SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

The Copenhagen School's widening security theory in relation to cybersecurity. Applicability and implications

Mihai Olteanu

mihaiolteanu48@yahoo.com

https://orcid.org/0009-0008-8263-0925

Intelligence and National Security, National Defence University "Carol I", Șoseaua Panduri 68-72, 050662 Bucarest, Romania

Abstract

This paper critically examines the relationship between cybersecurity and Copenhagen School's widening security theory, with the aim of assessing the possibility of applying this theoretical framework to the cyber realm. As cybersecurity is a relatively recent addition to the security discourse, this research explores whether the Copenhagen School's traditional framework, which was primarily focused on securitisation processes in the five main sectors (military, political, economic, environmental, and societal), adequately encompasses the unique aspects and dynamics of cyber domain. The research question is: Why the cybersecurity field can't become a separate constructivist sector? The study begins with a detailed overview of both cybersecurity landscape and Copenhagen School's fundamental principles to provide the context for a comparative analysis of the Copenhagen theory and contemporary cybersecurity literature. In doing so, the research delves into the features of cybersecurity, with a focus on the evolving nature of cyber threats and vulnerabilities. By performing a qualitative analysis of the existing literature, the paper assesses the limitations of integrating these two concepts, ultimately concluding that cybersecurity lacks the distinct characteristics required to be considered a separate sector under the Copenhagen School's framework. The findings contribute to the ongoing discussions regarding the adaptation of traditional security theories to address contemporary security challenges in the digital age.

Keywords:

security studies, Copenhagen school, digital age, technological advancements, cyber threats

Article info
Received: 24 August 2024
Revised: 5 September 2024
Accepted: 1 September 2024
Available online: 21 October 2024

Citation: Olteanu, M. (2024) 'The Copenhagen School's widening security theory in relation to cybersecurity. Applicability and implications', *Security and Defence Quarterly*, 48(4), pp. 40–58. doi: 10.35467/sdq/193049.

Introduction

Over the past four decades, the cyber field has continuously gained importance due to the rise in the number of attacks, some of which have had a significant impact on the security of states. The first major cyberattack ever encountered was caused by the Morris Worm in 1988, a type of malware which was capable of self-replication from one computer to another without any human interaction and constantly searched for new computers to compromise (Meeuwisse, 2017, p. 161). The worm managed to compromise computers used by Purdue University, Massachusetts Institute of Technology, and the National Aeronautics and Space Administration (NASA) (Jajoo, 2021), while also representing the first case of a person convicted under the Computer Fraud and Abuse Act in 1989 (Federal Bureau of Investigation [FBI], n.d.).

The Morris Worm was just the beginning for a massive amount of cyberattacks conducted by individuals, states, and organisations. The well-known April 2007 cyberattack campaign against the Estonian authorities completely shut down the infrastructure of the entire government and ministries while also proving that states are capable of using cyberattacks as a political tool, considering that the whole campaign was determined by the relocation of a memorial commemorating the Soviet liberation of the country from the Nazis (Herzog, 2011, pp. 2–3). Moreover, the 2015 cyberattacks against the energy sector in Ukraine underlined that the cyber field would also become an important component of military strategies (Plėta *et al.*, 2020, pp. 4–5).

The realm of cybersecurity has developed into a distinctive domain, characterised by various types of actors and attacks, primarily delineated by their motivations. Within this context, there are entities engaging in cyberattacks with the aim of advancing political objectives, securing economic advantages, or advocating for specific ideological beliefs (Li and Liu, 2021, pp. 8179–8181). Therefore, global dynamics heavily influence the frequency and targets of cyberattacks, highlighting the interconnected nature of international context in cybersecurity.

The most complex form of cyberattacks is the Advanced Persistent Threat (APT), usually conducted by state actors, aiming for cyber espionage and using the most evolved tactics, techniques, and procedures. Generally, the Russian and Chinese APTs have been dubbed as being the greatest threats against North Atlantic Treaty Organisation (NATO), considering their use of the highest level of technical capabilities to collect intelligence and strategic data (Olszewski, 2018).

On the other hand, although with a lower level of technical complexity, the COVID-19 pandemic has precipitated a discernible upswing in cyberattacks, particularly those underscored by financial incentives. The widespread adoption of remote work and increased reliance on digital communication platforms during the pandemic created fertile ground for cybercriminals seeking financial gains. Likewise, the pervasive anxiety prompted by the pandemic, along with an inherent curiosity for detailed information, led a high number of people to open malicious emails. This context was exploited by financially motivated cyber actors which conducted ransomware attacks using the COVID-19 pandemic as a tool to access computers. During the period spanning from 31 December 2019 to 14 April 2020, there were approximately 30,000 cyberattacks specifically related to COVID-19, and in March 2020, there was a documented surge of 600% in phishing attacks and (Lallie *et al.*, 2021, p. 3).

Finally, there is another subset of actors propelled by ideological motivations, endeavouring to advance and advocate their specific systems of beliefs. These ideological cyber actors

distinguish themselves by deploying attacks characterised by a lower level of complexity, and greatly influenced by the international political landscape (Yunos *et al.*, 2017). Depending with their ideological stance, these actors may support a varied range of causes, encompassing issues such as the decriminalisation of soft drugs, supporting the cause of Ukraine, or environmental protection.

One group that particularly fits the description mentioned above is KillNet, a notorious ideologically motivated cyber entity, which was mainly active after the 2022 Russian invasion in Ukraine. KillNet specifically directs its attacks towards countries supportive of Ukraine, across multiple industries, including notable victims, such as government entities, financial institutions, and critical sectors. It is believed that KillNet has affiliations with Russia and is potentially supported by the Russian government. This geopolitical connection adds a layer of complexity to its activities, suggesting a broader strategic agenda intertwined with state interests (Warren *et al.*, 2023, pp. 95–98).

In the light of the continuous growth of the importance of cybersecurity and the escalating array of multifaceted threats, the ascension of this field to a pivotal strategic component is unmistakable. The digital field's rapid evolution underlines the growing relevance of cyber threats and risks for organisations, be they are public or private. Moreover, the cyberattacks presented prove that this field can be used to support the interests of different state and non-state actors.

This paper aims to examine the relationship between cybersecurity and the Copenhagen School's widening security theory. The objective is that of understanding whether or not the theory could be extended to the cyber realm, creating a new sector inside the traditional framework focused on five sectors (i.e. military, political, economic, environmental, and societal). This paper argues against the development of a separate cybersecurity sector in the Copenhagen School framework, having as its main argument the fact that the cyber realm is already a component of the other five existing sectors. Moreover, to prove this point, some of the most relevant cyberattacks, which have been securitised as a part of the initial five sectors, are analysed.

The Copenhagen School's security theory uses "securitisation" as a central concept, describing the process through which securitising actors use the speech act to socially transform various problems (referent objects) into security matters that justify the adoption of extraordinary measures (Buzan *et al.*, 1998, pp. 25–32). The Copenhagen School broadens the concept of security to include multiple sectors, namely: military security (focused on threats to the survival of the state), political security (the stability of political systems and governance structures), economic security (threats to economic welfare), societal security (threats against societal identity), and environmental security (threats to the natural environment and ecological stability) (Buzan *et al.*, 1998, pp. 7–10).

