recently emerged. In the information age, when there were no serious attacks on computer systems, Westrin also mentioned the threats against information infrastructure. He marked those critical infrastructures have now reached a vital security point. Westrin explained that in the past, the vulnerabilities that occurred in societies were generally predictable and externally sourced. However, the author indicated that these threats were now called insider threats, and it was complicated to predict them, and mentioned that information could be stolen and used for malicious purposes. Westrin explained that a problem occurring in critical infrastructures could impair trust in the social field, which he describes as a network society (Westrin, 2001: 71). The author specified that today's telecommunication and computer systems are spreading into the whole social and state sphere. All areas are integrated, from energy to transport, service, finance, and government services. Therefore, the security of these areas can be expressed as important to ensuring national security.

Some authors also contributed to the studies in the literature by defining the new era as the information age. Keohane and Nye focused more on increasing interdependence and power in the information age. The information revolution has not yet taken place and some state that we are still at the beginning of this process. However, the authors defined the new world as a world in which security and force matter less and countries are connected by multiple social and political relationships' (Keohane and Nye, 1998). They highlighted that it is not only about politics but also social factors. Although it is understood that security and power are pushed to a secondary plan here, it is noted that security has reached a more prominent point in this period, as states have just discovered the importance and status of critical infrastructures.

CYBERSECURITY STUDIES AS A SUB-BRANCH OF SECURITY STUDIES

The Formation of Security Studies

It is widely accepted that security studies emerged as a sub-branch of international relations during the Cold War (Baldwin, 1995: 118). Security studies were viewed as a specific field of research rather than as a discipline. One of the main factors in developing security studies is the emergence of the Cold War and the systems created as a result. Especially after the atomic bomb development, US foreign policy and technological developments in the military field allowed the field to expand (Nye and Lynn-Jones, 1988: 8). Another reason for the emergence of security studies is that the security approach in the interwar period focused only on military issues in a very narrow academic way. Therefore, after the Second World War, the idea that the issue of security is a military issue that should not be left to military generals has prevailed. In this context, the field of study has emerged with the inclusion of civil experts and institutes in this field. It is noteworthy that the development of the studies mainly proceeds in the context of the debates over the theories, schools and concepts of IR (Birdişli, 2019: 79).

Security studies generally expanded in the Anglo-American world after the Second World War. The special situation in its development here was that concepts, assumptions and findings assisted the USA to survive, meaning that discourses and policies have shaped security studies and strategies to ensure the national security of the USA. This situation has centred security studies in the West over time. In the first period of studies, security in the USA was examined under the name of National Security Studies and was called Strategic Studies in the United Kingdom. Ultimately, the basic assumptions of both nomenclatures became apparent as the military dimensions of state and security (Bilgin at ell., 1998: 134).

RAND Corporation was the main producer and contributor of security studies between 1950 and 1970, during the golden age of security studies. This issue has led academics to approach national security issues from a more military perspective due to the easy access to information and the close relationship with the US Department of Defence (Walt, 1991: 214). According to other authors, the golden age refers to the deep intellectual debates that occurred between 1955 and 1965 regarding the security of nuclear weapons, the control of weapons and how to use them. After the first formation of security studies, the phase has progressed differently and developed more through deterrence. Deterrence theory is expressed as one of the successful outcomes of this period (Baldwin, 1995: 123) According to Waver and Buzan, deterrence theory has emerged as an essential turning point in security studies or as the founding myth of their expression. Furthermore, deterrence theory has enabled civilian experts (e.g. political elites and academics) to take more active roles in the field and nurture the policy field by easing military institutionalization (Waver and Buzan, 2017).

Since the beginning of the Cold War, national security has been defined narrowly by US administrators and policymakers, and extreme military terms have been emphasized. The purpose here is that the discourse created through military methods will be

accepted more quickly by the public. This situation started to be criticized towards the end of the 1980s. The excessive increase in allowances for military expenditures, especially in the USA, caused other areas to be neglected. This situation gave rise to two issues. First, that paying attention to military security allows other areas to be ignored and reduces overall security. Secondly, it contributes to widespread militarization of IR and increases the atmosphere of insecurity in the long term (Ullman, 1983: 153). Because of this, towards the end of the Cold War, the need to redefine national security was introduced. During this period, national security, in a broader sense, was affected by many situations, such as demographic structures, environmental disasters, transboundary migration, access to energy resources, and using scarce resources. Because of all this, the boundaries of national sovereignty have become more ambiguous, and there is a need to redefine national security (Mathews, 1989: 162).

Security studies have been shaped by different stages from the emergence process to the present day. The hypothetical structure of each period has shaped security studies in ontological, epistemological and methodological terms. Undoubtedly the biggest breaking point of security work was the collapse of the Berlin Wall, the end of the Cold War and the collapse of the Soviet Union. According to Bilgin, security approaches after the 1990s were accepted as the new security approach because after the 1990s, military issues were no longer the only security issues. Security issues have expanded and developed theoretically, including humans and the environment (Bilgin, 2010: 73). In the post-1990 period, thought and discipline began to be questioned and criticised in every sense, and the formation of new schools and theories was increasingly influential. The multifaceted expansion of liberalism, the growing importance of schools such as feminist theory, social construction and critical security studies have led to the evolution of the theoretical framework. These theoretical and critical thinking environments have led to states' level of analysis of the nation and the individual (Smith, 2020: 61).

In the post-Cold War period, some journals and articles were influential in the progress of security studies. International Security Journal is one of the most notable of these. In the post-Cold War readings of this journal, it was emphasized that technological activities were directly central to military elements. Thus, revolutions in the military field, air defence systems and conventional technologies were included in the security readings (Miller, 2001: 9). This situation has had an academic impact on including Internet and cybersecurity issues in security studies over time. As a result, a number of journals have started to consider cybersecurity as a sub-branch of security studies with theoretical frameworks, such as the Copenhagen School.

