JOURNAL OF MODERN SCIENCE

Tom 4/53/2023

www.jomswsge.com

DOI: doi.org/10.13166/jms/176103

Marek Górka

Koszalin University of Technology, Poland

ORCID iD: 0000-0002-6964-1581

CONCEPTUALISING SECURITISATION IN THE FIELD OF CYBER SECURITY POLICY

KONCEPTUALIZACJA SEKURYTYZACJI W OBSZARZE POLITYKI CYBERBEZPIECZEŃSTWA

Abstract

In recent years, securitisation theory has become known as one of the most influential ideas for traditional 'narrow' security theory within international relations. Well, developed in response to the need to expand security studies after the Cold War, securitisation theory offers a method for studying security as a product of certain socio-political discourses and practices. Securitisation involves the study of political decision-making and aims to understand more and more precisely who identifies threats and in whose interest and to whom this is addressed, why, under what circumstances and what determines the success of the process.

This article will attempt to analyse securitisation theory to explore the discursive features of cyber security, using a multi-actor approach that considers the role of state and non-state actors in the creation and management of cyber security discourses. The aim is primarily to answer the questions: which issues are constructed as threatening in cyber security discourses and practices? To which referent objects are they addressed and by which actor(s)? And to which audiences are they directed? Whom do such messages and practices reinforce and/or exclude?

Keywords: *securitisation, cyber security policy, cyber security strategies, digital threats*

Streszczenie

W ostatnich latach teoria sekurytyzacji stała się jednym z najbardziej wpływowych nurtów tradycyjnej *wąskiej* teorii bezpieczeństwa w obrębie stosunków międzynarodowych. Rozwinięta w odpowiedzi na potrzebę rozszerzenia studiów nad bezpieczeństwem po zakończeniu zimnej wojny, teoria sekurytyzacji oferuje metodę badania bezpieczeństwa jako produktu określonych dyskursów i praktyk społeczno-politycznych. Sekurytyzacja obejmuje badanie procesu podejmowania decyzji politycznych i stara się coraz bardziej precyzyjnie zrozumieć, kto identyfikuje zagrożenia, w czyim interesie, komu są one adresowane, dlaczego, w jakich okolicznościach i co determinuje sukces tego procesu.

Niniejszy artykuł podejmie próbę analizy teorii sekurytyzacji w celu zbadania cech dyskursywnych w obszarze cyberbezpieczeństwa, wykorzystując podejście wieloaktorowe, uwzględniające rolę aktorów państwowych i niepaństwowych w tworzeniu i zarządzaniu dyskursami dotyczącymi cyberbezpieczeństwa. Celem jest przede wszystkim odpowiedź na pytania: jakie kwestie są konstruowane jako zagrożenia w dyskursach i praktykach związanych z cyberbezpieczeństwem? Do jakich obiektów odnoszą się te zagrożenia i przez jakiego (lub jakich) aktora(-ów)? I do jakich odbiorców są one kierowane? Kogo takie komunikaty i praktyki wzmacniają i/lub wykluczają?

Słowa kluczowe: *sekurytyzacja, polityka cyberbezpieczeństwa, strategie cyberbezpieczeństwa, zagrożenia cyfrowe*

Introduction

Securitisation theory today offers one of the most attractive analytical tools in critical security studies in both traditional and digital dimensions. What makes the features of cyber discourse relevant is its political significance. The creation of new cyber doctrines and strategies is now the rule rather than the exception, which makes the process of defining the concept of cyberspace relevant. Notions of power, domination and control are part and parcel of cyber discourse.

The paper is intended to fill a gap from the hitherto insufficiently researched field of cybersecurity securitisation. The perceived lack of research analyses in the existing literature is partly due to the rapidly developing cyber technology initiating many processes, the effects of which are not all immediately apparent, and their impact on political, economic or social life is also not fully understood.

This paper aims to assess the contribution of securitisation theory to the understanding of both traditional and contemporary security policy issues. More specifically, it is an attempt to reflect on the identification of the challenges facing the contemporary state.

The article analyses the decision-making process of power. It points out that a key element of securitisation theory that needs to be taken into account is the conditions that influence how threats are perceived and on the basis of which knowledge government intervention techniques are implemented (Hansen, 2011, p. 358; Munster, 2009, p. 15; Wæver, 2011, pp. 465-480). So, one can conclude that securitisation theory expresses a particular understanding of security (influenced by speech act theory) with a distinctive analysis of power. For this reason, 'security' becomes a specific speech act that can succeed under certain conditions, namely in situations where 'the securitising actor uses the rhetoric of an existential threat and thus has significant political effects' (Buzan, O. Wæver, J. de Wilde, 1998, p. 25).

Thus, the idea behind securitisation is to give the issue enough weight to gain the consent of the public, which enables the authority to use whatever means it deems most appropriate. In other words, securitisation combines the politics of threat design with the politics of threat management (Balzacq, 2011, p. 3).

Also central to the argument of the topic is the assumption that securitisation theory is useful in describing the development of new security issues and policies. So, the theory sees the development of a modern form of governance that is functionally linked to cyber technology.

Securitisation. A definitional construct

According to the theorists of the Copenhagen School, security should be read in the context of a 'state of emergency', which leads to the claim that security threats are always existential to the survival of a specific reference object, which may be the state, population, territory, but also identity, culture, organisational stability, social order, environment or financial system (Peoples, Vaughan-Williams, 2010, p. 80).

However, it is also worth noting in this context that currently the state does not have a monopoly on security policy and, in addition to state institutions, there are public sector actors who can also initiate the securitisation process.

Therefore, it is very important to understand the process and dynamics of securitisation, in the context of seeking answers to the questions of who can deal with security, on what issue and in what situation (Buzan, Wæver, Wilde, 1998, p. 31). In this vein, the Copenhagen School defines securitisation as *a process in which an actor declares a particular problem, dynamic or actor to be an <<existential threat>> to a particular referent object* (Ibid. p. 69).

An important argument put forward in securitisation theory is that every issue is a public issue, but originates from different sectors, namely military, political, economic, social, environmental or technological. Any such sector can be securitised when the issue is presented as an existential threat, requiring specific emergency measures to justify action outside normal political procedures

(Ibid. p. 24). The main explanatory point of securitisation theory is thus the idea of a speech act through which non-politicised issues can be politicised. Against such a background, securitisation appears as an action to present an issue as urgent and existential, so it must be dealt with decisively and before other issues (Ibid. p. 29). Emergency measures and the 'urgency' of a particular situation are distinctive features of securitisation theory (Floyd, 2011, pp. 427-439).

