Artificial Intelligence: The EU's response to China's rising influence

How does the European Union face a Security Dilemma in response to China's Artificial Intelligence ambitions?

Harvey James Mantock

Department of Global Politics Studies, Malmö University
Bachelor of Arts – European Studies
14 ECTS
Spring 2024
Supervisor: Inge Eriksson

1. Abstract

The purpose of this research is to investigate the question: How does the EU face a security dilemma in response to China's AI ambitions? The thesis explores the theory of the security dilemma associated with neorealist/structural realist approaches as it aims to predict the behaviour of states in an international anarchic system. The pace of the AI race and its applications in military use contribute to a rising security threat because Europe is lagging China and US in its strategy to become a global leader in AI. Growing tensions globally, including the war in Ukraine, together with a backdrop of deteriorating diplomatic relations with China bring political urgency to Europe's security dilemma. The exclusion of AI for military use from the scope of the AIA implies a lack of EU-wide legal and ethical provisions for military use of AI. Member States will inevitably adopt different approaches leading to inefficiencies and divergences in oversight. Europe should develop a framework for accommodating dual-use and military AI for defensive and offensive objectives. With a risk of member states adopting different positions, the Commission is likely to introduce a new post for a Defence Commissioner to respond to the unfolding security dilemma. European security dilemma risk mitigation includes establishing a competitive AI ecosystem within meaningful timelines, extending the development of foreign policy that accommodates response to security threats from innovative AI-led military developments in other states, and greater collaboration with US and China to influence future standards for use of autonomous weapons system and digital security.

Keywords: European Union, China, Artificial Intelligence, Anarchy, Neorealism, Security Dilemma, Cybersecurity, Lethal Automated Weapon Systems, Defence

Contents

2. List of Abbreviations

AI	Artificial Intelligence
AIA	Artificial Intelligence Act
AIDP	Artificial Intelligence Development Plan
AWS	Automated Weapons System
CFSP	Common Foreign and Security Policy
CPC	Communist Party of China
DDoS	Distributed denial-of-service
EC	European Commission
EDF	European Defence Fund
ESDP	European Security and Defence Policy
EU	European Union
ICBM	Intercontinental Ballistic Missiles
IR	International Relations
LAWS	Lethal Automated Weapons System
MAIL	Model Artificial Intelligence Law
NATO	North Atlantic Treaty Organization
PLA	People’s Liberation Army
PRC	People’s Republic of China
R&D	Research & Development
US	United States
USSR	The Union of Soviet Socialist Republics

3. Introduction

Innovation in Artificial Intelligence (AI) in the last decade has changed many aspects of our private and public lives. Governments are embracing AI in areas of education, healthcare, communication, security, and defence. According to some authors, competition for AI innovation in the defence industry has been escalating, reflecting similarities to the Cold War's nuclear arms dynamics. This is illustrated by the aggressive pursuit of AI advantages by US and China for military purposes(Stokes, 2023). Even if the status of an arms race is questionable(Scharre, 2021), military competition in AI is certainly fuelling unprecedented investment in AI applications and innovation in defence.

China is increasingly committed to AI innovation in its defence sector, with goals to be a "world-class military" by the mid-century(Stokes, 2023). The Chinese government and specifically the Communist Party of China (CPC) has committed to initiatives including the New Artificial Intelligence Development Plan (AIDP) (2017). A comprehensive policy document outlining China's goals, with the purpose for China to be the global technological leader in AI-led military capability by 2030(Khanal, 2024; Webster, 2017). Particularly in AI theory, technology, and application. Government-funded programs and private sector projects are supported by billions of dollars investment by the CPC to support this goal(Khanal, 2024). The US has similar initiatives and policies on AI, supporting a US-led competitive and strategic edge in the form of the American AI initiative. This was initiated under the Trump administration in February 2019, with goals to strengthen and reinforce American leadership in AI with the recognition of the significant importance of AI in the economics and security sectors(*Artificial Intelligence for the American People, US White House, 2021*, 2021).

When it comes to the AI race generally, the EU lags behind China and the US (Castro, 2021). A report by the European Court of Auditors has raised grave concerns about the lack of EU development in an AI ecosystem associated with an enormous gap in funding, thus challenging the EU's ambition to be recognized as a global leader in cutting-edge, ethical, and secure AI("Artificial Intelligence: EU Must Pick Up The Pace," 2024). From 2018 to 2023 the EU spent €32.5 billion in AI companies(*AI Investment: EU and Global Indicators*, 2024) but the investment gap between US and

EU is €10 billion . Some of these EU funds are allocated via the European Defence Fund (EDF), which received €8 billion ("Artificial Intelligence: EU Must Pick Up The Pace," 2024) for the period 2021-2027 for the purpose for research and development of military material(Akkerman, 2022). The objective of this R&D budget is to develop new weaponry with integration of AI into existing armaments or develop entirely new weapons with technological improvements including Generative AI, which can be used to enhance targeting systems or have more capable unmanned drone systems. With the existence and allocation of funds placed by the EU for research purposes and defence, there is willingness for Europe to participate in the AI arms race(Akkerman, 2022). But the dominance of the US and China indicates the emergence of a globally asymmetric AI ecosystem that minimises European priorities and could lead to enormous concerns for Europe. This phenomenon has its basis in the Security Dilemma theory discussed in detail within this thesis. Europe is mindful of the direct and indirect as well as purposeful and inadvertent threats that will inevitably emerge with the weaponizing of AI in other regions. The security strategy needs to evolve to include innovative AI technologies and to mitigate the risks that are foreseen by experts. Within the global anarchic system, Europe needs to understand the impacts of its under-developed AI ecosystem as it relates to defence and security, a growing concern that has been brought to our attention with a progressively deteriorating relationship with China, challenging its ambitions for AI in security.

Why does Europe need to respond to China's ambition for autonomous weapons systems? These technologies have unlimited potential for catastrophic impact(Hendrycks, 2023). While Europe seeks cooperation with China, China's diplomatic commitments to EU values are not entirely matched by its alleged continued development of lethal autonomous weapons systems (LAWS), nor its record of indifference to cyberattacks on EU infrastructure, perpetuated by individuals or entities from mainland China.

With these geopolitical dynamics in mind, the current climate of tensions in middle east, the ongoing war in Ukraine, this thesis is a timely opportunity to explore the urgency for increased EU investment and clear strategy in maintaining defence capabilities fit for attack by AI-assisted warfare. Given China's ambiguous framework of ethical AI development and their ambitious objective to lead innovation in AI

military platforms, the assessment of threat from autonomous weapons systems (AWS) via China is necessary for the EU's future security. The thesis provides a critical review of the gaps in Europe's defence systems in the wake of President Trump's criticism of EU's lack of investment in military capabilities and the increased focus on competition with China.

Leaning on realism theories, the EU's dependence on deterrence is discussed in the wake of innovative autonomous platforms for which frameworks are not yet in place to comply with established rules of war or AI competition. The novelty of this subject is that the future security of Europe is rarely viewed through a Realist/Neorealist perspective for future advances in AI-led technologies.

As shifts in the balance of power and international relations between global actors lead to new tensions, Realist perspectives may help explain the dynamics of the arms race. But is this framework still relevant for the disruptive potential of AI in future security and war strategies?(Glaser, 2011) Robert Jervis, an American political scientist and a prominent figure in International Relations theory was renowned for elaborating on concepts such as the Security Dilemma(Jervis, 1978). The latter stipulated that nations operate within an anarchic system, prone to phenomena escalation due to perceptions of threats, which contribute to arms race. The goal of states is to be technologically superior to their perceived adversaries. His thinking was reflective of a time period rooted in the Cold War, and the nuclear arms race between the US and USSR. In my research I find that authors who have written extensively about the AI arms race between the US and China, increasingly minimise the potential for Europe to compete. Military competition in AI is certainly fuelling unprecedented investment in AI applications in defence(Scharre, 2021) and Europe is lagging behind(Castro, 2021).

The theories of Herz and Jervis, articulated via the Security Dilemma are the basis of the theoretical research for this thesis(Herz, 1950). Reports encountered in this research indicate the EU's strength in AI innovation is in the development of a regulatory approach. The driver of EU's action and achievement in the AI field is largely expressed via legislation and ethics, while under-achieving as an innovative and competitive actor in a globally competitive anarchic system. The EU introduced the AI Act (AIA) in 2024("Regulation (EU) 2024/1689," 2024). The AIA is not intended to

cover the defence sector, and we must look elsewhere for a developing vision for the role of AI in Europe's defence strategy. Indeed, the exclusion of security and military application of AI from the AIA provides hope and opportunity that the EC will ensure strategy together with budget to accelerate the contribution of ethical AI innovation in the continued development of defence strategy.

China's AI legislation is not far behind. A proposed Model AI Law (MAIL), known as the China Model Law has been drafted by the Chinese Academy of Social Sciences(Zhu, 2024). The spirit of China's planned legislation is enthusiasm for technological advancement and sustainable AI development while maintaining a firm line on risk mitigation and safety.

Aside from the common purposes that each region's legislation aims to fulfill, the backdrop of rising deterioration in the EU-China relationship is noteworthy, and this deterioration inevitably spills over into the sectors of AI and defence. According to EU Parliament reports(*EU-China relations*, 2022), the EU interprets China's ambitions in AI to be that of a competitor and hopes for cooperation as a partner in the development of AI.