Cybersecurity Studies in Security Studies

Information has become the leading research subject for security policies and a factor whose reliability must be ensured in the 2000s. Information has reached a functional and complementary position which is at a more critical point than military and physical materials. While knowledge contributes to developing technology, it has also caused a change in world politics. Classical security reading approaches have become

inadequate in the twenty-first century. As with the wars of the Gulf and Kosovo, technology produced by knowledge has changed the course of battles. Due to the Internet and fiber-optic cables, information has reached a point where it can be accessed worldwide simultaneously. Of course, in this process, it has created security vulnerabilities and weaknesses within itself.

Along with this realization, there have been studies on the point of network security. As an organizational form and actor, networks have enabled the differentiation. of world politics and developed new approaches. Post-2000 networks and the capture of these networks by some enemies led to the development of different tools and expanded analysis units. However, these networks occur not only with the Internet. The themes of these forms of organizations, such as terrorist groups, which are called social networks and arose in post-industrial societies, are also accepted as networks. Al-Qaeda, which came to the fore with the 9/11 attack, is one of the social networks that is cited as an example (Deibert and Stein, 2002).

The concept of cyberterrorism started to be used in the literature after the 9/11 attacks. Cyberterrorism is briefly expressed as an attack on all critical structures owned by any state through a computer. The purpose of such attacks is intended to intimidate the government or civil society within the target country. The impact of the 9/11 attacks on the development of the concept of cyberterrorism has become significant. It has led to many countries attempting to prevent security vulnerabilities in computer networks to ensure national security (Lewis, 2002). The attack of terrorist groups on the twin towers of the USA led to another transformation in terms of security. The events of September 11 increased the interest in computers, IT and security. This attack, in which computers and radar systems were seized remotely, caused many nation states, especially the USA, to form new discourses and strategies in security.

After the attack on the twin towers, the significance of concepts such as information security, computer security, communication security and cybersecurity increased considerably as the number of studies multiplied. Security studies experts dealing with cyber-related issues have worked using similar concepts. The concept of cyber warfare was developed in 1992 by Der Derian and in 1993 by Arquilla and Ronfeldt. Network warfare and network security were developed in 1996 and 2001 by Arquilla and Ronfeldt and also by Deibert and Stein in 2002. Der Derian's work in 2003 is also essential. In addition, Bendrath's study in 2003 focused on the protection of critical infrastructures. Denning's study in 1999, Deibert's study in 2003, Der Derian's study in 2003 and Latham's study in 2003 all focused on information security and information warfare. The purpose of specifying these studies is to show the transition of cybersecurity studies to the field of security studies (Hansen and Nissenbaum, 2009: 1156).

Studies on security underwent major changes after 2001. The phenomenon of war has changed; the importance of asymmetric tactics and strategies has intensified, and its priority for national security has been understood. Thus, the effect and power of globalization, the Internet and the technological developments of states have increased enormously (Erendor, 2018: 59). For countries, the importance of asymmetric power has become evident in any possible war situation. In this context, an idea has been developed that modern and technology-related phenomena such as cyber and information warfare should be addressed (Kay, 2004: 17).

The works in which the security of critical infrastructures, information society, the global information age and cybersecurity are discussed in the literature have increased in recent times. Especially after 2001, the intensity and depth of these studies were increasingly addressed in IR theories. Some authors have systematically discussed the shift from traditional security understanding to security understanding in the information age. Within the study, the authors' analyses were mainly in IR theories. There has been a detailed study on the comparison between the arguments of the theories relating to cybersecurity (Eriksson and Giacomella, 2006). In addition to the direct IR studies, when cybersecurity studies are evaluated within security studies, the protection of information and all critical infrastructures produced by information become a priority area, and governments begin to invest in these areas to ensure cybersecurity. National cybersecurity strategies and action plans followed these investments. First, the USA published its national cybersecurity strategy document in 2003 (Tarhan, 2020b: 41).

Initially, cybersecurity is generally used in the same sense as information security in the literature, but there are opinions stating that these two concepts differ in terms of content and features. For example, according to Rossouw von Solms and Johan van Niekerk, "cybersecurity is different from information security, although it is generally used as a similar term for information security." Information security protects information, an asset, from possible damages that may arise from various threats and vulnerabilities. On the other hand, they stated that cybersecurity is the protection of cyberspace, those who function within it and any of their assets that can be accessed through cyberspace (Solms and Niekerk, 2013: 101).

Cybersecurity studies has been shaped according to the content and discussion topics of the studies over time. What has been expressed here is shown as the underlying reasons for the need to redefine national security and national interests. The rapid increase in global interdependence through telecommunication has brought about increased risks. Therefore, there has been a development and change in the national security approach. The difference in national security approaches has progressed in parallel with cybersecurity studies. In the early periods, when cybersecurity studies were integrated into security studies, its place in the social sciences dictionary was at a developmental stage. With the expansion of technological parameters, technical terminology began to emerge. Although it was seen that there was no agreed ontology on all aspects of cyberspace in this early period (Choucri, 2016: 6), it was deemed sufficient to be evaluated in security studies.

The increasing use of social media has caused many bureaucrats and state leaders to move towards this area to develop their diplomacy using these new methods. Especially according to the liberal school, increasing access to cyberspace supports the development and dissemination of political ideas, civil society and organization, and the development of transnational social networks. Thus, liberalism asserts that diplomacy may diversify and transition to digital diplomacy due to cyberspace, while believing that cyber access will shape state behaviour. Likewise, it is argued that it may affect state and international politics (Choucri and Reardon, 2012: 7). Therefore, cybersecurity studies have become a national imperative for many nation states and, over time, a top priority area for governments. Furthermore, it is thought that both economic

infrastructures and national security will be improved by strengthening cybersecurity and providing more rigorous defence (Nojeim, 2020).

Changes in classical security studies have had a significant impact on the cybersecurity evaluation within security studies. Some of the primary studies in the literature show that the shift in security and redefinition efforts are different. Barry Buzan's work, which is generally accepted and often referenced, is one example of these studies. This work has been remarkable because it encompasses more than just industry and military elements. Barry Buzan divided security into five sectors, one of which was technology (Buzan, 1983) and the work has had a significant influence on future research. However, because elements such as technology for classical realism and positivist thought have always been discussed in the low politics field, it was noted towards the end of the Cold War that technology and cyberspace played a role in high politics. In this sense, Buzan's work paved the way for today's cybersecurity and technology studies to be a significant factor in state and national security studies.