The existing literature is mainly focused on proving that a successful securitisation on the cyber field has been conducted. However, there is a gap in security studies regarding the possibility of extending the process of securitisation towards the creation of a new sector, alongside the five already existing, and this paper intends to fill this gap. Furthermore, such an analysis is relevant considering the importance of the cybersecurity field, which has continuously grown over the last three decades (Fadziso *et al.*, 2023, pp. 4–8) and was not taken into consideration initially by the Copenhagen School's widening security theory. This provides the relevant context to evaluate whether the original theory of five sectors could be broadened to include a cyber sector. In doing so, this paper looks into the cybersecurity field through the lenses of the Copenhagen School's widening security theory in three steps: firstly, the paper evaluates the securitisation of the field, as this is a basic

constructivist requirement to analyse a sector; secondly, the paper analyses the existing five sectors in correlation with cybersecurity threat reports published by important private companies regarding the activity of cyber threat actors; and thirdly, the cybersecurity field is evaluated through the three types of units involved in security analysis: referent objects, securitising actors, and functional actors, aiming to understand whether the cyber realm has unique features, in comparison with the other five sectors.

Methodology

Starting from the research question, namely whether cybersecurity can become a new constructivist sector, the research method adopted in this paper is primarily focused on qualitative analysis of academic literature related to the intersection of cybersecurity and the Copenhagen School's securitisation theory. This approach involves a detailed evaluation of the key arguments presented by scholars in the field, particularly in relation to the extension of the Copenhagen School's sectoral analysis to encompass the cyber domain. The study examines the existing literature to assess how the concepts of securitisation, referent objects, securitising actors, functional actors, the five security sectors, and the competition for resources interact with the realm of cybersecurity. This relation is also evaluated from a technical standpoint, considering the particularities of the cyber field.

No primary data collection was undertaken, as the research relied on a review of the existing scholarship, which provided sufficient depth and breadth to address the research question.

The first research method used to approach the main question of the paper is focused on qualitative text analysis conducted on the academic literature related to the chosen topic, with the aim of evaluating the main arguments provided by different authors regarding the possibility of extending the constructivist framework. Moreover, the second part of the research uses as its method an interdisciplinary analysis, based on the interaction between the technical features of the cybersecurity field and the theoretical coding framework of the Copenhagen School related to the most important concepts, such as securitisation, referent objects, speech act, and different actors.

Literature review

Hansen and Nissenbaum (2009, p. 1157) provided some arguments in favour of defining cybersecurity as a separate sector according to the constructivist theory. One of their arguments was that the development of cyber-related strategies, laws and institutions directly supports the idea that this field has been securitised according to the constructivist theory. A similar perspective was supported by Aydindag (2021, pp. 8–11), which argued that the cyber field has been completely securitised, particularly in Turkey, where this field is even used to censor media and the Internet. Similarly, Cavelty (2020, pp. 13–14) argues that the heightened recognition of cybersecurity as a significant national and international concern signifies a complete securitisation of the matter. Her work argues that cybersecurity is incorporated into numerous national and international security strategies and related documents. Santaniello (2022) underlines the continuous nature of the securitisation process in the field of cybersecurity, and the efforts of official democratic authorities to support this process. Górka (2023) underlines how the states are becoming more dependent on technology, meaning that newer and greater cyber threats are faced constantly, and this becomes a securitisation component, as cyberattacks may create existential problems for a high number of nations. Jantunen and Huhtinen (2011) also argued that a securitisation

of the cyber field has been conducted in the United States, as their analysis reveals that "cyber" is consistently associated with threat, portraying the United States as vulnerable and technologically outdated, while the adversary is seen as skilled and resourceful, which require the adoption of exceptional security measures. However, although this article acknowledges that a complete securitisation in the cyber field has been conducted, as demonstrated by the authors presented above, this argument is not sufficient to prove the existence of a new entirely separated sector, especially considering that other matters have been securitised successfully over the last decades. One such example is terrorism, as argued by authors, such as Karyotis (2007) in his analysis focused on Greece and by Dolinec (2011) in his study presenting the use of mass media in the process of securitising the issue of terrorism. Another example is the securitisation of nuclear energy, which was shown to be successfully securitised in the Association of Southeast Asian Nations (ASEAN) region (Han, 2013). These matters have been securitised and are not included as separate constructivist sectors, even though they existed before the cyber field.

Hansen and Nissenbaum (2009, pp. 1163–1164) also argued in favour of creating a new sector by emphasising the distinctions of the cyber sector, compared to the other sectors previously theorised by the Copenhagen School. Notably, this comparison extended to sectors, such as the economic and environmental, which share the most common features with the cyber sector. Lobato and Kenkel (2015) provided a similar perspective in their analysis focused on Brazil and the United States, arguing that a new sector could help to distinguish cyber threats from other types, clarifying the separation between securitisation and militarisation trends while also capturing the unique dynamics of online threats. This view was also supported by the work done by Cavelty and Egloff (2021), who pointed out that technification is one unique feature of cybersecurity and that this has become a great challenge. Although these arguments are valid, the claim of this study is that a cyber sector exists only if one can identify different referent objects, securitising and functional actors (Buzan *et al.*, 1998, pp. 36–42). As the following sections argue, the cybersecurity is a component of any of the five sectors, rather than a completely separate field.

Fouad (2019, pp. 635–637) argued that in cybersecurity, threats are perceived as deliberate attacks, but it is difficult to objectively argue that something is an existential threat to a referent object. This is because the majority of cyberattacks are non-kinetic and indirectly conducted, which makes it difficult to see them as urgent. Similarly, Hansen and Nissenbaum (2009, p. 1164) argue that the process of cyber securitisations lacks a comparable history of foundational incidents but portrays important risks. This combination of envisaging cascading disasters and the absence of a precedent of such magnitude introduces a significant ambiguity into cybersecurity discourse. Although the perspective of the three authors is valid, over the last two decades some important cyberattacks (some of them physical) have occurred, proving the risks involved by the lack of cybersecurity.

From the opposite perspective, Burton and Lain (2020) underline a counterargument opposing the incorporation of cyber domain as a novel constructivist sector. Their contention revolves around the potential detrimental effects that such inclusion may inflict upon both broader society and realm of national security. Additionally, the research advocates for the normalisation of cybersecurity practices. This shift would entail a recalibration of how cyberattacks are perceived, emphasising their actual impact, rather than relying solely on anticipated consequences and worst-case scenarios. Similarly, Thumfart (2022) argues that there is no need to create a dichotomy between securitisation and desecuritisation in the field of cybersecurity, as, regardless of the status of the cyber field, both private and state actors need to act to assure continuous access to information and Internet services.

In summary, most of the arguments identified in the literature are in favour of the securitisation of cyber domain, particularly in the context of establishing it as a new sector alongside the five sectors outlined in the constructivist theory of the Copenhagen School.

Cybersecurity—towards a wider approach?