With current reports of Europe's failings in AI innovation, conflicts in various regions, the subject of this thesis is timely and is explored with the research question: How does the European Union face a Security Dilemma in response to China's Artificial Intelligence ambitions? The response is multi-dimensional and provides opportunity for further research for practical solutions to mitigate risk to Europe's security strategy.

4. Literature Review and Theoretical Discussion

The Origins and evolution of Theories as a basis for the Security Dilemma

"The Security Dilemma is a situation in which actions by a state intended to heighten its security, such as increasing its military strength to making alliances, can lead other states to respond with similar measures, producing increased tensions that create conflict, even when no side really desires it"(Herz, 1950). This quote exemplifies the foundations and tenants of realism, later followed by neorealism. Realism focuses on the emphasises on the conflictual sides and the competitiveness of international relations.

Within this understanding of world affairs, states primarily act out of self-interest, and prioritise maximisation of their power through security. The key proponent of this thinking was Hans Morgentahu, a 20th century political scientist, who believed that humans have a natural urge to dominate others, or what he described as Animus Dominandi(Solomon, 2012). This was later followed by Neorealism or Structural Realism as defined by Kenneth Waltz in his book 'Theory of International Politics'(Waltz, 1979), in which he set himself apart from classical realism by emphasising that the anarchic nature of the international system is the main cause for states seeking power maximisation and not the inherent desire of human nature to dominate and be on top.

In the anarchic system, systemic pressures on global actors incentivizes them to pursue security enhancements out of fear of being outpaced by potential rivals. A historical example of this would be the arms race between the United States and the Soviet Union during the Cold War, which is the period in which many of these political scientists conceptualised these theories. Offshoots of Neorealism include Defensive Realism also elaborated by Waltz and Walt in the 1980s, which suggests that nations primary concern is maintenance of their own security rather than the maximising of power(Lobell, 2017). Walt explains that the Defensive Realist school of thought always incorporates the Security Dilemma, as states seek to maintain their security rather than maximising power, thus defending themselves in face of security risks that are constantly changing in the anarchic system of international affairs. This is in stark contrast to proponents of Offensive Realism, advocated by political scientists such as

John Mearsheimer, who whilst similarly acknowledging the Security Dilemma, argues that states are inherently aggressive and seek power maximisation, in order to achieve or maintain global hegemony(Mearsheimer, 2001). All of these schools of thought take into account the Security Dilemma, which arises when a state's increase in military innovation causes another state's insecurity, which in turn fuels an arms race or conflict(Herz, 1950; Jervis, 1978). As a hypothetical example: If Country A develops 500 ICBMs (Intercontinental Ballistic Missiles), Country B is likely to view this as a disadvantage and a security hazard to its own safety. It will respond by developing 600 ICBMs of its own to respond to a perceived security risk and keep an edge over Country A. This illustration, although simplistic, reflects the logic of the Security Dilemma. However, each school of thought, while all commonly sharing the concept of Security Dilemma have a different emphasis and interpretations in their approach.

The AI revolution and its potential for autonomous warfare as key subjects for this thesis justify the application of security dilemma theory to support the perceived threat and inevitable responses that Europe needs to consider given China's ambitions and achievements in these military objectives.

Realism and Neorealism

Classical Realism theories expressed by Herz and Morgentahu, emphasises on the nature of human beings and power politics, which fuels the anarchic system, and thus competition, leading to a Security Dilemma(Herz, 1950; Williams, 2004). Neorealists such as Waltz and Walt highlight that the anarchic structure of the international system forces states to work on matters of security, to mitigate risk of being at a disadvantage to potential rivals, forcing them to investment in security, as a response to a heightened Security Dilemma(Lobell, 2017).

Neorealists deviate into Defensive and Offensive Realism, both of which rely on the Security Dilemma, but explain the phenomenon through different understandings: Defensive as the name implies bases security on Defence posturing and maintenance, whereas Offensive stresses power maximisation and aggressive behaviour. The Security Dilemma is a crucial mechanism in understanding how states navigate an anarchic system, and this concept is particularly useful when analysing the resulting tensions or potential tensions that can emerge, even from Defensive posturing.

This is relevant in the context of a deterioration in the EU-China relationship – the indifference shown by China when called to take greater responsibility for cyberattacks from China mainland on European government and commercial targets. Many such targets are attributable to groups with some links to Chinese government. The attacks represent offensive posturing which Europe finds increasingly problematic as a security risk.

Anarchic System

The Security Dilemma theory is often attributed to Jervis through his work 'Cooperation under a Security Dilemma'. He elaborates that in the anarchic system, as there is no central authority or international institution capable of wielding a monopoly of violence on a would-be aggressor, states are forced to work around a logic of self-help, survival, and security. Jervis' stances are grounded in neorealist and defensive realist traditions which argue that states are bound to the structure of the international system, under which they operate in a logic of defence and contrary to logic found with offensive realists. According to Jervis, states ought to maximise their own security and not seek to maximise power. The international system provides incentives for states not to engage in acts of aggression, out of fear that it might cause coalitions threatening the aggressive state. However, paradoxically he also acknowledges that the Security Dilemma also leads to an escalation of state arms race, since one country might perceive another country's self-security as an act of aggression. This phenomenon is highlighted by Jervis in multiple historical examples such as WW1 and the armament race between European powers, using the example of the United Kingdom and Germany, reflective of the time period of his analysis, the Cold War and the nuclear arms(Jervis, 1978).

Offence-Defence Differentiation

Jervis also wrote about the Offense-Defence differentiation, a concept which fits into the Security Dilemma, because if states successfully demonstrate their new weaponry developments are intended for defensive and offensive purposes, then the Security Dilemma is stable. However, if the Offense-Defence differentiation becomes indistinguishable, other states will assume the worst, leading to heightened tension and security dilemma. The interpretation and perceptions of threats plays an important role

in shaping security dilemma(Jervis, 1978). Successfully managing interpretation of defence development as a non-offensive milestone, can encourage greater diplomacy-building, transparency and communication leading to cooperation. This is the objective of Europe in the EU-China strategic plan to which Europe is committed (*EU-China - A Strategic Outlook*, 2019)

Jervis further elaborates by working on his four worlds in Offence-Defence (extract, Section IV. Four Worlds, page 211(Jervis, 1978)):

	Offence has the advantage	Defence has the advantage
Offensive Posture not distinguishable from Defensive One	1. Doubly dangerous	2. Security dilemma, but security requirements may be compatible
Offensive Posture distinguishable from Defensive One	3. No security dilemma, but aggression possible. Status Quo states can follow different policy than aggressors. Warning given.	4. Doubly stable

He describes how offence and defence posturing differ according to the circumstance of the Security Dilemma in question, as described by his Four Worlds where in either Offense or Defence has an advantage. This is a key component of the security dilemma, as it dictates which stance states are more likely to adopt for their survival: an offensive stance implies that aggressive postures have the advantage and may include a pre-emptive strike. On the other hand, states may feel that enhancement of their security is best served by defensive posturing.

These theories provide relevant context to the research question, as the EU like any other major international actor seeks security and survival within the international anarchic system. However, in an age of an increasingly complex and technologically advanced global landscape, China's ambitions for AI in defence must be considered by Europe as potentially threatening, not because of an inherent or direct threat coming from China, but because of the wider use of AWS by trading partners of China with all the implications that might entail and power asymmetry that may emerge to Europe's disadvantage.

International Relations Theory and Impact on the Balance of Power

This section includes presentation of some concepts relating to the place of AI in international relations (IR). IR theory is an ever-evolving field and no doubt, AI provides new dimensions. Notably the substantial advances in the fields of computer processing, big data and machine learning have all sparked interest and investment by global leaders in AI (Arsenault & Kreps, 2024). In the case of our research question : defence, cybersecurity and weapons development are subject to monumental revolution with advances in AI.(Arsenault & Kreps, 2024). This has potential implications on international relations as AI is described as a "world-transforming development"(Arsenault & Kreps, 2024).

In *Artificial Intelligence and International Relations Theories (Ndzendze & Marwala, 2023)* (Chapter: AI and IR), applications of various theories such as Realism, Liberalism, Constructivism and Dependence Theory are explored using these theories with the development of AI in IR. They first make note of the fact that scientific development and technology have always been at the forefront in global politics. Referring to historical examples such as the Cold War between scientific achievements and the race towards technological superiority, illustrated by events such as the USSR's achievements with the launch of first person in space, Yuri Gagarin, or Sputnik I, the first satellite into space. These technological milestones exacerbated US anxieties and led them to send a man to the moon, in order to convey a message or "signalling" to the Soviets that US still had a technical advantage in this period of intense rivalry.

Similarly with AI, scholars have made comparisons of competition between the US and China in current events, and the implications this has for global power and the balance of power around the world. Technological innovations and the politicisation of emerging technologies (sometimes called technopolitics) are not unique to AI and have semblance with other historical events(Arsenault & Kreps, 2024). In their chapter on Realism (Realism and AI(Ndzendze & Marwala, 2023)), several meaningful points for AI in the Offense-Defence calculus are presented with the understanding of AI as a valuable instrument for economic and military power. Thus, developing disruptive AI solutions in the defence sector fits with Realism theories, since Realists claim that states

are ultimately motivated by power and relative gain over one another(Arsenault & Kreps, 2024).

The perception of AI as a balance-shifting technology increases a state's interests in pursuing these relative gains, as is the case currently between the US and China(Arsenault & Kreps, 2024; Castro, 2021). They perceive that AI innovation and status of AI advancement represents a balance of power in their favour, perhaps assessed by the number of AI patents they have, and the technologies they export relative to their rivals.