In the evaluation of cybersecurity studies directly in security studies, the contribution of the securitization theory of the Copenhagen School is significant. Nissenbaum used this theoretical framework to evaluate cybersecurity by adhering to the structure and arguments of securitization theory. Then, focusing on the changes over time, he underlined why and how cybersecurity studies differ from computer and network security. According to Nissenbaum, computer security directly refers to specific networks and a narrowly specialized situation, only focussing on technical issues. At the same time, cybersecurity studies are identified with national security policies on a broader scale because cybersecurity studies are discursively securitized and have political goals (Nissenbaum, 2005). This study is essential both for the evaluation of the cybersecurity issue in security studies and for applying the securitization theory in this field. According to Buzan et al., they emphasized that the sector generally considers five sectors, one of them was technology. Nissenbaum's work is essential for adopting a new sector with its own analysis units and its own field of study. She argued that apart from the five sectors, a sector called cybersecurity studies should also be formed This work is regarded as a pioneer work in security studies discussing cybersecurity (Garcia and Palhares, 2014: 275).

Cavelty advocates the evaluation of the cybersecurity field under security studies and puts forward that new analysis units should be added. According to the author, along with new analysis units, threat policy should also be expanded so that the securitization theory can be applied in the field of cybersecurity. However, the author directly states that cybersecurity studies should be evaluated within security studies (Cavelty, 2010: 23–25). Beyond the securitization theory and the five sectoral distinctions created by the Copenhagen school, it is also advocated that cybersecurity studies should be determined as a different sectoral study area. This sectoral distinction, categorized by Buzan, has begun to be insufficient for cybersecurity and security studies. The reference objects of security studies are associated with cybersecurity, using concepts such as excessive securitization, daily security practices and technicalization (Hansen and Nissenbaum, 2009).

Cyber threats created through computers are considered the most severe threat to national security. These new threats are different from other post-Cold War threats. The

main reason is that national security studies have always been about the construction of threats and the definition of those threats. Unlike environmental problems, social movements, the economy and other transboundary threats, cyber threats have occupied a significant position in the field of national security. This is because the risks posed by cyber threats are much more pronounced and associated with future events (Cavelty, 2010). In other words, these threats are more easily securitized, and reference objects are accepted socially. Furthermore, cyber threats are defined by concepts such as the number of cyber-attacks, cybercrimes, cyber terrorism, cyber espionage, cyber fraud, and cyber warfare. Therefore, it seems possible to evaluate cybersecurity within security studies.

In developing cybersecurity studies in the literature, increasing interest in science and technology studies (STS) can be noted, apart from those mentioned above by theoretical and IR experts. In addition, the securitization of cybersecurity has revealed how cyber threats in this field are discursively applied and for what political purposes they are created (Stevens, 2018: 2).

DIFFERENT VIEWS ON THE MULTIDIMENSIONAL NATURE OF CYBERSECURITY

Cybersecurity started to take place on the international agenda as well beyond national issues. Situations such as Estonia 2007, Georgia 2008, Stuxnet 2011, Aramco 2012, Ukrainian Grid 2015, and the USA 2016 elections were instrumental in influencing this. In fact, cyber-attacks and cyber threats, to which the concept of cybersecurity refers and is related, were partially used before 2007. However, its effect was not as significant as in the Estonian case. The Estonia incident attracted significant attention because for the first time, a state could not use its critical infrastructure due to a cyber-attack. Unlike many previous attacks and cybercrimes, it had consequences beyond espionage and information leaking (Estonian Foreign Intelligence Service, 2020). Attacks targeting the entire information infrastructure of Estonia caused the country to come to a standstill. This cyber-attack was undoubtedly neither the first nor the most extensive attack to take place, but this was the first cyber-attack recorded in literature against national security (Davis, 2007). Although the Estonian government has tried to describe it as cyber warfare, its attempt to define it has not been entirely successful (Farwell and Rohozinski, 2011: 32). But these attacks were used for the first time to destroy a country's entire digital infrastructure. To this date, cybersecurity has generally existed in the field of espionage as cybercriminals have infiltrated corporate and individual computer systems. The attack on Estonia targeted all civil and economic infrastructure in the country and paralysed society (Ruus, 2008).

The sharing of the news of the attacks on Estonia with the global public is a win for the country and other nations as other countries learned of this threat due to the awareness shared by Estonia. It was realized that cybersecurity is unrelated to a country's economic, demographic or political level. The significance and possible effects of the Estonian cyber-attacks drew the attention of the international community and resulted in the creation of international policies and collaborations to combat potential future cyber-attacks. It was a critical reminder for states to strengthen

and enhance their cyber warfare capability. Furthermore, organizations, such as the North Atlantic Treaty Organization (NATO), the European Union, and other states made more concrete and timely implementations of their work in this field (Herzog, 2011; Kozlowski, 2014: 239).

Stuxnet was another critical incident, first used as a cyber weapon in 2011 to sabotage Iran's nuclear program and was the first time that a physical cyber-attack was organized (Collins and McCombie, 2012: 80). The Stuxnet virus was so intricately designed that it took more than a few years to create the virus. After this incident, states increased their cyber capacity and started to use it for defence and other purposes. Initially, the dawn of the Internet was often defined as a utopian term for promoting and protecting human rights. It represented a space that would lead to the democratization and realization of human rights, liberating all knowledge, empowering individuals and weakening the state by making it more transparent and accountable (Tarhan, 2020). However, this view of the internet has changed over time, and the platform has now become an arena for conflict. This attack has brought about offensive and defensive discussions in cyberspace. Stuxnet has signalled how issues such as deterrence in cyberspace can emerge. In addition, the creation of a cost situation in cyber operations has come to the fore, because the creation of the Stuxnet virus cost more than just damage to Iranian nuclear power plants (Slayton, 2016: 97). These two critical attacks have led to an increase in academic studies. Cavelty used the bibliometric data used to analyse the literature on cybersecurity to confirm that studies of cybersecurity have increased approximately seven times in academic studies since 2007 (Cavelty, 2018: 24).