The theory of the Copenhagen School originally aimed to open up the possibility of conceptualising security beyond military affairs, while providing a criterion for distinguishing security from other policies (Wæver, 2010). The contemporary dominance of cyber threats is a reinforcement of this assumption. It is the formulation of the political problem in terms of emergency measures, survival and urgency that makes security policy unique and places it outside normal politics. In this form, securitisation is the specific utterance through which the problem is constructed as a security issue (Wæver, 2002). In other words, it is only by labelling a particular phenomenon a security issue that this phenomenon is 'promoted' to the security agenda (Wæver, 2004). By stating that a given reference object is threatened in its existence, the securitiser claims the right to extraordinary measures to ensure the survival of the reference object. The matter is then transferred from the realm of normal politics to the realm of crisis politics, where it can be resolved quickly and without the normal (democratic) rules and regulations of policy-making.

One of the principles of securitisation most often cited by researchers refers to the move from 'normal' politics to 'special' politics. It is a movement that takes politics beyond the established rules and captures the problem as a special kind of politics. Securitisation can therefore be seen as a more extreme version of politicisation. Theoretically, any public issue can be located on a spectrum from non-politicised pole (meaning that the state does not address a particular problem and it is not in any way subject to public debate) through politicised field (meaning that the issue is part of public policy that requires government decisions and resource allocation) to securitisation (meaning that the problem is presented as an existential threat that requires emergency action and thus justifies action beyond normal political procedures) (Buzan, Wæver, Wilde, 1998, pp. 23-24).

In other words, securitisation theory automatically assumes that the 'movement' of securitisation is a shift from normal politics, where things are done through a 'democratic process of governance', to one of special politics, where the use of emergency measures is justified. This raises questions about the operation of securitisation under totalitarian or other non-democratic governance conditions, where there is no 'democratic' control over the implementation of security rules and where it is difficult to distinguish between 'normal' and 'special' policies (Vuori, 2008, p. 69).

Securitisation is used by political leaders for a variety of purposes. The most common uses of this theory are to establish a hierarchy of political priorities, deterrence, legitimise past actions, introduce social control, preserve the status quo and define one's own identity of 'self' in opposition to 'other' (Ibid. p. 76).

Although many decision-makers may invoke 'security' to achieve their policy goals, the securitisation process is only successful if it is relevant to the audience and thus leads to the acceptance of a particular claim (Roe, 2004, p. 281). The notion of audience has therefore become a key issue for securitisation theory. Acceptance or rejection may be a legal and formal step, or it may consist of informal agreement and moral support. This makes it possible to distinguish between empowering audiences who influence the debate by agreeing or disagreeing (Balzacq, 2011, p. 9). It is therefore necessary to determine which actors have enough social capital in a given field to make effective claims (Williams, 2003, pp. 511-531).

Whether the threat is material or ideological, it is difficult for security elites to legitimise the export of security by military means, firstly because of the potentially high cost – not only in terms of lives and money, but also in terms of credibility – and secondly because intervention goes against the norms of democracy and sovereignty that characterise the international system today (Olsson, 2015, p. 429). Arguments that seek to legitimise the security act are presented to audiences who need to be persuaded that external problems require an emergency response involving, among other things, military commitments abroad. Such a framework clearly invokes the securitisation approach from the Copenhagen School. The attempt to securitise threats outside one's own territory in order to legitimise foreign military intervention rarely goes unchallenged and in fact usually leads to intense international criticism.

This ambiguity around securitisation draws attention to the uncertainty and high risk, as political elites are uncertain about the consequences of a particular decision. In other words, any military action carries the risk of unpredictable political, economic, military or social costs. The argument presented here is twofold: the crux of the decision to engage in foreign military intervention, despite a successful securitisation process, carries an element of ambiguity and instability.

It is argued that the success of securitisation efforts ultimately depends on them becoming a routinised part of the political process. Thus, the success of securitisation determines the ability of political elites to implement emergency measures without having to further legitimise their actions (Watson, 2009, p. 28). In other words, the implementation of emergency measures becomes part of established and institutionalised practices (Olsson, 2015, p. 435). This notion of institutionalisation is closely related to the concept of desecuritisation, which has been described as the transfer of a particular issue from the emergency defence sequence into the ordinary public sphere (Buzan, Wæver, Wilde, 1998, p. 29). Thus, the proposed measure becomes a normal and routine process in which actors have acquired the necessary consent and competence to deal with the problem situation.

The more lasting success of securitisation depends on embedding the engagement within institutionalised contextual factors, such as the formation of identities, values, attitudes or recourse to established alliances (Mirow, 2016). It is also important to remember that in order to define a specific political context, a number of assumptions need to be made about the nature of society, the political situation, the economic situation, the role of religion in society and cultural factors, among others.

The securitisation of cyber security as a research challenge

Recent developments towards digitalisation are forcing even greater efforts regarding the security of the digital space. This is also evident in the number of studies applying securitisation theory to cyberspace is steadily growing and the topic is likely to find increasing interest among researchers as well as security policy observers. The importance of this area stems from two interrelated trends. Firstly, states, societies, businesses and individuals are increasingly relying on cyber-based data, systems and technologies. This provides fertile ground for many actors to develop new securitisation activities that identify various threats. Secondly, the preoccupation with cyberspace fits well with attempts to seek out new threats that have been occurring among security professionals and bureaucracies since the end of the Cold War.

In his risk society thesis, Ulrich Beck assumes that we are now living in a 'second modernity' in which risk can be conceptualised as 'a systematic way of dealing with the dangers and uncertainties caused and introduced by modernisation itself' (Beck, 1992). This period of 'reflexive modernity' is marked by the dominant force of unknown, incalculable and uncontrollable dangers that 'straddle' spatially, temporally and socially (Beck, 2002, pp. 39-55). Beck's risk society thesis can be seen as a security discourse. It can be seen that the risk society is the dominant discourse adopted by most actors when constructing cyber threats.

The securitisation of cyberspace means making it a national security issue. This is particularly troublesome for developing countries, where the use of network technologies is growing faster than anywhere else in the world. The rapid proliferation of network technologies, such as mobile phones and the Internet, has been accompanied by a widespread belief in their potential to strengthen democracy. While there is evidence to support this belief, there is also evidence of restrictions on rights and freedoms in cyberspace. Across the world, states are enforcing control over cyberspace to ensure that the content therein suits their own domestic and foreign policy interests.