The EU as a Global Actor and Arguing for a Neorealist perspective

The introduction of Security Dilemma theories in this thesis suggests that the EU operates in a neorealist framework. Neorealism theory emphasises survival and security while operating in an anarchic system. Furthermore, the EU's multilateralism, institutional nature and complex internal structure of various member states makes the use of neorealism challenging to capture the decision-making processes and policies of the EU. This reminds us of a famous quote attributed to Henry Kissinger: "Who do I call if I want to call Europe?"(Gera, 2012). This rhetorically speaks to the problem that the EU's complexity makes it difficult for the EU to provide a unified response on matters of foreign policy.

The EU actively works on building and sustaining the cooperative international order through its multilateral institutions (e.g., European Commission, European Parliament etc.) cooperating with other institutions such as the United Nations or the World Trade Organization. This cooperative approach is more in line with liberal and constructivist approaches. It must be also stated that neorealism also utilises the analysis of shifts in global power (e.g., the rise of China for example) to understand the perspective of states responding to such shifts.

The EU's different role of being something "Other" than a traditional power such as China or how the USA is studied and viewed through lenses such as the EU as Normative power, conceptualised by Ian Manners(Manners, 2002). This underlines the EU's role based on how it approaches international relations and shaping global power through governance and norms. For instance, its interaction with China involves

dialogues on human rights (*China: 39th Human Rights Dialogue with the European Union Took Place in Chongqing*, 2024). The neorealist thought process gives limited insights on these matters as they deal with the role of norms, ideas and identity, all of which are central to the EU's external actions.

However, neorealism or structural realism can provide some valuable insights into the EU's behaviour and interactions with other world powers, such as China. In an article entitled Return of the Jedi: Realism and the study of the European Union, by Sten Rynning critiques the perception that Realism is too simplistic or "outdated" in order to grasp the EU's role as a global actor or in its stance on foreign policy(Rynning, 2005). For instance, he challenges the stereotypic view that the "simplistic" Realist standpoint on state-centrism and power cannot be used due to the cooperative nature of the EU. He argues this is false, by showing that Realism whether Classical or Structural can provide valuable insight into EU policies, for instance by reframing Realist concepts such as viewing the EU's actions as part of a global balance of power(Rynning, 2005). Structural Realism can help explain EU foreign policy by situating it in a wider global context and power dynamics including in relation to other powers such as China or the USA. He argues further by stating that in foreign policy analysis, the framework of Realism can help shed light in that foreign policy decisions are influenced by broader structural forces (anarchic system, the desire for security etc.). The integration of Realism in EU studies can enhance the understanding and perceptions of the EU security strategy and foreign policy in response to ever-changing global dynamics/shifts and potential external threats(Rynning, 2005).

To legitimise further the use of Realism in its analysis of EU IR, the author Hyde-Price made a critique on the concept of Normative Power Europe, while challenging the term and ideas that the EU only influences IR through norms, values, and soft power. He argues against these liberal and idealist interpretations, finding them reductionist and the underestimation of power dynamics and systemic pressures which shape EU policies(Hyde-Price, 2006). He does this by showing for instance that the EU serves as a tool for its member states to manage the wider world and its external environment, and balance out between soft and hard power strategies. The author showcases this with the development of the Common Foreign and Security Policy (CFSP) and the European Security and Defence Policy (ESDP), both of which deviate from the normative or

civilian led endeavours that the EU "normally" takes, specifically these policies and initiatives are a response to systemic changes in the international system rather than being based on normative driven policies (Hyde-Price, 2006),

In the case of my research question as presented in the Introduction, here are several forms in which the EU's position as a global actor within the dynamic of IR and the role AI can highlight neorealist elements, and notably in the context of China's rise and prominence in the field of AI, especially in Defence applications. Structural Realism suggest that China's ambitions in AI for defence purposes would alter the global balance of power, which the EU relies on because its identity and security is also dependent on a stable, fair and rules-based world order(*Shared Vision, Common Action: A Stronger Europe*, 2016). The EU within this framework would need to assess its own security needs and technological capabilities in the wake of China's ambitions. Systemic pressures and power dynamics of AI globally would necessitate the EU to also think about its strategic autonomy, as Hyde-Price demonstrated in his work. The EU's development of the CFSP/ESDP was in response to the era of Unipolarity under the US i.e., the increased need for the EU to not be overly dependent on the US, and its ability to act militarily and independently in its own neighbourhood (Hyde-Price, 2006).

The concept of strategic autonomy is well suited to the guise of the research question as it also responds to new threats including China's advancements in AI. Further readings on the concept of Security Dilemma, under which one's state pursuit of security, or enhancement of AI in this case, leads to the increased security in others. This is implicitly supported by the article's discussion of power maximisation and security competition. And the purpose of this research purpose is to find out whether the EU perceives China's AI ambitions as a threat, which in turn could trigger a security dilemma within the EU.

The power dynamics associated with the development of AI as a force multiplier in IR has important implications in the realm of global security, strategic autonomy, competition, and survival. I find it relevant and timely to investigate the thesis research question further: How does the European Union face a Security Dilemma in response to China's Artificial Intelligence ambitions?

EU-China's bilateral relations and AI

At the EU-China summit, 7th December 2023, talks were held between the president of the Commission Ursula von der Leyen and president of the European Council Charles Michel with President of the People's Republic of China (PRC), Xi Jinping. The objective of this summit was to discuss and clarify concerns in the bilateral relationship from both sides. They discussed matters of trade, which emphasised importance due to the volume and frequency, with Der Leyen mentioning: "We trade EUR 2.3 billion of goods every single day" (European Commission, 2023). In this summit they discussed de-risking and decoupling in matters of self-reliance and dependency, and diversification of supply chains. And the desire of both the EU and China to increase their resilience. Van der Leyen highlighted: "In light of increased geopolitical frictions, it is important for us to strengthen and diversify our supply chains" (European Commission, 2023). They discussed various global issues such as the war in Ukraine, Climate Change as well as concerns on the potential for instability in the South China seas, with the EU emphasising the risk for regional and global stability. Should the PRC proceed to change the status-quo by force, because of its active rhetoric in favour of reunification with Taiwan as "vital for the rejuvenation of the Chinese nation"(Xinhua, 2022). Also mentioned in the summit was the "digital topic" and specifically AI, according to which they discussed the enormous potential for good AI has for their respective societies and in their governance models,

Security landscape of AI – US, China, and EU

On matters related to Defence and Security, AI has an enormous role to play as we have seen with our previous sub-sections on the balance of power that AI has in IR, particularly looking at the US, China and in our case the EU. AI creates a problem of what is known as dual-use dilemma which means that it can be used for both civilian and military purposes. Such developments refer to overlapping of innovation AI for both military and civilian purposes. An example is the internet precursor, the ARPANET system (Advanced Research Projects Agency Network), a wide network and internet precursor invented mainly for US military to share information and data across vast distances in case of nuclear attack(Packard, 2020). China for instance has adopted a Military-Civil fusion strategy to integrate technological innovation to military

applications(Carrozza, 2022). The US has also been implementing and decoupling on AI technologies for over a decade with the establishment of the Defence Advanced Research Projects Agency (DARPA) and the Joint AI Centre Department (JAIC), specialized in AI initiatives. By decoupling from civilian use, the US can more tightly control access to such technologies from Russia and China, maintaining competitive advantage. Dual use classification of software technologies for example, makes it more difficult to restrict access to China and Russia, posing several problems for trade controls. The pursuit in the development of AI in defence creates a "dual-use" security dilemma, fearing that one power might gain a strategic advantage over the other. This has impacts on the balance of power globally as AI can greatly enhance the speed and intensity of conflicts and military operations, increasing miscalculations the likelihood of conflict (Carrozza I. et al, 2022).

In the context of the thesis research question, a dual-use security dilemma in the EU stems from China's advancements in AI, which may have a malicious nature for the EU region. By the EU as a bloc aligns with the USA as an ally, through alliances such as NATO, and China's goal of reshaping the world order in its image through a "multipolar world order" means that the EU at the very least has cause for concern for Chinese AI ambitions for defence purposes. This dynamic of strategic competition means that the EU has an interest in reinforcing its own regulatory and innovative edge in AI to compete with US and China.

5. Research Question

How does the European Union face a Security Dilemma in response to China's Artificial Intelligence ambitions?

There are three aspects underpinning our research. The first is that the EU is operating in an international system that is bound to logic of anarchy and systemic pressures which impact global power and competition including decisions relating to the security needs of each global actor. Reference to historical examples of the Cold War or the space race between the US and the USSR in the Cold War illustrate this assumption. Technology is a pivotal aspect of these power changes, similar to technological advances during the Cold War as the Soviets and the United States sought to gain a competitive edge relative to each other. This phenomenon is unfolding today with the role of AI in international affairs. Within this system, AI exacerbates the security dilemma between powers (e.g. the current arms race between the US and China).

The second assumption is that the EU must deal with the realities of China's ambitions in AI, which to a lesser degree means that it must also deal with the problematic use of Dual-Use AI as described (in the Data Analysis section). This means that AI technologies may have dual use applications in both civilian and military settings. The EU's bilateral relations with China have been subject to recent deterioration, though not to the same extent as for US and China. Certain competitive stances with China where its interests and those of the EU do not align heightens the Security Dilemma for the EU, exacerbated by AI competition. To explore this further, we consider two areas for study in the Data Analysis section for further study:

- LAWS
- Cybersecurity

Both of which have importance interest from all actors given their potential in the Offense-Defence calculus.