After the Stuxnet attack, one of the main focuses of cyber-attacks has been global energy sectors and multinational companies, as well as critical infrastructure. One of them is the self-replicating virus attack on Saudi Aramco's computer network on 15 August 2012. The damage caused by the virus, which infected about 30,000 windows-based machines, is regulated within two weeks. These attacks against the Saudi Arabian national oil and gas company, known as Aramco, which has critical importance to the global energy markets, were worrying for the world's energy markets. After Stuxnet, these attacks, which directly target critical energy infrastructures, turned out to be caused by the virus Shamoon (Bronk and Tikk-Ringas, 2013: 81). Although the US indicated that it was caused by Iran, no clear connection was found between this attack and the Iranian state, as the indications were based on assumptions and inferences (Thomas and Buchanan, 2015: 27). Aramco was again the target of attacks in 2017, and the joint project of Aramco with another company was targeted and the computers went down (Perlroth and Krauss, 2018; Groll, 2017). Aramco was also exposed to another attack in 2021, a ransom plan being arranged so that stolen data would be deleted in exchange for $ 50 million in cryptocurrency (CNBC, 2021).

Although these attacks are generally regarded as turning points, the escalation in the intensity and impact of these attacks, which took place in the last quarter-century, encouraged increased cooperation in the international arena. The desired cooperation and international negotiations, as well as new attacks, have been effective in transforming cybersecurity studies into a multifaceted discipline. An example of another important and impactful event that took place on an international scale is the cyber-

attack targeting Ukraine's Power Grid on December 24, 2015. Approximately 225,000 electricity consumers were affected by this attack (Lee et al., 2016). The attack on Ukraine appears to be the first attack to successfully target a country's electricity infrastructure. This attack was noted as being carried out by Russian hackers (Lindsay, 2017; BBC News, 2017). It is noteworthy that these attacks on Ukraine, following the Estonian and Georgian attacks also targeting critical infrastructures were also for political purposes. The attacks on Ukraine are cited as a model of the Russian hybrid war. The aim of cyber-attacks with this unofficial war doctrine is to minimize the power of the opposing states before physical conflict (Darıcılı, 2014: 10). These attacks were not interrupted, being renewed in 2016 and again during the 2022 Russia-Ukraine War by the Russian military group "Sandworm" (Tidy, 2022).

There have also been attacks that were organized to directly interfere in a country's internal affairs and affect the election process. The 2016 US election was the first time that there were notable cyber-attacks directly linked to this issue. The US accused Russia of leaking important stolen information in order to influence the election process and political parties (Homeland Security, 2016). This situation primarily targeted American self-government and damaged the democracy being established in cyberspace, and deterrence in the field of cybersecurity is faced with bad scenarios (Fidler, 2017). There have also been attacks that directly target essential water resources, although these attacks are mostly organized for ransomware and crypto theft (Hassanzadeh et al., 2020).

Cyber-attacks are designed to send a political signal, cause physical destruction and disruption or to change the course of crisis situations that may occur in the future. In a way, it means that cyber operations have become a powerful propaganda tool (Jensen et al., 2019: 7). For example, after the Stuxnet attacks, were Iran's alleged attacks targeting US banks and Saudi Aramco a message against Stuxnet? Was the attack organized by Russia in the 2016 US elections a political attack designed to disrupt the election process, rather than a direct military or physical attack? Another example is North Korea's attack on Sony Pictures in 2014, was this a political attack on the American entertainment world to send a political signal? In general, such attacks fall into the gray zone, which is considered as the classical dichotomy between war and peace (Nye, 2017: 49). This situation can be explained by the cybersecurity dilemma caused by cyber operations. Cyber operations are at a point lying between espionage and the use of force, which can lead to misunderstanding or escalation of the risk situation (Slayton, 2016: 73).

In addition to the political, economic, social, and technological reasons for cyber-attacks, the power struggle in cyberspace is one of the main factors in the formation of these attacks. The USA, one of the most important cyber actors on a global scale, has been in an intense power struggle with China in recent years. In the last decade, the competition between China and the USA, especially in cyberspace, has turned into a critical battleground (Sánchez and Akyesilmen, 2021: 53). The power struggle between the two countries has mostly occurred in the form of cyberespionage operations. An agreement was signed between the two countries in 2015 to stop the cyberespionage attacks between the two countries in order to prevent the increasing espionage and the deciphering of important information (Bey, 2018: 32). This agree-

ment directly led to the resurfacing of cyber governance discussions between the USA and Russia-China.

In general, China advocates further expansion of state sovereignty in cyberspace. In this context, the Chinese government argues that states should also have sovereignty in cyberspace, as in other areas such as land and water (Hsu and Murray, 2014: 2). In line with this approach, the Chinese government sees cyberspace as more US-centered and therefore problematic in many ways. It is argued that the US National Security Agency's PRISM (codename) covert surveillance program reveals the problem of information and network security in cyberspace (Greenwald and Macaskill, 2013). According to China, PRISM facilitates the collection of personal and business data from many American organizations that have a global presence, including Google, Facebook, Yahoo, Apple, and Microsoft. The purpose of the monitoring and surveillance mechanism here includes China and Russia and US allies such as the EU and its member states. For many, the PRISM case illustrates that the United States is leveraging existing Internet governance mechanisms for its own national interests. Therefore, compared to the USA, China prefers sovereign states as the main administrative unit in cyberspace as well as in the physical world. Beijing generally emphasizes two views: first, states should be able to claim sovereignty in cyberspace, and second, states should not interfere with other states' sovereignty in cyberspace (Zeng, et al., 2017: 440). These discussions are still ongoing, and no clear consensus has been reached as yet. However, any possibility of Balkanization in cyberspace will move it away from the common global phenomenon that is characteristic of it, and shift it to a more national judicial order. In this case, information and communication benefits will decrease (Cornish, 2015: 158). The emergence of this problem will gradually strengthen the anarchic structure of cyberspace. Therefore, such situations and events prove that cyber security studies in general are increasingly a multidisciplinary field of study.