Most of the academic literature on cyber security focuses on threats without sufficient theoretical underpinning referring to securitisation theory. One of the few exceptions, however, are studies using the Copenhagen School's securitisation theory to examine cyber security discourses and practices (Hansen, Nissenbaum, 2009, pp.1155-1175; Cavelty, 2008).

However, the literature on cyber securitisation remains very limited in terms of its engagement with the complexity of the cyber sphere. This is evident in analyses that focus on official discourses created and developed by governmental parties. However, such an approach does not apply to the multi-stakeholder nature of the cyber sphere and ignores the extent to which non-governmental actors create and manage relevant threat discourses. This 'state-centric' approach is problematic because it does not reflect the diversity of cyber-security discourses, but only emphasises the militarised, geopolitical discourses adopted by some decision-makers that reinforce perceptions of reality according to a friend versus foe logic.

It is therefore worth outlining some of the dilemmas that have emerged with the debate on emerging cyber security threats. Since the end of the Second World War, strategic studies have developed a broad theoretical framework based on newly developed nuclear weapons technology, communication technologies and industrialisation. Securitisation necessitates an analysis of some of the dilemmas of cyber threats emanating from cyberspace, which would significantly affect the strategy of state defence and international stability.

In general, a cybersecurity policy is the basis for a strategy and a set of industry-specific rules, requirements and instructions that protect cyber infrastructure and shape behaviour in the use of information resources. As a rule, policies are developed by technical experts through analysis, documentation and support representing the proposed and selected direction needed to influence the command and control process with security risks in mind.

Cyber security policies are encountered in a wide and varied range, starting from international, regional or national policies to the smallest public and private entities in many areas of activity. These state struggles with new digital challenges and efforts directed at annihilating cyber threats or progressively reducing them are not only a matter of policy, but also of technology, economy, economics and society.

Cyber threats can no longer be described as an 'emerging' security problem; rather, they are already exerting a significant, sometimes primary, influence on the most relevant contemporary international policy developments with increasing frequency and consequences. Cyber threats have become so ubiquitous, complex and dynamic that they represent a significant force capable of destabilising the situation both in many states and in the international system as a whole. Cyber threats have thus become a real global security problem for which no state has yet found any solution.

Among researchers, a position is increasingly being pushed to conceptualise cyber security separately from the national security sector. This is for several reasons, first and foremost it is emphasised that the cyber sector is characterised by a complex constellation of public-private responsibilities, moreover, within cyberspace there is a multitude of threats, which are not only incidental but also widespread in nature, thus also affecting individuals. Furthermore, in addition to policy makers, cyber experts also play a huge role here (Hansen, Nissenbaum, 2009, p. 1171). Cyber security becomes a terrain that depends on the 'expert authority' of the computer scientist and the policy expert.

The also unique interconnection between state, economy and society raises the question of whether cyberspace should not be seen as part of the broader topic of critical infrastructure security (Ibid. p. 1162). Cyber securitisation therefore requires an interdisciplinary effort, as it is at the intersection of many disciplines. The technical underpinnings of cyber-security, for example, require researchers in international relations to acquire an understanding of the main technical methods and, conversely, computer scientists need to be more aware of the politicised domain in which they design applications and how their decisions may affect the relationship between security and freedom.

Traditional international threats are giving way to decentralised network threats from non-state actors, and the spectrum of irregular conflicts is expanding. This perception of threats from unknown and unknowable non-state actors has permeated the way security policy theorists formulate thoughts about future conflicts (Coker, 2009, p. IX). It is easy to see how unknown, anonymous and malicious organisations fit into the overall paradigm of securitisation of cyberspace. The very term 'anonymous entity' in international relations evokes the image of a decentralised, ambiguous, non-state organisation operating outside the traditional legal and political framework (Ibid. p.70).

In line with the thinking of the Copenhagen School theorists, network security and individual security are very serious when defined by their connection to the state, nation, society and economy. Securitisation also engages the past as a legitimate reference, by, among other things, making historical analogies and comparisons of certain events in order to evoke emotions among the audience such as 'cyber Pearl Harbor' . (Bumiller, Shanker, 2012). However, it is worth considering whether this perspective on threat perceptions is an exaggeration, with catastrophic visions merely reflecting the political interests of certain decision-makers.

Unlike traditional factors (such as the size of military forces, economies based on gross domestic product – GDP, among others – or even population or geographical size (Walt, 1998, pp. 34-46), cyber capabilities are more difficult to quantify despite some states being identified as cyber powers. With most major states now committing serious resources and wanting to pursue strong, comprehensive cyber capabilities, any one investment in cyber research and development can threaten multiple adversaries and even some allies at the same time.

Since 2007, at least 15 countries have established cyber commands or dedicated military units focused on cyber defence and offensive capabilities (Nakashima, 2012). In 2007, government spending on cybersecurity was less than $10 billion worldwide; by 2012, the total had exceeded $50 billion with further increases (Cavelty, 2012). Indeed, every strategically important country reports increasing cyber security budgets, the most commonly counted indicator in formal analyses of the arms race. Moreover, dozens of official sources from many governments cite the rapid, destabilising growth of cyber security as the main justification for intensifying their own efforts and increasing their budgets (Zwilling, Klien, Lesjak, Wiechetek, Cetin, Basim, 2020).

Cyber security now exerts a dominant influence on the strategic dynamics of the international system and on the internal security of some nation states, both reflecting and reinforcing the increasing prioritisation of cyber operations by nation states. In line with this assertion, it can be presumed that cyber operations between states will accelerate in frequency and intensity.

Efforts by states to enhance their own security often diminish the security of others, provoking a balancing act by other political actors to take reactive action. In the case of cyber capabilities, awareness of adversary capabilities is a significant part of overall defence competence.

Consequently, the models of today's political and military alliances may be redefined in order to adapt them to a situation in which cyber competition (also in the form of cyber espionage, among other things) between allies is taken into account.

The large number of actors operating in the cyber space or using cyber technology suggests that the current international relations cyber dimension is very challenging and prone to complex and unpredictable changes. Thus, the actions and responses of states simultaneously influence each other and the nature of changing threats.

The perception of cyber threats has undoubtedly influenced the foreign policy process. The cyber discourse emanates from domestic actors, so it is increasingly necessary to follow this process at the international policy level.