The final aspect of this research question explores what the EU's options are to mitigate risks posed by the security dilemma. According to Jervis' the mitigation of risks was a possible instrument to ease threats or perception of threats (Jervis R., 1978). Options explored within this framework are as follows:

1. The EU member states cooperate to deal with external threats
2. The EU cooperates with like-minded partners such as US
3. The EU cooperates with China

This means that the EU in its complex and multilateralist format, can to a lesser degree cooperate either within its own Union, through member states to deal with external threats or it can partner with other like-minded partners such as the US or within NATO framework. Or ultimately cooperate with China to see how the EU and China can change their perceptions and behaviours (As discussed in the Data Analysis).

Our goal is to explore the general theory of neorealism and the Security Dilemma as conceptualized by Jervis' in the role and perspective of the EU in the ever-shifting technological landscape and the impacts on geopolitics(Mearsheimer, 2001).

For this research, when we operate in the framework of Neorealism and the Security Dilemma, with the assertion that as the EU faces a Security Dilemma, it feels compelled to adopt strategy and policy to keep up with the technological progress of China, for example. Europe's multicomplex identity and stances make its navigation of technological competition more nuanced than traditional powers (i.e. competing in the arms race whilst staying in line with its normative identity). Nonetheless, like any other global actor, it seeks its security and survival relative to other powers in the context of the security dilemma.

And so, how does the EU operate in the anarchic system with all the challenges that AI competition presents?

Thus, the ambitions of one actor make the other feel unsafe due to their posturing. i.e. if China makes heavy investments in AI such as with LAWS or in Cybersecurity, then these tools will shift the balance of power. The EU has concerns about the intent of these tools regarding China's ambitions and could again face a perception of a threat.

6. Theoretical Framework: Jervis' Security Dilemma

Jervis' Security Dilemma was chosen because of its focus on the role of technology in international affairs. Specifically, Jervis focused on the way that technology blurs the Offense-Defence calculus in international affairs(Jervis, 1978). Another aspect of Jervis' theory that is relevant for our analysis is the 'Four Worlds for Offense and Defence' which helps explain under which circumstances the security dilemma has a higher risk of exploding into conflict or staying relatively stable depending on his Four Worlds for Offense and Defence. The security dilemma deals with the perception of threats and the notion of subjective security responses, underscoring the power of perception in shaping global politics(Jervis, 1978). This is also illustrated by how China perceives US presence in Asia, opposing the necessity for absolute security by US, which it finds provocative and unnecessarily confrontational (Xinbo, 2000)

The theoretical framework of the Security Dilemma is an essential tool in the research of this thesis. We acknowledge in the literature review that the EU, like any other global actor in this anarchic system, is sensitive to systemic changes globally. This includes developments of AI for military use and dual-use innovative AI technologies. Europe recognizes the influence of AI initiatives on the global power balance and the role China will play in the future world order.

As discussed in the literature review, the offense-defence concept is also useful in understanding the increased potential for AI assisted strategies in offensive as well as defensive capabilities. Related to the Security Dilemma, the actions of one state forces response from other states. Materialism should also be considered with this framework, as primary drivers for such responses are political and economic. influencing the nature of potential military response under the blanket of national or regional security.

The research analysis uses empirical evidence to test relevant hypotheses about state behaviour and desire to influence international relations between states in the anarchic setting.
Cognitive biases and misjudgements can exacerbate the security dilemma leading to wide swings in responses. The systemic theory of the security dilemma theory also contributes to the system structure in shaping state behaviour, consistent with the neorealist approach of anarchy and power distribution.

For this research we see structural power in a multipolar system and the EU is like any other actor in this anarchic system. The EU as a collective entity also seeks to influence technological trends, ensuring its future as a key influencer when AI becomes a central focus point on the dimension of power. It also needs to survive and thrive in the globally competitive AI arms race and not fall behind the pace set by China.

The EU seeks technological sovereignty and strategic autonomy in AI development. It does so by not only investing in AI financially (though, not persuasively)(Csernatoni, 2024), but also does so through regulatory and normative stance power, by setting global standards and attempting to force other competitors such as China to apply to its regulatory framework and values. Although to a much lesser extent than the US and China, the EU also seeks technological advancements through AI in military settings and cyberspace, such as with security imperatives in Cybersecurity and in its exploration of LAWS, that it fully supports a ban thereof, but may conduct related R&D under strict oversight to better understand such capabilities in conflict.

Research in LAWS and cybersecurity are necessary for Europe to support a growing security need and is considered defensive posturing in the offensive-defensive theory, in response to China's AI ambitions. Or that it can reinforce its own security by looking inwards and enhance internal EU cohesion between member states to bolster defence on AI. Or that it can mitigate security by forming closer partnership with allies such as in the USA, within the framework of NATO. By using these theories and concepts, this thesis offers a valuable analysis of the phenomenon of EU responses to AI ambitions.

7. Methodology

To utilize Jervis' Security Dilemma framework, we use three ideas from his work: Firstly, anarchy: our analysis necessitates an understanding of how the EU will respond to AI innovation, particularly when it is applied to defence, security, and warfare. In a structural realist framework, each player is subject to the systemic forces of competition that will inevitably stem from AI innovation and will need to respond to any security threats identified. This is backed up by theory covered in the theoretical discussion but also reports of experts and commentary from public officials of the EU.
Secondly, we will explore potential impacts that may lead to Offense-Defence blurring in the face of heightened Security Dilemma in Europe. Specifically, we will conduct a case study analysis of two applications of AI in Defence, that are relevant for both the EU and China: LAWS and Cybersecurity. Considering the research question on "China's AI ambitions" this case study can prove invaluable as both areas of research and related policies are a part of its ambitions to enhance its own perceived security, particularly in its rivalry with the US and its goals in Asia.

LAWS, also known as robot killers, can increase the People's Liberation Army's (PLA) capability of waging warfare on potential adversaries such as the USA and its desire to change the status quo in the region.

The case of cybersecurity is highly relevant in the AI innovation race and related development of capabilities in cyberspace, i.e. increased speed of cyber-attacks, more sophisticated malware, or DDoS (distributed denial of service) attacks, espionage, etc. Cyberattacks of various forms have occurred on EU territory whether it be on official institutions, companies, or individuals.

Lastly, we will use risk mitigation to conduct policy analysis to assess the opportunity to identify mitigations of the EU Security Dilemma responses or lack of response in a growing recognition that future security is at risk. This also calls for an assessment of internal and international cooperation, possibly with China, the US, and/or NATO.

8. Sources

Literature on theories of International Relations and how states respond to perceived threats in an anarchic system is widely regarded to support the security dilemma, realist, and neorealist positions. Leaders in the field include Hertz, Jervis, Waltz, Walt and Mearsheimer (Herz, 1950; Jervis, 1978; Mearsheimer, 2001; Walt, 2022; Waltz, 1979). Analysis of their theories, application thereof, and critical analysis of those theories provide strong relevance for application to European security issues that present with the evolution of AI military initiatives by China. Historical references, the post-war EU-US relationship and Europe's somewhat dependence on US for security needs also provide context to the changing realities for Europe in the face of an AI revolution.

This body of literature provides a robust framework for the theoretical analysis of the research question. Much of this theory was established prior to the current revolution in AI-assisted warfare, but analysis of the drivers of threat and eventual conflict benefits from the same theoretical framework. The empirical material gathered through literature research and prior studies in European Affairs provides the body of research on which the theoretical research for this thesis is based. The application of this theoretical framework of realism and neorealism has not been applied systematically to European security considering the AI revolution and the AI-led arms race, particularly in the current deteriorating EU-China relationship, with China being a leading power in the AI race. The novelty of this research lies in the opportunity to apply IR theories to an evolving field of AI as it relates to European defence and security.

AI initiatives and application to security strategy as a research subject indicate a paucity of peer-reviewed literature for either region, Europe, or China, but also speaks to the novelty of the field in terms of future analysis of the security dilemma. Recognition of security risk presented by the AI race and Europe's lagging position behind China and the US is prominent in many reports, such reports often solicited by government and semi-state bodies. The increased volume of reports and assessments in very recent years, particularly in 2024, speaks to the political interest in the potential threat to security that AI initiatives in China and other states present. Evidence of security threats in Europe is largely reported in the form of news reports, providing valuable

context to the research question, and informing political urgency that Europe needs to take measures to assess and limit security risk.

In general, this thesis brings to light the lack of academic research in recent years, partly illustrated by the gap between theory and increasing records of security threats, namely the use of cyber-attack cases by China in Europe, to inform the region's priorities, assessment of risk, solutions for defence.

9. Data and Analysis

The data analysis is structured in as follows:

- The Security Dilemma in an Anarchic System
- The Geopolitical Context of EU-China Relations
- Case Studies:
  - LAWS
  - Cybersecurity
- Risk Mitigation and Discussion

The Security Dilemma in an Anarchic System

EU as an anarchic system

Europe's anarchic system serves as a model for how anarchic systems evolve and how military defence has evolved within the European anarchic system. Alexander Wendt identified three cultures in the anarchy framework, each affecting a state's foreign policy behaviour(Spara, 2020), comprising:

- The Hobbesian culture – a "kill or be killed" mentality where there is no cooperation and a predisposition to accumulate relative military power
- The Lockean culture, wherein there is a mutual respect of sovereignty between states, but there is a possibility of war, and
- The Kantian culture, in which a pluralistic security community arises in which the likelihood of war is negligible.