DISCUSSION

The early writings on cybersecurity studies mostly covered security vulnerabilities and defence mechanisms that should be created against potential attacks. Therefore, it has started to be evaluated theoretically in security studies in the context of securitization theory. However, the scope and content of cybersecurity studies have expanded over time. Cybersecurity studies are considered as a combination of these disciplines that benefit from many different disciplines within the cyber field. It draws on many different sciences, from mathematics to computer science, from economics to law and psychology, and from international relations to sociology. Cyberspace is not only a technical and physical dimension but also a field of study that affects human and human behaviour and directly affects human life (Dawson and Thomson, 2018).

Even though cybersecurity has become an integral part of cyberspace, it is still a relatively recent term in the literature for security studies and policy formation. In terms of use area and scope, it appears that the definition of cybersecurity can be evaluated in security studies. On the other hand, it seems that it may be assessed under a different heading, such as cybersecurity studies. Many analyses are carried out

conceptually, although the theoretical structure has not yet been completely developed. Cybersecurity draws on a variety of disciplines to examine its concepts on a practical level. Using the concept directly evokes engineering and technical situations involving individuals. However, although cybersecurity has been a field of study that overlaps with the technical security area, it covers more than that (Nissenbaum, 2009: 64). In its current form, the concept is developing as a multidisciplinary field, encompassing all aspects of human life, from politics to economy, education and health systems. Therefore, it should be evaluated beyond security studies.

In today's climate, security studies are also intertwined with many complex problems and analyses provided by IR alone are not sufficient in solving these issues. Therefore, security studies must also consider the humanities, engineering sciences and social sciences. For example, researchers dealing with environmental problems collect data by partially dealing with the field of biology. In addition, cybersecurity, the subject of this study, cannot only address the social sciences. It is a subject of study that computer and engineering sciences can also contribute to by providing vital technical information. The fact that security studies are a field of study in IR or that its origins depend on IR is not enough to consider the complex nature of this field of study, which requires more information. Therefore, it is clear that security studies should be considered as more of a multidisciplinary field (Williams, 2013: 1–12). The dominant concept discussed has drawn attention to national security and military issues and in ensuring security in general. However, narrow definitions have expanded over time, causing new security problems or areas to be added to this field of study. Recent studies show that security situations that occur in different areas are now included in the definitions, such as environmental security, human security and cybersecurity (Schlag at el., 2016).

Developments in the field of cybersecurity are an emerging field of study that has not yet been completed in terms of theory and practical implications. Despite this, cybersecurity studies are academically state-centred and definite conclusions can be made. Especially in the field of security studies, it is examined through concepts such as system and order, which only normally include competition between states. Although this is valid for many issues in the field of cybersecurity, it causes non-state actors and their effects on these actors to be partially ignored. Therefore, the idea that cybersecurity studies should be examined with both global and interstate dimensions has gained importance (Kello, 2013: 37–37). This situation partially strengthens the idea that this field of study should be increasingly multidisciplinary.

Cybersecurity studies have escalated to become the subject of global security, from security of individuals to the security of nation-states. In this process, the concept, which was initially used only to ensure the security of computer science and computer-related situations, was evaluated in security studies to become a fundamental subject of international relations. However, the progress of cybersecurity studies as an area that needs to be resolved and cooperated globally has caused it to cover many different areas and approaches. Cybersecurity studies has become a multi-disciplinary field of study beyond international relations. Due to today's digital conditions and the fact that people's lives are intertwined in many different ways, from their physical lives to the critical infrastructure of states, it has turned into a field where scientific data from many different disciplines are examined (EU, 2020: 15).

***

Security studies deals with state and military as a subject of research and has continuously progressed towards the current situation of how to ensure national security. However, changing world politics and the international system necessitated a change in security studies. The structuring of nation-states, which is the subject of IR, is now very different from the Westphalia order in 1648. It has now become challenging to understand the logic of Cold War-era security studies, the theories of IR, and today's security problems without considering cybersecurity, which is now one of the most critical factors in security studies. In this context, today's problems should be considered again with this addiction situation. However, this situation should not be limited to security studies and IR only, and joint studies should be carried out with different disciplines.

Cybersecurity sees little value in security studies because many researchers in this field use technological developments in a generalised framework. Whilst this generalization still remains broad, cybersecurity has been explicitly discussed in literature in the post-2007 period. The 2007 Estonian attacks caused many states to realize the seriousness of cybersecurity and begin to take action. Furthermore, in the academic environment, many experts have worked seriously to solve the cybersecurity problem, leading to a change in pre-existing risks and vulnerabilities since the Estonian incident.

Today, cybersecurity studies are developing as a separate and distinct field of study. Many different topics, such as cyber warfare, cyber-attacks, cyber terrorism and cyber intelligence have been discussed to ensure cybersecurity. Issues such as the security of critical infrastructures have always been the priority of states. In the Second World War, only areas such as oil facilities and factories producing military equipment were considered primary critical infrastructures. Today, due to the growing role of technology, this area has expanded and encompasses all human-related sectors. Cybersecurity studies started as a sub-branch of different IR and security studies. At the current point in time, it has become more diverse and is evolving to become a multidisciplinary field.

Cybersecurity studies have developed by being evaluated among IR theorists and security experts, but it does not yet have the characteristics of being a different field of study and discipline. However, it would not be wrong to state that it has expanded as a field of study. The fact that IR and many other disciplines contain study subjects also allows this field to be evaluated as a multidisciplinary field.

REFERENCES

Anderson R. H., Hearn A. C., *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA*, "The Day After...in Cyberspace II", RAND.

Arquilla J., Ronfeldt D. (1993), *Cyberwar is Coming!*, "Comparative Strategy", 12: 141–165.

Arquilla J., Ronfeldt D. (1996), *The Advent of Netwar*, RAND, Santa Monica.

Arquilla J., Ronfeldt D. (2001), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND.