A state with a higher level of cyber technology development (tends to have a higher international statute) and is more exposed to cyber threats or cyber wars, and thus has more experience in how to repel cyber attacks and how to deal with digital problems. In the same way, a state that has previously been more exposed to cyber attacks will be much more efficient in its securitisation process. Such actors also find it much easier to gain international support and allies for planned retaliatory actions. An illustration of this is the digital attacks carried out in 2007 against Estonia's critical infrastructure. The government in Tallinn received support from NATO and EU allies. It is uncertain, however, whether Estonia alone would have succeeded in securitising the event internationally; this was certainly helped by the country's membership of NATO, which enabled small states' security concerns to be highlighted internationally.

Non-governmental organisations, leaders and some international institutions can therefore substitute for policy makers or participate in the securitisation process in the international arena. For example, the UN can carry out securitisation by identifying a particular problem as a 'threat to international peace and security' (Buzan, Wæver, Wilde, 1998, pp. 149-151). In addition, organisations with different objectives have different impacts when securitising, for example, the World Health Organisation will not have the same impact on securitising a historic site as UNESCO and, conversely, UNESCO will not achieve a securitising effect in the area of global health issues.

The media is an important platform for the performance of the speech act, both in domestic and international securitisations. Where the media is state-controlled, usually the audience sees what the government wants them to see, and thus what serves the decision-makers in achieving their securitisation objective. International media, on the other hand, are not concerned with just one country and are usually private media. Their influence plays an important role in the securitisation process, setting priorities, setting the agenda, identifying solutions and providing a platform for leaders to perform their speech acts on the international stage (Shipoli, 2010, pp. 58-61).

A major unknown and challenge for both policymakers and researchers of international cyber security is the problem of the existence of a reliable mechanism for attributing cyber incidents. Knowledge in this area is necessary in the development of international law to establish the responsibility of states for acts of aggression committed in cyberspace. Cyber security policy is therefore characterised by a high level of asymmetry that renders attribution-specific defence strategies obsolete (Rivera, Hare, 2014, p.104). For example, packets used in attacks can be altered before reaching their target, and their original addresses can be removed by bots. Therefore, attribution is not entirely reliable because attacks can be installed by a third party. And even if they are attributed to a particular state, the consequence may turn out to be a political organisation or an individual working for their own interests (Libicki, 2009). Furthermore, defining cyber capabilities is often more a matter of speculation than knowledge. Unlike military weapons, cyber offensive tools cannot be observed, quantified and, in most cases, cannot be recognised prior to an actual attack (Schutte, 2012, p.8). In recent years, the line between offensive and defensive cyber operations has also become blurred.

Cyber threat as an enabler of securitisation

The issue being securitised is presented as existential and, although it may or may not be real, it must be constructed and presented in a certain way.

The public debate on cyber threats, points to the existing discrepancy between the increasing importance of cyber threats and the lack of events to justify this elevated status (Cavelty, 2008, pp. 19-36). Some scholars have argued that the excessive use of exceptional measures to accompany cyber threats raises a question mark over the meaning of securitisation? (Cavelty, 2008, p. 26). But does this conjecture fit a political reality filled with a huge number of cyber incidents? The trend towards increased securitisation in the field of cyber threats, is predominantly the result of the application of traditional military thinking.

The sources of the securitisation discourse are similar in nature to those motivations that treat cyberspace as a comparable domain to other militarised areas. The securitisation discourse takes cyberspace as a warfighting domain and applies a military perspective to the analysis of threats emanating from cyberspace, so observers of the securitisation of cyberspace may use the same logic that strategic studies developed during the Cold War for other domains, which is a key problem. This is because threat assessment is not based on a critical analysis of the consequences of cyber attacks, of technological developments, of possible defensive measures, but, on the contrary, on a creative imagination of 'what might happen if governments are not prepared', just as they were not prepared for the terrorist attacks of 11 September 2001, or for the attack by Japanese forces on the military base at Pearl Harbor (Lawson, 2001).

The current world is interconnected by an economic, political interdependence that has never been so developed in human history. Also noteworthy are the democratic values firmly embedded in international laws, which are protected by international organisations. Consequently, a different approach is to be expected in the strategies of states wishing to influence the political world order than a significant cyber-attack with huge physical consequences.

In fact, there has not been a single cyber attack threatening world peace to date. The most important one is repeatedly mentioned in the literature. Well, in 2010, the Stuxnet virus was used (Farwell, Rohozinski, 2011, pp. 23-40), which attacked nuclear centrifuges and disrupted Iran's nuclear programme, paralysing it for several years (Nicoll, 2011, pp. 1-3). The attack appeared to be a sabotage or covert intelligence operation and would be extremely difficult to repeat or carry out again.

To execute such an extremely precise and clandestine operation requires a prior intelligence operation to guarantee success; especially when any cyber weapon is a double-edged sword that can be used against the attacker in retaliation. There is also the question of who was actually behind the attack? This is not clear due to the well-known problem of attribution of responsibility in cyberspace, which makes it significantly more difficult to determine the origin of the attacker (Mudrinich, 2012, pp. 167-206).

Cyber attacks are inherently dangerous. But although, as researchers have argued, 'we have already come close to catastrophe several times, cyber threat scenarios are still largely in the domain of our imagination (Boer, Lodder, 2012). The same applies to cyber warfare. So far, cyber warfare has not happened, but 'it belongs primarily to the realm of what can happen' (Werner, Boer, 2017, pp. 39-60).

Illustrative of this securitising attitude are statements publicly reporting the possible realities of cyberwarfare, while referring to 'Hiroshima' or 'the next Pearl Harbor', emphasising the unpredictability and catastrophic consequences (Ibid.). In 2000, for example, Richard A Clark, former US National Coordinator for Security, Infrastructure Protection, Counterterrorism and adviser to Presidents Clinton and Bush, coined the term 'digital Pearl Habor'. Twelve years later, Leon Panetta, former US Secretary of Defence, paraphrased Clark, indicating that the US was facing a 'cyber-Pearl Harbor' (Bumiller, Shanker, 2012).

However, according to Bendrath, the word 'cyber' often has more to do with rhetoric and hidden agendas than actual threats. He also argues that the media, government officials and intelligence agencies form a circle in which they invent worst-case scenarios (Bendrath, 2003, pp. 49-73).

