LUND UNIVERSITY • CENTRE FOR EAST AND SOUTH-EAST ASIAN STUDIES

A Japanese perspective of the China threat in cyberspace

Author: Giulia Saccone
Supervisor: John Hennessey

Master's Programme in Asian Studies

Spring semester 2024

Abstract

In the last two decades, Japan has articulated a more proactive cybersecurity posture amid the increasing sophistication of cyberattacks and the relevance of technology for society. Those initiatives revolve especially around the response against China's grey zone activities, which are not exclusive to cyberspace, and emerge as a result of issues in other domains. However, Japan has never directly attributed the threat label to China due to the complex relationship between the two countries.

This research has analyzed the securitization moves employed by Japan in its Defense White Papers from 2019 to 2023 through the transversal securitization theory applied to content analysis. Findings indicated a strategy based on the classical interests of middle powers that securitizes a major actor, employing motives related to the latest evolution of technologies applied to cyberspace. The results also showed a tendency to use explicit threat markers when the White Papers employ the words of allies: a strategy that adds a further level of indirectness while not sacrificing the threatening effect. Moreover, in the later White Papers, it was possible to observe a broadening of the roster of third actors and typologies of cyberattacks mentioned, demonstrating an increasing cyber maturity and reflecting Japan's diplomatic results.

Keywords: Sino-Japanese relations; Japan; China; Japan cybersecurity; Cyber policy; Securitization; Copenhagen School; Security studies

Acknowledgments

My gratitude goes to Lund and Keio University for the two years full of an enriching academic environment. The knowledge and opportunities I gained here have been invaluable in shaping my research and personal growth. A deeper sense of thankfulness goes to my classmates of the MA thesis in Asian Studies, from whom I had the opportunity to learn, feel inspired and lean on in two foreign countries, amid communal challenges.

My heartwarming thanks go to my grandparents and my mother, the first reasons why I am here and why I will keep going, finding my way, getting used and learning to navigate those *interesting times*. Thank you again for your unconditional support and love.

I would like to express my most sincere gratitude to Flavio Storino, my partner and Jordan Everetts, my best friend, without you I think I would still be stuck fighting against my fear of confirmation bias, and probably this thesis would be full of obscure English words and inaccessible periphrases. Having a person with whom I can share fraternal affection and another one with whom I am not afraid to face the future is one of the greatest fortunes that a person can have. Lastly, I would like to extend my sincere thanks to Dr. Morreau for making me stick to the plan.

Index

1 Introduction....6
1.1 Context and Problem Statement....6
1.2 Research question, thesis aims and structure....9
2 Literature review....11
2.1 Securitization theory and its relative evolution....12
2.2 Securitization of cyberthreats....13
2.3 Evolution of the contemporary sino-japanese relations from the Second Abe tenure (2012-2020) to the Kishida premiership (2021-PRESENT)....15
2.4 Japan's cybersecurity evolution....17
2.5 China's internet policy and Japan's perception....18
2.6 Positionality statement....21
3 Theoretical framework....22
3.1 The constructivist approach to cybersecurity....22
3.2 The transversal securitization theory....23
3.3 Limits of the realist and liberalist school....26
4 Methodology....28
4.1 Audit trail....29
5 Presentation and analysis of data....31
5.1 White Papers....31
5.2 Analysis....33
5.2.1 Securitization of the Cyber domain....33
5.2.2 Cyberattacks conducted by China....35
5.2.3 Linkage with other issues....38
5.2.4 Information and Cognitive Warfare....41
5.2.5 China's Tech policy....43

4.3 Concluding Remarks 44
6 Conclusions 48
References 50
Appendices 59
Codebook I 59
Codebook II 62
Distribution of the codes throughout the years 66
Query criteria 67

1 Introduction

1.1 Context and Problem Statement

The increasing symbiosis between the physical and cyber dimensions has amplified the effects of cyberattacks, which nowadays are becoming more sophisticated and frequent due to the increasing global frictions. For this reason, the 2021 National Cybersecurity Strategy of Japan demanded the adoption of active cyber defense, which implementation plan has been presented in the 2022 National Security Strategy (NSS) (NISC, 2021; Osawa, 2023c). This tactic entails the capacity to intercept, analyze, and simultaneously use legitimate countermeasures to mitigate a network security breach to redirect the attack to a secure server or to unharmful files used as bait (Osawa, 2023a). The initiative was accompanied by an enhancement of the National Center for Incident Readiness and Strategy for Cybersecurity (NISC) aimed to upgrade it to a cyber policy coordination institution with supervision powers on the cyber units of the Japan Self-defense Forces (JSDF) with an expansion of its relative units (Osawa, 2023b). Following, in June 2024, the Government started the discussion to submit the necessary amendments to the existing regulations in contradiction with this initiative – namely the Telecommunications Business Law, the Act on the Prohibition of Unauthorized Computer Access, and the Penal Code – to submit it to the following Diet session in September 2024 (Osawa, 2023c; The Japan News, 2024; The Japan Times, 2024).

Indeed, in the last decade, Japan has focused its endeavors on cyberspace to curb the increasing state-sponsored espionage campaigns (i.e. the advanced persistent threats or ATPs) perpetrated by Beijing. The APT campaigns were generally aimed to steal sensitive information related to the industrial and trade sectors in light of industrial enhancement plans, such as the Made in China 2025, and the civil-military fusion (CMF): the application of dual technologies developed in the civilian field in the warfare equipment (Osawa, 2023c; Zenglein and Holsman, 2019; Van Wie Davis, 2021). The repeated cyberattacks have also increased the concern of public opinion regarding the phenomenon, as demonstrated by a poll conducted by the Cabinet Office, where 52% of Japanese people allocated cybercrime as the second highest concern, and among this sample, 41% of them demanded a higher proactiveness of the authorities against internet crimes – e.g. unauthorized access and phishing scams (Vosse, 2024).

Japan's counteractions were based on deterrence by denial – i.e. the creation of barriers to disincentivize cyberattacks (Van Wie Davis, 2021) – and to intensively collaborate with the

US in the domain, while expanding its network of partners with the Free and Open Indo-Pacific (FOIP) vision, which also functioned as a structure for an intensive cyber capacity building (CCB) activity in the ASEAN area (Malachinski, 2023; Ukhanova, 2022; Vosse 2024). Additionally, as a reaction to the APT campaigns, the Kishida tenure in 2021 finally institutionalized the concept of economic security with the Act on the Promotion of Ensuring National Security Through Integrated Implementation of Economic Measures Economic Security Promotion Act (i.e. Economic Security Promotion Act).

In the provision, cybersecurity is seen as a key factor for ensuring a critical supply of critical commodities and protecting the innovation of cutting-edge or dual technology from property theft (Osawa, 2023c), indeed it is not a coincidence that the strategy focuses on the protection of the most vulnerable sectors, namely: the manufacturing, aerospace, and automotive, usually targeted by hackers with illicit exfiltration of intellectual property intention (Cyfirma, 2023).

In the same year, the NISC also published the current cybersecurity strategy, where – on contrary to the 2018 one – China was addressed openly as an alleged perpetrator of cyber espionage and as an actor pursuing cyberattacks to change the status quo with grey-zone situations. In the following year the 2022 NSS not only created the necessity of developing Japan's cybersecurity with active cyber defense, but it also showed Japan's development of the contemporary cyber threat landscape, with the inclusion of information warfare as a reaction to Russia's strategy in Ukraine, which has been used by the Japanese government as a parallelism with China's activities in Taiwan and the South China Sea (O'Shea and Maslow, 2024). The 2022 NSS revision is indicative not only of Japan's protection of economic security and other cybersecurity objectives but also of its perception of the contemporary cyber threats landscape: as abovestated the document is also aimed to combat information warfare in the light of Russia's strategy in Ukraine. The event has been used as an effective parallel for the crisis in the Taiwan Strait caused by China (O'Shea and Maslow, 2024), and information warfare is an extensive practice perpetrated by both actors. It is necessary to specify, although, that the Russian and Chinese techniques differ: the former is perpetrating a strategy characterized by propaganda aimed at creating unrest, eroding the adversary morale through fake social media accounts run by the intelligence or third-party contractors, who aim to grow their engagement in their target community also through interactions with real influencers aimed to amplify their contents. The latter prefers a strategy based on an

overwhelming quantity of content to foster a pro-China narrative as a support of its strategical interests in the targeted geographical areas with content farms, fake accounts active in not only Western audience-dominated platforms like X and Facebook but also WeChat, which is highly used by Japanese people (Direstra et. Al 2020).

Regardless, both countries aim to undermine the democratic regimes of the adversaries, taking advantage of the high degree of connectivity among diverse actors that the liberal use of the internet can offer (Paterson and Hanley, 2020). Cyberespionage assists this scope with phishing and malware aimed to extract precise information on the targets of the information warfare, to foster a more effective narrative as observed in the Russian interference in the 2016 US elections (Paterson and Hanley, 2020).

This evolution in cyber policy is the umpteenth symptom of a shift in the complex SinoJapanese landscape. The academia has already noticed a departure from the policy of engagement through liberal deterrence (Ueki, 2020; Sahashi, 2020; Huges, 2016) to a strategical competition followed by opposition at the rhetorical level based on the values fostered at the international level in the second Abe administration (2012-2020) (Goodman, 2022). The contraposition in cyberspace is expressed at the general level with Japan's promotion of multistakeholder cyber governance, where actors voluntarily abide by non-legally binding rules based on a transposition of the current international law in cyberspace; contrasted by China's authoritarian model, where the state protects the national social harmony from social interference and applies the rule of law in cyberspace under the principle of Internet Sovereignty (Mirza, 2020).

According to this evolution, an individual may expect a characterization of China by Japan as a:

- 'Key security issue/problem'
- 'Risk'
- 'Serious/grave threat'
- 'Unprecedented/imminent threat'
- Matter affecting 'fundamental/indispensable domain'

These are the threat markers observed by Oren and Bummer (2020) and indicative of what the Copenhagen School describes as securitization: the process of creation of a threat demanding extraordinary measures to induce the audience to endorse those measures due to the feeling of menace to national security (Buzan, Wæver and de Wilde, 1998).

The theory has been developed to understand why certain types of issues become security problems, and under which circumstances this phenomenon takes place (Balzacq 2011).

However, after a careful reading of the sections regarding the Chinese activities in cyberspace, China is always described as a "challenge" "serious concern" or "problem", despite the depiction of Beijing as a threat to Tokyo by scholars and journalists. This phenomenon is not limited to the field of cyberspace, but as Dell'Era (2024) notices, is recurrent also in the context of maritime disputes in official documents with a particular type of threat-building process, named by the author as transversal securitization.

1.2 Research question, thesis aims and structure

This coexistence of cyberattacks motivated by industrial and intelligence reasons, the delicate economic interdependence and geographical proximity distinguish China from the other countries that target Japan in cyberspace – i.e. North Korea and Russia – and that Japan itself has been constantly put China under the category of threats in the cyberspace in its Defense White Papers. Therefore, against these considerations, this research will follow the consequential research question:

- How has Japan transversely securitized China in cyberspace in these last five years?

And to provide an analytical answer, the following sub-research questions will be pursued:

- Which are the most mentioned cyberattacks throughout this period?
- What were the issues related to their representation?
- Which cyber policies advanced by China does Japan perceive as the most threatening?

Considering that the White Papers operate a selection of all the cyberattacks that happened in a year not only in Japan, but also at the expense of third parties, helps us to understand the securitization choices of the Japanese government. At the same time, observing which policies are frequently nominated allows us to understand the variation of Japan's priority in terms of policies and another dimension of the China threat in cyberspace from 2019 to 2023. This thesis will focus specifically on the securitization moves and their thematical variations. However, the adoption of a constructivist base implies a non-distinction between objective

and subjective threats. In this thesis, cyberspace is conceptualized as the integration of software, data, user activities, hardware and critical infrastructures, hence topics such as information warfare with traditional media and spokespeople, or its integration in multidomain operations are not discussed.

The research questions will be answered with a content analysis of Japan's Defense White Papers from 2019 to 2023 to find the recurring themes that characterize the China threat in this domain. The process will follow an indicative and deductive manner: with the first codes deducted from the literature review, and the following induced by the content analysis. The codes will then be analyzed qualitatively and quantitatively to observe the trends in the last five years.

The theoretical frame that will guide the research is the theory of transversal securitization developed by Dell'Era (2024): the author develops further the securitization theory through the analysis of the securitization techniques used by Japan against China in the maritime domain: Japan has never framed China directly as a threat, but only its behaviors. On these occasions, direct references to Beijing were avoided or it was rather downplayed as a challenge. Therefore, this research transposes the transversal securitization theory to the cyber domain aiming to propose a typical case study, following a longitudinal approach to corroborate how China has been increasingly becoming a threat in the last five years and to observe how its attributes have been changing according to the emergence of new technologies and issues.

The evolution of the securitization theory has moved away from the strict definition of a discourse and over forms of securitization, which however have not been applied to the China threat in cyberspace (Dell'Era, 2022; Balzacq, 2011; Eroukhamnoff, 2018; Moore, 2020). Furthermore, the recent literature on contemporary Sino-Japanese relations has focused on the security development understood in a broader scope (O'Shea and Maslow, 2024; Hengibotham, Leiter and Samuels, 2022) or preferred to explore specific case studies as the contraposition of the BRI and FOIP digital connectivity plans (Moore, 2020) or on the Huawei case (Lee, Han and Zhou, 2022), often giving the threat of China for granted and just presenting focal moments of the relationship without allocating them in a broader time flow.

Therefore this research is pursued to analyze Japan's securitization moves against China in cyberspace to understand how this threat has been articulated in the last five years throughout its Defense White Papers, and as an exploration of the transversal securitization theory

applied to a different domain and with a different method and to the literature on the development of Sino-Japanese relations, with a particular focus on cyberspace, a domain that does not only impact on the traditional security domains – e.g. through multi-domain operations – but also the economic one and the civil dimension.

Moreover, the study of the evolution of the interaction between those state actors in such contested domains, which are respectively the second and fourth largest economies in the world and both located in the East Asia region, contributes to the development of the field of Asian Studies, deepening the understanding of the recent dynamics in the region in a domain where other regional actors are focusing their endeavors, in particular for economic growth (Kasih, 2023).

The thesis will pursue the following order: after having deduced the major themes brought up by the academia regarding China in cyberspace and identified the research gap in which the thesis inserts itself through the literature review, in the following chapter, the research will present the transversal approach to securitization in light of the evolutions of the Copenhagen School. Subsequently, there will be an illustration of the data chosen for the analysis and the process conducted to select the content that will be analyzed in light of the theoretical framework, which will be followed by the conclusions illustrated in the last part.

2 Literature review

This chapter aims to present the academic gap in which this research is positioned and hence aims to contribute. The gap is formed by an intersection of the existing literature on securitization applied to cybersecurity, and the contemporary Sino-Japanese relations, encompassing the chosen period (2019-2023) on cyberspace. The chapter also serves as a source of the recurring themes, operationalized as initial codes for the content analysis illustrated in the Appendices to answer the main question of this thesis, namely how Japan securitizes China, and its sub-questions regarding the most threatening policies advanced by the latter, the most frequent represented typology of cyberattacks and the contemporary issues bound to the securitization moves. For this reason, particular attention has been paid to the trends in each sub-section.

Therefore, the chapter proceeds in the following order: the first section is used to present the evolution of the securitization theory driven by the research provided to overcome its limits and its relative application to the cyber domain. Then, the Sino-Japanese relations during the timeframe are contextualized, along with the relative evolution of Japan's cybersecurity and its threat perception amid China's internet policy.