In 2018, interviewed by Leonie Tanczer, when asked about the five sectors and the possibility of including a new one in the conceptual framework developed by the Copenhagen School, Buzan (2019, pp. 115–122) stated that "there is therefore absolutely nothing set in stone about sectors" and that the whole mechanism behind creating them was based on empirical research conducted at the end of the 20th century. Moreover, when talking particularly about the cyber field as a new sector, Buzan (2019, pp. 115–122) stated that there is quite a debate about whether cyberspace is a component of other sectors, or rather a separate sector with some distinct characteristics on its own. Therefore, one could make a case for each of the two perspectives.

The statements made by Buzan (2019), along with the aforementioned idea that "securitisation" is a central concept of the Constructivist approach, and the current literature that argues in favour of an already existing securitisation process in the cyber field (Cavelty, 2020, pp. 13–14; Jantunen and Huhtinen, 2011), set the ground for the debate revolving around the creation of a new security sector. As pointed out in the previous parts of the paper, the first step towards identifying the existing sectors was to look into the processes of securitisations that have been conducted. The cyber field was securitised over the last decades (mainly after the occurrence of massive cyberattacks), therefore the debate should be focussed on the next constructivist step—the creation of a new sector.

This section of the paper evaluates the arguments identified in the literature and tries to ascertain whether they justify the establishment of a new cyber sector, in addition to the already existing ones.

Securitisation through cyber institution and strategic documents

It has been argued that the importance of cybersecurity justifies the establishment of a new constructivist sector focused on cyber issues (Hansen and Nissenbaum, 2009, pp. 1168–1171); this claim also being supported by the existence of cyber field in numerous objectives and strategies (Cavelty, 2020, pp. 13–14). Counterarguments may be raised concerning these assertions. Primarily, asserting the importance of cybersecurity as a field does not inherently justify the creation of an entirely new sector. When comparing the cyber domain with counterterrorism—an equally crucial security concern for many nations—one might observe that both have become intrinsic to discussions on national security (Albahar, 2019). However, constructing a compelling case for the establishment of a distinct constructivist sector exclusively dedicated to counterterrorism remains challenging. One could argue that the discussion about counterterrorism has been shifted from normal politics towards matters that require extraordinary measures, resources, and investments, as the safety of population, history, or culture may be endangered by acts of terrorism conducted by extremist groups (Helbling and Meierrieks, 2022, pp. 978–981). The discussion about a hypothetical counterterrorism sector is relevant because this matter has also been securitised and, from a similar point of view, could have been considered a distinct sector. However, as is also the case with the cyber sector, the terrorist threat has been included in the five previously existing constructivist security sectors. The same line

of reasoning is applicable to organised crime, illegal migration, and medical crises, such as the COVID-19 pandemic (Oshewolo and Nwozor, 2020). While these issues have grown in importance and are acknowledged as integral components of national security, they are effectively accommodated within the already established sectors, including the military, political, and economic domains. This raises the question of whether the distinctiveness of the cyber domain warrants the creation of an entirely new constructivist sector, especially when other pressing concerns are placed within the existing theoretical framework. Therefore, the central counterargument here is that simply evaluating an action as being extremely important for national security is not sufficient to define a separate constructivist theoretical framework. Moreover, the establishment of institutions and strategic documents is not an argument that supports the creation of a separate sector. As mentioned earlier, various institutions at both national and international levels address issues like terrorism (European Counter Terrorism Center) or propaganda (Moldavian Anti-Propaganda Centre) (Necsutu, 2023). However, there is no compelling rationale for establishing a new constructivist sector specifically centred on propaganda or terrorism, as this would require a separate set of reference objects, securitising actors and functional entities which define the dynamics of new theoretical framework.

The inclusion of a cyber realm in the five other sectors

It has been contended that significant differences exist between the economic and environmental sectors and the potentially new sector of cybersecurity (Lobato and Kenkel, 2015). This aspect contributes to the overall argument that the cyber domain possesses ample distinctions, compared to other sectors, making a case for the presence of sufficient unique characteristics that warrant the establishment of a new theoretical sector (Hansen and Nissenbaum, 2009, pp. 1163–1164). However, some counterarguments can be made about this statement when evaluating the connection between each of the five sectors and cybersecurity.

Over recent decades, multiple major cyberattacks have occurred, such as the Stuxnet campaign and the WannaCry ransomware attack, proving that there is a high level of risk. However, it is important to point out the fact that the occurrence of these incidents did not prompt the securitisation of a new constructivist sector, but rather was used to support the already existing five sectors. Still, it is important to understand the long-term impact of such cyberattacks, as private entities and official bodies reacted to such events. EUROPOL and the Dutch police developed the *no more ransom* platform, a free online tool that is being constantly used by individuals to prevent themselves being compromised by ransomware campaigns. Following the Stuxnet cyberattack, the European Network and the Information Security Agency called for higher cybersecurity measures for European critical infrastructures, as similar attacks were expected to reoccur. Since then, the EU has been working constantly to create regulation that would develop the level of cybersecurity measures in its member states, notably the Directive on Security of Network and Information Systems, enacted in 2016, and the directive on measures for a high common level of cybersecurity across the Directive EU 2016/1148 (NIS 2 Directive) adopted in 2022.

Hence, when Estonia was targeted in 2007 by Russian groups and the whole government infrastructure became unavailable, the authorities did not focus their speech on the cyber field *per se*, but rather on the fact that Russia, the already existing threat, was using a new way to attack the Estonian territory. A whole process of digitalisation and cybersecurity development occurred in Estonia over the next decade, but it was always advocated based on the Russian threat, rather than the importance of cyber field itself. The securitising

actors that supported the development of cybersecurity in Estonia were the same ones that performed the speech act for military sector (Czosseck *et al.*, 2011), as the referent object was identical. A similar approach was seen regarding terrorism in European countries and the United States, as the stake was also their territorial integrity against external threats. When talking about hacktivists, these groups were seen as already existing extremist groups that started advocating their cause through cyber means, as in the case of the attacker Gaza Cyber Gang, associated with Palestinian activists (Wang *et al.*, 2021). The same was the case for financially motivated cyber criminals, which were securitised as an extension of already existing organised crime groups addressed by the existing government bodies (Whelan *et al.*, 2023).

A notable shift occurred in the operational domains of various actors, marked by the extension of their existing activities into cyber space. According to NATO's operational domain classification, where cyber issues were integrated in 2016, it can be inferred that the alliance perceives cyber realm as an additional area requiring defence, parallel to land, sea, and air (Shea, 2017, pp. 19–21). In the case of the three pre-existing operational domains, a distinct securitisation process was not individually conducted for each one of them. Instead, the speech's referent object was focused on the military sector, specifically emphasising territorial integrity. Moreover, the cyber realm is acknowledged as yet another domain that demands appropriate protection against potential attackers.