In support of the above argument: firstly, most cyber attacks, which are seen as the most serious in history, were not technically existential. The theft of military, commercial or personal information cannot affect the survival of the state, the private sector or any individual. Similarly, denying customers/citizens access to certain services through denial of service (DOS) attacks is not an existential threat to anyone. However, this does not mean that cyber threats cannot be underestimated or presented with urgency. Secondly, the indirect nature of most cyber attacks and the non-physical nature of their consequences, while not undermining their seriousness and urgency, acts as an impediment rather than a threat to existentiality. Most discourses emphasise these 'destructive' implications, including huge financial losses that can slow down the economy, loss of productivity and global competitiveness, loss of customer confidence in information infrastructure, etc. And although they are not presented in terms of 'survival', these destructive implications are still seen as an immanent, urgent and serious threat to national security.

Whether cyberspace really poses a threat is therefore irrelevant; what is crucial is the speech act that constructs the image of threat. The use of such 'apocalypse language' is therefore spreading uncertainty, fear and doubt (Armerding, 2017). These raise several questions: why do policymakers use this language of doom? Does apocalyptic language create a cyber threat scenario? Why is cyberspace constructed as a threat? To answer these, it is useful to apply the theory of securitisation, which offers an explanation of why certain issues become existential threats.

Securitisation as part of cyber security policy

The foundation of politics is the competition between actors in the public space, which stems from differing priorities and ownership of divergent resources. Successful securitisation justifies prioritising selected issues over other phenomena or processes (Fierke, 2007, p. 108). When an issue is successfully presented as an existential security threat, then this justifies exceptional policy measures (Peoples, N. Vaughan-Williams, 2010, p.76).

Calling war, however, is not straightforward. Important questions arise about who is involved in interpreting and identifying threats. Some actors will be more effective in labelling security issues than others. This depends on their credibility and their right to speak to the right audience. A securitisation actor needs sufficient social and political capital to convince an audience of an existential threat. At present, the authority appears to be emerging from two poles of cyber security: state security actors and digital security actors with their own forms of securitisation. Some issues are also easier to securitise than others, given their historical links to existential violence (Ibid.). The cyber-environment is relatively new in this respect, as it does not really have a history of violence like conventional forces whose experience stems from armed conflict.

The discussion of cyberwar is part of a rhetorical chain that prepares the ground for 'violence' in cyberspace and support for this action. It is this dynamic through which language constructs perceptions and influences political attachments that underpins securitisation theory.

Calling DDoS attacks a type of war carries with it a historical set of associations and assumptions about the appropriate way to deal with these problems and the choice of appropriate actors to deal with them. *War* is traditionally the domain of military institutions, and responses include the use of force. Therefore, the use of the term 'war' is a metaphor referring to more familiar linguistic descriptions of physical conflict. The concept of 'information war' is a similar securitisation move, applying military metaphors to, for example, industry and commerce (Munroe, 2005). The securitisation of the problem carries with it a particular kind of crisis politics in which dimensions such as space and time – allowed for debate, participation and negotiation – are necessarily limited and bring into play a particular militarised way of thinking (Peoples, N. Vaughan-Williams, 2010, p. 83). It can also be noted that the prefix 'cyber' also performs a certain securitising function. This prefix is an evocative way of using more prosaic terminology, evoking an innovative, modern and technological world.

As a result of the speech act, the issue is labelled as a security threat by the securitisation subject and, through rhetorical speech or persuasion, the audience finds some resonance. The issue is treated as a security threat requiring emergency action that the decision-maker believes will stop the threat. In other words, no issue is objectively a security problem, but the securitisation actor gives it credit according to the perception of security. According to Williams, *in securitisation theory, 'security' is treated not as an objective condition, but as the outcome of a particular social process* (Williams, 2003, p. 513). Therefore, what counts as security practice in one time period or location (e.g. Central Europe) does not necessarily count in the same way as security practice in another time period and region (e.g. Western Europe).

In security analysis, part of the problem is identifying the starting point. Well, what is an important security issue for one state may not be so important for another state. In other words, while the military sector may dominate the security picture in one state, in another state the issue of digital R&D and economic innovation may be a priority and determine policymakers' perceptions of security.

The identification of existential threats can be interpreted in different ways, well, not all threats are existential for all states and therefore governments perceive threats differently, requiring different sets of emergency actions and different responses from the public and private sector organisations (Brandt, Turner-Zwinkels et al., 2021).

Creating a traditional or cyber security programme raises a number of serious issues, some of which can be addressed due to the specificities of a particular state or region. In addition to an individual threat picture, each state has an individual security culture, determined by individual social, historical, legal factors. Consequently, countries differ in the way they adopt innovations and exhibit different behavioural styles when using and connecting information systems (OECD, 2002). Thus, the list of operators' responsibilities in one country may be more comprehensive or more restrictive than in another.

This position is in line with the research perspective formulated within the Copenhagen School. Thus, the main idea is to combine linguistic and security theory to create a critical discursive interpretation of security (Buzan, Wæver, Wilde, 1998, pp. 149-151). In the literature, questions often arise as to whether securitisation is realised through 'the utterance itself' or a social process? The legitimacy of this question stems from unfinished considerations about whether the speech act should be considered a more universal or contextual phenomenon (Stritzel, 2007, p. 364). Securitisation theorists emphasise that the whole situation must be taken into account if one wants to perceive the similarity between individual utterances and the process between the speech act and the constructed political reality. Embedded in the notion of speech act is the connection between utterance and impact, which points to the potential danger, or even threat, associated with the misuse of utterances thanks to which both what is said and the way in which it is said can have a negative impact on the recipient of the information. An example of this is articulated warnings, threats, insinuations, which in the international space have the potential to provoke and construct dangerous situations and therefore must be seen in political terms as a threat to the state, which itself represents the interests of citizens.

The Copenhagen School points out that securitisation is created while speaking, i.e. the meaning of security is given in a speech act that reveals power structures and configurations, whereby this speech act is not only an expression of possible threats, but can also be a manifestation of an attempt to dominate or shape one's own image. Ole Wæver made a further distinction, indicating that we perceive a particular problem as a threat not because there is an actual threat, but rather because the problem has been presented to us as a threat (Wæver, 2011, pp. 17-40). As a result, questions arise: what is the nature and criteria of public acceptance of government decisions? Can the theory apply to multiple, politically disparate audiences? What are the functions and types of public acceptance? Does every government present the same problem in an identical way? Does the presentation of security depend on the dominance of a particular political doctrine at a given time, which is the dominant thought at the level of government? Are specific views represented by policy-makers also determined by historical context and political experience? In order to answer these questions, it is first necessary to describe the meaning of the concept of 'security culture', which, as it turns out, is central to securitisation, since one of the main assumptions of this theory is that it is an intersubjective process and that its success depends on the consent of the audience.