2.1 Securitization theory and its relative evolution

This section is instrumental in understanding the underlying theoretical framework of this research. In fact, the Copenhagen School of Securitization was developed in the post-Cold War epistemological debate on security studies as a theoretical framework for the structural and processual analysis of the concept of security (Stritzel, 2014). Therefore, the following evolutions have to be addressed to illustrate the gaps that have been filled, making the doctrine more applicable to the fields of cybersecurity and content analysis.

The initial approach is exemplified by Wæver's (1995) declaration: "*Something is a security problem when the elites declare it so*", which allows an understanding of security as a political construction elaborated by one or more actors and determined by the historical and sociopolitical context (Wæver, 2008).

More precisely, Buzan, Wæver and De Wilde in their "*Security – a new framework for analysis"* (1997) illustrate the process of securitization, namely when threats become so: it requires a preliminary identification of a referent object – i.e. the threat – by the enunciator, who has to articulate the existence of the threat through a discourse – i.e. the securitizing move – where the characteristics, the rationale, and the implications of a threat are thus presented. This act is aimed at dissuading the audience (which could be the public opinion or a selected social group, such as legislators) to create an intersubjective understanding of this threat.

The authors pose a caveat: the ultimate scope of the securitizing process is the acceptance by the audience that the referent object in question is a threat, demonstrated by the creation of a platform of discussion, to which an endorsement of extraordinary measures may follow. Furthermore, a securitizing act is necessary but not sufficient for the securitization to take place, but it is its determinant initiator. The caveat opens two gaps: the method to understand how a selected audience creates a debate is not provided, and there is also the presumption

that the securitization process happens in liberal democracies, however, even if this limit does not concern this thesis, it is necessary to report that the research has demonstrated that this practice has taken place in countries with different regimes (Vuori, 2008; Grančayová, 2021; Balzacq, 2011; Kam and Clarke, 2021) as a response to the initial eurocentrism of the framework.

Another limit of the first generation of the Copenhagen School has been the lack of reflection on problems of empirical application, which has generated a consistent number of contextual approaches to the securitization theory (Dell'Era, 2022; Balzaq, 2011; Stritzel, 2014; Eroukhmanoff, 2018; Moore, 2020; Van Wie Davis, 2022), which have brought a reconsideration of the language employed by the enunciators. Indeed, Eroukhamanoff (2018) challenges the assumption that securitization should happen with a direct labeling of the referent object as a threat. The author highlights the covert securitization of the Muslim community by the US presidents, which has enabled the audience to accept policies such as the War on Terror in 2001 and the Muslim Ban in 2017. In fact, indirect speech has been regarded as a move to preserve the reputation and diplomatic relations of the enunciator, and at the same time as an effective habitus aimed at persuading the audience and making them feel more at ease in endorsing the securitizing move.

Likewise, Dell'Era (2022) argues against the mainstream overt representation of the threat and challenges the assumption of Japan's threat perception of China (e.g. Govella 2020). The analysis demonstrates how Japan has cultivated the image of China as a maritime threat through the securitization of the domain, as developed in the following chapter. This research demonstrates the necessity of a context-based application of securitization theory to fill the gaps left by Buzan, Wæver and De Wilde (1997). Moreover, it corroborates the position of authors who, investigating Japan's Huawei ban and the contraposition between the FOIP and the BRI, have shown how Japan has not challenged China directly (Malachinski, 2023; Moore 2020, Lee, Han and Zhou, 2022; Kowlikoski and Hall, 2021), hence leaving room to an application of the theory in cyberspace, another contested domain.

2.2 Securitization of cyberthreats

The academia has also tried to apply the framework on cyberspace, addressing the gaps left by the Copenhagen School and innovating the analytical framework.

Dunn Cavelty's work "*From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse*" (2013) closely examines the characteristics

attributed by non-state actors to threats in cyberspace, contributing to analyzing the visible discursive practices at the state level, where a strong influence from the military sector emerges, as corroborated in the Japanese context by Ukhanova (2022), Jiang (2023), Govella (2020), O'Shea and Maslow (2024), and characterized by a major emphasis on critical infrastructure control and territoriality. Furthermore, it corroborates the choice of the Defense White Paper as an analytical unit for this thesis.

The increasing militarization of cyberspace is also reported by the author in "*Cybersecurity between hypersecuritization and technological routine*" (2020) and it is used as a point of departure by Thumfart (2022) to further contribute to aiding the gaps left by the Copenhagen School regarding the analysis of securitizing speech acts in *stricto sensu*, which would exclude cybersecurity from its range of analysis due to the high technicality and synthetic style that characterize the field. Therefore, he interprets the securitizing moves on the concept of discourse as a meta-linguistic process.

Another gap highlighted by Thumfart (2022) is the lack of conceptualization of objective threats. This is partially compensated by Lupovici (2021), who in "*The dual-use security dilemma and the social construction of Insecurity"* conjugates the constructivist securitization theory with the realist security dilemma, expanding its application to nontraditional domains, proving how the security dilemma (the doubt of an actor to improve their coercive capabilities amid the build-up of the adversary) is exacerbated by the subject's knowledge and social understanding of the technologies adopted by the adversary, all mediated by international norms and the knowledge mediated by socio-scientific actors. This insecurity escalates in a securitization process, resulting in a spiral of mutual development of the respective technological capabilities.

The securitizing actor sees the adversary's dual technology as a strategic threat or an innovation gap, a strategic advantage in terms of security and economy, or as a challenge to the counterpart's dominance and prestige. In the case of the Huawei ban, China was perceived by the US as a challenger to its technological hegemony, and the company provided a technology for engaging in the same surveillance that the US is known for engaging with. Lupovici also regards that the delay in the ban by the allies is grounded in a different intensity in the perception of China as an existential threat, hence a generalization that does not consider the context of the securitizing actors.

Lee (2023) further contributes to the field illustrating the different characteristics of securitizing moves in cybersecurity based on the circumstance, the audience and the timing.

From this analysis it emerges that the degree of information disclosure, the medium used for the statement, and the time difference from the incident to the attribution varies depending on the channel used: technical, criminal, official or unofficial policy. Moreover, the details disclosed in the attribution are the result of a tradeoff among scope, the geopolitical context, and the target audience, providing a rationale for the few details in the attribution statements for the international audience by Japan noted by Soesanto (2020). Furthermore, Lee provides another further explanation to Soesanto's (2020) analysis noticing how actors' support of a cyberattack attribution statement can shape the normative environment of cyber operations. Moreover, the author, citing Haely and Jervis (2020), argues that in periods without a major crisis, or in the case when both parties seek to prevent further escalations public attribution may function as a "pressure release valve", similar to the state of Sino-Japanese relations according to Aoyama (2023).

2.3 Evolution of the contemporary Sino-Japanese relations from the Second Abe tenure (2012-2020) to the Kishida premiership (2021-PRESENT)

The contextualization of the Sino-Japanese relations both outside and inside cyberspace provides the context to the analysis of the Chinese cyber policies and contemporary issues, presented in the White Papers with a concise register while demonstrating the increasing militarization – and securitization – of Japan's cyberspace. Furthermore, the case studies of the Huawei ban and the BRI/FOIP competition have been presented in this section both as corroboration of Dell'Era's framework and to provide further context for the thesis itself. It has to be pointed out that the review encompasses analyses adopting different frameworks to provide a better understanding of the context. Additionally, the discussion of the China internet policy is focused on Japan's threat perception to circumscribe the focus to the research questions.

Regarding Sino-Japanese relations, it is evident through an analysis of diachronic studies that Japan is pursuing a strategic ambivalence aimed at becoming more independent amid the US-China competition and the light of a fear of abandonment by the US. Hence, we can observe a slow weakening of the economic relationship between Japan and China started by the Abe administration, and an erosion of the separation between the political and economic relations that has been guiding the Sino-Japanese relations since their normalization in 1973

(Ueki, 2020; Sahashi, 2020; Huges, 2016; Goodman, 2022; Bhubhindar, 2024; Miao, 2021). More recently, as Bhubhindar (2024) shows, the Kishida administration has shown a major commitment to the classical stances of a middle power, and consequentially, emphasizing its contraposition with the Chinese behavior.

In fact, Japan has upheld a rhetoric based on the promotion of already established norms and values aimed at maintaining the status quo to preempt great powers from inference through a cage of rules, institutions, and accountability and, at the same time, prevent the rise of alternative great powers that could undermine middle power interests (Kavalski, 2014; Hatakeyama, 2019).

However, both Miao's (2021) and Bubhindar's (2024) works focus more on the security aspects, suggesting a sharper shift in this field, compared to the economic one. Instead, Aoyama (2023) focuses comprehensively on the situation and grounds her claims on the strategic triangle theory: the Sino-Japanese relationship remains steady despite becoming progressively fragile since the intensification of the Japan-US cooperation to balance China, but due to the latter's asymmetrical threat perception – for which the US constitutes a greater threat than Japan – China does not respond to Japan's assertive stances on its strategical core interests as vigorously as to the US ones.

On top of that, Aoyama (2023), Goodman (2022), and Miao (2021), adopting an incrementalist approach, highlight that Japan cannot adopt a sharp negative stance against China due to the strong economic bonds between Japanese and Chinese companies.

Contrarily, O'Shea and Maslow (2024), while analyzing the major commitment of Japan to international defense, argue that the 2022 Russian full-scale invasion of Ukraine served as a moment of punctuated deterrence that has been securitized to create popular consensus and to focus the policy-making in bolstering Japan's security posture to contain China in the region, amid the threat posed by Beijing in the South and East China Seas and the Taiwan Strait. The same position is supported by Henginbotham, Leiter and Samuels (2022), who with the analog theory of the window of opportunity have interpreted the 2022 Russian invasion as an occasion to address the fear of abandonment by the US deepening their collaboration and show an open commitment to the stability of Taiwan.

Moreover, their research offers a deeper analysis of Japan's posture, with particular regard to the new domains for conflict and its shortcomings in policy-making that prevent Tokyo from taking full advantage of those new areas to balance China in the region. Their analysis

of the cyber domain shows a reinforcement of the cyber warfare section, with the establishment of the Cyber Defense command, and its expansion to 4000 units of personnel expected in 2027, coupled with a regularization of cyber defense arrangements as a whole-of government approach in pursuit of an improvement of the cross-domain operations. Therefore the authors, while using a different framework, highlight the pattern of securitization engaged by Japan.

2.4 Japan's cybersecurity evolution

Soeasanto's (2020) hotspot analysis of the Chinese cyberattacks against Japan from 2011 to 2019 offers an optimal chronology of the most important state-sponsored attack of China against Japan, an evaluation of their respective cybersecurity policies and a consideration of the effects of these attacks from a more technical point of view. Noteworthy is the Tick group's Japan-specific attack vector and APT10's cyber espionage in Japan and 16 other countries. Moreover, the author attributes the repeated cyberattacks to the Government's choice to ban Huawei in 2019 as a securitizing move and he recognizes the increasing joint US-Japan initiatives and declarations on cyberspace as an effort to respond to those cyberattacks, hence a further securitization of the domain.

The author provides useful observations regarding public attribution statements noticing the scarcity of technical information on Japan-specific attacks, leading to lower global cybersecurity prioritization before 2019. Furthermore, Soeasanto's work is instrumental in excluding cases of hacktivism in the chosen timeframe, since he observes a decrease in attacks occurring on the 18th of September, the anniversary of the Mukden incident.

The significance of the APT10 attack is reported also by Ukhanova (2022), who through a document analysis uses this attack as the exemplification of the consolidated Chinese practices of conducting state-sponsored cyber espionage and demonstrating an increasing reinforcement of its defensive cyber capabilities, in trend to Dunn Cavelty's (2020) and Thumfart (2022) research. China is also posed as a "common enemy" for easing the issue of the US-Japan alliance burden sharing in cyberspace.

Moreover, the author regards that Japan has not been relying on the normative aspects of the internet to develop its policy, rather it has been focusing on technical advancements to reinforce its cyber defense in order to protect the science and technology progress achieved, entering hence in a virtuous circle.

On the contrary, this behavior is perceived as counterproductive by Govella (2022), who analyzes the evolution of Japan's policy in contested commons after WWII. The author, as the abovementioned ones, highlights the increasing frequency of cyberspace with security, and correlates the evolution of the current cyber policy with the capacity-building (CCB) initiatives with third countries that share concerns regarding China, North Korea and Russia, and promoting dual-use technologies with defensive purposes.

The attacks perpetrated by these actors are regarded by Bartlett (2020) as one of the main driving forces for the "*exclusively defense-oriented policy*" based on deterrence by denial. The breaches are a demonstration of the development of offensive cyber capabilities by other regional actors, which thus represents a threat to national security, paired with the increasing reliance of the country on ICT technologies, and the legal constraints posed by the general defense-oriented policy constitute the causes of this approach.

In fact, as Osawa demonstrates in his policy paper "*Direction of Japan's New Cybersecurity Policy*" (2023a) and in his commentary "*How Japan Is Modernizing Its Cybersecurity Policy*" (2023b), what has prevented Japan from assuming an active cyber defense are the substantial legislative barriers contained in specific and primary legislative resources. In his works, he also shows consistency with the research produced regarding Sino-Japanese relations that perceives the 2021 Russian invasion as the window of opportunity for Japan to restructure its defense policy (O'Shea and Maslow 2024, Leiter and Samuels 2022). In particular, the hybrid conflict conducted by Russia has pushed Japan to try adopting an active cyber defense to prevent state-sponsored cyber espionage and cyber sabotage or denial of services aimed at paralyzing critical infrastructures. Those attacks have a further impact on the economic security of Japan, due to their unfair and forced transfer of technology, especially in the warfare sector, as demonstrated by China which has been increasingly committing cyber espionage towards Japan since 2016 through at least 10 state-sponsored groups as claimed also by Soeasanto (2020), Goodman (2020) and Moore (2022).

2.5 China's internet policy and Japan's perception

The literature regarding Japan's cybersecurity policy individuates the state-sponsored attacks as the major source of threats posed by China due to their impact on Japan's economic security (Bartlett, 2020; Ukanova, 2022; Osawa, 2023c). Those attacks are part of what Wan Wie Davis (2021) and Kello (2021) define respectively *shadow war* and *unpeace*: a state of

mid-spectrum rivalry where an actor deploys cumulative cyberattacks also relying on private contractors to conduct actions that fall below the threshold of conflict, in virtue of disrupting the opponent day-to-day governance. This is enabled by the lack of an international legal consensus and a blind application of the *ius ad bellum* to cyberspace, allowing authoritarian states to exploit its ambiguities (Kello, 2021; Kono, 2017).

Those acts of cyberespionage are part of a strategy to obtain know-how developed by foreign companies for the Made in China 2025 policy, which aims to foster the competitivity and self-sufficiency of indigenous companies of high-tech industries, with particular regard to the ones focusing on the development of dual-technologies (i.e. technologies with civil and military application), with a consequential alignment of the objectives of the industry to the national ones, as Zenglein and Holzmann (2019) report in their policy paper.

Due to the nature of their work, the policies are not analyzed through a particular framework, but it is useful to understand the scope of cyberespionage and how Made in China 2025 is part of a chain of policies for industrial and military development: the enhancement of dual-use technology and cybersecurity industries contribute to the Civil-military fusion (CMF), which entails the integration of AI, IoT, 5G and other cutting-edge technologies. These are in turn applied to intelligentized warfare, an integrated multi-domain strategy that employs AI-assisted weaponry, equipment, and methods (Cheung, 2019; Yatsuka, 2020; Can and Veira, 2022).

China is also active in the debate regarding the international standards of cyber governance, where it fosters its indigenous concept of internet sovereignty, which Mirza (2021) presents as the consideration of the internet as a national domain, where the state applies the rule of law, grants social harmony, hence freedom from external interferences.