Furthermore, the fact that cyber issues were included in each of the already existing sectors can be seen even when evaluating them individually. Firstly, when speaking about the political sector, it is rather impossible to conduct an analysis on referent object, securitising actors, and functional actors without including cyberspace. The legitimacy of a state can be threatened by cyberattacks as well as internal sovereignty of the ruling authority. For example, online propaganda against a certain political entity or government could be conducted through cyber means in order to destabilise authorities. Shults (2021, pp. 14–17) argued in his work that multiple state-sponsored cyber groups conduct attacks in order to support propaganda against Western governments. Also, from a different point of view, the securitising actors, such as political leaders and governments, could also be using the cyber field in order to prevent any threats to international legitimacy or internal sovereignty. That is mostly the case for states, such as China and Russia, but still it proves that the cyber realm is an important component of the securitising activity in the political sector (Creemers, 2017, pp. 87–89). Finally, functional actors, such as political activists, may use cyber means to promote their objectives in the political sector. Cyber actors, dubbed hacktivists, conduct operations to compromise and expose governments or officials in order to promote their political objectives (Kyška, 2014). Some of the most relevant cyber actors that provide support to these claims are as follows: APT29, which has been attributed by Mandiant to Russia's SVR and conducted diplomatic attacks against strategic targets, such as Turkey, India, and an Embassy of the Czech Republic (Jenkins *et al.*, 2023); APT40, which has been attributed by Mandiant to the Chinese government and conducted attacks against states, such as Belgium, the United States, the United Kingdom, and Germany (Plan *et al.*, 2019); and the hacktivist group KillNet, publicly reported as a pro-Russian hacktivist group by Microsoft, targeting states that support Ukraine (Azure Network Security Team, 2023).

Secondly, in the military sector, the cybersecurity field was also included as an important component that influences the activity of securitising actors as well as the functional actors and referent objects. Prolific cyberattacks, such as the Stuxnet campaign against the supervisory control and data acquisition (SCADA) systems used in the Iranian nuclear program, proved that the physical security of a territory cannot be assured without taking into account cybersecurity (Kumar *et al.*, 2022). Therefore, the military sector, like the

political one, uses cyber means to securitise the referent objects. One could also make a case that cyber actors are functional actors for both political and military sectors, as they can greatly influence the securitising processes and other important actions closely connected to these sectors (as in the case of hybrid war). Among the most relevant cyberattacks reported by the specialists and supporting the inclusion of cyber in the military sector is the black energy campaign conducted by the SANDWORM APT, as reported by Mandiant (Hultquist, 2016). The cyber attacker was attributed to the Russian GRU by private companies, such as MITRE (2017) and Mandiant (Proska *et al.*, 2023).

Thirdly, the economic sector's referent objects, such as national key industries, are greatly endangered by the evolution of ransomware attacks during recent decades. There have been numerous successful cyberattacks that targeted financial entities in order to gain money as quickly as possible. Notably, the WannaCry ransomware campaign, which was conducted in 2017, managed to infect networks located in over 150 countries, generating significant financial losses for many private and public entities (Ghafur *et al.*, 2019). Furthermore, a discussion on economic security is incomplete without incorporating the realms of Internet banking and crypto currencies, both representing digitally dependent financial dimensions highly vulnerable to cyberattacks and, inherently, in need of being securitised. Among the most important cyberattacks that provide support for this argument and have been investigated by the cybersecurity industry are the DarkSide ransomware (Trend Micro Research, 2021), Conti ransomware (Flashpoint Intel Team, 2022), and Revil ransomware (Fraser, 2021).

Furthermore, the societal domain is also profoundly impacted by the cyber field. The values and identity safeguarded by securitising actors become susceptible to risks due to the constant activities of various cyber groups and cyberattacks. The endeavours of hacktivist groups, in particular, can extend to directly assaulting the cultural beliefs of specific communities through the dissemination of propaganda and disinformation. Notably, there exist several hacktivist groups operating in the Middle East and North Africa (MENA) region, aiming to portray distinct communities as threats to other states. One such example is the Gaza Cyber Gang, which conducted multiple campaigns in MENA, many of them targeting Israeli people and their identity (Antoniuk, 2023). Moreover, the KillNet group, which has become prolific after the Russian invasion in Ukraine, constantly conducted cyberattacks against pro-Ukrainian countries, fighting against the cultural identity of anti-Russian Ukrainian citizens and promoting messages such as "As a gift from our team in honour of the Independence Day of Ukraine – hold on! Attack on 3 large gas station networks in Ukraine" (*The Cyber Express*, 2023) or "(…) there is no historical territory, actually a fictional country" (Eclectic IQ Threat Research Team, 2022). Therefore, as argued before, cyber groups and cyberattacks are relevant functional actors for the sector of societal security, as they are able to widely promote certain rhetoric that directly endangers a set of values or the cultural identity of any community. There are cases in which hacktivists also act as securitising actors for the societal sector, such as the campaign of the ANONYMOUS group that targeted Middle East countries to support the Arab Spring movement, as reported by cybersecurity companies (Crowdstrike, 2022).

Ultimately, the significance of the cyber field in the environmental sector is noteworthy, serving not only as a platform for promoting diverse securitisation processes but also as a tool utilised by hacktivists to advocate for their environmental ideals. Sustainable global development is an objective advocated by multiple hacktivist groups while conducting cyberattacks against governments and private companies that endanger the ecosystem. In 2010, one such group, named Decocidio, shut down the website of the European Climate Exchange and replaced it with the message "Super promo – climate on sale: Guaranteed profit!" as an action to support their anti-carbon trading objective (Phillips, 2010).

Another example is the activity of the hacktivist group Guacamaya that stole and published around 10 terabytes of emails from government agencies in Chile, Mexico, El Salvador, Colombia, and Peru as part of their claimed activity of fighting against all forms of environmental devastations and exploitations (Vicens, 2022).

In conclusion, the cyberattacks investigated in threat reports by private industry underline the fact that the cyber component is now an integral part of the securitisation processes within all five constructivist sectors. Consequently, any discussion about the military, economic, societal, political, and environmental domains includes consideration of cyber groups, encompassing hacktivists, state-sponsored attackers, or financially motivated groups.

The absence of unique referent objects, securitising actors, or functional actors

One could argue that if there are noteworthy differences between a potential cyber sector and the already established five sectors, this divergence serves as a justification for the expansion of the theoretical framework articulated by the Copenhagen School. Expanding the theoretical scope to accommodate the unique attributes and dynamics of the cyber domain would then enhance the framework's comprehensiveness and applicability in understanding the evolving landscape of security challenges. Therefore, the potential referent objects, securitising actors, and functional actors of a hypothetical cyber sector should be analysed.

Regarding the referent objects, these would have to be technical assets that need to be protected and are existentially threatened. These objects have an extremely wide variety, ranging from government networks, official websites, classified networks, internal communication platforms, data bases, Supervisory Control and Data Acquisition (SCADA) infrastructures (which support vital functions, such electricity production), to individual devices used by each person, Internet banking, and personal data. The range of referent objects is so wide that it is difficult to enumerate, let alone describe the process of their securitisation (Kamiya *et al.*, 2021). However, one may argue that the referent object is simply data and information, so that the objective of the securitising actor is to present them as being existentially threatened (from the perspective of confidentiality, integrity, and availability) and therefore in need of being securitised. Still, one problem remains, taken individually, each one of these referent objects is directly linked to one of the five sectors. It is impossible to talk about classified networks or SCADA infrastructure apart from military and political security as well as to securitise the Internet separately from the societal security or the Internet banking independent of economic security.