The post-war European system realised an unprecedented transformation in how it perceived sovereignty and war. The founding of the EEC in 1957 represents a strong normative turn. A Lockean system of rivalry within Europe shifted toward a Kantian system of friendship wherein war was no longer an option, with cooperation between European powers a means of strengthening the region. A deeper willingness to commit to established treaties and international law were strengthened by the development of many supranational institutions.

But the anarchical nature of Europe presents daily newsworthy developments speaking of political volatility, a reminder of the conflict-ridden history of the region. We are currently experiencing wild swings in politics between right and left at national levels. In the US, President Trump threatened allies with pulling US out of NATO. For US, the alliance with EU in its current form is less interesting due to competing priorities, particularly in Asia(Brands, 2024). Europe has greatly benefitted from the US security commitment and military protection via NATO and troop deployments. With the post-war Marshall Plan, the US ensured a way forward for transnational structures leading to the establishment of the EEC and EU("Marshall Plan - European Recovery Act," 1948). US presence in EU facilitated collaboration by allowing former enemies to pool their resources without compromising their security. Under the allied occupation, Germany transformed from an autocracy to a democracy. Welfare programs were introduced which marginalized radical left and right. US was powerful enough to protect Europe and yet distant enough that it posed no threat. Europe has become a powerful global player where democracy and cooperation are the norm.

The future position of Europe in the global anarchic system

Fast forward to 2022 with the Russian invasion of Ukraine, it seems the US is less willing to support Europe as it did previously. Indeed, the US considers Europe an economic competitor which may be driving its current promise to distance itself from European affairs and long-standing commitments. China is increasingly perceived to pose threats to US interests in Asia. And, US requires more efforts, resources and funding on this security matter, perhaps at the expense of its current commitment to Europe.

If US were to abandon support for Ukraine to focus on other priorities, Europe would be required to fill the gap. If successful, Europe could eventually strengthen its global position as a pillar of liberal world order by sustaining Ukraine to defeat Russia. Within the global anarchic system, Europe must assess what security strategy will support its future needs, in which AI innovation in defence is rapidly subject to transformation many ways. An independent, geopolitically powerful Europe sounds great, but the framework for governing its security strategy is under consideration(Barigazzi, 2024). Moreover, a Europe that can handle its own security

affairs would and should be much more heavily armed than it is today. Defence spending would have to double in many countries. With the loss of the US nuclear umbrella, front-line states, particularly Poland would need their own nuclear weapons.

Anarchy and the Security Dilemma

The security dilemma introduced by Robert Jervis is rooted in the concept that when aiming to increase its security, the anarchic state may employ means of increasing security that inevitably threaten the security of other countries, resulting in competition and eventually war.

Jervis speaks of a "spiral model" as interactions within the anarchic international system - where there is no hierarchical superior, coercive power that can resolved disputes or enforce law, in which individual states are seeking only to improve their own security - end up straining international relations and increasing risk of security threats.

Examples of the security dilemma are presented (Bergman, 2021; Nagi, 2022; Walt, 2022):

- Russia's response to NATO's expansion eastwards: Adding NATO members to increase the security of these new members triggered Russia to engage in a sequence of activities which contravened the UN Charter, including seizing Crimea and invading Ukraine.
- Further afield, Israel's assassination of Iranian scientists is legitimized by its desire to enhance its security (Bergman, 2021) and
- Saudia Arabia intervened in Yemen to ensure the security of Riyadh(Nagi, 2022).

Such efforts to increase security invariably include increasing one's defence capabilities prompting others to do likewise leading to increased tensions between states who may otherwise enjoy more stable relations. The theory of security dilemma and the broader spiral model constitutes a convincing balance between war and peace via interaction of IR(Tang, 2010).

Furthermore, there are two variables which influence the security dilemma, including the offence-defence balance and the offence-defence differentiation(Glaser, 2011).

Offence-defence balance and offence-defence differentiation

The line between defensive capabilities being perceived as offensive is highly sensitive. In theory, if a state's defensive capabilities are clearly perceived only as defensive, then the risk for healthy international relationship is low; it's when it becomes difficult to distinguish defensive from offensive capabilities that international relationships become strained. This concept of offence-defence differentiation is highly relevant in the current pursuit of AI for military and warfare competition(Beiping, 2024). Cooperation structures can reduce such risks but cannot eliminate the tensions that are inevitable in the pursuit of AI advantage.

The offence-defence balance is sensitive to AI technological progress and advantages. This was also true in the case of nuclear weapons where the first nuclear attack will lead to nuclear retaliation. We will see the same situation emerge with advances in AI which will influence the offence-defence balance because weaponry retaliation will be a deterrent from initial strike. This of course depends on state policy and decision-making.

In the fullness of time, application of Jervis theory requires further development in the face of more experience with AI progress in military applications. The latter may include controversial development of Lethal Autonomous Weapons Systems (LAWS), which are platforms with increasingly powerful potential to select, target and engage autonomously and without human decision input.

Currently, there is no global framework or common agreements to assess interaction between different states on the implementation of LAWS. In his review, Sacks explores the disruptive potential of LAWS on deterrence and proposes a framework to better understand various theories' applicability in the current competitive environment and in a crisis situation where concerned nations may decide to use LAWS(Sacks, 2023).

Geopolitical Dynamics

EU Reports of a Deterioration in EU-China Relations

In 2022, the EU released a report on EU-China bilateral relations and concerns of deteriorations relating to trade measures against EU, countermeasures to sanctions on human rights, economic coercion and China's position on the war in Ukraine (*EU-China relations*, 2022). The perceived ambiguous record of China triggered several statements by EU on China's short-comings and requests for attention to areas including their lack of influence on Russia's aggression against Ukraine, and lack of action by China against malicious cyber-attacks in EU from China territory(*EU-China relations*, 2022). Russia's attack on Ukraine is an unambiguous breach of the UN Charter. Europe expected China to use its influence on Russia. Moreover, as Russia increasingly criticizes Europe for supporting Ukraine, China is not responding with clarity required to challenge Russia and in doing so is indifferent to the UN's Charter and to Europe's security(Borrell, 2023). Within the 2022 report on deteriorating relations, Europe clearly referenced the prior 2019 "Strategic Outlook" Joint Communication as a valid framework for strengthening relations between the two regions(*EU-China - A Strategic Outlook*, 2019).

So, on the one hand, Europe seeks a strong positive relationship with China, while acutely aware of the indirect and direct challenges and threats that China presents to the region(Menegazzi, 2024).

China's anti-American Global Security outlook emphasises the priority of national security supported not only by economic, political and defence strategies, but also by non-traditional risks associated with AI and data(Chen, 2024).

Threats to the Security Environment

Europe has benefitted from support from US and NATO for decades without necessitating investment in defence for decades. But the aggression against Ukraine has shattered that stability and Russia's flagrant undermining of the UN Charter without condemnation from China raises fear and anxiety for Europe's security. The NATO defence alliance, for whom deterrence and defence posture are core strategies in

preventing conflict need more support to safeguard freedom and security(*Deterrence and Defence*, 2024).

Europe lacks conventional combat power and is strongly criticised by the US under the Trump administration for lack of investment in defence and security (Horschig, 2024).

Case Studies

Case Study: LAWS (Lethal autonomous weapons systems)

LAWS (Lethal Autonomous Weapons Systems) have enormous potential for destruction and loss of life. The US Congressional Research Service defines these as 'a special class of weapon systems that use sensor suites and computer algorithms to independently identify a target and employ an onboard weapon system to engage and destroy the target without manual human control of the system.'(Sayler, 2024)

By looking at the difference in how the EU and China are choosing to regulate LAWS, we can understand the type of Security Dilemma that the EU finds itself in.

1. *EU's regulatory approach requires human control*

The central premise of the EU's regulation of LAWS is the concept of "meaningful human control". Meaningful human control is a legal test that imposes two conditions on funding requests by the European Defence Fund: tracking and tracing. Tracking requires the system to be able to respond to the moral rationale for the system design and intended potential use, and tracing to ensure that outcomes of the system can be traced to at least one human along the chain of design and operation(Santoni de Sio, 2018).

At the heart of EU regulation then, we can see what is in effect a prohibition on EU funded *fully autonomous* LAWS, which by necessity will stifle the development of such technology. These legislative measures reflect the EU view that current international law is insufficient to safeguard human life in accordance with the UN Security Council(*Protection of Civilians in Armed conflict*, 2023).

2. China says it will commit to ban LAWS but is developing LAWS

China has a more ambiguous approach to regulating LAWS, but looking at its broader geo-political ambitions, we can garner that it has little intention of seriously regulating LAWS.

In 2017, the country set out a roadmap of targets to 2030 in its' New Generation Artificial Intelligence Development Plan. The plan mentions the "first-mover advantage" in becoming "the world's primary AI innovation centre" (Webster, 2017). A year later, the Chinese delegation to the UN's Group of Governmental experts on LAWS committed to a new protocol for the Convention on Certain Conventional Weapons to ban the use of LAWS(*Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, 2001). However, it was reported by a third party "Stop Killer Robots", that the delegation "stressed that [the ban] is limited to use only." Moreover, it was reported on the same day that the Chinese air force proclaimed intentions to evaluate advances in fully autonomous swarms of drones in the quest for future intelligent-swarm combat(Kania, 2018).