Baldwin D. (1995), *Security Studies and the End of the Cold War*, "World Politics", 48(1): 117–141.

BBC News (2017), *Ukraine power cut 'was cyber-attack'*, 11 January 2017, https://www.bbc.com/news/technology-38573074 (30.04.2022).

Bendrath R. (2001), *The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection*, "Information & Security: An International Journal", 7: 80–103.

Bey M. (2018), *Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition*, "The Cyber Defense Review", 3(3): 31–36.

Bıçakcı S. (2014), *NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik* (*NATO's Emerging Threat Perception: Cyber Security in the 21st Century*), "Uluslararası İlişkiler", 10(40): 101–130.

Bilgin P. (2010), *New Approaches on Security Studies: New Security Studies*, "Stratejik Araştırmalar", 8(14): 69–96.

Bilgin P., Booth K., Lones R. W. (1998), *Security Studies: The Next Stage?*, "Naçao e. Defesa", 84(2): 131–157.

Birdişli F. (2019), *Teori ve Pratikte Uluslararası Güvenlik; Kavram-Teori-Uygulama* (*International Security in Theory and Practice: Concept-Theory-Application*), Seçkin, İstanbul.

Boys J. D. (2018), *The Clinton Administration's Development and İmplementation of Cybersecurity Strategy (1993–2001)*, "Intelligence and National Security", 33(5): 755–770.

Bronk C., Tikk-Ringas E. (2013), *The Cyber Attack on Saudi Aramco*, "Survival", 55(2): 81–96.

Buzan B. (1983), *People, States and Fear: The National Security Problem in IR*, Wheatsheaf Books, England.

Buzan B., Hansen L. (2009), *The Evolution of International Security Studies*, Cambridge University Press, New York.

Cavelty M. D. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge, London–New York.

Cavelty M. D. (2010), *Cyber-Threats*', in: *The Routledge Handbook of Security Studies*, (eds.) M. Dunn Cavelty, V. Mauer, Routledge, London–New York.

Cavelty M. D. (2017), *Siber Güvenlik* (*Cybersecurity*), in: *Çağdaş Güvenlik Çalışmaları* (*Contemporary Security Studies 369–371*), trans. Nasuh Uslu, (ed.) A. Collins, Role Akademik Yayıncılık, İstanbul.

Cavelty M. D. (2018), *Cybersecurity Research Meets Science and Technology Studies*, "Politics and Governance", 6(2): 22–30.

Cavelty M. D., Wenger A. (2020), *Cybersecurity Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science*, "Contemporary Security Policy", 41(1): 5–32.

Choucri N. (2012), *Cyberpolitics in IR*, The MIT Press, Cambridge, Massachusetts.

Choucri N., ReardonR. (2012), *The Role of Cyberspace in IR: A View of the Literature*, Paper Prepared for the 2012 ISA Annual Convention San Diego, CA.

CNBC (2021), *Saudi Aramco facing $50 million cyber extortion over leaked data*, 22 July 2021, https://www.cnbc.com/2021/07/22/saudi-aramco-facing-50m-cyber-extortion-over-leaked-data.html (30.04.2022).

Collins S., McCombie S. (2012), *Stuxnet: The Emergence of a New Cyber Weapon and its Implications*, "Journal of Policing, Intelligence and Counter Terrorism", 7(1): 80–91.

Cornish P. (2015), *Governing Cyberspace through Constructive Ambiguity*, "Survival", 57(3): 153–176.

Darıcılı A. B. (2014), *Rusya Federasyonu Kaynakli Olduğu İddia Edilen Siber Saldirilarin Analizi* (*Analysis Of Alleged Cyber Attacks From Russian Federation*), "U.Ü. Sosyal Bilimler Enstitüsü Dergisi", 7(2): 1–16.

Darıcılı A. B. (2018), *Askerileştirilen ve Silahlandırılan Siber Uzay* (*Militarized and Armed Cyberspace*), in: *Sosyal ve Beşeri Bilimlere Dair Araştırma Örnekleri* (*Social and Human Sciences Research Examples, 311–327*), (ed.) Ali Acaravcı Nobel Akademik Yayıncılık, Ankara.

Davis J. (2007), *Hackers Take Down the Most Wired Country in Europe*, "Wired Magazine", last modified 21 August 2007, https://www.wired.com/2007/08/ff-estonia/ (04.06.2021).

Dawson J., Thomson R. (2018), *The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance*, "Frontiers in Psychology", Review article, https://doi.org/10.3389/fpsyg.2018.00744.

Deibert R. J., Stein J. G. (2002), *Hacking Networks of Terror*, "Dialog-IO": 1–14.

Director of National Intelligence, Press Release, Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security (7 October 2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (30.04.2022).

Erendor M. E., Tamer G. (2018), *The New Face of the War: Cyber Warfare*, "Cyberpolitik Journal", 2(4): 57–74.

Eriksson J., Giacomello G. (2006), *The Information Revolution, Security, and IR: (IR)relevant Theory?*, "International Political Science Review", 27(3): 221–244.

Estonian Foreign Intelligence Service, *International Security and Estonia*, https://www.valisluureamet.ee/pdf/raport-2020-en.pdf (19.01.2021).

European Union, 2020, *Cybersecurity Our Digital Anchor a European Perspective*, Publications Office of the European Union, Luxembourg.

Farwell J. P., Rohozinski R. (2011), *Stuxnet and the Future of Cyber War*, "Survival: Global Politics and Strategy", 53(1): 23–40.

Fidler D. P. (2017), *The U.S. Election Hacks, Cybersecurity, and International Law*, "Articles by Maurer Faculty", 2607.

Garcia S. M., Palhares A. I. (2014), *Reflections on Virtual to Real: Modern Technique, International Security Studies and Cyber Security Environment*, in: *Cyberspace and International Relations Theory, Prospects and Challenges* (269–280), (eds.) J.-F. Kremer, B. Müller, Springer, Berlin.

Gompert D. C. (1998), *National Security in the Information Age*, "Naval War College Review", 51(4): 22–41.