When discussing securitising actors, there is also a wide range of entities that may perform the speech act for different referent objects of the hypothetical cyber sector. For example, regarding the protection of data and information from the infrastructure used by the state or the citizens of a specific state, the securitising actor would be government advocating for investments in the development of networks that support certain functional areas. A bank may also perform the speech act when promoting the necessity of different layers of cybersecurity to be adopted by its customers, while a political party would securitise its sovereignty by labelling online propaganda as part of the existential threats, urging for protective measures.

The crucial aspect here is the near impossibility of defining distinct securitising actors exclusively for the cyber domain. Generally, the only actors advocating solely for this

domain are government bodies or international agencies, often extensions of various international organisations, such as the EU or NATO (Lété and Pernik, 2017). Furthermore, delineating referent objects for the cyber field proves challenging, as they are intertwined with the referent objects of the other five sectors. Similarly, these five sectors cannot perform the act of speech without including cyber-related issues.

The final point that should be made is that cybersecurity holds another particularity which would make it difficult to fully accomplish the speech act. While the external threats have already been portrayed as being truly important for national security, the cyber field is highly characterised by internal vulnerabilities rooted in technical, procedural, and human factors. Unlike traditional security domains, such as military or economic, which predominantly face external risks, the cyber landscape presents a distinctive set of challenges. The features of cybersecurity involve safeguarding digital assets not only from external adversaries but also from internal weaknesses that can appear from within a private or public organisation as well as from personal devices (Breda *et al.*, 2017). Regarding the technical infrastructure, vulnerabilities can arise from outdated software, unpatched systems, or inadequate network configurations (Thomas and Chothia, 2020). Addressing these internal technical vulnerabilities is crucial to fortifying a system against potential cyberattacks. Equally important are procedural vulnerabilities, which may stem from lapses in security protocols, insufficient access controls, or poorly defined incident response plans. Mitigating these procedural gaps is also essential for establishing a robust cybersecurity posture (Kim and Lee, 2018). Furthermore, human factors play a pivotal role in cybersecurity, with insider threats posing a substantial risk. Employees, whether unintentionally or maliciously, can become conduits for cyber vulnerabilities. This emphasises the importance of ongoing training, awareness programs, and a security-conscious organisational culture to minimise human-induced risks (Khan and Madnick, 2021).

In essence, the distinctiveness of cybersecurity lies in its various features requiring a comprehensive approach that addresses not only external threats but also the internal vulnerabilities arising from technical shortcomings, procedural weaknesses, and human factors. Hence, a speech act that would aim to securitise the cyber field should not only be focused on facing the existential threat with necessary resources but also on preventing this threat from having the opportunity to succeed. A complete securitisation would require that each person from any public and private organisation is aware of the risks as well as capable and willing to undergo necessary measures to prevent these risks from materialising.

Possible arguments in favour of a new cyber sector

Although the previous section explained the main arguments that underscored the inherent difficulties in crafting a dedicated conceptual framework for the cyber sector, it is important to acknowledge that there still exist a few points that may be used to make a case for the creation of this new dimension in the constructivist theory.

This section of the paper is used to further discuss the facts that could be used to advocate in favour of the extension of the Copenhagen School's framework. Although these arguments pose less importance for the whole theoretical debate, it is important that they are taken into consideration so that the picture of this discussion would be complete. Therefore, the constructivist theory states that the individuality of the sectors may be seen in the case of security dilemmas. One state can be threatened in one sector and decide to react in another sector in order to achieve a state of security, such is the example given regarding the conflict between Turkey and Syria, in which the first state is threatened

through the Kurdish issue and responds through economic measures against the second (Buzan *et al.*, 1998, p. 169).

Extending this conceptual framework to the cyber field, one can make a case that it is possible for a cybersecurity complex to exist separately from the other sectors and, therefore, to prove the individuality of this new sector. Moreover, it could be argued that an entity may use cyber capabilities to promote its objectives, while other means are unavailable or may be seen as too much of a risk. China, for example, has been constantly accused of conducting cyberattacks against Western countries, particularly against the United States and EU member states (European Union Agency for Cybersecurity [ENISA], CERT-EU, 2023) while publicly denying these accusations and blaming the Western side of targeting its infrastructures (AP News, 2023). However, the economic relations between the Chinese side and Western countries have continued to develop, reaching important levels both for the EU (European Parliament, 2023) and the United States (US Trade Representative, 2023). Therefore, one may argue that there is a separate security complex between different Western states and China in the cyber field, which is treated individually from other sectors, such as the economic one. However, this argument lacks a proper background analysis regarding the objectives of the cyberattacks conducted by the Chinese authorities against Western targets and, therefore, cannot draw a conclusion on whether or not these actions were an extension of other sectors, such as the military or the political ones.

Moreover, the same case could be made when discussing about the North Korean cyberattacks and their targets. It has been reported several times (most recently in September 2023) that North Korean hacking groups are targeting traditional partners, such as Russia, aiming to collect strategic intelligence that may support national industrial development (Satter, 2023). There have also been publications that stated that the US intelligence targeted partner countries' officials, such as Germany's Angela Merkel, in espionage operations, most recently with the alleged help of Danish military intelligence (Henley, 2021).

Although it is difficult to understand whether this information is true and what the objectives behind these operations may have been, an argument can be built regarding the possibility for a cybersecurity complex to exist separately from the other five sectors. In February 2022, Russia gained access inside the American company Viasat's satellite infrastructure and rendered inoperable broadband modems mainly used by the Ukrainian military and various government agencies (Steinbrecher, 2022). It should be underlined that, although Russia gained access inside the entire Viasat infrastructure used for communications in different parts of the world, it mainly aimed (although unsuccessfully) to render inoperable the devices used in Ukraine. Therefore, Russia's objective was to both sabotage Ukraine and avoid a cyber conflict with other European partners, proving that there was an assessment regarding a possible separate area of warfare in the cyber sector (Csernatoni and Mavrona, 2022). These examples are useful to demonstrate the existence of strategic goals between some of the existing categories of cyberattacks. The state-sponsored attacks are generally seen through the lenses of attempts to accomplish, or support the accomplishment, of strategic goals. The Russian attack against the Viasat satellite infrastructure or the Chinese cyber operations against European countries are not enough to solely provide strategic gains for the governments. Still, these cyberattacks are part of greater strategies to obtain sensitive intelligence that may later be used to support long-term governmental objectives. A report published by the US Department of Justice, US Department of Homeland Security, and the Cybersecurity and Infrastructure Security Agency (CISA, 2021) on the activity of the Russian group APT29 underlined that the cyberattacks conducted aim to obtain strategic information to serve the interests of the Russian government.