While it is difficult to access any accurate data on the level of investment China has made into LAWS so far, the country is indeed investing in its fully autonomous weapon capability and is not seriously committed to protective regulations.

3. Where does that leave Europe in the Security Dilemma?

The absence of a global AI framework with international standards creates risk for Europe internally and internationally. An AI arms race may impede the creation of a global AI governance framework – the "regulatory dilemma" which describes the tension between regulation and innovation (government and industry). Internally, the exclusion of AI for military use from the AIA means that there is no EU-wide legal and ethical framework in place for military use of AI. Member States will inevitably adopt different approaches leading to gaps in regulation and oversight. Europe should develop an internal framework for dual-use and military AI. In terms of the security dilemma, this will challenge a unilateral European action plan for development of AI assisted weaponry. With a risk of member states adopting different positions, the Commission is likely to introduce a new a new post for a Defence Commissioner to

respond to the unavoidable geostrategic reforms necessary to respond to the security dilemma.

Beijing has made it clear (diplomatically) that human involvement in weapons systems engagement decisions remains a priority. In 2012, the Pentagon released a directive mandating that autonomous and semi-autonomous weapons systems be designed to allow humans appropriate oversight and management of the use of force employed by those systems. Decision-making processes will also remain squarely within the legal boundaries of the codified rules of engagement and law of war. China's military, however, has remained more ambiguous as to its stance on the use of autonomy in lethal warfare. Beijing has both called for the prohibition of autonomous weapons, through a UN binding protocol in 2016, and issued its New Generation of AI Development Plan, in 2017 – which served as the foundation for its development of autonomous weapons.

While China is committed to autonomy and AI-enabled weaponry development the concern for Europe is whether the working ethical framework is in place to mitigate catastrophic risk. The People's Liberation Army (PLA) follows the CCP for guidance on military ethics as the CPC provides political context on ethical guidance. PLA stress the unity of scientific and revolutionary aspects in military ethics, emphasizing that it is not just about ethics but also a practical model of socialist core values(Metcalf, 2022). The PLA will have ultimate decision in selection of developments for deployments that give China advantages and efficiencies(Kania, 2020).

Within these reforms, Chinese military scientists are engaged on ethical aspects (Jie, 2019; Metcalf, 2022) suggesting that military decisions in autonomous weapon system development is somewhat guided by norms of war morality. Nonetheless, the People's Republic of China (PRC) are engaged in sales of such arms to regions outside the NATO alliance, and this presents a threat to Europe. Despite the encouraging engagement on common ethical concerns, some scenario may present wherein a conflicting pragmatic approach by the PRC may prevail. Given the assumed likelihood of such scenario, Europe should continue to evolve to mitigate such risks. Furthermore, the absence of official policy in China makes it difficult to predict how the PLA will interpret the terms and conditions required to ensure meaningful human control. For

now, the West's hope is that the PLA will not relinquish control to autonomous systems which would be inconsistent with the spirit of strict command of control in accordance with over-centralized decision-making PLA processes(Kania, 2020).

Case Study in Cybersecurity

Cybersecurity is an integral component of Europe's security strategy(*The EU's Cybersecurity Strategy for the Digital Decade - Joint Communication to the European Parliament and the Council*, 2000). Regardless of business sector concerned, security and reliability of digital tools are significant to Europe's economy, connectivity and democracy. Cross-sector inter-dependencies of digital networks and information systems provide a crucial landscape for business continuity.

The main threats to cybersecurity include

- Ransomware
- Malware
- Social engineering threats
- Threats against data
- Threats against availability: Denial of service
- Threats against availability: Internet threats
- Disinformation and misinformation
- Supply-chain attacks

Cybersecurity is essential for ensuring business continuity and security. Cyber-attacks have far-reaching consequences for functionality but also data security. The threat landscape is compounded by geopolitical tensions with digital services and the financial sector being the most sensitive targets. Despite the potential magnitude of impact from such attacks, the preparedness of the public and business owners is low, with a shortage of cybersecurity skills in the workforce.

In China, multiple institutions are responsible for regulating and promoting AI, including, Cyberspace Administration of China (CAC) which primarily controls online content and participates in the development and enforcement of the Country's cybersecurity, data security and privacy laws. CAC is a hybrid organization that spans both the Party and the state(Zhang, 2024).

One of the most notable legislative developments, the Cybersecurity Law of the PRC (2017) imposes strict requirements on data protection and storage of Chinese user personal data which must be strictly retained within China – a challenge for multinational companies i.e. pharmaceutical companies including China in global clinical studies may be required to restructure their data storage and processing strategies to comply with China's new law.

Another important law is the Data Security Law (2021) which classifies data based on significance for national security, economic development, and social public interests. Compliance with this law requires regular risk assessments by companies, even for activities outside China. The implications are requirements for China-based data centres and cloud services.

AI enhanced cybersecurity options are increasingly necessary in China which is leading to substantial growth in its cybersecurity industry, reaching 30.8B USD in 2023 with an increase in the number of listed companies increasing to 28. This radical transformation, initially focused on protecting government infrastructure has now expanded to cover cybersecurity for other sectors(Moore, 2023). To mitigate risk, companies are heavily investing in cybersecurity models and sub-models focussed on different aspects of cybersecurity including attack detection, operational management, traceability, knowledge management, data protection, code security and vulnerability analysis(Si, 2024).

Transformative technologies include quantum computing to support cryptographic security, developing encryption methods that are near-impossible to break and Internet of Things (IoT), expanding cybersecurity landscape(Moore, 2023).

Geopolitical conflicts are increasingly extending to cyberspace making cyberspace not just an area of opportunity but a battleground for control and influence (Pleil, 2023). The US National Security Strategy (2022) identifies China as a systemic rival in the context of strategic competition – "the only competitor with both the intent and, increasingly, the capability to reshape the international order".

To assess the impact of China's achievements and ambition in cyberspace, the US have conducted regular risk assessments in recent years. The EC communicated to

Parliament and Council a list of important security issues, including cybercrime and cybersecurity(*The EU's Cybersecurity Strategy for the Digital Decade - Joint Communication to the European Parliament and the Council*, 2000). The annual cost of cybercrime to the global economy is estimated to have reached €5.5 trillion at the end of 2020. Russia's military aggression in Ukraine has heightened this threat with mobilisation of many hacktivists, cybercriminals, and Russian state-sponsored groups.

A 2015 assessment of cybersecurity threats (Van der Meulen, 2015) in EU describes the challenges of defining the concept of threat requiring analysis of threat assessments, broadly categorized as threats to individual, organizational, supply chain or societal. Perpetrators of potential cybersecurity threats include:

- States
- Profit-driven cybercriminals
- Hacktivists and extremists

Accounts of hacking activities from Russia and China have been reported in Europe in 2024. Such cyberattacks ranging from hacks of politician's phones to massive data breaches including an attack on Ukraine's largest telecoms provider, Kyivstar: the perpetrator thought to be Sandworm, a Russian military intelligence cyberwarfare unit. Spyware has been detected on devices of two MEPs and a staffer from the European Parliament's defence subcommittee; unsecured hotel lines were intercepted to record a top secret conversation among top military officers discussing military aid for Ukraine and China was accused by the UK government for attacks on its institutions including their Ministry of Defence (MoD) in an attack that exposed the personal details of thousands of troops via the contractor-run MoD payroll system(Starcevic, 2024).

Non-Government based hacking groups, known as advanced persistent threats (APTs), are active against EU businesses and governments and include a number of groups tied to various arms of the PLA or CRP according to the EU Agency for Cybersecurity (ENISA) and the Computer Emergency Response Team of the EU (CERT-EU) (Greig, 2023).

There is increased effort to characterize cyberspace as the fifth domain of warfare after air, space, sea and land, as a consequence of increased volume of cyber attacks in recent years and the increased economic consequences of these attacks.

As discussed with traditional military technologies, the prospect of a 'cyber security dilemma' is presented by the potential for conflict or war if states race to develop superior cyberattacks: could such escalation between states trigger war? Since the security dilemma is at the core of realist understanding of IR theory and is a key reference for explaining state behaviours and foreign policy, it's reasonable in this case to apply the concept of realist and neorealist theory on state actions in cyberspace.

By applying the neoclassical realist framework, this question is discussed by Arslan, using neorealist analysis of state behaviour in cyberspace, relying on quantitative methods. Using two regression analyses with a dataset of over 4000 samples, it is concluded that as states build more cyber security capacity, they tend to engage in more disruptive actions against other states in cyberspace. It appears from the record of attacks on EU government and industry presented above, offensive initiatives by states (or affiliated non-state organizations) are more efficient than those defence mechanisms in targeted states, which seem to fail the security objective. The theoretical framework of neorealism and the security dilemma indicates an offense-defence dynamics within the realm of cyberspace. Does building cyber security capacity increase tendency to execute cyber-attacks on other states? Arslan's conclusion leans into the offensive line of neorealism as technological advances in a state is more likely to lead to offensive action; a states cyber capacity building is seemingly synonymous with cyber power building, deployed when opportunities present to secure power advantage over another state. (Arslan, 2023)

In another paper, the analysis using the Neoclassical Realist (NCR) framework argues that unchecked escalation toward a cyber security dilemma is not obvious based on qualitative assessment (Beckerman, 2022). However, my analysis favours the quantitative assessment by Arslan based on the robustness of the data sets use for the analysis.