On the international level, each state is an equal participant in the normative debate and abstains from imposing its standards on other actors. The author hence poses the promotion of internet sovereignty as a response to the alleged US imposition of its internet governance standards, while disenabling the debate, creating conditions for its cyber espionage and attacks and damaging the Russian and Chinese reputation with public attributions based on unclear proofs. Mirza's interpretation of the promotion of the internet sovereignty standards sheds light on the asymmetries of power in the international debate, while Van Wie Davis (2021) adds that the refusal of the application of human rights law in cyberspace and the rejection of cyberattacks as an act of force – which would constitute a ground for retaliation – are supported to continue its actions of *unpeace* without any ground for kinetic response.

Two exemplary cases of Japan's perception of China's industrial and international internet policies are provided by the Huawei ban and the competition between the Belt and Road Initiative (BRI) and FOIP.

In the first case study, Lee, Han, and Zhou (2022) and Kolikowski and Hall (2021) include Japan along with other middle powers to analyze their behavior in light of their commitment to the US alliance. Lee, Han, and Zhou (2022) pose Japan's reaction in light of the alliance halo theory, where allied states are supposed to support each other also in areas where not explicitly required: the subjects banned Huawei with an explicitness proportioned to their strategic interests toward China.

However, the studies treat the ban as something exogenous, not focusing on the internal dynamics that have led to this decision, or on the legal and intelligence ties between Huawei and China's Ministry of State Security. Kolikowski and Hall (2021) instead interpret the behavior of Japan, Germany, and the UK as a form of decision-indecision due to their security alliance with the US and economic ties with China. The authors recognize that the framework does not apply to Australia, which was the very first country to ban Huawei. Regardless, this study is useful to understand Japan's ban, based on the rise of cybersecurity standards to make Huawei cyber espionage activities unfeasible, without ever addressing the company directly, and coupled with financial support to autochthonous companies that chose to abandon it, which also creates a distance equilibrium between Japan, China and the US. The reaction can be also interpreted under the transversal securitization framework since Japan has securitized the domain with behaviors attributable to Huawei.

Moore (2020) provides a thorough explanation of the securitization process hinted by Soesanto (2020): the Huawei ban is the result of the Australian and US securitization of China based on a continued history of intellectual property theft and human rights abuses supported by Huawei technology, which has induced other countries to perceive the company as a threat. His research in facts provides a more optimal description of the phenomenon, with an analysis of Huawei's legal obligations to provide access to foreign data to the PCC intelligence in light of the internet sovereignty principle, and a description of Huawei's past allegations from Western actors, which provide an optimal ground on why securitization is an optimal framework to describe the phenomenon, rather than cyber orientalism.

The comparative studies on China's Digital Silkroad (DSR) – the digital connectivity policy associated with the BRI – and the Free Fair and Secure Cyberspace (FFSC) – the digital

version of Japan's FOIP – provide further grounds for Japan's threat perception of China in cyberspace.

Mochinaga (2020), with his policy paper, addresses the normative impact of the strategic competition in the cyber domain, visible in the indirect competition between China's internet sovereignty and Japan's free data flow with trust. Furthermore, Japan in its FOIP never challenged China, directly, preferring to call the policy a vision, rather than a strategy – unlike the US which has shaped its FOIP as a direct challenge to China.

A more updated version regarding the promotion of FFSC – hence exclusively focused on Japan – is provided by Malachinski (2023). The author points out how Japan's endeavors are almost exclusively of a technical nature, and the CCB initiatives are insufficient to develop cyber norms in the target countries. Nevertheless, improving partners' capabilities is instrumental to preventing cyberattacks from China, which exploit the IP addresses of third countries, targeting Japan due to its political proximity to the US and for cyberespionage (Bartlett 2023), which is also instrumental for the goal of Society 5.0.
Malachinski goes beyond the FFSC application against China, helping to understand the general strategy adopted by Japan: the former was already addressed as a "concern" in cyberspace since 2013 Japan's Defense White Paper, and considered "the biggest threat" by the author, if compared with North Korea and Russia for the consistency and magnitude of its cyberespionage – exemplified by the 2016-2017 campaign on JAXA and other 200 Japanese research institutes – and for its endeavors in controlling the technology supply chain given by the BRI (Malachinski, 2023).

2.6 Positionality statement

The recent production of securitization theory has significantly advanced the understanding of how language and performative acts contribute to the construction of threats. It has highlighted the role of various stakeholders in this process and expanded its application beyond traditional speech acts to include broader performative acts. Furthermore, the novelty of the indirect securitization frameworks may have limits detectable with applications to other domains, such as cyberspace. Regarding the literature on Sino-Japanese relations, it has been proved how the negative shift is more perceivable in the security sphere, while the overall context remains stable, hence not open to direct acts of securitization, as demonstrated by the Huawei ban (Kowlikoski and Hall, 202; Moore, 2020).

However, also this field of research has preferred to focus on the overall cybersecurity evolution of stark case studies, such as the Huawei ban or the contraposition of the FOIP to the BRI. Nevertheless, those represent only a part of the nodal *loci* of the securitization move engaged by Japan against China in the cyber sphere. In the meantime, cyberattacks are presented but not fully explored, except for Soesanto (2020), who however focuses mainly on the technical aspects and provides a context that encompasses the period from 2011 to 2019. Furthermore, the threat posed by China is mostly taken for granted, but its constituencies are not fully explored at the discourse level.

3 Theoretical framework

This chapter unfolds the transversal securitization framework developed by Dell'Era in her *"Securitizing Beijing through the maritime commons: the 'China threat' and Japan's security discourse in the Abe era"* (2024) as a perspective for the analysis of the relationship of China and Japan in cyberspace. The choices are motivated by the fact that this particular framework allows deeper observations of the attributes referred to China in the light of the Sino-Japanese relation, which is characterized by a complex equilibrium based on geographical proximity, intense trade, and industrial interest, hence does not allow direct acts of securitization without the risk escalation of the diplomatic relations On top of that, this particular theory has been chosen instead of the classical framework of securitization amid the progress of the scholarship shown in the literature review.

The chapter hance follows a bipartite arrangement, where the first half discusses the constructivist approach to cybersecurity and the transversal securitization framework. While, the second part entails a comparison of the realist and liberalist approaches to cybersecurity, with a presentation of their limitation in the analysis of threats, which is aimed to reinforce the choice of this theoretical framework.

3.1 The constructivist approach to cybersecurity

This thesis is located in the constructivist stream. Hence state actors are regarded as subjects whose understanding is shaped by the external influences in a dynamic process, consequently

molded by the personal views and biases of the stakeholders. Briefly, reality is not objectively understandable but mediated by subjective assumptions (Bryman, 2016). This perspective is congenial to cybersecurity since cyberspace is a purely man-made domain under constant development, which is subjected to political, social, and economic pressures. And its governance requires the collaboration of state and private actors – e.g. social networks and critical infrastructure owners – which are consequently driven by their subjective interests and understandings (Katagiri, 2021; Ciolan, 2014). Moreover, constructivism being concerned with the interpretation of the covert meaning of actions, is optimal for understanding the circumstances and rationales for public attribution of cyberattacks (Lee, 2023).

Additionally, cyberattacks have an impact at the level of ontological security – i.e. the state's ability to protect its idea of self – since they disrupt the routine of their citizens, and challenge the idea of the state as a security provider – already posed in the discussion by the involvement of non-state actors in this field – and as a guarantor of the rule of law (Lupovici 2023). The ontological security is further challenged by cyberterrorism and information warfare: the first leverages the individual's fear of random victimization and the "lawlessness" of cyberspace, the latter aims to destabilize the trust in the institutions, which is vital for democracies (Ciolan 2014, Paterson and Hanley 2020).

3.2 The transversal securitization theory

As briefly presented in the literature review, Buzan, Wæaver and De Wilde (1997), define the concept of threat based on classical military-political terms as an entity that poses an existential threat to the survival of a referent object. In essence, the enunciator presents an element as something that must be curbed with measures that depart from the status quo, since its existence jeopardizes the stability of the country.

How those threats justify extraordinary governance choices and the underlying process is defined as securitization, which can be divided into three steps:

- Creation of an existential threat
- Call for emergency actions
- Creation of a platform of discussion by the audience, which accepts the threat and legitimizes the extraordinary countermeasures

Therefore, security is interpreted as a dynamic process, where threats are presented and accepted by the audience based on their knowledge, context and bias, who provides and endorses measures that have an impact on different actors The dynamism is further provided by desecuritization: a different path that relocates the threat in the discourse of normal politics (Thierry, 2011).

The scholarly contribution of the last twenty years has contributed to a better understanding of the components of the threat-building process: the typologies of securitization moves, which vary according to the different types of audiences, the rhetorical devices, and the context in which securitization happens, transposing the application of the theory beyond the performative speech acts of the enunciator – e.g. interviews (Wilkinson, 2011) and newspaper articles (Zijian, 2019).

Hence, those advancements conferred a new conception of securitization: from a universal pragmatic act to a pragmatic sociological practice that determines the general and efficacious communicative actions that define what jeopardizes security. Moreover, thanks to the case studies conducted in the last twenty years we have assisted in a detachment from the *a priori* established universal principles in favor of analysis concerned with the congruence of different factors – e.g. language, audience targeted, construction of practices and external variables – to evaluate the effectiveness of the securitization process (Thierry, 2011)

How those variables affect the process of securitization is clearly exposed by Dell'Era's "*Securitizing Beijing through the maritime commons: the 'China threat' and Japan's security discourse in the Abe era*" (2024), which stems as a reaction to the first generation of the securitization theory. It assumes that the enunciator has to openly address the threat as such – and discrepancies between studies that have assessed the effect of the China threat on Japan's security policies changes and the factual reticence of Japan's elite to address China directly as a threat, preferring attributes such as attention or subject of concern.

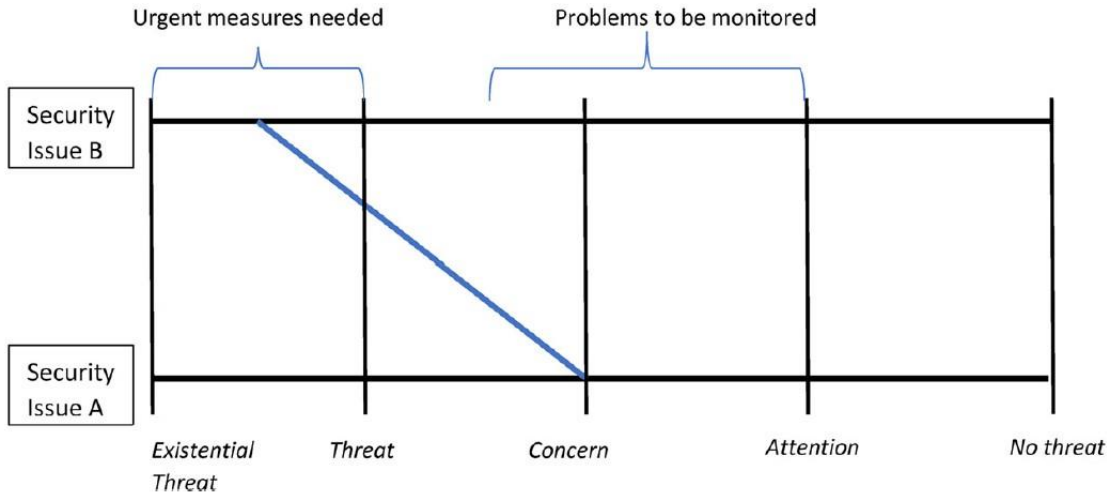
Basing her approach on the Oren and Brummer studies (2020a, 2020b) of this irregularity, she uses their classification of threat perception intensity to develop the framework of transversal securitization, which revolves around the different degrees of threat perception. The author then takes their developed grammar and attributes to different values a precise level of urgency and corresponding securitizing behavior (Table 1).

Table 1: Transversal securitization grammar adapted from Oren and Brummer (2020)

Scale of threat	Definition	Discoursive Marker	Level of urgency	Securitizing behaviour
Attention	'Entity capable of inflicting damage but that is not interested in doing so"	'Matter of Attention' 'Scrutiny'	Lacking urgency of action/measures	Requiring scrutiny, monitoring, observation, or analysis
Concern	'Entity capable of inflicting damage but whose intentions remain unclear'	'Issue' 'Challenge' 'Serious/grave concern' 'Problem	Lacking urgency of action/measures	Requiring scrutiny, monitoring, observation, or analysis
Existential threat	'Entity capable of inflicting damage and hostile'	'Matter requiring imperative action' 'Existential threat' 'Matter of 'survival or ' Matter affecting 'vital domain/interests'	Urgency of action/measures	Requiring emergency countermeasures

Specifically, the issue, although its high degree, is framed under moderate levels of concern, and its behaviors or features are linked to a domain constellated with elements having the discursive markers typical of existential or average threats. This hence results in a major level of urgency projected on a subtler securitized subject, resulting in a relation that Dell'Era (2024) conceptualizes with the following graph (Table 2).

Table 2: a visual representation of the transverse securitization, where behaviors attributable as a threat in the domain are related to the ones linked to the subject, defined as a challenge



The technique is employed in case of uneven and broad audiences such as the one of the English translations of the Defense White Papers, which should endorse the eventual securitizing actions engaged by the enunciator while refraining from openly antagonizing the threatening actor. And it is adopted in the situation where the enunciator and the threatening subject are in a state of engagement and rivalry, in which the actors maintain close relations in particular spheres that could be jeopardized by an act of securitization. In fact, as observed in the literature review, despite the perceived negative shift in Sino-Japanese relations, there are still areas where their respective stakeholders are still interacting, such as e-commerce, hence a direct securitization of China by Japan on cyberspace would entail damage to the interactions in that specific sector and possible retaliation by China.

3.3 Limits of the realist and liberalist school

Realism is widely applied in cybersecurity, particularly in the understanding of cyberwarfare. Synthetically, the theory perceives states as unitary rational actors interacting in an anarchic international order in pursuit of their interests and security, which entails the competition for the survival of the state and, in the case of offensive realism, the preservation of the status quo through the balance of power to maximize their survival in an anarchic world; and in case of offensive realism, the increment of power in the most cost-effective way

to ensure dominance (hence survival) in the anarchic international order (Craig and Valeriano 2008).

However, despite apparent anarchy in the cyber domain the existence of two types of state governance, namely the authoritarian and the liberal/multistakeholder, exemplified by China for the former and The US and EU for the latter, provides an embryonal sense of order, which can be supported by regional organizations, as noticed also by Poetranto and Gold (2021). Moreover, the realist school assumes that the anarchy in the domain, in the absence of a form of equilibrium or dominance, will eventually lead to a breakdown, with the network of partnerships between like-minded partners established through the FOIP (Malachinski, 2023). Moreover, the general literature on realism applied to cyberspace conceives cyberwar in the classic terms of conflict, not considering alternative forms such as shadow warfare, typical of China (Wan Wie Davis, 2021).

Regarding the notion of deterrence realism, Craig and Valeriano (2008) admit that "traditional notions of power and war do not necessarily translate well to the cyber domain" due to the lack of destructiveness of classical cyber-attacks, which is achieved instead in hybrid operations, stemming hence doubts on the efficiency of this concept applied exclusively to the cyber domain (Craig and Valeriano, 2008). On top of that, realism conceives threats as objective menaces to state interests and, therefore does not dedicate particular attention to its constitution in the state official documents.

The literature on cybersecurity, however, has shown an attempt to bridge constructivism and neorealism with Lupovici's "*The dual-use security dilemma and the social construction of insecurity"* (2021) proving how the security dilemma is exacerbated by securitization acts, especially regarding dual-technologies, expanding the application of securitization to nontraditional domains. The security dilemma states that actors who increase their military capabilities induce other states into a state of insecurity, since the mutual increase of the defense capabilities may bring an equilibrium or an escalation, determining a reciprocal increase in their own assets, which is exacerbated in the case of dual technologies. Furthermore, the enunciators use one of those following rationales to securitize an opponent's dual-use technology: the device can become a strategic threat or gap between the parties; it creates an innovation gap and hence a strategic advantage both at the security and at the economic level; or is just a challenge to the actor's supremacy and prestige.