The second element that should be discussed is also based on the constructivist theoretical framework, which states that security is built on the process of elevating different issues to the rank of priorities and, therefore, the sectors will politically continuously fight against each other to achieve greater public importance (if not the greatest) (Buzan *et al.*, 1998, pp. 159–160). Therefore, one could make a case about the existence of a conflict between this so-called cyber sector and other pre-existing sectors, the former having the main objective to be successfully securitised and, inherently, winning the prioritisation contest. If a cyber sector could exist (or already exists), then an analysis should be conducted regarding the competition for resources and prioritisation against the other sectors. It could be argued that the advocates of cybersecurity ask for resources and investments to increase the level of awareness and cybersecurity skills for the general population. A chief information officer (CIO) would normally advocate to the government in favour of investments towards cybersecurity education for the staff of the public administration in order to reduce the success rate of phishing campaigns or to prevent an APT campaign from gaining access inside the network and, therefore, collecting strategic information. Hence, a CIO would usually compete with other ministries for resources and, inherently, for a higher rank in the scale of prioritisation. This competition would be necessary, as the resources for security possessed by an entity (be it a state or a private organisation) are limited and used in relation to perceived threats. If a cyber sector is to be established, the securitising actors would ask for investments to protect the referent objects (mainly IT infrastructures) and, in doing so, would compete for supremacy with the other five sectors. This would create the premises for active competition for resources between the cyber and traditional sectors, established in the process of widening security and, therefore, a process of prioritisation, considering the limited nature of financial resources. Still, it could be discussed (if enough data is found) whether or not this is a sufficiently strong argument to counterbalance the others discussed in the previous section.

The need for allocating resources to the cyber sector should be argued from the constructivist perspective by taking into consideration the necessary competition with the other five sectors. Fundamentally, for the cyber sector to exist, it should be viewed not just as a distinct domain but as an essential pillar that supports each component of security. The central argument for a fair allocation of resources could be built around the idea that success or failure in the cyber domain directly and integrally affects all other sectors. To strengthen this argument, it would be essential that those advocating for resource allocation to the cyber sector be individualised and distinguish themselves from security actors in other sectors.

The above two arguments were brought up mainly as points of discussion, as their strength is not theoretically sufficient to prove the existence of cyber sector. Moreover, one should find further arguments (if any) beside the two presented in this paper in order to prove that the constructivist cyber sector now exists.

Conclusions

This paper engages in an analysis of the ongoing debates surrounding the conceptualisation of a dedicated cyber sector within the Copenhagen School's widening security theoretical framework. The central debate of the paper revolves around an inquiry into whether cyberspace merits recognition as an independent sector or functions as an integral component within the existing sectors.

Therefore, key arguments presented by scholars in favour of a cyber sector were analysed. The existence of institutions and strategies related to cybersecurity was acknowledged,

yet counterarguments pose critical questions regarding whether the importance of cybersecurity alone justifies the establishment of a new constructivist sector. Analogies drawn with other pivotal security concerns, notably counterterrorism, underscore the contention that the importance of an issue does not inherently necessitate a distinct sector.

Moreover, the establishment of institutions and strategic documents, advocated by proponents, was concluded as being insufficient for the establishment of a new sector. It is contended that issues of equal significance, such as terrorism or propaganda, find accommodation within the existing theoretical framework. The analysis extended to the examination of the cyber domain's distinctiveness from the existing sectors. Noteworthy considerations include the role of cyber realm in threatening state legitimacy and internal sovereignty within the political sector, its integral role in securitising referent objects in the military sector, and its impact on norms and values within the societal sector. The economic sector interacts with cyber threats to key public and private industries, while the environmental sector sees cyberattacks conducted by hacktivists in order to advocate environmental ideals. The paper concludes with the assertion that the cyber component has become intricately integrated into the securitisation processes across all five constructivist sectors.

Exploration of potential referent objects, securitising actors, and functional actors for a hypothetical cyber sector reveals challenges in defining distinct actors solely for the cyber domain, as referent objects, functional actors, and securitising actors remain connected with the existing sectors. Moreover, the paper emphasises that major cyber incidents, such as Stuxnet or WannaCry, did not catalyse the securitisation of a new constructivist sector but instead reinforced the existing sectors, such as military or economic security. Finally, the distinctiveness of cybersecurity is underscored by internal vulnerabilities rooted in technical, procedural, and human factors. The imperative for a comprehensive approach is highlighted, emphasising the necessity to address not only external threats but also internal weaknesses, thereby necessitating widespread awareness and preventative measures at both individual and organisational levels. Therefore, it is difficult to pinpoint an external cyber threat, since most of the vulnerabilities exist internally.

The existing literature is predominantly focused on demonstrating the successful securitisation of cyber domain, leaving a gap in security studies regarding the possibility of creating a new sector. The objective of this paper was to try to fill that gap by examining the state of cybersecurity through the lenses of the Copenhagen School's widening security theory.

This paper argued against the existence of a distinct cybersecurity sector in the constructivist segment from the field of international relations. However, it had some important limitations, which are to be acknowledged in this section.

Firstly, the temporal context is important, as the discussion is based on information available up to a certain point in time (i.e. 2023), and the evolving nature of cybersecurity threats could render some analyses outdated or subject to change. Moreover, the text provides a broad theoretical overview, so the depth of analysis on individual cyber incidents or specific cybersecurity strategies is limited. Hence, a more granular examination could provide additional insights.

Furthermore, the discussions primarily focus on examples and perspectives from Western countries, potentially limiting the generalisability of conclusions to a global context. A more diverse set of case studies could enhance the analysis.

The paper also draws heavily on the perspectives of a limited number of experts, as the total number of papers focused on this topic is low. In this sense, there is a potential lack of diversity in viewpoints, which may expose the paper to subjectivity.

The main body of the paper is focused on arguments against the creation of a new sector within the constructivist theory, and that may run the risk of generating subjectivity when choosing the data. However, to provide an unbiased analysis, the paper includes a section entitled "Possible arguments in favour of a new cyber sector."

The arguments brought up in this paper open the path to a set of additional questions that may be addressed for a better understanding of the connection between cybersecurity and the constructivist theoretical framework. In conjunction with this paper, it would be important to analyse how adaptable the Copenhagen School's framework is to the evolving nature of cybersecurity threats, and also to what extent the existing theoretical frameworks adequately capture the nature of cyber threats (including issues such as attribution, anonymity, and non-state actors). Would it be useful for the realm of security studies to expand the constructivist theory?

It would also be important to analyse how different states perceive the role of cyberspace in their national security, and whether there are notable variations in the integration of cybersecurity across the economic, political, and military sectors. Also, if there is a case to be made on cyberspace as a separate sector, what would be the political implications?

Funding
This research received no external funding.
Conflict of Interest
No potential conflict of interest was reported by the author.
Data Availability Statement
Not applicable.

References

Albahar, M. (2019) 'Cyber attacks and terrorism: A twenty-first century conundrum', *Science and Engineering Ethics,* 25(25), pp. 993–1006. doi: 10.1007/s11948-016-9864-0.

Antoniuk, D. (2023) *Suspected Hamas-linked hackers target Israel with new version of SysJoker malware.* Available at: https://therecord.media/updated-sysjoker-backdoor-malware-targets-israel (Accessed: 2 December 2023).

AP News. (2023) *China calls hacking report 'far-fetched' and accuses the US of targeting the cybersecurity industry.* Available at: https://apnews.com/article/china-us-hacking-report-cyberattack-c08a9f52926c8524cf86131324c69fe6 (Accessed: 3 December 2023).

Aydindag, D. (2021) 'Copenhagen school and securitization of cyberspace in Turkey', *La Revista Psicología Educativa*, 9(1), pp. 1–19. doi: 10.20511/pyr2021.v9nSPE1.850.