Risk Mitigation and Discussion

Introduction to Risk Mitigation in response to the security dilemma

As discussed above, assessment of security risks is necessary to build an effective mitigation plan and to manage future security dilemmas triggered by the AI revolution.

The military sector is increasingly dependent on AI with the use of ChatGPT-like platforms for decision-making, facial recognition systems for identifying targets and autonomous drones for targeted killing. Europe is clearly delayed by several technological generations in reaching the achievements of China, not only in weaponry, but also in surveillance capabilities ("Artificial Intelligence: EU Must Pick Up The Pace," 2024). AI enables information superiority, an essential component of defence security through data and intelligence.

Europe is increasingly aware of risks that Chinese business may present in many sectors that rely on AI solutions. Chinese companies had been acquiring significant stakes in major European assets. Response to such risks are illustrated by the 5G telecommunications infrastructure roll-out in 2019 – 11 EU countries have now used legal powers to impose restrictions on Chinese suppliers such as Huawei and ZTE . This follows the ECA special report (*5G roll-out in EU*, 2022) triggered by concerns on Chinese 5G vendors that might present a security risk for EU due to laws in China.

While the AI regulation dilemma – the balance between state control and innovation - is the same for all regions, the solutions may be very different. China's AI regulation provides for state control more than EU, but not at the expense of their 2030 goal of becoming global leader in AI. Therefore, the potential influence of China on a future global framework is likely.

Internal cooperation to mitigate risks

Because the AIA excludes AI for military use, there is no EU-wide legal and ethical framework in place for military use of AI. Member States will inevitably adopt different approaches leading to gaps in oversight. Member States will be at risk of working independently which will lead to a net inefficiency for Europe. Europe should develop an internal framework for dual-use and military AI. A comprehensive debate on the future framework on Europe needs requires risk assessment of China's AI technologies, and risk mitigation needs to be both defensive and offensive. Given the recent increase in cybercrime and the cost to the region, further investment is necessary for defence security. Additionally, while EU's commitment to provide harmonized EU foreign policy, this presents regulatory dilemma for cooperation with China for instance.

The absence of a global AI framework with international standards creates risk for Europe internally and internationally. An AI arms race may impede the creation of a global AI governance framework.

Strengthening ties with US and NATO – benefits and challenges

Despite President Trumps criticism of Europe and NATO, the US remains Europe's closest ally and strategic partner. EU-US collaboration on trustworthy AI remains an important priority for Europe, but should not be driven by a US-led goal of urgency to challenge China. President Macron has counselled for a reduction in Europe's dependence on US and to avoid tensions between Washington and Beijing. The vision implied is for a European strategic autonomy to become an independent, distinct and influential third superpower in the AI race.

Engaging & Cooperation with China

Collaboration is a two-way street with both parties expecting to benefit. Regarding the EU-China relationship indicates a shift from industrially-sensitive to environmentally-focussed projects though several industrial focussed collaborations with Chinese military-linked universities are still funded by Europe (Vandermeeren, 2024). These collaborations have published on a range of military topics including drone target tracking and missile guidance. Between 2017 and 2022, more than 16,000 AI-related papers were published with Chinese colleagues though many were related to AI applications in medical settings, but many collaborators had links to China's military. These collaborations are discouraged by some EU thought leaders in light of current geopolitical climate and the deteriorating EU-China relationship. But the problem is funding – of the papers disclosing sources, 80% were funded by China with 60% from the Chinese government, thus allowing Chinese collaborators more influence on what research is prioritized. In these collaborations, China seeks expertise and Europe seeks funding. Another issue is that co-authored papers make up a bigger proportion of European research, while 80% of China's AI research in 2020 was published only in Chinese-language journals. These imbalances indicate that Europe is dependent on China(Matthews, 2023).

Scenario Analysis

The narratives of AI arms race and security threats increase the probability of risky development of AI for military use. The AI regulatory dilemmas (balance between state control and innovation) is that in making developments safe for humans, it may present obstacles for European's achieving successful developments that compete with Chinese technologies as defensive or offensive strategies(Pernot-Leplay, 2024). The EU chose to move fast on AI regulation to make it a global standard. China, while necessitating state control in the sector, it imparts flexibility and support through various policy tools and funding that are industry friendly, generally favoring AI adoption and development. Another way of maintaining state control is via China's process for public spending on the sector. In the absence of a global AI framework, divergences in different regional legislative provisions, particularly in the field of military use of AI suggest a future of instability and risk that compels China and EU to increase efforts to remain competitive, rationalized in the theory of the security dilemma.

Discussion

Europe's objective in the global AI race is to become the world-leading region for developing and deploying cutting-edge, ethical and secure AI. The OECD definition of an AI system is a "machine-based system capable of influencing the environment by producing an output (predictions, recommendations or decisions) using machine and/or human-based data and inputs to formulate options for outcomes designed to operate with varying levels of autonomy." (*OECD AI Principles*, 2024).

Political and security strategies in China necessitate urgent development of AI led innovation for military and defence objectives. Their financial commitment supports this goal. With the speed at which development proceeds in the absence of international framework and heightened perception of threats from US allies in the Indo-Pacific region, Europe and its allies have good reasons to be concerned about China's commitment to AI in military systems. In a very real way, the security dilemma for Europe is heightened by the commitment and achievements of China in this field.

Investment in China's AI-led innovation in military systems includes:

- Robotics
- Swarming technologies
- AI and ML
- Unmanned systems development
- Advancing missile technology
- Military robotics and unmanned ground vehicles
- Unmanned surface vessels and autonomous submarines
- Advanced unmanned systems with limited autonomy

In the absence of policy or guidance from the CRP, it is difficult to predict how the PLA will approach issues of human control over autonomous systems. Centralized control over the military has been a hallmark of the PLA(Metcalf, 2022).

China's New Generation Artificial Intelligence Development Plan sets out a roadmap of targets to 2030 with goals of "first-mover advantage" to becoming "the world's primary AI innovation centre"(Webster, 2017). It is not clear to what extent China is achieving its goals. In response to China's AIDP, the US considers China's progress a threat to US economic and military power(Webster, 2017).

10. Conclusion

The objective of this thesis was to explore: “How does the European Union respond to its Security Dilemma in the face of China’s Artificial Intelligence ambitions?” Jervis’ understanding of the Security Dilemma in the framework of neorealism provides a theoretical framework to analyse the security risks that present for Europe considering China’s ambition to become global leader in AI(Jervis, 1978). Case studies of LAWS and cybersecurity provide insights on divergences between the two regions on ethical use of AI for military and security objectives.

Europe is forced to compete in an anarchic system with China representing a key source of challenge for Europe’s security. Coinciding with a perceived deterioration in EU-China relations, some aspects of the military use of AI are perceived as threats to global security. In two case studies, we take a closer look at LAWS and cybersecurity as threats of this nature require urgent political attention to assess necessary steps to ensure Europe’s future security.

Risk mitigation is explored as part of a measured response to Europe’s security dilemma that are perceived to heighten with China’s achievements in developing autonomous weaponry. Additionally, the global geopolitical tensions with wars ongoing in middle east and Ukraine, coinciding with a deterioration in EU-China relationship create pressure on Europe to recognise and mitigate security threats. The data analysis brings together a body of empirical data to support the theoretical framework to explore the research question.

Novelty in the field of AI innovation and perception of incalculable risk creates political urgency for Europe(Barigazzi, 2024). Innovation in the field of AI-led weaponry in China is not entirely transparent making risk assessment for European security challenging. The increased volume of reports, particularly in 2024, of cyberattacks in Europe speaks to increased failure at some level of European cybersecurity defence mechanisms. Recognition of security risk presented by the AI race and Europe’s lagging position behind China and the US is prominent in many reports, such reports often solicited by government and semi-state bodies(*EU-China relations*, 2022). Evidence of security threats in Europe is largely reported in the form of news reports, providing valuable context to the research question, and informing

political urgency that Europe needs to take measures to assess threat and limit security risk.

In general, this thesis brings to light the opportunity for academic analysis of security threats with the revolutionary application of AI to weaponry by China and US, a race that Europe is lagging behind for many reasons("Artificial Intelligence: EU Must Pick Up The Pace," 2024; Castro, 2021).

The need for academic research in the field of security is evidenced by the volume of reports solicited by European institutions to help guide security and defence strategy. Mobilisation of expert resources to secure relevant foreign policy and internal framework will support the strategic goal of the EU ambition to be recognised as a global leader in cutting-edge, ethical and secure AI. Establishing a European AI ecosystem and growth of AI innovation will contribute to Europe's desire to become a global influence in future AI innovation development and regulation.

It is concluded that Europe's options in terms of response to the security dilemma unfolding include:

- Doubling down on investment and tangible achievements to support a viable and thriving AI ecosystem within a meaningful timeline
- Internal cooperation between Member States to support European objectives in assessment of security threat and development of a solution-oriented AI ecosystem for the region
- Cooperation with US without increasing Europe's dependence
- Cooperation with China without compromising Europe's values for safe and ethical use of AI for military purposes

With more experience of how AI innovation is changing the battlefield and with Europe's desire to influence the safety of this field, future academic research will better inform how to navigate the complexity of this global anarchic system. Europe is behind in the AI race for now, but with current political urgency and strong ethical values, it is not too late for Europe to participate to the global application of innovative AI for its security needs. Global technopolitical strategy needs Europe to counter the risk of China's appetite for power, using autonomous weapons system without the framework that humanity deserves.