Liberalism, the doctrine allocated in the opposite of realism, conceives the international order as an opportunity for cooperation between actors to maximize the well-being of all the

actors, hence implying multi-stakeholder global governance as constructivism does (Meiser 2018). This objective is achieved through the role of national and international institutions, guarantors of security, which help to explain its complex multistakeholder mechanism in cyberspace.

However, in the state of current affairs, both national and international institutions are not strong enough to be perceived as such, as demonstrated by the threat posed by cyberattacks to national ontological security and the lack of consensus in the application of international law in cyberspace (Devi and Rather 2019, Kello 2021, Katagiri 2021, Kono 2017)

4 Methodology

Due to the nature of the research questions, which aim to unveil the trends in the securitization moves of Japan against China in cyberspace, the methodological choice has fallen on qualitative and quantitative content analysis, resulting first in a deductive and then an inductive process and an interpretive ontology. The choice of pairing the qualitative with the quantitative method lies in an intention to focus on the linguistic features of the White Papers, with regard to the contextual meaning of the text (Hsieh and Shannon, 2005). The chapter opens with the methodological considerations grounded in the choice of content analysis, and it follows with an explanation of how the transversal securitization theory, which is based on a discourse analysis, has been applied to analyze the content of the White Papers. Ultimately, the coding process with the due differentiations between the quantitative and qualitative analyses is illustrated in the audit trail. The second and first codebooks are presented in the Appendices section, along with the longitudinal display of the quantitative results used in the summative analysis.

Securitization theory is often associated with critical discourse analysis, thanks to the possibility of posing the evolution of securitization moves in the sphere of the enunciator's practices. However this research tackles the threat-building process with content analysis, since similarly to the former, it aims to study how enunciators use and manipulate symbols in a discourse, but the content analysis provides the advantage of quantifying the data to establish trends, which is the aim of the sub-questions of this research and to evaluate the

presence of the threat and challenge markers identified by Dell'Era (2024), while minimizing the biases and allowing the replicability of the results thanks to the codebook (Balzaq, 2021b; Krippendroff, 2022). Those markers have been identified with the Text search query of Nvivo, reported in the Appendices section.

Furthermore, it could be argued that since the transversal securitization theory was elaborated based on discourse analysis, it would have been more orthodox following the same method, nonetheless, Dell'Era (2024) was aiming to identify the strategies adopted by the second Abe Administration based on the recent developments of the academia on the securitization theory – which are reported in the Literature Review – while this research accepts the existence of this indirect form of securitization, and it aims to study its application in another domain. Furthermore, the type of data chosen allows us to understand how both the depiction of the domain and the representation of China coherently every year.

4.1 Audit trail

The selected unit of analysis for this content analysis is the paragraph (i.e. a unit of text bracketed by carriage controls). This choice allows a major accuracy, reproductivity and thus reliability since syntactical distinctions are objective mediums. However, at the same time its size provides a broader semantical development of the China threat in cyberspace and a deeper description of the circumstances, and it is deemed as an optimal quantitative unit since it can describe the magnitude of the threat in the cyber domain (Krippendroff, 2022). Indeed, one of the aspects tackled by the qualitative process of this research is the identification of the "most threatening" Chinese policies, or related issues, such as countermeasures, which can be articulated in the documents with periphrases, as it can be shown in the 2021 White Paper respect of the Huawei ban:

> "Considering this situation, the United States, deeming the use of foreign-made equipment in the ICT supply chain and bulk-power system as a threat to national security, issued Executive Orders in May 2019 and May 2020 restricting such use"

The first step entails the isolation of the passages regarding the general securitization of cyberspace and the ones referring directly to China. The operation is done with a directed qualitative content analysis (Hsieh and Shannon, 2005), namely a deductive application of the

themes that emerged in the literature review, allowing codes to be created and their application via Nvivo.

This first analysis is done to verify the presence of those themes which are listed in the Codebook I in the Appendices and to understand the constitutive elements of the general and China-specific issues in cyberspace, since in the securitization move there is a selective emphasis on the aspects of a phenomenon (Eriksson and Giacomello, 2014).

The directed analysis functioned as a quantitative base for the detection of the thematic variations and patterns and cross-coding references (Hsieh and Shannon, 2005) Therefore, a second qualitative analysis based on a conventional approach is performed to refine the codes resulted in the directed process though merges of existing ones, deletion of the absent or underrepresented in the domain and the enrichment of the set with new themes emerged, as visible in the Codebook II. This is also done because the directed analysis may be based on biases which in turn may lead to a noncomplete evaluation of the phenomenon, which is further explored with a second conventional one (Hsieh and Shannon, 2005).

The Codebook II is then employed to produce a quantitative account of the contents through the same software to derive the frequency and the variation of the *leitmotiv* in five years to understand which typology of attacks are most represented and which are the technologies and the ideological features that have been securitized and in relation of which contemporary events. Furthermore, the wide unit of analysis has led to the compresence of themes, emphasized by the use of matrices, that are interpreted under a summative content analysis, namely an interpretation of the codes based on the context generated by the cross-sections (Hsieh and Shannon, 2005).

Then, an ulterior analysis is performed to distinguish between threatening and challenging behaviors among the themes. This is done by researching the threat and challenge markers developed by Dell'Era (2024) – illustrated in the Theoretical Framework chapter – among the codes, distinguishing between the ones referring to the context and the ones referring to China's behaviors in cyberspace to understand the indirect methods employed in the securitization moves of Japan on China in the cyber domain.

5 Presentation and analysis of data

This chapter intends to present the White Papers from 2019 to 2023 as a source of data and analyze the empirical findings – i.e. the securitization moves – according to the code listed in the second codebook and in light of the transversal securitization. This process entails the evaluation of the qualitative and quantitative analysis correlated with the research of the threat and challenge markers reported in the first chart of the Theoretical framework chapter to identify the trends in the securitization of cyberspace and how those behaviors may jeopardize the international security environment, in the report of Chinese cyberattacks, in the contemporary issues associated to them and in the Chinese policies that impact on its security. Ultimately, the evidence is summarized and reorganized according to the corresponding edition of their respective White Paper to systematize them in a longitudinal case study.

5.1 White Papers

To analyze how Japan is building the idea of the China threat in cyberspace the data for the analysis will be gathered from the White Papers of the Defense of Japan issued from 2019 to 2023 by the Ministry of Defense (MOD). Indeed these documents, along with the NSS and the cybersecurity strategy, are one of the instruments that Japan uses to articulate this cyber threat landscape, and the one that is released on an annual basis, allowing a longitudinal observation.

From an ideological standpoint, the MOD is also a decisive actor in the constitution of the security environment surrounding Japan through its White Papers, where the domains, context, and actors regarded as threats are defined and contextualized with the state of current affairs. Those threats are molded according to the self-perception, priorities, and values of the Japanese government, which through a selective cognitive process highlights the aspect of the actors that are deemed as threatening or reassuring according to the type of relationship engaged.

Although the target is not formally established in any of the documents taken into analysis, we can infer that the intended audience is both national and international: both are composed of policymakers, foreign ministries whose activity entails consideration of Japan's defense landscape, industrial stakeholders of the defense sector and press agencies which popularize the contents to a general audience. Moreover, in the case of this research is due to add the

Japanese and international Computer Emergency Response Teams (CERTs) and cybersecurity and data vendors.

Although the national and international audiences share the same category, the perlocutionary value (i.e. the intended meaning and emotions conveyed) differs. In the case of an international audience, the intent is to legitimize Japan's policy choices amid the contingent international situation and at the same time deny an eventual breach in the relationship with China and avoid eventual economic retaliations (Dell'Era 2024). The perlocutionary effect toward the national audience goes beyond this: it aims to push NISC policymakers to craft programs aimed at enhancing a more aggressive posture in cyberspace with particular regard to cyber warfare, and due to the sense of urgency, exert pressure on the legislators for their adoption.

The decision is also motivated by the compliance of the MOD White Papers with Scott's four criteria for assessing the quality of documents (Scott, 1990). In fact, in light of their officiality, they can be deemed as *authentic*, representing the governmental perspective on the regional situation and its defense policy, objectives, and current state of affairs. They are *credible* as a representation of the Japanese process of securitization of China in cyberspace, hence revealing the underlying biases. In fact, as Abhram (1996) stated – according to Brymann (2014) – the value of governmental documents resides in the biases that they reveal. They are *representative* in the context of qualitative research. Indeed, as Brymann asserts: no case has a statistical value (2014). Nevertheless, the Defense White Papers used in this research are publicly available on the official website of the Ministry of Defense in the English language, hence deemed as representative of the governmental position on the security situation and the actor's standpoint, approach, and objectives related to its defense policy.

Regarding cyberspace, they are meant to present the strategy adopted amid technological progress and the latest geopolitical evolution. In light of this research, they convey the evolution of the themes employed by Japan's government to securitize China in cyberspace, relating to the salient cyber governance policies elaborated by PCC, the contemporary issues related to its securitization, the most threatening application and the attacks reported in the White Papers. In pursuit of its aims, the analysis of the white paper has to be conducted concerning their context and the self-perception of Japan with particular regard to their first parts: the Security Environment Surrounding Japan.

5.2 Analysis

5.2.1 Securitization of the Cyber domain

The analysis of the domain is at the basis of the transversal securitization since it functions as a free zone where threats are addressed broadly and without necessary specification, leaving room to address threatening behaviors reducible to the subject, which is in turn described as a concern when the discourse focuses specifically on it. The second qualitative analysis also revealed a perception of the general security environment threatened by the new use of cyberspace or by technologies associated with the domain.

In all five documents emerges a state of insecurity due to changes in the status quo, caused by interstate competition and military build-up, and catalyzed by the persistence of gray zones and hybrid warfare, which since the 2021 document are regarded as "*persistent*". This status of uncertainty is leveraged by certain actors to create a more favorable international order for themselves – explicitly exemplified by China (MOD 2019, 2020, 2021, 2022, 2023).

In particular, the dual-technological development of warfare, could *"drastically change*" its future, prompting uncertainty in the global security environment (MOD, 2020), functioning as the rationale for the establishment of a multi-domain defense force. This necessity however disappears in the 2022 document, probably due to the acceptance by the audience of these operations, however, the uncertainty exasperated by the dual-use technology persists. And it is for this reason that the 2021 Paper is presented as proof that the MOD and the JSDF can protect Japan "*in the midst of a drastically changing security environment*", coherently with Japan's and its allies' commitment to securing a stable international order expressed in the 2022 NSS.

The emphasis on diplomacy is one of the saliences of the 2019 White Paper along with the delineation of the cyber threats and trends common to the five Papers. They encompass the military reliance on ICT infrastructures, which exposed them to possible attacks by China and Russia, mentioned in the section regarding cyber threats and believed to bolster their cyber capabilities for disrupting the telecommunications of the adversaries.

The 2020 document explicitly defines China as a "*disruptor of the status quo"*, emphasizing hybrid warfare practices, including grey-zone situations, whose definition is further explored. The 2021 Paper reports that China and Russia use the pandemic as an occasion to employ

information warfare to undermine trust in the EU and US, and it frames them as actors "*shaping a favorable international order*", hence changing the status quo, vital for Japan's interests. Besides, the uncertainty of grey-zone episodes evolves into a "more serious situation without any clear forwarding", becoming a rationale to Japan for take "*measures not limited to military ones*", probably alluding to a will to engage in forms of non-traditional security, as exemplified by the reference on the Huawei ban in the section on trends in cyberspace. Furthermore, the correlation between APT and state-sponsored attacks based on the need of conspicuous resources reduces any eventual ambiguity in the attribution starting from the 2020 White Paper.

The 2022 White Paper uses Russia as a securitizing expedient for China's grey zone situations and hybrid warfare in the East and South China Seas and Taiwan through agile solutions, preemptively deterring the unilateral changes of the status quo, amid the hybridization of warfare. The language employed in the documents tries to balance the boldness of the description of the pair as actors that are "*forcibly changing the world order*" to which Japan "*resolutely continues to oppose*", while downplaying attributes as "*unprecedented challenges*" and "*global issues*", coherently to the transversal securitization principle. Furthermore, in 2022 is it observable an intersection between economic security and cybersecurity with the recognition of cutting-edge technologies as vital to societal and economic stability, with a consequential association of any cyberespionage act targeting these technologies as a threat to national security.

The 2023 White Paper intensifies the uncertainty which is expected to increase along with the US-China rivalry and a lack of leadership which has created a "*new era of crisis*". Moreover, the instability is exacerbated by a change in the paradigm of security due to hybrid warfare, which increases the threat of cyberattacks. Indeed, cyberattack capabilities are associated with the ability to influence people's judgment – i.e. cognitive warfare – and disrupt critical infrastructure information, exemplified by the Microsoft Corporation mail service software attack (MOD, 2022).

Moreover, it has been noticed an increasing emphasis on cyberattacks aimed at stealing information, as shown in the chart below (Table 3).

Table 3: number of mentions of information theft

Year	2019	2020	2021	2022	2023
Information theft mentioned in the section	2	3	3	6	5

In fact, information theft is also the most common Chinese cyberattack reported in the list of "Threats in cyberspace", especially through APTs as shown later in Table 6.

5.2.2 Cyberattacks conducted by China

Indeed, China's information dominance has been pointed out as its priority to achieve modern military power and the intelligence of the Chinese military forces. Australia, Taiwan, the US, and EU countries have repeatedly attributed acts of cyberespionage to hacker groups sponsored by China (MOD, 2023). A salient feature of the White Papers is that the sum of the attacks by the Chinese government or its affiliated actors mentioned throughout the documents, are almost always to the detriment of third countries, which are the primary source of documentation in the White Papers for this type of incidents, as shown below (Table 4).

Table 4: number of cyberattacks targeting third actors

Country	Australia	EU	Japan	US	Taiwan
N. Of coding references under the code "Cyberattacks"	1	1	9	28	4

In the section regarding Chinese cyberattacks in 2019, all the cyberattacks mentioned were information theft, two to US state institutions and one to a US Navy contractor, classified in this study as a private institution. Of particular salience is the attack operated by APT10: a group affiliated with the Tianjin State Security Bureau, which conducted information theft on companies that develop dual-use technologies located in Japan and other 10 different

countries. The extensiveness of the attack has probably led Japan to issue a press statement, which optimally displays the transverse securitization strategy.

From the 2020 paper, the APT10 attack on Japan is distinct from the one on the US. It should be noticed that in the description of the attack on Japan, there are no temporal expressions, inducing the reader to think that it could have happened in occurrence with the US one – in 2018 – or recently.

The US is indeed the second most mentioned actor since Japan regards the alliance with the United States as the cornerstone of its security policy, as proved by the dedicated chapter in the third section of each Paper. Therefore, its numerous mentions could be used as an expedient to securitize China through its statements: in the 2019 edition, we find the US 2019 World Wide Threat Assessment Report, where China "poses the greatest cyber threat to the US" (MOD, 2019). This in turn jeopardizes also Japan since the actor entails a close collaboration through joint cross-domain operations through CBM sharing and cooperation in the protection of critical infrastructures and services.

In 2021 we can observe the same pattern on the list. Moreover, there is a mention of the July 2020 information theft attack prosecuted by the US Department of Justice, aimed at stealing intellectual property and trade secrets related to the COVID-19 vaccine. Always concerning COVID-19, in the section on Sino-Australian relations there is the mention of an attack against the Australian Government and critical infrastructures conducted allegedly by China as a form of pressure related to economic security in the aftermath of a request for an independent investigation on the diffusion of COVID-19 by the Chinese Government. Returning to the list, it is also mentioned the 2021 investigation conducted by the Japanese authorities regarding a series of cyberattacks against 200 companies – including JAXA – operated by the group TICK, known also as APT40, affiliated to the PLA.