Azure Network Security Team. (2023) *KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks.* Available at: https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/ (Accessed: 13 January 2024).

Breda, F., Barbosa, H. and Morais, T. (2017) 'Social engineering and cyber security', in *INTED 2017 proceedings,* Valencia, Spain pp. 4204–4211. doi: 10.21125/inted.2017.1008.

Burton, J. and Lain, C. (2020) 'Desecuritising cybersecurity: Towards a societal approach', *Journal of Cyber Policy*, 5, pp. 449–470. doi: 10.1080/23738871.2020.1856903.

Buzan, B. (2019) 'Technology: From the background to opportunity (interview)', in Kaltofen, C., Carr, M. and Acuto, M. (eds.) *Technologies of international relations continuity and change.* Cham: Palgrave Pivot, pp. 115–122.

Buzan, B., Wæver, O. and Wilde, J.D. (1998) *Security: A new framework for analysis*. Colorado: Lynne Rienner Publishers, pp. 168–170.

Cavelty, M.D. (2020) 'Cybersecurity between hypersecuritization and technological routine', in Tikk, E. and Kerttunen, M. (eds.) *Routledge handbook of international cybersecurity.* London: Routledge, pp. 11–22. doi: 10.4324/9781351038904-3.

Cavelty, M.D. and Egloff, F.J. (2021) 'Hyper-securitization, everyday security practice and technification: Cyber-security logics in Switzerland', *Swiss Political Science Review*, 21(1), pp. 139–149. doi: 10.1111/spsr.12433.

Creemers, R. (2017) 'Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century', *Journal of Contemporary China*, 26(103), pp. 85–100.

Crowdstrike (2022) *Hacktivism: Types and examples.* Available at: https://www.crowdstrike.com/cybersecurity-101/hacktivism/ (Accessed: 13 January 2024).

Csernatoni, R. and Mavrona, K. (2022, September) 'The artificial intelligence and cybersecurity nexus: Taking stock of the European Union's approach', *EU Cyber Direct*. Available at: https://carnegieendowment.org/research/2022/09/the-artificial-intelligence-and-cybersecurity-nexus-taking-stock-of-the-european-unions-approach?lang=en&center=europe (Accessed: 3 October 2024).

Cybersecurity and Infrastructure Security Agency (CISA) (2021) *What is Cybersecurity?* Available at: https://www.cisa.gov/news-events/news/what-cybersecurity (Accessed: 30 November 2023).

Czosseck, C., Ottis, R. and Talihärm, A.-M. (2011) 'Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security', *International Journal of Cyber Warfare and Terrorism*, 1(1), pp. 24–34. doi: 10.4018/ijcwt.2011010103.

Dolinec, V. (2011) 'The role of mass media in the securitization process of international terrorism', *Politické Vedy*, 13(2), pp. 8–32.

Eclectic IQ Threat Research Team (2022) *Killnet effectively amplifies Russian narratives but has limited DDoS capabilities.* Available at: https://blog.eclecticiq.com/killnet-effectively-amplifies-russian-narratives-but-has-limited-ddos-capabilities (Accessed: 2 December 2023).

European Parliament (2023) *EU–China trade relations.* Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/753952/EPRS_ATA(2023)753952_EN.pdf (Accessed: 3 December 2023).

European Union Agency for Cybersecurity (ENISA), CERT-EU (2023) *JP-23-01—Sustained activity by specific threat actors.* Available at: https://cert.europa.eu/static/files/TLP-CLEAR-JointPublication-23-01.pdf (Accessed: 3 December 2023).

Fadziso, T., Thaduri, U.R., Dekkati, S. and Ballamudi, V.K.R. (2023) 'Evolution of the cyber security threat: An overview of the scale of cyber threat', *Digitalisation and Sustainability Review,* 3(1), pp. 1–12.

Federal Bureau of Investigation (FBI) (n.d.) *Famous cases & criminals.* Available at: https://www.fbi.gov/history/famous-cases/morris-worm (Accessed: 30 November 2023).

Flashpoint Intel Team (2022) *Conti ransomware: Inside one of the world's most aggressive ransomware groups.* Available at: https://flashpoint.io/blog/history-of-conti-ransomware/ (Accessed: 13 January 2024).

Fouad, N. (2019) *The peculiarities of securitising cyberspace: A multi-actor analysis of the construction of cyber threats in the US (2003–2016).* Coimbra: Academic Conferences and Publishing International.

Fraser, J. (2021) *Response when minutes matter: When good tools are used for (r)evil.* Available at: https://www.crowdstrike.com/blog/how-falcon-complete-thwarted-a-revil-ransomware-attack/ (Accessed: 13 January 2024).

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. and Aylin, P. (2019) 'A retrospective impact analysis of the WannaCry cyberattack on the NHS', *Digital Medicine*, 98, pp. 98–105. doi: 10.1038/s41746-019-0161-6.

Górka, M. (2023) 'Conceptualising securitisation in the field of cyber security policy', *Journal of Modern Science,* 53(4), 263–290. doi: 10.13166/jms/176103.

Han, E. (2013) 'The securitisation of nuclear energy post-September 11 and its impact on ASEAN's nuclear aspirations', *Communication Politics & Culture,* 46(1), pp. 22–38.

Hansen, L. and Nissenbaum, H. (2009) 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly,* 53(4), pp. 1155–1175. doi: 10.1111/j.1468-2478.2009.00572.x.

Helbling, M. and Meierrieks, D. (2022) 'Terrorism and migration: An overview', *British Journal of Political Science,* 52(2), pp. 977–996. doi: 10.1017/S0007123420000587.

Henley, J. (2021) *Denmark helped US spy on Angela Merkel and European allies—Report.* Available at: https://www.theguardian.com/world/2021/may/31/denmark-helped-us-spy-on-angela-merkel-and-european-allies-report (Accessed: 6 December 2023).

Herzog, S. (2011, Summer) 'Revisiting the Estonian cyber attacks: Digital threats and multinational responses', *Journal of Strategic Security*, 4(2), pp. 49–60. doi: 10.5038/1944-0472.4.2.3.

Hultquist, J. (2016) *Sandworm team and the Ukrainian power authority attacks.* Available at: https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team (Accessed: 13 January 2024).

Jajoo, A. (2021) A study on the Morris Worm. arXiv preprint arXiv:2112.07647. doi: 10.48550/arXiv.2112.07647.

Jantunen, S. and Huhtinen, A.-M. (2011) 'American perspectives on cyber and security', *Journal of Information Warfare,* 10(3), pp. 1–15.

Jenkins, L., Atkins, J. and Black, D. (2023) *Backchannel diplomacy: APT29's rapidly evolving diplomatic phishing operations.* Available at: https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing (Accessed: 24 January 2024).

Kamiya, S., Kang, J.-K., Kim, J., Andreas, M., and Stulz René M. (2021) 'Risk management, firm reputation, and the impact of successful cyberattacks on target firms', *Journal of Financial Economics,* 139(3), pp. 719–741. doi: 10.2139/ssrn.3135514.

Karyotis, G. (2007) 'Securitization of Greek terrorism and arrest of the Revolutionary Organization November 17,' *Cooperation and Conflict,* 42(3), pp. 271–293. doi: 10.1177/0010836707079932.