Understanding the phenomenon of security culture is necessary to take into account the social, cultural and ethical aspects that are unique to each country. It is also important in the perspective of analysing the factors on which success in marginalising threats depends. In other words, there is no security culture that does not reflect societal behaviours, attitudes and values.

Thus, despite the general consensus among many governments as to the terminology of security and cyber-security, there is a perceived difference in effectiveness in achieving stable state functioning. Introducing similar cyber defence solutions is proving to have the potential to produce different results, highlighting on this occasion the complexity of factors that influence the outcomes of an effective cyber security strategy. One of the main explanations for this phenomenon is the security culture, which depends on the specific characteristics of social groups, so that certain values are individually adopted and then translated into behaviour. This element proves to be an essential aspect to understand the conditions affecting the success of cyber security strategy implementation in an international environment.

From the point of view of the social sciences, definitions of culture vary enormously: anthropology proposes a holistic approach to the concept, social psychology a rather constructivist perspective, and the security sciences have narrowed the meaning of the term and consider security culture as the sum of knowledge that generates behaviours that can help maintain national security, defend national values and achieve state goals.

For many years, in which technical protection was a thoroughly researched, funded and developed element, security education played a minor role. After some time, the reality with cyber threats proved that cybersecurity needed to include a cybersecurity culture as a fundamental point of reference. A similar position was expressed by the International Telecommunication Union (ITU), in a communiqué in which it is considered that *cyber security requires the development of a cyber security culture and acceptable user behaviour in the new digital reality* (Gcaza, Solms, Vuuren, 2015, pp.1-11).

To understand cyber security, knowledge of cyber security culture is required. Values specific to different cultures are acquired through socialisation, and therefore it can be considered that the implementation of measures or programmes to facilitate cyber security depends on the society.

Another highly debated topic in the securitisation literature is the time perspective. This is due to the intersubjective alignment of security policy with time and context, whereby specific events can be perceived as a vital threat to the community (Mutimer, 1997, p. 90). Political actors must choose critical moments when trying to convince audiences that they are right (Balzacq, 2011, pp.1-30). Also, issues that exist in a national or international perspective need different time periods for securitisation. Indeed, international securitisation brings together more actors in its framework than domestic securitisation (Shipoli, 2010). Moreover, the bigger the problem, the more actors involved. The experience of policy-makers is also important, as it influences the efficiency with which security issues are discussed. It is also important what kind of power and political position these actors have, as it will be difficult for a small state to securitise an international conflict, as opposed to a state with a strong political and military position.

Collective memory is also an important element, which is a special semantic reserve for securitization strategies, in which the sphere of the self, such as personal memory, can be used as a source of tactics in the securitization process. Research from the Copenhagen School indicates that memory shares many common features with the process of constructing and evaluating specific narratives, the interplay of past and present socio-cultural phenomena present in the process of shaping individual and collective experiences. A typical example of the relationship between securitization and historical experience is nation-building, that is, the top-down production of memory that is sustained by state institutions, which is expressed, among other things, in the use of specific symbols or in the evocation of certain past events in international discourse (Renan, 1996).

Securitization theory is future-oriented in contrast to history, but these disciplines are complementary in the process of constructing a concrete description of events. Securitization movements often involve the consideration of new threats; that is, threats that are not yet obvious but are already affecting social life, such as terrorism. However, in such cases they often appeal to memory and past events in order to reinforce and legitimize political decisions.

To conclude, it is worth considering whether the path to successful securitization is treated as a one-way road from the speaker's side to the audience, or whether it also takes place from the audience's side, which undertakes a joint *negotiation* or can be seen as a result of the violent emotions that initiate the process? In answering this question, it is worth emphasizing that securitization is always socially constructed. Whether the issue is threatening or not depends largely on who interprets and presents it. The audience to whom speech acts are addressed also plays an important role in this process; moreover, it is the audience that provides the context for adoption, "which can be seen as a unique tool for managing public space (Balzacq, Léonard, Ruzicka, 2016, p. 495). Buzan, de Wilde and Waever stated that "successful securitization is not determined by the securitizer but by the audience (Buzan, Wæver, Wilde, 1998, pp. 31). Without an audience that accepts the problem as a security issue, there can be no securitized problem. The public must accept such a message, not necessarily in a referendum, but tacit agreement to use means that would not normally be used is also acceptable. Their consent gives security actors the right to use any means to ensure the survival of the reference object. The public is the most distinctive building block between domestic and international securitization. One of the most important building blocks of securitization is speech, so it is a communicative activity that influences the audience and compels them to act accordingly (Wæver, 2011, pp. 46-86.).

To summarize this part of the work, it should be pointed out, first, that the act of securitization is implemented in different ways, through social contexts, cultural backgrounds and historical conditions. Second, any socially perceived level of security, results from a process of negotiation between policymakers and citizens. People, in turn, consent to any additional security measures that they necessarily feel are a significant burden due to costs in the form of, among other things, restrictions on movement, bans on entry to certain places, increased taxes, reduced social benefits, the withholding of information, the initiation of hostilities, the suspension of civil liberties or other measures that reduce the comfort of daily life. So, when there is rhetorical acceptance of an existential threat and its acceptance by the public, further actions follow, such as the application of emergency measures (Jackson, 2006, p. 313). The audience must therefore agree with the actor's proposition that *given the threat, it is necessary to introduce and apply certain tools* (Roe, 2008, p. 622). This limitation of norms does not contradict the universal principles of a democratic state. Even the liberal tradition recognizes and justifies the suspension of normal rules in emergency situations. Moreover, the existence of organized violence (identified with the armed forces) is considered a manifestation of modern state power (Huysmans, 1998, p. 571). This viewpoint, therefore, treats securitization as a decision-making process with regard to the use of extraordinary means. A specific grammar of securitization is thus activated, providing a rhetorical justification for the application of selected rights, obligations, or deviations from previously accepted norms. In this sense, securitization movements can be understood as an attempt to transform the existing system of political practices (Searle, 2009, p. 19).