The 2022 White Paper, regarding the structure of the chapter dedicated to the Chinese cyberattacks, follows the same scheme: five out of six attacks target the US, and the mention of the APT10 action targeting Japan, confirming the significance of this cyberattack for the actor. Instead, in 2023 we can observe a major variety of actors who suffered cyberattacks by China, presumably to convey how the situation does not concern only Japan's closest partners, but also other allies.

In particular, the Belgian government was a victim of repeated malicious cyber activities operated by the state-sponsored groups APT27, APT30 and APT31 and the DDoS on the

Taiwanese presidential office website that occurred in concomitance with Pelosi's visit. The Belgian attack involves state-sponsored groups that either have attacked Japan's industries (e.g. APT31) or critical infrastructures of states involved in the South China Sea (e.g. APT30) (Malpedia, 2024; CFR, 2020), which may be interpreted as a subtle method to establish an image of China in the cyberspace not solely as a threat for actors who are intensely involved in the region but also to geographically distant like-minded partners, such as the European ones, who have recently started to collaborate with Japan, as demonstrated by the Agreement for Air services (MOFA, 2023). Despite the exacerbation of the SinoEuropean relations, although, there are no transversal securitization acts referred to this collective actor in the Papers. Moreover, the 2023 edition mentions an attack on a US security company by the APT41, a group that also hit Japan in 2022 with the operation RestyLink, which is not however reported in the Paper (Koike, 2022)

The Taiwanese mention is linked with the issue between China and Taiwan, specifically to the 2022 Strait crisis, which reaches a peak in its mentions in the 2023 White Paper, as demonstrated below (Table 5).

Table 5: mention of the Taiwanese issue

Year	2019	2020	2021	2022	2023
N. of Coding References	1	2	0	8	15

This cyberattack – along with other actions engaged by China on that occasion in the cyber domain – is mentioned throughout the document, especially in the context of the PLA's five-day integrated-domains training. Furthermore, the impact of the Taiwan issue is evincible by the dedicated column in this edition.

China is further securitized through Taiwan, especially in the 2023 document: not only in the section relative to threats in cyberspace, but also through Taiwan's National Defense Report (NDR) "*recognizes China as a security threat in cyberspace*" due to its practice of cyber theft and unlawful information correction during peacetime, but also a development of the grey-zone techniques that are likely to be employed by China "*to seize Taiwan without a fight*" displayed during Pelosi's visit where China conducted attacks on infrastructure and systems (DDoS), cyber espionage, and Cognitive and Information warfare. The repetition of the threat attribute reinforces the securitizing move if it is paired with the NDR quote that the

acquisition of China's cyber, land and air superiority would signify a "*very great threat*" to Taiwan, present in the 2022 edition (MOD, 2022).

As abovementioned, information dominance is deemed a priority by China, and during the analysis, it was noticed increasing mentions of APTs conducted by China or its sponsored actors, as is shown by the matrix below (Table 6).

Table 6: intersection of the codes APT and Chinese cyberattack

Year	2019	2020	2021	2022	2023
cross-references	3	4	6	6	5

The strong emphasis is further corroborated by the peak of correlations reached in 2021: this is due to the presence of the past attacks mentioned in the 2019 and 2020 White Papers to the ones related to information theft regarding the development of the COVID-19 vaccine.

In 2022 the quantity remains constant, although there is a change in the content: the APT40 – i.e. Tick group – attack on 200 Japanese companies is not mentioned anymore in favor of the Microsoft corporation mail server attack, presumably in an effort to diminish the idea of Japan as a vulnerable actor in the domain.

The decrease in 2023 instead is attributable to a wide heterogeneity but a minor quantity of cyberattacks listed. Moreover, the Paper mentions the APT41 campaign on the US government network, which lasted from 2022 to 2023, and during the same period, the group has also spied on Japanese academics and think tanks (Koike, 2022; Cyware Alerts, 2022). Here we can infer how Japan started to increasingly perceive information theft as a more pressing threat, especially in correlation with the increasing informatization of the army, which is increasing their capabilities in data appropriation – e.g. through APT.

5.2.3 Linkage with other issues

It is observable how the perception of the China threat in cyberspace is a byproduct of tensions related to other domains. This family of codes emerged inductively during the qualitative analysis of other codes, as can be shown from the matrix (Table 7).

Table 7: intersection of types of cyberattacks and contemporary issues

	Critical Infrastructure Attack	Cyberespionage or information theft	DDoS
BRI or FDI for technological acquisition	0	5	0
COVID 19	0	2	0
Taiwan issue	1	2	1
Economic Security	0	12	0

Therefore, the underlying rationale of the attack and the broader context in which they take place is inferable.

The BRI – i.e. foreign direct investment – is seen as a tool associated with unfair technology transfer, allegedly via cyber espionage for the CMF coherently for all five documents. Worthy of attention is the second passage dedicated to the BRI code in the 2019 edition, where Japan reports the words of the ex-vice President Mike Pence who regards the BRI as a *tool for forced technology transfer* – e.g. imposition of Huawei devices for 5G – and *intellectual property theft* of the recipient countries, and as a device for espionage and theft of military technological secrets.

Those allegations are also supported by the joint case filed by Japan, the EU and the US at the WTO in 2019, where it is reported that Japan held and expressed its concern for several years regarding this matter, since Chinese regulations on import and export of technologies via joint-ventures deny the creators' rights on patents against the Chinese party subsequent the expiration of the contract (WTO, 2019).

Similarly, the concern against forced technology transfer is present in the 2023 statement of the Japan-U.S. Economic Policy Consultative Committee, where the parties state their *commitment to preventing the theft and military application of their emerging technologies, which could potentially threaten the international peace and security* (METI, 2023). The forced technology transfer is one of the practices used by China which led Japan to institutionalize the concept of economic security in 2021 under PM Kishida to safeguard intellectual properties and bolster the technical-oriented CCB under the FOIP towards economic partners that are also involved in the BRI (Osawa, 2023c; Malachinski, 2023).

The cyber espionage-economic security coupling is associated with the constant reference to Australia's Huawei ban with the mention of the actor's initiative to establish a Critical Infrastructure Center after the Chinese acquisition of Port Darwin – defined as a *concern* – becomes a constant. The primary duty of the center is to identify the Australian infrastructures that are a risk of espionage and sabotage, which sales must be consequentially blocked.

Critical infrastructures are in fact a referent object of securitization moves of the cyber domain that remains stable throughout all the five years, with further mentions in light of the Chinese instrumentalization of the 5G technology – i.e. the Huawei case – especially in the 2020 edition. This could be inferred as a part of the big indirect securitization move against Huawei, as also stated in the literature review.

In 2021 the issue of economic security becomes salient in light of the US-China technological competition which is evident both in the trade war on semiconductors and in the light of cyber espionage, which serves as a cause to enact protectionist measures on general technological exports. However, the economic-security factor becomes explicit only in the 2022 Paper, where it appears as a separate chapter in the first part of the document, where the initiatives listed account for export control measures engaged not solely by the US, but also by Australia to prevent the import of devices having backdoors for cyberespionage – similar to the Huawei case.

However, the related securitizing move against China appears in the 2023 edition, in the specific section on trends concerning economic security, Huawei is defined through the UK words as a *"high-risk vendor*" and South Korea is said to "*recognize the threat*" of excessive dependence on potential opponents for vital industrial products, and its consequential initiative to rebuild its supply chain without China.

In the White Papers, information theft is also associated with COVID-19, in particular in 2021 regarding the Chinese DDoS attack on the Australian government after its demand for an investigation regarding COVID-19, as abovementioned. Furthermore, a stronger link is provided with the 2020 US prosecution of two individuals tied to the Chinese government, who conducted a cyberattack aimed to steal intellectual property related to the development of a vaccine for the virus, which has been reported in the section regarding Chinese cyberattacks of the 2021 and 2022 White Papers.

As abovementioned, the Taiwan situation is used to securitize China, especially in the 2022 and 2023 documents using Taiwan's NDR. Furthermore, the 2022 section shows an intersection between the US-China competition and the Taiwan situation, where the former exacerbates the latter, creating a "*sense of crisis*", since Taiwan's stability is perceived as indispensable for the international order (i.e. status quo). However, regarding these exact words, in the 2023 Paper, the intersection of US-China-Taiwan is not present, and the situation is mainly discussed in the dedicated column, probably to confer more emphasis on the Taiwan situation *per se.* Indeed, according to the 2022 NSS, China's maritime activities around Taiwan have threatened Japan's security as well, and as regarded by Japan in the 2023 White Paper, the stability of Taiwan is indispensable for the international community.

5.2.4 Information and Cognitive Warfare

This code has been created based on the securitization move of the 2022 NSS, where information warfare perpetrated by Russia in the full-scale invasion is seen as one of the driving forces for establishing active cyber defense (Osawa 2023a, b). Its inclusion is furthermore justified by the Japanese *habitus* of associating the Russian action with Chinese behavior towards Taiwan and the attempts "to unilaterally change the status quo" in the East and South China seas.

The cognitive warfare code has emerged inductively. Despite a lack of an official definition and its tight intersection of elements with information warfare, we can distinguish it as a set of activities aimed at controlling the environmental stimuli to manipulate the mental state and behaviors of the target (who is a user of modern information technologies) with neurological resources rather than communication techniques, such as biases, tunneling of attention errors of judgments and perception overflow with the aim of arise an opposition to the target's government decisions (Hung and Hung, 2020; Fenstermacher et al., 2023). Therefore, the difference between the two warfare resides in the target (decision maker vs. generical user), and the focus (knowledge vs. cognitive process).

China's cognitive warfare on Taiwan is characterized by intimidation by the military, disinformation, content farms and bilateral exchanges to induce Taiwanese citizens to regard the conflict with China as imminent – through the demonstration of kinetic capabilities – and harmful to the socio-cultural and economic interdependence (Hung and Hung, 2020).

Furthermore, since both strategies entail activities within and outside of cyberspace, only the latter has been taken into consideration.

In the 2019 White Papers information and cognitive warfare are called respectively media and psychological warfare – which along with the legal one – constitute the Three Warfares policy, which are part of the PLA mission since 2003 to build an international supportive international audience towards China's military operations and interests, weakening the enemy military and civilian personnel and manage eventual legal repercussions of the China conduct. The general mentions of information warfare show great consistency since its general definition of the 2019 White Paper as part of hybrid warfare, used in interstate competition and grey-zone operations.

It starts to be directly associated with China in the 2020 document as a part of its propaganda to ameliorate its reputation during the pandemic exploiting the social confusion, and as a support to its vaccine diplomacy and dispatch of medical personnel in the most infected areas. In this edition, China is also used as an example of how certain countries may use the situation to *build regional or international orders favorable to themselves*, which leads Japan to regard the pandemic as a "*great concern*" since it could intensify the strategic competition among estates.

The theme of *great concern for the pandemic* used as an expedient for hegemony is also present in the 2021 document, where China's information war is paired with the Russian campaign to damage the US and EU vaccine's reputation to bolster their vaccine diplomacies for the abovementioned aim. However, the 2021 cybersecurity strategy does not delve into the problematization of this phenomenon, finding in the advancement of digital literacy a long-term solution.

The issue becomes more salient in the 2022 Paper, where concerning Taiwan, information warfare is regarded as a *strong concern,* and the use of botnets both by China and Russia on social networks to foster their positions, raise unrest, and *undermine the foundation of democracy* providing the grounds to the expansion of Japan's national security to nontraditional domain, as reported in the 2022 NSS. The strategy is posed in correlation with intelligentized warfare due to its inherence to the information and cognitive domain. Indeed, the increasing salience of those two can be inferred from the 2022 introduction of the section regarding information warfare and the considerations made in the 2023 section on threats in cyberspace, where AI-supported cyberattacks and capabilities are associated with the ability to influence people's judgment (MOD, 2023). Furthermore, in the latter, the Three

Warfares are regarded as a "*risk*", since they are part of the hybrid warfare, a phenomenon that is constantly taking place, as stated in the outline, especially in the Indo-Pacific region, and meant to *change the paradigm of security*.

5.2.5 Tech policy

The CMF is the central node between technological development and application to the military section, while Intelligentized Warfare – a policy crafted in June 2019 – entails the application of IoT systems and AI in the air, land, sea, air, space, electromagnetic, cyber, and cognitive warfare. Therefore, from the 2020 Paper onwards, we can see a discrete incremental correlation between the two, since CMF is regarded as the key or indispensable to developing Intelligent warfare (MOD, 2022). However, CMF prioritizes the informatization of the army, the policy that has led to the creation of the PLA's Strategic Support Forces (PLASSF), the section that also China to conduct hybrid-warfare operations and cyberattacks of espionage and defensive nature (MOD 2019, 2020).

The overall aim of this chain of policies is to rapidly acquire cutting-edge technologies applicable to the army to conduct hybrid warfare. The same concept is presented as a *leitmotiv* in all the five outlines of the White Papers as a catalyzer for gray zone situations, hence *insecurity in the international environment*.

The CMF appears for the first time in the section regarding military trends of neighboring countries of the 2019 White Paper, preluded by China's tendency to pursue a military buildup without transparency in new domains, defined later as a *serious security concern* for Japan, which also prompts China to engage more cooperatively in the international stage. In the same document, the policy is related to the US Huawei ban and other initiatives against China inherent to economic security. The ban therefore arises from interstate competition, defined in the introduction as enhanced by hybrid warfare and as an exemplification of the *increasing security issues* generated by the interdependency among countries.

This is consistent in the 2020 Paper, which regards the Chinese military build-up via dual-use technologies – e.g. AI applied to Intelligentized warfare – as a catalyst for intrastate frictions *and dramatical change of the future of warfare*: those technologies strengthen its insecurity connotations, enhancing the securitization spiral. In the same document, China is also regarded as an actor that is pursuing this type of development through the theft of intellectual properties via APTs, which appears in the list of threats in cyberspace for the first

time in this edition as state-sponsored attacks, which are supposedly applied to the Intelligentized warfare, deemed as a necessary policy to compete with the US.

In the 2022 document, the CMF is explicitly regarded as a catalyst of insecurity, hence gray-zone situations which require "*complex measures*". An example are the 2022 amendments to Japan's NSS, where active cyber defense is proposed as a solution to deceive and repel cyberespionage attacks and information warfare, which can be bolstered with the use of AI. Moreover, a stronger feeling of insecurity towards this policy is presented with the US Interim Guidance, which regards the theft of dual-technology data as a threat not only to the national but also to economic security. The US initiative is related to Japan assessing that eventual data leakages would *threaten* not only the US but also its allies. Moreover, the eventual response by China is posed as a counteraction to exacerbate the tensions in the environment, as stated in the outline. The level of threat of the CMF cements the grave attention that should be paid to the Intelligentized warfare, which mentions are more frequent due to its use during Pelosi's visit to Taiwan.

In the 2023 White Paper, there is a coherency of elements regarding CMF and Intelligentized Warfare, hereby defined as a *risk*, thanks to the emphasis conferred on cutting-edge technologies applied to warfare used as *a catalyst of interstate competition* and to the cyberattacks defined as *real threats*. Furthermore, the considerations by the UK and South Korea of China as a "*high-risk vendor*" or a "*threat*" to South Korea, which is rebuilding its supply chain without it.

4.3 Concluding Remarks

The 2019 White Paper provides the starting point, hence the common themes to all five White Papers: the state of *insecurity due to the change in the status quo* of the environment due to the technological military build-up based on dual technologies and hybrid warfare which hence threat the ontological security of Japan as a middle power – and the emphasis on the cyber diplomacy based on the free, fair and secure cyberspace (hence, the FOIP), However, the 2019 document presents basic definitions of cyber threats such as information warfare and an emphasizes the Huawei ban – mentioned 4 times (2 of them in connection with Australia) – which may indicate that the securitization spiral given by the dual technologies is not highly perceived or manifested.