Greenwald G., MacAskill E. (2013), *NSA Prism program taps in to user data of Apple, Google and others*, Guardian, 7 June 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (04.05.2022).

Groll E. (2017), *Cyberattack Targets Safety System at Saudi Aramco*, Foreign Policy, 21 December 2017, https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/ (30.04.2022).

Hansen L., Nissenbaum H. (2009), *Digital Disaster, Cybersecurity, and the Copenhagen School*, "International Studies Quarterly", 53: 1155–1175.

Hassanzadeh A., Rasekh A., Galelli S., Aghashahi M., Taormina R., Ostfeld A., Banks K. M. (2020), *A Review of Cybersecurity Incidents in the Water Sector*, "American Society of Civil Engineers", 146(5): 03120003, https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686.

Herzog S. (2011), *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, "Journal of Strategic Security", 4(2): 49–60.

Homeland Security (2016), *Joint Statement from Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (18.11.2021).

Hsu K., Murray C. (2014), *China and International Law in Cyberspace*, "US–China Economic and Security Review Commission Staff Report".

Jensen B., Valeriano B., Maness R. (2019), *Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist*, "Journal of Strategic Studies", https://doi.org/10.1080/01402390.2018.1559152.

Johnson D. R., Post D. (1996), *Law and Borders: The Rise of Law in Cyberspace*, "Stanford Law Review", 48(5): 1367–1402.

Kay S. (2004), *Globalization, Power, and Security*, "Security Dialogue", 35(1): 9–25.

Kello L. (2013), *The Meaning of the Cyber Revolution Perils to Theory and Statecraft*, "International Security", 38(2): 7–40.

Keohane R. O., Nye Jr, J. S. (1998), *Power and Interdependence in the Information Age*, "Foreign Affairs", 77(5): 81–94.

Kozlowski A. (2014), *Comparative Analysis of Cyber-attacks on Estonia, Georgia and Kyrgyzstan*, "European Scientific Journal", Special Edition 3, 10(7). https://doi.org/10.19044/esj.2014.v10n7p%p (22.05.2021).

Krepinevich A. F. (2012), *Cyber Warfare: A "Nuclear Option"?*, Center for Strategic and Budgetary Assessments, Washington.

Lawson S., Middleton M. K. (2019), *Cyber Pearl Harbor: Analogy, fear, and the framing of cybersecurity threats in the United States, 1991–2016*, "First Monday", 24(3), https://doi.org/10.5210/fm.v24i3.9623 (24.08.2021).

Lee R. M., Assante M. J., Conway T. (2016), *Analysis of the Cyber Attack on the Ukrainian Power Grid*, E-ISAC and SANS ICS, Washington.

Lessig L. (1996), *The Zones of Cyberspace*, "Stanford Law Review", 48(5): 1403–1411.

Lewis J. A. (2002), *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies.

Lindsay J. R. (2017), *Digital Policy, Regulation and Governance Restrained by Design: The Political Economy of Cybersecurity*, https://doi.org/10.1108/DPRG-05-2017-0023.

Mathews J. T. (1989), *Redefining Security*, "Foreign Affairs", 68(2): 162–177.

Messmer E. (1999), *Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says*, CNN.com, 12 May 1999, http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/ (03.05.2022).

Miller S. E. (2001), *International Security at Twenty-five: From One World to Another*, "International Security", 26(1): 5–39.

National Research Council (1991), *Computers at Risk: Safe Computing in the Information Age*, The National Academies Press, Washington, DC, https://doi.org/10.17226/1581.

Nissenbaum H. (2005), *Where Computer Security Meets National Security*, "Ethics and Information Technology", 7: 61–73.

Nojeim G. T. (2020), *Cybersecurity and Freedom on the Internet*, "Journal of National Security Law & Policy", accessed 9 August 2020, https://jnslp.com/wpcontent/uploads/2010/08/09_Nojeim.pdf (05.06.2021).

Nye J. S. (2017), *Deterrence and Dissuasion in Cyberspace*, "International Security", 41(3): 44–71.

Nye J. S., Lynn-Jones S. M. (1988), *International Security Studies: A Report of a Conference on the State of the Field*, "International Security", 12(4): 5–27.

Perlroth N., Krauss Clifford (2018), *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*, "The New York Times", 15 March 2018, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html (30.04.2022).

Rid T., Buchanan B. (2015), *Attributing Cyber Attacks*, "The Journal of Strategic Studies", 38(1–2): 4–37.

Ruus K. (2008), *Cyber War I: Estonia Attacked from Russia*, "European Affairs", 9(1–2).

Sánchez K. V., Akyesilmen N. (2021), *Competition for High Politics in Cyberspace: Technological Conflicts Between China and the USA*, "Polish Political Science Yearbook", 50(1): 43–69.

Schlag G., Junk J., Daase C. (2016), *Transformations of Security and Security Studies: An Introduction to the Volume*, in *Transformations of Security Studies Dialogues, Diversity and Discipline*, (eds.) G. Schlag, J. Junk, C. Daase, Routladge, New York.

Slayton R. (2016), *What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment*, "International Security", 41(3): 72–109.

Smith M. E. (2020), *Uluslararası Güvenlik (International Security)*, trans. Ramazan Gözen, Felix Kitap, Ankara.

Solms R. V., Niekerk, J. V. (2013), *From Information Security to Cybersecurity*, "Computer & Security", 38: 97–102.

Stevens T. (2018), *Global Cybersecurity: New Directions in Theory and Methods*, "Politics and Governance", 6(2): 1–4.

Tarhan K. (2020a), *Ulusal ve Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik* (*Cybersecurity as a Component of National and International Security*), in: *Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları* (*New Global Threat: Cyber Attacks, Cybersecurity and Policy Practices, 33–50*), (ed.) Fulya Köksoy, Nobel Yayıncılık, Ankara.

Tarhan K. (2020b), *Klasik Soğuk Savaş'tan Küresel Siber Soğuk Savaşa Siber Uzay Kavramının Analizi* (*Analysis of The Concept of Cyberspace from The Classical Cold War to The Global Cyber-Cold War*), in: *Güvenlik, Teknoloji ve Yeni Tehditler* (*Security, Technology and New Threats, 193–211*), (ed.) Ali Burak Darıcılı, Nobel Yayıncılık, Ankara.