Securitization is fully achieved if the recipients accept the introduction of extraordinary measures to marginalize or remove an existential threat, thus it is possible to legitimize the exceptional tools used by power (Buzan, Wæver, Wilde, 1998, pp. 31). The perspective thus presented, proves that securitization is a product of the social, organizational and political context. The ability of policymakers and security experts to persuade others depends on their own prestige, their resources and their ability to offer and present a coherent view.

Conclusion

This article uses the idea of securitization put forth by the Copenhagen School to examine the specifics of the construction of public discourse on cyber security. By discussing the logic of threats and vulnerabilities in the construction of cyber threats, it sought to show how threats including those of a digital nature are securitized which justifies the need for greater security and a certain level of risk acceptance by the public.

Threat attribution is also one of the important features of the construction of cyber threats. Discourses attributing cyber threats to Russia, China, Iran and North Korea have been growing for many years, taking advantage of the antagonistic relationship between these countries and the United States. Such discourses portray cyber threats as urgent and threatening, but never to the point where they threaten the existence of the state and its citizens.

In summary and conclusion, it is worth reiterating observations about the multi-stakeholder nature of cyber security and observations about the co-creation of that security by a wide range of actors representing different, and in some cases conflicting, interests. It can be argued that there is no single discourse on cyber security or cyber threats, and it is simplistic to assume that there is even a single discourse that represents every securitization actor, be it government or the private sector. This diversity explains why the assumption and logic of securitization theory can only apply to some, but not all, cyber security discourses.

Consequently, in order to fully understand the nature of politics and cybersecurity, there is a need for research that encompasses a much broader picture, drawing knowledge from disciplines such as history, cultural studies, anthropology, politics, sociology and religion. The exploration of the topic of the importance of new technologies also forces the issue to be placed in the research area of both regional and international circles. The analysis of the actions taken by entities with superpower (hegemonic) ambitions, requires more attention to how the securitization process operates at different levels, both horizontally and vertically. Also crucial to a broader description of the changes taking place is the fact that once the securitization process has begun, its intensity and consequences are difficult to predict.

Having presented the analysis of securitization, there is a conviction that it still needs to be developed with new research fields, as the theory has great potential. Cybertechnology will be an important sector that will contribute to the further development of securitization theory. Researchers will have to find the answer to the question: who can resist securitization and how? The awareness that securitization is being used for good and bad purposes prompts and motivates the search for an effective way to resist such moves implemented by the authorities.

Growing dependence on digital technology is inevitable, making the future more threatening than the present. Cyber technology is inherently vulnerable and thus impossible to fully secure. The call for *greater security* becomes justified because the more a country depends on cyber technology, the more inevitable cyber threats become. They are consistently treated by government circles as a security challenge, meaning that the problem is presented as an existential threat, requiring emergency measures and justifying action beyond the normal bounds of political procedure (Ibid.). In other words, the proclamation of the consequences resulting from cyber threats already in itself creates a new social order in which standard policy is bracketed (Balzacq, 2005, p. 171-201).

As mentioned, cyber discourse is synonymous with threat discourse. Since cyber is conceptualized through the description of threats, it falls between the military and civilian worlds as a domain. The militarization of cyber discourse reflects a certain political agenda. It is also a characteristic phenomenon that when the word *cyber* is said, people immediately think of security. Recognizing the Internet as a tool for information exchange, it is seen as a battle space. It is puzzling that some information is considered dangerous on the Internet, but publishing it in other (traditional) media does not generate controversy and public debate.

Cyber threat scenarios *still belong, for the most part, to the domain of the public imagination*(Boer, Lodder, 2012). Documents or statements by policymakers repeatedly prove that they are used to construct cyber threats. Thus, there is a successful securitization of cybersecurity in the public space. Through the aforementioned speech acts, digital communications are presented as an existential threat. It doesn't matter whether cyberspace is actually a threat, it only acquires this nature through the use of the language of annihilation. Policy makers specifically use this language because they have the necessary authority to carry out effective securitization. Thus, cyberspace is elevated from the realm of normal politics into the realm of securitization.

References

Armerding, T. (2017). How likely is a 'digital Pearl Harbor' attack on critical infrastructure?, https://nakedsecuritv.sophos.com/2017/08/18/how-likelv-is-a-digital--pearl-harbor-attack-on-critical-infrastructure. Access 12.11.2022.

Balzacq T. (2011). A Theory of Securitization: Origins, Core Assumptions, and Variants W: T. Balzacq (ed.). Securitization Theory: How Security Problems Emerge and Dissolve, London, New York: Routledge: 1–30.

Balzacq, T. (2005). The three faces of Securitization: Political Agency, Audience and Context, European Journal of International Relations, 11/2: 171-201.

Balzacq, T., Léonard, S., Ruzicka, J. (2016). Securitization' Revisited: Theory and Cases, International Relations: 30/4, s. 495.

Beck, U. (1992). Risk Society: Towards a New Modernity, London; Newbury Park, Calif: SAGE Publications Ltd.

Beck, U. (2002).The Terrorist Threat: World Risk Society Revisited, Theory, Culture & Society, 19/4: 39-55.

Bendrath, R. (2003).The American Cyber-Angst and the Real World – Any Link?, W: R. Latham (ed.), Bombs and Bandwidth: The emerging relationship between information technology and security, New York: The New Press: 49-73.

Boer, L. J. M., Lodder, A. R. (2012). Cyberwar: What Law to Apply? And to Whom?, W: R. Leukfeldt, W. Stol (eds.), Cyber Safety: An Introduction, The Hague: Eleven international publishing.

Brandt, M. J., Turner-Zwinkels F. M., B. Karapirinler, Van Leeuwen F., Bender M., van Osch Y., Adams B. (2021).The Association Between Threat and Politics Depends on the Type of Threat, the Political Domain, and the Country, Personality and Social Psychology Bulletin, 47/2: 324-343.

Bumiller, E., Shanker, T. (2012), Panetta warns of Dire Threat of Cyberattacks on U.S., https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html. Access12.08.2022.

Buzan, B., Wæver, O., de Wilde J. (1998). Security: a new framework for analysis, Lynne Rienner, Boulder, 25.

Cavelty, M. D. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, CSS Studies in Security and International Relations. London; New York: Routledge.

Cavelty, M. D. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, London: Routledge, 26.

Cavelty, M. D. (2008). Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate, Journal of Information Technology & Politics, 4/1: 19–36.