Regarding the cyberattacks reported, the US is the most mentioned actor (28 references against the 4 of Australia and the 4 of Taiwan), coherent with the Chinese asymmetric threat perception, which could drive Japan to use the US attacks as an exemplification of the threat in cyberspace. The most recurrent cyberattack reported is the information theft, operationalized in the context of the BRI (i.e. forced transfer of technology) or state-sponsored attacks – i.e. APT, which is linked with the perception of economic security as the most mentioned contemporary issues related to cyberspace. This tight connection between the US, which is the most important Japan allied with which engages in frequent CBM measures, and cyber espionage reinforces the description of China as the greater cyber threat for the former actor, and in turn, also for its allies.

The CMF is the most frequently mentioned policy (8 times) and is defined as *a serious security concern* and is regarded to be brought up also through the export of 5G infrastructures, which are deemed a *concern* in the context of the Australian Huawei ban, and as a subject of attention in the box dedicated to this policy.

The 2020 White Paper provides an explicit image of China as a *disruptor of the status quo*, hence a menace to the environment essential to Japan. The description of its information warfare becomes more detailed, and it is connected with the COVID-19 pandemic, and regarded as a "*great concern*" as a clear demonstration that China is trying to create an international system favorable to itself.

Furthermore, this White Paper establishes a clear correlation between the APT and state involvement, emphasized by the fact that four out of five cyberattacks listed under the China column are of this nature and that the APT10 attack on Japan is treated separately from the one against the US. Indeed, the APT10 focused its actions on dual-use technology development firms, and the Paper poses this in connection with China's effort towards the CMF, which remains the most mentioned policy and is deemed as a contribution to the *dramatic change in the future of warfare*, hence deserving "*strong attention*", due to its effects on economic security. These features, along with the already existing public attribution, suggest a higher level of threat perception related to the dual-use security dilemma. The anxiety towards the Chinese warfare progress is reinforced by the report of statements of third actors involved, where Australia functions as an attributor of *concern* regarding China's ICT sector and the US to describe Chinese military rapid development as *alarming*. Their mention can function as an ulterior resource to enrich the "challenging image" repertoire of the transversal securitization of China.

The 2021 White Paper associates China with a more tense image of the security environment, with the grey-zone situation deemed as "*persistent*" due to hybrid warfare. This edition further explores China's information warfare, through the expedient of vaccine diplomacy – inherent to the COVID-19 code, a sub-code of the contemporary issues – efficiently pursued by China to damage the EU and US reputation. Moreover, also Australia is presented as a victim of Chinese cyberattacks (a DDoS), due to its request for a transparent investigation of COVID-19, consequentially emphasizing the image of China as a non-transparent actor that pursues coercive grey-zone initiatives against Japan's like-minded countries.

This reinforcement could be interpreted as the rationale for Japan for taking "*measures not limited to military ones*", probably alluding to the protection of its economic security, which also involves the secrecy of intellectual properties, a frequent target of progressively sophisticated cyberattacks.

The economic security-cyberespionage-China relation goes in parallel with the list of attacks associated with the actor in the document, where the espionage breaches accounted for five out of six cyberattacks.

The 2022 White Paper presents a more explicit securitizing language, as revealed by the description of China and Russia as countries "*forcibly changing the world order*" which Japan "*resolutely continues to oppose*", due to its necessities as a middle power. However, the countries are not presented as threats but rather as *unprecedented challenges* and a global issue, coherently with the theoretical framework. In the section of the White Paper regarding cyberspace, the transversal securitization is visible in the China-cyberespionage-economic security nexus: China is described as a country conducting cyber espionage for its national security agenda – e.g. CMF – while Japan's development of cutting-edge technologies (a vital instrument for social and economic stability) is threatened by this activity, exemplified by the APT10 attack, which has been a constant in the past editions.

Dual technologies are also a referent object to emphasize the threat to economic security, demonstrated by its frequency among the sub-codes of the contemporary issues across all the White Papers and its new dedicated section in this document. China's cyberespionage on dual-use technologies is also posed as a *threat* transposing the US interim guidance words, which considers any Washington information leakage as a threat to its allies. The US factor is also present in the Taiwan issue, which is exacerbated by the Sino-American frictions,

resulting in a sense of *crisis* that disrupts the stability of an area of regional and global importance.

Indeed, the Taiwan issue is the second most mentioned circumstance, and its NDR serves to address China as a "*very great threat*" in the case of cyber capabilities superiority. Taiwan NDR is also used to expose China's information and cognitive warfare strategies, with particular regard to the latter, since the 2022 Strait crisis was an occasion to observe this new conduct in action, which could be the probable reason for its major frequency of mentions in the document if compared to the CMF, the most recurrent policy so far.

The 2023 White Paper poses the US-China rivalry as the principal factor in insecurity in the actual "*era of crisis*", along with a lack of international leadership. As seen in the previous edition, the Taiwan issue functions as a theater for the exacerbation of this conflict, and its importance is highlighted by its frequent mentions (15 times in 2023, as opposed to the 7 of 2022) and its related special column where China is defined as "*a security threat in cyberspace*" as a consequence of the 2022 Strait crisis and frequent activities of cyber espionage. In fact, in this edition, the Taiwan issue is as mentioned as the economic security. If compared to the past document, the 2023 Paper presents a shorter list of cyberattacks conducted by China, but a higher heterogeneity of actors, with the DDoS on Taiwan's government website and the APT31, APT27 and APT30 espionage campaigns on the Belgian government. In particular the latter mentions a group that has previously targeted Japan (the APT31), one involved in governmental spyware (APT27), and another one involved in the South China Sea issue (APT30), allegedly to reinforce the idea of China as a global threat that concerns not only countries involved in the region but also other like-minded allies. Indeed, cyber espionage remains the most mentioned type of attack, however, contrary to the 2022 and 2021 editions, the major targets are state institutions, and the APT attacks are related to the aforementioned against the Belgian government, and the APT41 on the US, which also attacked Japanese companies in 2022 (Koike, 2022).

Furthermore, the UK is present in the section regarding economic security where its consideration of China as a *"high-risk vendor*" for 5G infrastructures is reported, and paired with the South Korean consideration of depending on an adversarial country for its supply chain as *a threat*, probably due to the possibility of dual-technology related information theft, which can be applied to the Chinese military development in light of the CMF policy.

6 Conclusions

This research examines Japan's shift from a defensive to an active cyber defense, as outlined in the 2022 National Security Strategy (NSS), in response to cyber threats from Russia and China. Despite these developments, Japan has not explicitly labeled China as a threat due to their complex historical, economic, and geographic ties, which could provoke retaliation. Academic studies on Sino-Japanese relations in the digital space have often focused on specific aspects, like the Huawei ban or the FOIP vs. BRI digital connectivity plans, without fully applying the securitization theory. This study, therefore, aims to trace Japan's evolving perception of China as a cyber threat, exploring how this perception develops in a domain increasingly critical to national security and civil society, without directly naming China as such.

Hence, Japan’s securitization moves have been analyzed by applying the transversal securitization theory on a qualitative and quantitative content analysis of the Defense White Papers from 2019 to 2023 to individuate the most represented cyberattacks, the most threatening Chinese policies in the domain and the contemporary issues related to them to provide an answer to the main research question: how has Japan transversely securitized China in cyberspace from 2019 to 2023?

As it emerged from the data, and coherently with the literature, it is possible to assert that Japan has transversely securitized China with an incremental approach, shifting from a cautious language in 2019 to a more explicit one in 2023, leveraging on the progressively wider repertoire of contemporary issues; focalizing on the information theft campaigns conducted by state-sponsored groups, particularly the ATP10, to highlight the illicit ways in which China procures intellectual properties and technologies to enhance its Intelligentized warfare through the CMF.

Those components create the idea of China as an insidious actor ready to invade the networks of countries promoting the liberal order and status quo to steal the latest developments with the intent of applying them to its army, to develop an unpredictable and ominous type of warfare that will destabilize the international equilibrium. The idea of threat is reinforced by the use of statements of third actors and by the report of attacks that have hit both itself and third actors, but it is likely to mention exclusively the damage suffered by those last ones.

The choice of content analysis – instead of a discourse examination – to apply the indirect securitization theory has facilitated the identification of those trends, shedding light on the incremental use of a stronger securitizing language and the instrumentalization of third actors' statements. Therefore, we can assess the validity of the content analysis method to study the process of transversal securitization. On top of that, a frequent use of "*crisis*" has emerged, a noun that does not appear in the challenge and threat markers reported in the Theoretical framework chapter, but it appears in those documents where it has been treated as a threat marker.

This thesis provided an articulation of the recent China threat in cyberspace, contributing to the understanding of this phenomenon, as well as to the analysis of the rationale behind Japan's shift from an exclusively defensive to an active cyber defense, providing the perspective of how middle powers shape the threat of the major ones with which they cannot enter into an open confrontation due to the eventual disruption of the status quo in which they thrive. This corroborates the findings of the academia exposed in the introduction and literature review, which however have been focused on the results of the threat, and not on its construction. Moreover, this thesis contributes to highlighting the negative shift in Sino-Japanese relations in the security field, which is buffered by the avoidance of harsh securitizing language, as demonstrated by data.

It should be addressed that the sole focus on the White Papers has allowed a broad understanding of the phenomenon in the domain. Further studies could focus on an integration of the 2018 and 2021 cybersecurity strategies 2022 NSS to provide a deeper image of the China threat, as well as how different narratives shape this discourse. Moreover, this research could function as a starting point for a comparative study of the securitization moves adopted by Japan on China and Russia, for an investigation on how the image provided in cyberspace might extend to other domains, or for a comparison of how other middle powers are building the threat of China in cyberspace.

References

ALLEA - All European Academies. (2023). The European Code of Conduct for Research Integrity, [e-book] DE: ALLEA - All European Academies, Available Online: https://doi.org/10.26356/ECoC [Accessed 17 August 2024]

Aoyama, R. (2024). Stability and Fragility in Japan-China Relations

APT10 GROUP. (2018). *FBI*, Available Online: https://www.fbi.gov/wanted/cyber/apt-10group

APT30. *Council of Foreign Relations*, Available Online: https://www.cfr.org/cyberoperations/apt-30

Balzacq, T. (ed.). (2010a). A Theory of Securitization: Origins, Core Assumptions, and Variants, in *Securitization Theory*, 0 edn, [e-book] Routledge, pp.15–44, Available Online: https://www.taylorfrancis.com/books/9781135246143/chapters/10.4324/9780203868508-8 [Accessed 17 August 2024]

Balzacq, T. (ed.). (2010b). Securitization Theory: How Security Problems Emerge and Dissolve, 0 edn, [e-book] Routledge, Available Online: https://www.taylorfrancis.com/books/9781135246143 [Accessed 18 August 2024]

Balzacq, T. (ed.). (2010c). The Limits of Spoken Words: From Meta-Narratives to Experiences of Security, in *Securitization Theory*, 0 edn, [e-book] Routledge, pp.108–129, Available Online: https://www.taylorfrancis.com/books/9781135246143/chapters/10.4324/9780203868508-13 [Accessed 17 August 2024]

Bartlett, B. (2020). Japan: An Exclusively Defense-Oriented Cyber Policy, *Asia Policy*, vol. 15, no. 2, pp.93–100

Bryman, A. (2012). Social Research Methods, 4th edn, London, England: Oxford University Press

Can, M. & Vieira, A. (2022). The Chinese Military-Civil Fusion Strategy: A State Action Theory Perspective, *The International Spectator*, vol. 57, no. 3, pp.85–10

Cavelty, M. D. (2020). Cybersecurity between Hypersecuritization and Technological Routine, in E. Tikk & M. Kerttunen (eds), *Routledge Handbook of International Cybersecurity*, 1st edn, [e-book] Routledge, pp.11–21, Available Online: https://www.taylorfrancis.com/books/9781351038898/chapters/10.4324/9781351038904-3 [Accessed 18 August 2024]

Cheung, T. M. (2018). The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities, *Journal of Cyber Policy*, vol. 3, no. 3, pp.306–326

China — Certain Measures on the Transfer of Technology. (2019). *World Trade Organisation*, Available Online: https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds549_e.htm

Chuang, Y. & Chang, Y.-T. Unveiling TeleBoyi: Chinese APT Group Targeting Critical Infrastructure Worldwide, *JpCERT*, Available Online: https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_8_yi-chin_yu-tung_en.pdf

Ciolan, I. M. (2014). DEFINING CYBERSECURITY AS THE SECURITY ISSUE OF THE TWENTY FIRST CENTURY. A CONSTRUCTIVIST APPROACH

Cognitive Warfare. *NATO*, Available Online: https://www.act.nato.int/activities/cognitivewarfare/

Craig, Anthony, and Brandon Valeriano. "Realism and Cyber Conflict: Security in the Digital Age," 2018.

Dell'Era, A. (2024). Securitizing Beijing through the Maritime Commons: The 'China Threat' and Japan's Security Discourse in the Abe Era, *The Pacific Review*, vol. 37, no. 1, pp.147–180

Direstra, R., Miller, C. & Moltrer Vanessa. (2020). Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives, *Internet Observatory Cyber Policy Center*

Eriksson, J. & Giacomello, G. (2014). International Relations, Cybersecurity, and Content Analysis: A Constructivist Approach, in M. Mayer, M. Carpes, & R. Knoblich (eds), *The Global Politics of Science and Technology - Vol. 2*, [e-book] Berlin, Heidelberg: Springer Berlin Heidelberg, pp.205–219, Available Online: https://link.springer.com/10.1007/978-3-642-55010-2_12 [Accessed 17 August 2024]

Eroukhmanoff, C. (2018). 'It's Not a Muslim Ban!' Indirect Speech Acts and the Securitization of Islam in the United States Post-9/11, *Global Discourse*, vol. 8, no. 1, pp.5–25

Euronews with AP. (2024). No Classified Information Leaked in Cyber Attack on Japan's Space Agency, Officials Say, *Euronews*, Available Online: https://www.euronews.com/next/2024/06/21/no-classified-information-leaked-in-cyberattack-on-japans-space-agency-officials-say

Extraordinary Press Conference by Foreign Minister KAMIKAWA Yoko. (2023). *MOFA*, Available Online: https://www.mofa.go.jp/press/kaiken/kaikenwe_000001_00015.html

Fenstermacher, L. H., Uzcha, D., Larson, K. G., Vitiello, C. A. & Shellman, S. M. (2023). New Perspectives on Cognitive Warfare, in L. L. Grewe, E. P. Blasch, & I. Kadar (eds), *Signal Processing, Sensor/Information Fusion, and Target Recognition XXXII*, Signal Processing, Sensor/Information Fusion, and Target Recognition XXXII, Orlando, United States, 14 June 2023, Orlando, United States: SPIE, p.19, Available Online: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/12547/2666777/Newperspectives-on-cognitive-warfare/10.1117/12.2666777.full [Accessed 17 August 2024]

Goodman, M. P. (n.d.). Strategic Ambivalence: Japan's Conflicted Response

Govella, K. (2020). Crafting Policy for Contested Commons: Insights from Japan's Approach to the Outer Space, Cyberspace, and Maritime Domains, *SSRN Electronic Journal*, [ejournal], Available Online: https://www.ssrn.com/abstract=3653615 [Accessed 17 August 2024]

Healey, J. & Jervis, R. (2020). The Escalation Inversion and Other Oddities of Situational Cyber Stability (Fall 2020), Available Online: https://repositories.lib.utexas.edu/handle/2152/83969 [Accessed 17 August 2024]

Heginbotham, E., Leiter, S. & Samuels, R. J. (2023). Pushing on an Open Door: Japan's Evolutionary Security Posture, *The Washington Quarterly*, vol. 46, no. 2, pp.47–67

Hsieh, H.-F. & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis, *Qualitative Health Research*, vol. 15, no. 9, pp.1277–1288

Hung, T.-C. & Hung, T.-W. (2022). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars, *Journal of Global Security Studies*, vol. 7, no. 4, p.ogac016

Japan (JPN) Export, Import and Trade Partners | The Observatory of Economic COmplexity. (2024). *OECD*, Available Online: https://oec.world/en/profile/country/jpn

Japan and China Trade | The Observatory of Economic Complexity. (2024). *OECD*, Available Online: https://oec.world/en/profile/bilateral-country/jpn/partner/chn

JAPAN THREAT LANDSCAPE. (2023). *Cyfirma*, Available Online: https://www.cyfirma.com/research/japan-threat-landscape/

Jiang, M. (2023). Chinese Cybersecurity Policies in the Age of Cyber Sovereignty, in M. Timoteo, B. Verri, & R. Nanni (eds), *Quo Vadis, Sovereignty?*, Vol. 154, [e-book] Cham: Springer Nature Switzerland, pp.77–90, Available Online: https://link.springer.com/10.1007/978-3-031-41566-1_5 [Accessed 17 August 2024]

Jiang, Min. "Chinese Cybersecurity Policies in the Age of Cyber Sovereignty." In *Quo Vadis, Sovereignty?*, edited by Marina Timoteo, Barbara Verri, and Riccardo Nanni, 154:77–90. Philosophical Studies Series. Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-41566-1_5.