Tidy J. (2022), *Ukrainian power grid 'lucky' to withstand Russian cyber-attack*, BBC News, 08 April 2022, https://www.bbc.com/news/technology-61085480 (30.04.2022).

Ullman R. H. (1983), *Redefining Security*, "International Security", 8(1): 129–153.

Verton D. (1999), *Serbs launch cyberattack on NATO*, FCW, 4 April 1999, https://fcw.com/1999/04/serbs-launch-cyberattack-on-nato/195288/ (03.05.2022).

Walt S. M. (1991), *The Renaissance of Security Studies*, "International Studies Quarterly", 35(2): 211–239.

Waver O., Buzan B. (2017), *Teoriye Dönüş Sonrası: Güvenlik Çalışmalarının Geçmişi, Bugünü ve Geleceği* (*After the Return to Theory The Past, Present, and Future of Security Studies*), in: *Çağdaş Güvenlik Çalışmaları* (*Contemporary security studies, 393–411*), trans. Nasuh Uslu, (ed.) Alan Collins, Röle Akademik Yayıncılık, İstanbul.

Westrin P. (2001), *Critical Information Infrastructure Protection (CIIP)*, "Information & Security: An International Journal", 7: 67–79.

Williams P. D. (2013), *Security Studies: An Introduction*, in: *Security Studies: An Introduction*, (eds.) P. D. Williams, M. McDonald, Routledge, New York, Second Edition.

Yılmaz O. (2017), *Küreselleşme Sürecinde Dönüşen Güvenlik Algısı Ve Siber Güvenlik*, (*Transforming Security Perception and Cybersecurity in The Globalization Process*), "Cyberpolitik Journal", 2(4): 22–43.

Zeng J., Stevens T., Chen Y. (2017), *China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"*, "Politics & Policy", 45(3): 432–464.

ABSTRACT

This study discusses the formation and development of cybersecurity studies since the creation of the Internet. Although the origin of cybersecurity studies dates back to the 1970s, hacking, malicious software, computer intrusions, and espionage attacks that took place in the 1980s led

cybersecurity studies to form in the area of computer science. By the 1990s, the Internet began to be used widely, and an increase in the level of attacks in cyberspace began to occur. This period was a major reason for the growth in writing on software and network security. Network security has become a key priority for governments and many industries. Cybersecurity studies have become a priority area in security studies with the increasing complexity of cyber threats towards 2000s. States and some supranational organizations have started to create cybersecurity strategies. The security of critical infrastructure and computer networks has begun to emerge as a high-priority area. It has been observed that the transition from classical security policies to modern security policies, which should be established in the information age, has begun. Cybersecurity studies were taken more seriously after the 2007 Estonian attacks, especially in the 2010s. In this period, the intensity of attacks on critical infrastructures and the occurrence of some physical attacks caused cybersecurity to deepen and become an issue on an international scale. Cybersecurity studies continue to be shaped by being influenced by many different disciplines, regardless of any discipline, with the important discussions and cyber incidents that have taken place in recent years. Therefore, the studies were handled from a multidisciplinary perspective.

Keywords: Cybersecurity, Cybersecurity Studies, Security Studies, International Relations, Multifaceted Approach

HISTORYCZNY ROZWÓJ BADAŃ NAD CYBERBEZPIECZEŃSTWEM: PRZEGLĄD LITERATURY I JEGO MIEJSCE W STUDIACH NAD BEZPIECZEŃSTWEM

STRESZCZENIE

W niniejszym opracowaniu omówiono powstawanie i rozwój studiów nad cyberbezpieczeństwem od momentu powstania Internetu. Chociaż początki studiów nad cyberbezpieczeństwem sięgają lat 70tych dwudziestego wieku, hakerstwo, złośliwe oprogramowanie, włamania do komputerów i ataki szpiegowskie, które miały miejsce w latach 80tych, doprowadziły do ukształtowania się cyberbezpieczeństwa w obszarze informatyki. W latach 90tych internet zaczął być powszechnie wykorzystywany i wzrosła ilość ataków w cyberprzestrzeni. Okres ten był głównym powodem wzrostu zainteresowania bezpieczeństwem oprogramowania i sieci. Bezpieczeństwo sieci stało się kluczowym priorytetem dla rządów i wielu branż. Wraz z rosnącą złożonością cyberzagrożeń w 21 wieku studia nad cyberbezpieczeństwem stały się priorytetowym obszarem w studiach nad bezpieczeństwem. Państwa i niektóre organizacje ponadnarodowe zaczęły tworzyć strategie bezpieczeństwa cybernetycznego. Bezpieczeństwo infrastruktury krytycznej i sieci komputerowych zaczęło wyłaniać się jako obszar o wysokim priorytecie. Zaobserwowano, że rozpoczęło się przejście od klasycznych do nowoczesnych polityk bezpieczeństwa, które powinny być tworzone w erze informacji. Studia nad bezpieczeństwem cybernetycznym były traktowane poważniej po atakach estońskich z 2007 roku, zwłaszcza w drugiej dekadzie 21 wieku. Obecnie intensywność ataków na infrastrukturę krytyczną oraz wystąpienie niektórych ataków fizycznych powodują, że problem cyberbezpieczeństwa pogłębia się i staje się problemem w skali międzynarodowej. Studia nad cyberbezpieczeństwem nadal są kształtowane przez wpływ nie jednej, lecz wielu różnych dyscyplin, także dzięki ważnym dyskusjom i incydentom cybernetycznym, które miały miejsce w ostatnich latach. Dlatego też badania prowadzono z perspektywy multidyscyplinarnej.

Słowa kluczowe: cyberbezpieczeństwo, studia nad cyberbezpieczeństwem, studia nad bezpieczeństwem, stosunki międzynarodowe, podejście wieloaspektowe

Article submitted: 01.01.2022; article accepted: 20.11.2022.