Cavelty, M. D. (2012). The militarization of cyber security as a source of global tension, W: A. Wegner (ed.).

Coker, C. (2009). War in an age of risk, Cambridge: Polity: IX.

Farwell, J. P., Rohozinski, R. (2001). Stuxnet and the Future of Cyber War, Survival, 53: 23-40.

Fierke, K. (2007). Critical approaches to international security, Cambridge: Polity:108.

Floyd, R. (2011). Can Securitization Theory Be Used in Normative Analysis? Towards a Just Securitization Theory, Security Dialogue, 42/4–5: 427–439.

Gcaza, N., von Solms R., van Vuuren J. (2015), An Ontology for a National Cyber-Security Culture Environment, Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA): 1-11.

Hansen, L. (2011). The Politics of Securitization and the Muhammad Cartoon Crisis: A Post-Structuralist Perspective, Security Dialogue, 42/4–5: 358.

Hansen, L., Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School?, International Studies Quarterly, 53/4: 1155-1175.

Huysmans, J. (1998). The Question of the Limit: Desecuritisation and the Aesthetics of Horror in Political Realism, Millennium – Journal of International Studies, 27/3: 571.

Jackson, N. (2006). International Organizations, Security Dichotomies and the Trafficking of Persons and Narcotics in Post-Soviet Central Asia: A Critique of the Securitization Framework, Security Dialogue, 37:313.

Lawson, S. (2001).Beyond cyber-doom: Cyberattack Scenarios and the Evidence of History, http://www.voafanti.com/gate/big5/mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attackscenarios – evidence-history_1.pdf. Access 12.09.2022.

Libicki, M. (2009). Cyberdeterrence and Cyberwar, RAND: Santa Monica.

Mirow, W. (2016). Strategic Culture, Securitisation, and the Use of Force. Post-9/11 Security Practices of Liberal Democracies, London, NY: Routledge.

Mudrinich, E. M. (2012). Cyber 3.0: The department of defense strategy for operating in cyberspace and the attribution problem, Air Force Law Review, 68: 167-206.

Munroe, I. (2005). Information Warfare in Business: Strategies of Control and Resistance in the Network Society, London: Routledge.

Mutimer, D. (1997). Beyond Strategy: Critical Thinking and the New Security Studies, W: C. A. Snyder (ed.), Contemporary Security Studies, Basingstoke: Macmillan: 90.

Nakashima, E. (2012). U.S. Accelerating Cyberweapon Research, The Washington Post, 2012, http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html. Access 12.08.2022.

Nicoll, A. (2011). Stuxnet: targeting Iran's nuclear programme, Strategic Comments, 17: 1-3.

OECD. (2021). Guidelines for the Security of Information and Systems and Networks, http://www.oecd.org/internet/ieconomy/15582260.pdf. Access 04.05.2021.

Olsson, Ch. (2015). Interventionism as Practice: On 'Ordinary Transgressions' and their Routinization, Journal of Intervention and Statebuilding, 9/4: 429.

Peoples, C., Vaughan-Williams N. (2010). Critical Security Studies: An Introduction, London: Routledge, 80.

Renan, E. (1996). What Is a Nation?, Trondheim: Tapir Press.

Rivera, J., Hare, F. (2014). The deployment of attribution agnostic cyberdefense constructs and internally based cyberthreat countermeasures, W: 6th International Conference On Cyber Conflict (CyCon 2014), 2014 6th International Conference On Cyber Conflict (CyCon 2014).

Roe, P. (2004). Securitization and Minority Rights: Conditions of Desecuritization, Security Dialogue, 35/3: 281.

Roe, P. (2008). Actor, Audience(s) and Emergency Measures: Securitization and the UK's Decision to Invade Iraq, Security Dialogue, 39/6: 622.

Schutte, S. (2012). Cooperation Beats Deterrence in Cyberwar, Peace Economics, Peace Science and Public Policy, 18/3: 8.

Searle, J. (2009). Language and Social Ontology, W: Ch. Mantzavinos (ed.), Philosophy of the Social Sciences: Philosophical Theory and Scientific Practice, Cambridge: Cambridge University Press:19.

Shipoli, E. A. (2010). International Securitization: The Case of Kosovo, Saarbrucken: Lambert Academic Publishing, 58–61.

Shipoli, E. (2010) International Securitization: The Case of Kosovo, Saarbrucken: Lambert Academic Publishing.

Strategic Trends, ETH Zurich CSS, Zurich, http://www.sta.ethz.ch/Strategic-Trends – 2012/The-militarisation-of-cyber-security-as-a-source-of-global-tension. Access 12.07.2022.

Stritzel, H. (2007). Towards a Theory of Securitization: Copenhagen and Beyond, European Journal of International Relations, 13/3: 364.

Van Munster, R. (2009). Securitizing Immigration: The Politics of Risk in the EU, Basingstoke: Palgrave Macmillan 2009.

Vuori, J. A. (2008). Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders, European Journal of International Relations, 14/1: 69.

Wæver, O. (2004). Aberystwyth, Paris, Copenhagen: New Schools in Security Theory and the Origins between Core and Periphery, International Studies Association, Montreal, 13.

Wæver, O. (2010). Podsumowanie programu badawczego: rewizje i przekształcenia teorii sekurytyzacji, W: Referat wygłoszony na dorocznym zjeździe International Studies Association , Nowy Orlean, LA , 17–20 lutego 2010.

Wæver, O. (2011). Politics, Security, Theory, Security Dialogue, 42/4–5: 465–480.

Wæver, O. (2012). Bezpieczeństwo: konceptualna historia stosunków międzynarodowych. Referat wygłoszony na dorocznej konferencji British International Studies Association, London School of Economics and Political Science.

Walt, S. (1998). International relations: one world, many theories, Foreign Policy (Special Edition: Frontiers of Knowledge), 110: 34–46.

Watson, S. D. (2009). The Securitization of Humanitarian Migration: Digging Moats and Sinking Boats, London: Routledge, 28.

Werner, W., Boer, L. J. M. (2017). It Could Probably Just as Well Be Otherwise, Risk and the Regulation of Uncertainty in International Law, M. Ambrus, R. Rayfuse (eds.), Rosemary; W. Werner, Oxford University Press, Oxford: 39-60.

Williams, M. C. (2003). Words, Images, Enemies: Securitization and International Politics, International Studies Quarterly, 47/4: 511–531.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, 62/1.