Jiji. (2023). China's Imports of Japanese Fishery Products down 99% in October, *The Japan Times*, Available Online: https://www.japantimes.co.jp/news/2023/11/19/japan/politics/china-imports-down-october/

Jiji. (2024a). Japanese Government Skips Submitting Active Cyberdefense Bill, *The Japan Times*, Available Online: https://www.japantimes.co.jp/news/2024/05/01/japan/active-cyberdefense-bill-skipped/

Jiji. (2024b). Japan Eyes New Law to Introduce 'Active Cyberdefense', *The Japan Times*, Available Online: https://www.japantimes.co.jp/news/2024/07/20/japan/politics/activecyberdefense-law/

Katagiri, N. (2021). Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks, *Journal of Cybersecurity*, vol. 7, no. 1, p.tyab009

Katagiri, N. (2023). The Promise and Challenges of Launching Cyber-Military Strikes: Japan's 'Cross-Domain' Operational Concepts, *International Relations of the Asia-Pacific*, vol. 23, no. 2, pp.297–324

Kello, L. (2021). Cyber Legalism: Why It Fails and What to Do about It, *Journal of Cybersecurity*, vol. 7, no. 1, p.tyab014

Van Wie Davis, E. *Shadow Warfare: Cyberwar Policy in the United States, Russia, and China*. G - Reference,Information and Interdisciplinary Subjects Series. Rowman & Littlefield Publishing Group, Incorporated, 2021. https://books.google.it/books?id=sWDGzQEACAAJ.

Koike, R. (2022). Operation RestyLink: 日本企業を狙った標的型攻撃キャンペーン [Operation RestyLink: A Campaign of Targeted Cyber Attacks on Japanese Companies], *NTT Security Holdings*, Available Online: https://jp.security.ntt/tech_blog/102ho8o

Kono, K. (2017). International Laws on Cyber Attacks That Do Not Constitute an Armed Attack, [e-journal], Available Online: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.nids.mod.go.jp/english/publication/briefing/pdf/2017/briefing_e201710.pdf&ved=2ahUKEwjb86nG6PuHAxXezgIHHZtEMmwQFnoECBcQAQ&usg=AOvVaw3sauBjh-ONF-ZwZh2OYvCz

Krippendorff, K. (2019). Content Analysis: An Introduction to Its Methodology, [e-book] 2455 Teller Road, Thousand Oaks California 91320: SAGE Publications, Inc., Available Online: https://methods.sagepub.com/book/content-analysis-4e [Accessed 17 August 2024]

Krolikowski, A. & Hall, T. H. (2023a). Non-Decision Decisions in the Huawei 5G Dilemma: Policy in Japan, the UK, and Germany, *Japanese Journal of Political Science*, vol. 24, no. 2, pp.171–189

Krolikowski, A. & Hall, T. H. (2023b). Non-Decision Decisions in the Huawei 5G Dilemma: Policy in Japan, the UK, and Germany, *Japanese Journal of Political Science*, vol. 24, no. 2, pp.171–189

Lee, H. (2023). Public Attribution in the US Government: Implications for Diplomacy and Norms in Cyberspace, *Policy Design and Practice*, vol. 6, no. 2, pp.198–216

Lee, J.-Y., Han, E. & Zhu, K. (2022). Decoupling from China: How U.S. Asian Allies Responded to the Huawei Ban, *Australian Journal of International Affairs*, vol. 76, no. 5, pp.486–506

Lupovici, A. (2021). The Dual-Use Security Dilemma and the Social Construction of Insecurity, *Contemporary Security Policy*, vol. 42, no. 3, pp.257–285

Lupovici, A. (2023). Ontological Security, Cyber Technology, and States' Responses, *European Journal of International Relations*, vol. 29, no. 1, pp.153–178

Malachinski, P. (2023). Japan's Indo-Pacific Strategy in Cyberspace

Manantan, M. B. F. (2021). Advancing Cyber Diplomacy in the Asia Pacific: Japan and Australia, *Australian Journal of International Affairs*, vol. 75, no. 4, pp.432–459

Masaaki, Y. (2022). PLA's Intelligentized Warfare: The Politics on China's Military Strategy, vol. 2

Max Zenglein & Holzmann, A. (2019). EVOLVING MADE IN CHINA 2025 China's Industrial Policy in the Quest for Global Tech Leadership, *MERICS PAPERS ON CHINA*, vol. 8

Miao, J. (2021). Back to Strategic Competition? Assessing Japan's Emerging China Policy under the Suga Administration, *East Asian Policy*, vol. 13, no. 02, pp.93–107

Mirza, M. N., Ali, L. A. & Qaisrani, I. H. (2021). Conceptualising Cyber Sovereignty And Information Security: China's Image Of A Global Cyber Order, *Webology*, vol. 18, no. 5, pp.598–610

MOD. (2019). Defense of Japan, Available Online: https://www.mod.go.jp/en/publ/w_paper/wp_2019.html

MOD. (2020). Defense of Japan, Available Online: https://www.mod.go.jp/en/publ/w_paper/wp_2020.html

MOD. (2021). Defense of Japan, Available Online: https://www.mod.go.jp/en/publ/w_paper/wp_2021.html

MOD. (2022). Defense of Japan, Available Online: https://www.mod.go.jp/en/publ/w_paper/wp_2022.html

MOD. (2023). Defense of Japan, Available Online: https://www.mod.go.jp/en/publ/w_paper/wp_2023.html

MOFA. (2022). National Security Strategy of Japan, Available Online: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.mofa.go.jp/fp/nsp/page1we_000081.html&ved=2ahUKEwiTtNrZ9PuHAxV_xQIHHbVsOmcQFnoECBMQAQ&usg=AOvVaw2fGMapLhbmDGLrjbgPFfms

Moore, G. J. (2023). Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies, *Journal of Chinese Political Science*, vol. 28, no. 1, pp.151–167

Mochinaga, Dai. "The Expansion of China's Digital Silk Road and Japan's Response." *Asia Policy* 15, no. 1 (2020): 41–60.

Nakashima Ellen. (2023). China Hacked Japan's Sensitive Defense Networks, Officials Say, *The Washington Post*, Available Online: https://webcache.googleusercontent.com/search?q=cache:https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/

NISC. (2018). 2018 Cybersecurity Strategy

NISC. (2021). 2021 Cybersecurity Strategy

Nitta, Y. (2014). Review of the Japan Cybersecurity Strategy, no. 290

Nobukatsu, K. (2023). Reading Japan's National Security Strategy, *Asia-Pacific Review*, vol. 30, no. 1, pp.7–25

O'Shea, P. & Maslow, S. (2024). Rethinking Change in Japan's Security Policy: Punctuated Equilibrium Theory and Japan's Response to the Russian Invasion of Ukraine, *Policy Studies*, vol. 45, no. 3–4, pp.653–676

Ogawa, H. & Tsuchiya, M. (2021). Cybersecurity Governance in Japan

Oren Eitan & Brummer Matthew. (2020). How Japan Talks About Security Threats, *The Diplomat*, Available Online: https://web.archive.org/web/20240716164513/https://thediplomat.com/2020/08/howjapan-talks-about-security-threats/

Oren, E. & Brummer, M. (2020a). Threat Perception, Government Centralization, and Political Instrumentality in Abe Shinzo's Japan, *Australian Journal of International Affairs*, vol. 74, no. 6, pp.721–745

Oren, E. & Brummer, M. (2020b). Threat Perception, Government Centralization, and Political Instrumentality in Abe Shinzo's Japan, *Australian Journal of International Affairs*, vol. 74, no. 6, pp.721–745

Osawa, J. (2017). The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?, *Asia-Pacific Review*, vol. 24, no. 2, pp.113–131

Osawa, J. (2023a). How Japan Is Modernizing Its Cybersecurity Policy, *Stimson*, Available Online: https://www.stimson.org/2023/japan-cybersecurity-policy/

Osawa, J. (2023b). Direction of Japan's New Cybersecurity Policy, *Asia-Pacific Review*, vol.

30, no. 3, pp.63–78

Osawa, J. (2023c). How Japan Defines Economic Security

Paterson, T. & Hanley, L. (2020). Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes', *Australian Journal of International Affairs*, vol. 74, no. 4, pp.439–454

Press Conference by Chief Cabinet Secretary Matsuno (Nov. 29 - Morning). (2023). *Prime Minister's Office of Japan*, Available Online: https://japan.kantei.go.jp/tyoukanpress/202311/29_a.html

Press Conference by Foreign Minister KAMIKAWA Yoko. (2024). *MOFA*, Available Online: https://www.mofa.go.jp/press/kaiken/kaikenwe_000001_00069.html

Reuters. (2010). China Lifts Rare Earth Export Ban to Japan: Trader, Available Online: China lifts rare earth export ban to Japan: trader

Sahashi, R. (2020). Japan's Strategy amid US–China Confrontation, *China International Strategy Review*, vol. 2, no. 2, pp.232–245

Schia, Niels Nagelhus, and Lars Gjesvik. "China's Cyber Sovereignty." Norwegian Institute of International Affairs (NUPI), 2017. JSTOR. http://www.jstor.org/stable/resrep07952.

Singh, B. (2024). Front-Line Guardian of the Status Quo: Japan under the Kishida Government, *International Affairs*, vol. 100, no. 3, pp.1287–1301

Soesanto, S. (2020). A One-Sided Affair: Japan and the People's Republic of China in Cyberspace: Hotspot Analysis, ETH Zurich, p.40 p., Available Online: http://hdl.handle.net/20.500.11850/389371 [Accessed 17 August 2024]

Stritzel, H. (2014). Security in Translation, [e-book] London: Palgrave Macmillan UK, Available Online: http://link.springer.com/10.1057/9781137307576 [Accessed 17 August 2024]

Thumfart, J. (2022). The (Il)Legitimacy ofCybersecurity. An Applicationof Just Securitization Theoryto Cybersecurity Based Onthe Principle of Subsidiarity, *Applied Cybersecurity & Internet Governance*, vol. 1, no. 1, pp.1–24

Ukhanova, E. (2022). Cybersecurity and Cyber Defence Strategies of Japan, *SHS Web of Conferences*, vol. 134, p.00159

Ueki, Chikako Kawakatsu. “Japan’s China Strategy.” *Security Challenges* 16, no. 3 (2020): 58–63.

Vosse, W. (2024). Japan’s Gradual Shift from Passive to Active Cyber Defense: Evidence from the Domestic Discourse and International Cooperation:, *Études françaises de renseignement et de cyber*, vol. N° 2, no. 1, pp.89–106

Vuori, J. A. (2008a). Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders, *European Journal of International Relations*, vol. 14, no. 1, pp.65–99

Vuori, J. A. (2008b). Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders, *European Journal of International Relations*, vol. 14, no. 1, pp.65–99

Wilkinson, c. “The Limits of Spoken Words. From Meta-Narratives to Experiences of Security.” In *Securitization Theory: How Security Problems Emerge and Dissolve*, 2011. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.routledge.com/Securitization-Theory-How-Security-Problems-Emerge-and-Dissolve/Balzacq/p/book/9780415556286%3Fsrsltid%3DAfmBOooY4ubjDNzrMSoKOeCGVwTSWySEm4Ux579vPF8IFXHxsJ3SQR0P&ved=2ahUKEwiasdnj342JAxX6_rsIHbLeBKIQFnoECC4QAQ&usg=AOvVaw2VXUjxKG6B5xSUa9LNYbPG.

Wang, E. (2022). EU’S Paradigm Shift towards the Rise of China, no. 124

サイバー空間をめぐる脅威の情勢等 [State of Affairs Concerning Threats in Cyberspace]. (2024). *警察庁　[National Police Agency]*, Available Online: https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

Appendices

This section provides the materials used in the analysis: the first and second codebooks, their disposition on a yearly base, and the text query conditions to structure the transversal securitization of China in cyberspace. Regarding the codebooks: the codes in bold represent the principal ones where the sub-codes are indicated in a plain format.

Codebook I

This codebook is based on the Literature review chapter, precisely, on the section regarding Sino-Japanese relations from 2019 to 2023, Japan's cybersecurity evolution and China's internet policy and Japan's perception.

Name	Description
Securitization of the domain	
Threats to the general security environment	Threats whose application is also suitable for the cybersecurity domain (e.g. the subversion of the status quo can also entail the pursuit of information warfare, or it can also entail the transformation of the concept of warfare)
Threats to the cyber domain	Actions pursued in cyberspace that jeopardize the ontological, national, or economic security of Japan
Militarization of cyberspace	Description and organization of the cyber domain in function of cyberattacks and threats
China tech Policies	
Civil-Military Fusion (CMF)	Application of dual-use technology developed in the civil field to the military compartment
Internet sovereignty	*Promotion of state control and rule of law in cyberspace, to create an internet free from external interference*
Made in China 2025	Initiative aimed to boost the self-sufficiency competitivity of the Chinese high-tech industries, with regard of dual-technology development. It is also part of the chain of policies to assist the CMF

Belt and Road Initiative	International infrastructure development plan aimed to improve the connectivity capacity of its partners with accessible investments and loans. The digital counterpart is the Digital Silk Road, through which China promotes its standard for infrastructure management and Internet governance
Cyberattacks	
Cyber espionage	Illicit subtraction of information with espionage campaigns made by state, private and state-sponsored actors.
State-sponsored attacks	Attacks perpetrated by actors not directly associated with the PCC. This is the most used strategy by China for information theft and disruptive cyber attacks due to the existing loophole in international law
Distributed Denial Of Service (DDoS)	Disruption of the normal traffic of a server. It is one of the attacks for which the countermeasures have been strengthened by 2022 NDS
Attack on a Critical Infrastructure	Attack on an infrastructure critical for the day-to-day functioning of a country. Their categorization is based on the Cybersecurity Policy for Critical Infrastructure Protection
Cutting-edge technologies	
AI	It is one of the main technologies of which China is fostering development. It can be applied to IoT and Information Warfare
5G	5G infrastructures are at the center of the Huawei ban, however, their securitzation can go beyond that specific episode, or Japan can avoid to mention directly that company
Contemporary issues related	
Huawei Ban	Indirect ban of Huawei amid the Australian allegations of the company having installed backdoors for cyber espionage on their devices in 2019. This code, on the contrary of the 5G one, is applied only when the company is mentioned
Russian Invasion	The 2021 full-scale Russian invasion of Ukraine has been frequently used by Japan to securitize China's claim on Taiwan and its behavior in the South China Sea. Regarding cyberspace, the Russian invasion is an exemplification of the strategies employable in cyberspace in wartime by a country. In particular, Russian information warfare is explicitly mentioned in the 2022 NDS as a reason for establishing a multi-domain defense force and switching to an active cyber defense
Taiwan	Taiwan has been an indirect referent object of Japan's securitization move amid the Chinese claims on the islands. Moreover, its invasion could represent a disadvantageous change in the status quo and an open manifest commitment to the cause by Japan demonstrates an alignment to the US interests

Territorial disputes and the South China sea	As for Taiwan, the South China Sea is the indirect referent object of the securitization of the Russian invasion, moreover, there are already precedents of cyberattacks related to this contingency: in 2014 the Moafee and Dragon OK group targeted Japan and other countries that have interests in the South China seas, and in 2011 Chinese hacktivists launched a DDoS against Japan's national police agency in reaction to the purchase of the Senkaku islands by the Tokyo governor.
Economic Security	The 2022 NDS amendments relative to cyberspace revolve around the concept of economic security, which is ensured by the adoption fo an active cyberdefese. In particular, the application of the concept in cyberspace entails a stable supply of critical commodities, where the innovation of cutting-edge technology is supported and protected from intellectual property theft
Third actor involved	
The USA	The USA are not only crucial to Japan's defense (and cyberdefense) due to the issues surrounding article 9 of the Constitution, but they play also a decisive role in Sino-Japanese relations as the major threat from the Chinese perspective.
Russia	Russia and its full-scale invasion of Ukraine are the threatening factors at the base of the 2022 NDS, in particular, Japan regards Russia's invasion a dangerous precedent for any Chinese territorial claim in the Asian region and as a demonstration of the possible cyberwarfare techniques available at the moment to a state.