Khan, S. and Madnick, S. (2021) 'Cybersafety: A system-theoretic approach to identify cyber-vulnerabilities & mitigation requirements in industrial control systems', *IEEE Transactions on Dependable and Secure Computing,* 19(5), 3312–3328. doi: 10.1109/TDSC.2021.3093214.

Kim, S. and Lee, H. (2018) 'Software systems at risk: An empirical study of cloned vulnerabilities in practice', *Computers & Security*, pp. 720–736. doi: 10.1016/j.cose.2018.02.007.

Kumar, R., Kela, R., Singh, S. and Trujillo-Rasua, R. (2022) 'APT attacks on industrial control systems: A tale of three incidents', *International Journal of Critical Infrastructure Protection*, 37(C). doi: 10.1016/j.ijcip.2022.100521.

Kyška, R. (2014) 'Hacktivists or cyberterrorists?: Webactivists as political actors', *CIVIS*, pp. 23–38.

Lallie, H.S., Shepherd, L.A., Nurse, Jason R.C., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. (2021) 'Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic', *Science Direct*, 105(1). doi: 10.1016/j.cose.2021.102248.

Lété, B. and Pernik, P. (2017) 'EU–NATO cybersecurity and cefense cooperation: from common threats to common solutions,' German Marshall Fund of the United States. *Security and Defense Policy,* 38, pp. 1–9.

Li, Y. and Liu, Q. (2021) 'A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments', *Energy Reports*, 7, pp. 8176–8186. doi: 10.1016/j.egyr.2021.08.126.

Lobato, L. and Kenkel, K. (2015) 'Discourses of cyberspace securitization in Brazil and in the United States', *Revista Brasileira de Política Internacional*, 58(2), pp. 61–76. doi: 10.1590/0034-7329201500202.

Meeuwisse, R. (2017) *Cybersecurity for beginners.* Hythe, Kent: Cyber Simplicity.

MITRE (2017) *Sandworm team.* Available at: https://attack.mitre.org/groups/G0034/ (Accessed: 13 January 2024).

Necsutu, M. (2023) *Moldova to create 'anti-propaganda centre' to counter Russian disinformation.* Available at: https://balkaninsight.com/2023/05/29/moldova-to-create-anti-propaganda-centre-to-counter-russian-disinformation/ (Accessed: 2 December 2023).

Olszewski, B. (2018) 'Advanced persistent threats as a manifestation of states' military activity in cyber space', *Scientific Journal of the Military University of Land Forces*, 50(3), pp. 57–71. doi: 10.5604/01.3001.0012.6227.

Oshewolo, S. and Nwozor, A. (2020) 'COVID-19: Projecting the national security dimensions of pandemics', *Strategic Analysis,* 44(3), pp. 269–275. doi: 10.1080/09700161.2020.1767911.

Phillips, L. (2010) *Hackers shut down EU carbon-trading website.* Available at: https://www.theguardian.com/environment/2010/jul/26/eu-carbon-trading-website-hacked (Accessed: 2 December 2023).

Plan, F., Fraser, N., O'leary, J., Cannon, V., Read, B. (2019) *APT40: Examining a China-nexus espionage actor.* Available at: https://www.mandiant.com/resources/blog/apt40-examining-a-china-nexus-espionage-actor (Accessed: 13 January 2024).

Plėta, T., Tvaronavičienė, M., Casa, S.D. and Agafonov, K. (2020) 'Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases', *Insights into Regional Development*, 2(3), pp. 703–715. doi: 10.9770/IRD.2020.2.3(7).

Proska, K., Wolfram, J., Wilson, J., Black, D., Lunden, K., Zafra, D.K., Brubaker, N., Mclellan, T. and Sistrunk, C. (2023) *Sandworm disrupts power in Ukraine using a novel attack against operational technology.* Available at: https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology (Accessed: 13 January 2024).

Santaniello, M. (2022) 'Towards a democratic model of cybersecurity', in Granata, P. and Sidoti, F. (eds.) *Financial intelligence and economic security*. Padova: Linea Edizioni, pp. 117–128.

Satter, R. (2023) *North Korea hackers going after Russian targets, Microsoft says.* Available at: https://www.reuters.com/technology/north-korea-hackers-going-after-russian-targets-microsoft-says-2023-09-07/ (Accessed: 6 December 2023).

Shea, J. (2017) 'How is NATO meeting the challenge of cyberspace?', *Journal of Information Warfare,* 7(2), pp. 18–29 .

Shults, I. (2021) *Information warfare in the digital age—Propaganda, cyberattacks and the protection of democratic institutions*. Quantico, VI: Peace and Prosperity Institute.

Steinbrecher, D. (2022) *Viasat KA-SAT attack.* Available at: https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022) (Accessed: 6 December 2023).

The Cyber Express. (2023) *KillNet hackers group strikes Ukrainian gas stations in cyber attack.* Available at: https://thecyberexpress.com/gas-station-cyber-attacks/ (Accessed: 2 December 2023).

Thomas, R.J., Chothia, T. (2020). Learning from Vulnerabilities - Categorising, Understanding and Detecting Weaknesses in Industrial Control Systems. In: Katsikas, S., et al. Computer Security. CyberICPS SECPRE ADIoT 2020 2020 2020. Lecture Notes in Computer Science(), vol 12501. Springer, Cham. doi: 10.1007/978-3-030-64330-0_7

Thumfart, J. (2022) 'The (il)legitimacy of cybersecurity'. *Applied Cybersecurity & Internet Governance,* 1(1), pp. 97–120. doi: 10.5604/01.3001.0016.1093.

Trend Micro Research (2021) *What we know about the darkside ransomware and the us pipeline attack.* Available at: https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html (Accessed: 13 January 2024).

US Trade Representative (2023) *The People's Republic of China—China trade & investment summary.* Available at: https://ustr.gov/countries-regions/china-mongolia-taiwan/peoples-republic-china (Accessed: 3 December 2023).

Vicens, A. (2022) *Hacking group focused on Central America dumps 10 terabytes of military emails, files.* Available at: https://cyberscoop.com/central-american-hacking-group-releases-emails/ (Accessed: 2 December 2023).

Wang, X., Xiong, M., Luo, Y., Li, N., Jiang, Z. and Xiong, Z. (2021) 'Joint learning for document-level threat intelligence relation extraction and coreference resolution based on GCN', in *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom)*, Guangzhou, China. New York, NY: IEEE, pp. 584–591. doi: 10.1109/TrustCom50675.2020.00083.

Warren, M., Štitilis, D. and Laurinaitis, M. (2023) 'The impact of Russian cyber attackers within the Ukraine situation'. *Journal of Information Warfare*, 22(1), pp. 88–106.

Whelan, C., Bright, D. and Martin, J. (2023) 'Reconceptualising organised (cyber)crime: The case of ransomware'. *Journal of Criminology*, 57(1), pp. 45–61. doi: 10.1177/26338076231199793.

Yunos, Z., Mohd, N., Ariffin, A. and Ahmad, R. (2017) 'Understanding cyber terrorism from motivational perspectives: A qualitative data analysis', *Journal of Information Warfare*, 16(4), pp. 550–557.