Codebook II

The following codebook has been developed after a further reading of the White Papers to eliminate or aggregate certain codes of the first codebook, and to insert the themes that emerged in the sections relative to cyberspace to provide better representations of the recurrent themes in the documents. This codebook is the definitive version taken as a departure point for the discourse analysis and for the thematical intersections shown in the Analysis chapter.

Name	Description
Securitization of the domain	Analysis of the threats in the domain according to Japan's perception. The selection criteria applied is the lack of any particular actor threatening this referent object.
General securitization move in the cyber domain	This code is generated from the union of the "Threats to the general security environment" and the "Threats to the cyber domain" and its aimed to present not only the existing threats in the cyberdomain but also how those behaviors impact the general security domain according to Japan's perception. The selection criteria applied are based on the definition of middle power presented in the literature review
Grey zone situations	This code describes a recurring theme that is jeopardizing Japan's security environment. Grey zone situations are actions that are not ascribable to peacetime or wartime, making hence difficult for the target country to address the situation with existing lawful solutions and leading it to take measures concerning non-traditional fields of security. In cyberspace, those grey actions might be state-sponsored cyberattacks on critical infrastructure, information warfare and other acts that allow the offender state to deny its involvement.
General stance on information warfare	Description of the challenges posed by information warfare to Japan and the general security environment without mentioning any particular actor.
Military build-up via dual-use technology in pursuit of hybrid warfare	Warfare upgrades of other countries induce insecurity on other actors, which according to Japan's perception, leads to inter-state competition. The insecurity is further exasperated by upgrades based on dual technologies which provide asymmetrical capabilities in pursuit of multidomain warfare.
China tech Policies	The code is formulated to answer the research question regarding the most threatening Chinese policy in cyberspace for Japan. As it has been noted cyberattacks are executed in

	pursuit of a strategy, furthermore the securitization of an actor can be also done with a contraposition of ideologies.
Civil-Military Fusion (CMF)	Application of dual-use technology developed in the civil field to the military compartment, part of the chain of policies through which China is boosting its military capabilities in a nonconventional way
Intelligentized Warfare	*Intelligentized Warfare entails the application of AI to military technology to improve the development of multi-domain warfare, with particular regard to cognitive warfare.*
Information and Cognitive Warfare	Although in the linear distribution of codes, they are separated, in the discussion cognitive warfare is associated with information warfare due to their similarities (e.g. misinformation and use of deep-fakes), and China's association of those two actions in the Three Warfare strategy, aimed to maintain individuals' perceptions to accomplish its strategic objectives
Informatization of The army	The informatization of the army is part of multi-domain warfare and it is executed by the PLA strategic support forces, who are in charge of outer space, cyberspace, and electronic warfare missions for intelligence support for all military forces
Holistic view of National Security	The holistic view of national security extends security to non-traditional domain such as economic security, cybersecurity, and energy security, but also to cultural security, which is emphasized in the description of the concept by Japan and described as "control and surveillance over the masses using ICT technologies"
Cyberattacks	
	China is regarded as an actor actively targeting Japan with its cyberattacks. Understanding which ones are mentioned in the White Papers helps to understand which breach has been the most significant for Japan
Cyber espionage	Illicit subtraction of information with espionage campaigns made by state, private and state-sponsored actors.
State-sponsored attacks	Attacks perpetrated by actors not directly associated with the PCC. This is the most used strategy by China for information theft and disruptive cyberattacks due to the existing loophole in international law, falling into the description of grey zone situation
Distributed Denial Of Service (DDoS)	Disruption of the normal traffic of a server and consequentially its functioning. It is one of the attacks for which the countermeasures have been strengthened by 2022 NDS

Attack on a Critical Infrastructure	Attack on an infrastructure critical for the day-to-day functioning of a country. Their categorization is based on the Cybersecurity Policy for Critical Infrastructure Protection
Advanced Persistent Threat (APT)	APTs are actors who conduct large-scale intrusions for specific goals, usually espionage, information theft or network disruption. APTs usually gain access to networks installing malware through social engineering or human intelligence and conduct operations for an extended period of time while remaining undetected. This period may vary and according to Fire Eyes is no less than 70 days, and in the attacks reported by Japan it usually encompasses a discrete number of years
Attack targeting Japan	It has emerged that Japan preferably avoids mentioning attacks that have involved it in the first-person, therefore the mention of these attacks is a significant element for the analysis of its securitization moves
State institution targeted	The choice of distinguishing the type of institution targeted helps the analysis to understand which are the most cited referent objects draw possible connections with relevant contemporary issues and provides further clues on Japan's threat perception
Private institution targeted	

Cutting-edge technologies

	Cutting-edge technologies are salient features of the contemporary military build-up. Since this research conceptualizes cyberspace as the integration of software, data, user activities, hardware, and critical infrastructures, the selection of cutting-edge technologies is limited to those that use cyberspace as their functioning infrastructure.
AI	It is one of the main technologies that China is fostering its development. It can be applied to IoT for Intelligentized or Information Warfare to accelerate the decision making thanks to its rapid access and operationalization of cloud databases
5G	5G infrastructures are at the center of the Huawei ban, however, their securitization can go beyond that specific episode, or Japan can avoid mentioning directly that the company. 5G infrastructure boosts the traffic capacity, hence the network efficiency. The application criteria for this code are the mention of the 5G technology, regardless of the presence of the Huawei case in the same paragraph.
Internet of things (IoT)	Devices equipped with sensors and software interconnected to a network to which they share real-time data. Their equipment with AI is at the center of Intelligentized warfare

Contemporary issues related

	This code has been created to answer the research question regarding the major contemporary issues related to the securitization of China in cyberspace.
Huawei Ban	Indirect ban of Huawei amid the Australian allegations of the company having installed backdoors for cyber espionage on their devices in 2019. This code, contrary to the 5G one, is applied only when the company is mentioned
Economic Security	Economic security, as defined in the Economic Security Promotion Act of 2022, consists of securitizing the stable supply of critical commodities, ensuring the safety of key infrastructures, supporting the development of cutting-edge technologies, and protecting their intellectual property
Taiwan	Taiwan has been an indirect referent object of Japan's securitization move amid the Chinese claims on the islands. Moreover, its invasion could represent a disadvantageous change in the status quo and an open manifest commitment to the cause by Japan demonstrates an alignment with the US interests
Territorial disputes and South China sea	As for Taiwan, the South China Sea is the indirect referent object of the securitization of the Russian invasion, moreover, there are already precedents of cyberattacks related to this contingency: in 2014 the Moafee and Dragon OK group targeted Japan and other countries that have interests in the South China seas, and in 2011 Chinese hacktivists launched a DDoS against Japan's national police agency in reaction to the purchase of the Senkaku islands by the Tokyo governor.
Covid-19	COVID-19 is particularly associated with China's information warfare and associated with countries that are "creating an international order more preferable to themselves"
BRI or Foreign Direct Investment (FDI) as a tool for technological acquisition	This code comes from the union of the BRI and the Made in China 2025 one since the White Papers tend to mention especially the former, while other projects are referred to under the umbrella term of foreign direct investments. BRI is an international infrastructure development plan aimed at improving the connectivity capacity of its partners with accessible investments and loans. The digital counterpart is the Digital Silk Road, through which China promotes its standard for infrastructure management and Internet governance
Third actor involved	
	It has been noticed by the second qualitative analysis that Japan preferably mentions cyberattacks on third countries. Understanding who they are helps to provide a perspective on Japan's alliance and on the contemporary issues related to the securitization of China in cyberspace. Russia is treated as a subcode although is not an allied.
The US	The USA is not only crucial to Japan's defense (and cyberdefense) due to the issues surrounding article 9 of the Constitution, but they play also a

	decisive role in Sino-Japanese relations as the major threat from the Chinese perspective.
Russia	Russia and its full-scale invasion of Ukraine are the threatening factors at the base of the 2022 NDS, in particular, Japan regards Russia's invasion a dangerous precedent for any Chinese territorial claim in the Asian region and as a demonstration of the possible cyber warfare techniques available at the moment to a state
The EU	The EU is a like-minded partner of Japan which has started to become increasingly involved in the region after the 2021 Indo-Pacific strategy. The code has been used as an umbrella term for all the EU countries and the UK since Japan still presents the two entities as correlated
Australia	Australia is regarded as a strategic partner due to its relevance in the region and its intense and positive bilateral relationships. Japan regards Australia as its most important ally after the US

Distribution of the codes throughout the years

This Charter has been used for the quantitative analysis of trends both in the perspective of the single documents and in the perspective of the timeframe of the case study.

Securitization of the domain

	A : DOJ2019_Full	B : 2020 Defense white pa...	C : 2021Defense white pa...	D : 2022 Defense white p...	E : Defence withe paper
1 : General securtizing mo...	4	3	5	5	11
2 : Grey-zone situations	1	2	1	4	3
3 : Information warfare ge...	2	0	0	2	5
4 : military build-up, hybrid...	5	6	7	12	6

China tech policies

	A : DOJ2019_Full	B : 2020 Defense white pa...	C : 2021Defense white pa...	D : 2022 Defense white p...	E : Defence withe paper
1 : Civil-military fusion	8	7	4	9	11
2 : Intelligentized Warfare	4	5	4	13	13
3 : Information Warfare	0	1	1	7	7
4 : Cognitive warfare	2	1	2	12	9
5 : Informatization of the A...	7	8	5	6	6

Cyberattacks

	A : DOJ2019_Full	B : 2020 Defense white pa...	C : 2021Defense white pa...	D : 2022 Defense white p...	E : Defence withe paper 2...
1 : Cyberespionage inform...	7	9	11	12	8
2 : State-sponsored attack	4	4	6	6	5
3 : DDoS	0	0	1	0	1
4 : Critical infrastrucure att...	0	1	2	4	4
5 : APT	2	3	2	0	2
6 : Japan targeted cyberat...	1	1	4	3	0
7 : State institution targeted	2	1	2	1	2
8 : Private insitution target...	1	2	4	5	1

Cutting-edge technologies

	A : DOJ2019_Full	B : 2020 Defense white pa...	C : 2021Defense white pa...	D : 2022 Defense white p...	E : Defence withe paper 2...
1 : AI	7	8	5	6	6
2 : 5G	3	3	5	4	4
3 : IoT	1	1	5	8	11

Contemporary issues

	A : DOJ2019_Full	B : 2020 Defense white pa...	C : 2021Defense white pa...	D : 2022 Defense white p...	E : Defence withe paper 2...
1 : Huawei ban	4	2	4	1	2
2 : Economic Security	4	3	7	13	15
3 : Taiwan	1	2	0	8	15
4 : Disputed Territories be...	0	0	2	3	1
5 : COVID 19	0	1	2	2	0
6 : BRI or FDI as tool to ac...	2	2	1	2	1

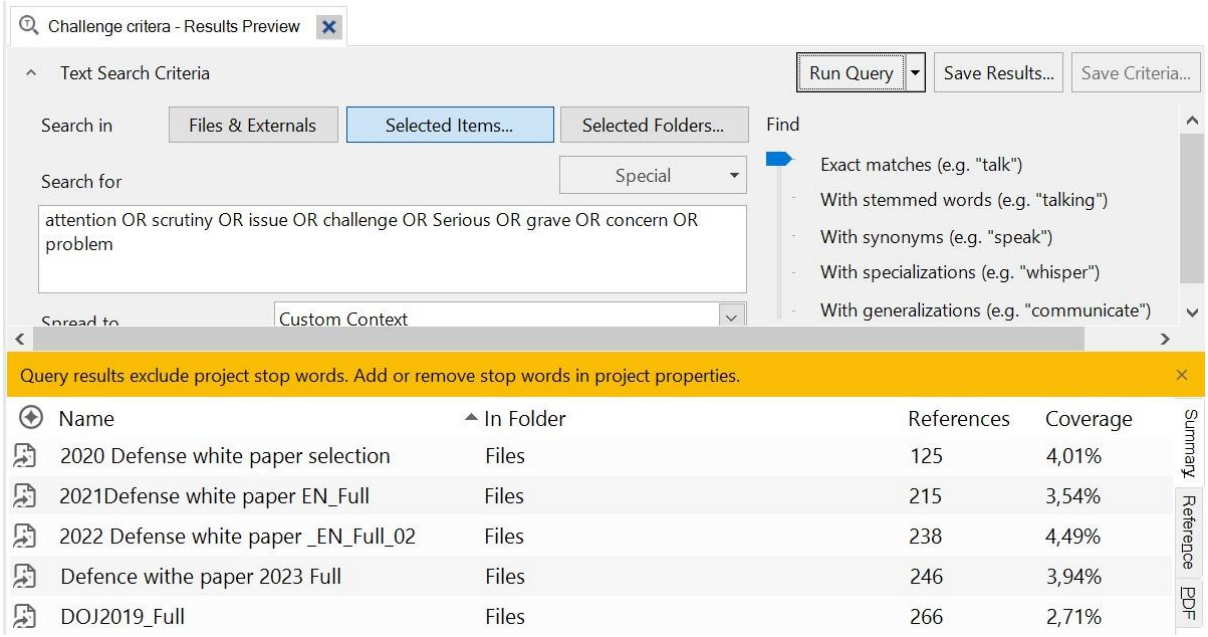
Third actor involved

	A : DOJ2019_Full	B : 2020 Defense white pa...	C : 2021Defense white pa...	D : 2022 Defense white p...	E : Defence withe paper 2...
1 : US vs. China	9	8	9	22	16
2 : Russia and China	7	5	7	4	7
3 : EU vs China	0	1	1	1	5
4 : Australia vs China	2	3	3	3	1

Query criteria

The transversal securitization theory discerns between threats and challenges through the markers reported in the chapter regarding the Theoretical Framework. This section presents the transposition of the markers in the query criteria used during the analysis with Nvivo. The customized context is the same adopted for the isolation of the content: the paragraph.

Challenge query criteria



Threat query criteria