11. References

5G roll-out in EU. (2022). https://op.europa.eu/webpub/eca/special-reports/security-5g-networks-03-2022/en/

AI Investment: EU and Global Indicators. (2024). (At a Glance: Digital Issues, Issue. https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/760392/EPRS_ATA(2024)760392_EN.pdf

Akkerman, M., Brunet, P., Feinstein, A., Fortin, T., Hegarty, A., Ní Bhriain, N., Rodriguez Alvarez, J., Sédou, L., Smidman, A., & Valeske, J. (2022). Fanning the flames: How the European Union is fuelling a new arms race. European Network Against the Arms Trade. https://www.tni.org/files/publication-downloads/fanning-the-flames-execsum-en.pdf

Arsenault, A. C., & Kreps, S. E. (2024). 959AI and International Politics. In J. B. Bullock, Y.-C. Chen, J. Himmelreich, V. M. Hudson, A. Korinek, M. M. Young, & B. Zhang (Eds.), *The Oxford Handbook of AI Governance* (pp. 0). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197579329.013.49

Arslan, A. S. (2023). *Neorealist Analysis of Security Dilemma in Cyberspace; A Quantitative Study*. https://preprints.apsanet.org/engage/api-gateway/apsa/assets/orp/resource/item/654535df48dad2312002b836/original/neorealist-analysis-of-security-dilemma-in-cyberspace-a-quantitative-study.pdf

Artificial Intelligence for the American People, US White House, 2021. (2021). https://trumpwhitehouse.archives.gov/ai/

Artificial Intelligence: EU Must Pick Up The Pace. (2024). https://www.eca.europa.eu/en/news/NEWS-SR-2024-08

Barigazzi, J., Posaner, J. & Kayali L. (2024). *EU Defense Commissioner: The pretigious-sounding job you really don't want*. https://www.politico.eu/article/eu-defense-commissioner-the-flashy-new-job-that-aint-all-its-cracked-up-to-be/

Beckerman, C. E. (2022). Is there a cyber security dilemma? *Journal of Cybersecurity*, 1-14. https://doi.org/10.1093/cybsec/tyac012

Beiping, L. (2024). *Experts see rival military exercises as sign of increasing conflict risk in Indo-Pacific*. https://www.voanews.com/a/experts-see-rival-military-exercises-as-sign-of-increasing-conflict-risks-in-indo-pacific-/7705867.html

Bergman, R. F., F. (2021). *The Scientist and the A.I.-Assisted, Remote-Control Killing Machine*. https://www.nytimes.com/2021/09/18/world/middleeast/iran-nuclear-fakhrizadeh-assassination-israel.html

Borrell, J. (2023). *EU-China Relations: A Candid Exchange on Our Differences*. https://www.eeas.europa.eu/eeas/eu-china-relations-candid-exchange-our-differences_en

Brands, H. (2024). Trump's Return Would Transform Europe. *Foreign Policy*. https://foreignpolicy.com/2024/06/26/europe-security-eu-nato-alliances-liberal-democracy-nationalism-trump-us-election/

Carrozza, I., Marsh, N., & Reichberg, M. (2022). *Dual-Use AI Technology in China, the US and the EU - Strategic Implications for the Balance of Power*. https://cdn.cloud.prio.org/files/6c0dc6db-c6b3-44a4-b775-126ff97588b4/Carrozza%20Marsh%20Reichberg%20-%20Dual-Use%20AI%20Technology%20in%20China%20the%20US%20and%20the%20EU%20-%20Strategic%20Implications%20for%20the%20Balance%20of%20Power%20PRIO%20Paper%202022.pdf?inline=true

Castro, D., & McLaughlin, M. (2021). *2021 Update - Who is Winning the AI Race: China, The EU or The United States?* https://www2.datainnovation.org/2021-china-eu-us-ai.pdf

Chen, Y. (2024). Fully Implement the Overall National Security Outlook. *CSIS: Interpret China*. https://interpret.csis.org/translations/fully-implement-the-overall-national-security-outlook/

China: 39th Human Rights Dialogue with the European Union Took Place in Chongqing. (2024). https://www.eeas.europa.eu/eeas/china-39th-human-rights-dialogue-european-union-took-place-chongqing_en#:~:text=The%20EU%20and%20China%20held,the%20EU%20and%20in%20China.

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. (2001). https://geneva-

s3.unoda.org/static-unoda-site/pages/templates/the-convention-on-certain-conventional-weapons/CCW%2Btext.pdf

Csernatoni, R. (2024). Charting the Geopolitics and European Governance of Artificial Intelligence. https://carnegie-production-assets.s3.amazonaws.com/static/files/Csernatoni_-_Governance_AI-1.pdf

Deterrence and Defence. (2024). https://www.nato.int/cps/en/natohq/topics_133127.htm

EU-China - A Strategic Outlook. (2019). https://commission.europa.eu/system/files/2019-03/communication-eu-china-a-strategic-outlook.pdf

EU-China relations. (2022). https://www.eeas.europa.eu/sites/default/files/documents/EU-China_Factsheet_01Apr2022.pdf

The EU's Cybersecurity Strategy for the Digital Decade - Joint Communication to the European Parliament and the Council. (2000). https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Gera, V. (2012). *Kissinger says calling Europe quote no likely his* https://www.yahoo.com/news/kissinger-says-calling-europe-quote-not-likely-145223724.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKKpdmcGFUIwznIyPylUPRXjYES80iUA2yhxHImrfCt-YyrNweOD_S8tB7TrfxKTrjEEtrnJaQqUBeqc8FdhgwreW0UMiAGNnquJU4erHhjJwvW3hThv1JQKakrLsB1fnDMTJXvwGt8ilYsRblwVr0sAr3kvp2Z5Jf-ZIufwXBaP

Glaser, C. L. (2011). The Security Dilemma Revisited. *World Politics*, *50*(1), 171-201. https://www.cambridge.org/core/journals/world-politics/article/abs/security-dilemma-revisited/0174D23352D9303257AAAC18911F3AB7

Greig, J. (2023). *Multiple Chinese APTs are attacking European targets, EU cyber agency warns*. https://therecord.media/multiple-chinese-apts-are-attacking-european-targets-eu-cyber-agency-warns

Hendrycks, D., Mazeika, M. & Woodside, T. (2023). *An Overview of Catastrophic AI Risks*. http://arxiv.org/pdf/2306.12001

Herz, J. H. (1950). Idealist Internationalism and the Security Dilemma. *World Politics*, *2*(2), 157-180. https://doi.org/10.2307/2009187

Horschig, D. M., S. (2024). *Europe Needs More Conventional Forces, Not Its Own Nukes*. https://www.csis.org/analysis/europe-needs-more-conventional-forces-not-its-own-nukes

Hyde-Price, A. (2006). 'Normative' power Europe: A Realist Critique. *jJournal of European Public Policy*, *13*, 217-234. https://www.scribd.com/document/265347526/normative-power-in-Europe-pdf

Jervis, R. (1978). Cooperation under the Security Dilemma. *World Politics*, *30*(2), 167-214. http://slantchev.ucsd.edu/courses/ps143a/readings/Jervis%20-%20Cooperation%20under%20the%20Security%20Dilemma.pdf

Jie, L. (2019). *Talk about the legal issues of intelligent warfare*. https://web.archive.org/web/20200215011803/http://news.gmw.cn/2019-07/20/content_33013497.htm

Kania, E. B. (2018). *China's Strategic Ambiguity and Shifting Approach to Lethal Autonomous Weapons Systems* (Lawfare, Issue. https://www.lawfaremedia.org/article/chinas-strategic-ambiguity-and-shifting-approach-lethal-autonomous-weapons-systems

Kania, E. B. (2020). *AI weapons in China's military innovation.* https://www.brookings.edu/articles/ai-weapons-in-chinas-military-innovation/

Khanal, S., Zhang, H., & Taeihagh, A. . (2024). Development of New Generation of Artificial Intelligence in China: When Beijing's Global Ambitions Meet Local Realities. *Journal of Contemporary China*, 1-24. https://doi.org/10.1080/10670564.2024.2333492

Lobell, S. E. (2017). Structural Realism/Offensive and Defensive Realism. *The International Studies Compendium Project*. https://oxfordre.com/internationalstudies/internationalstudies/abstract/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-304?print

Manners, I. (2002). Normative Power Europe: A Contradiction in Terms. *JCMS 2002*, *Volume 40*(Number 2), 235-258. https://www.princeton.edu/~amoravcs/library/mannersnormativepower.pdf

Marshall Plan - European Recovery Act, (1948). https://www.archives.gov/milestone-documents/marshall-plan#:~:text=On%20April%203%2C%201948%2C%20President,economic%20infrastructure%20of%20postwar%20Europe.

Matthews, D. (2023). *Europe still working with China on military and surveillance uses of AI, report finds*. https://sciencebusiness.net/news/ai/europe-still-working-china-military-and-surveillance-uses-artificial-intelligence-report

Mearsheimer, J. J. (2001). Anarchy and the Struggle for Power. In *The Tragedy of Great Power Politics* (pp. 29-42). https://edisciplinas.usp.br/pluginfile.php/5526008/course/section/6018533/MEARSHEIMER%20J.%20%282001%29.%20The%20Tragedy%20of%20Great%20Power%20Politics%20-%20Cap%202.pdf

Menegazzi, S. (2024). Europeans Worry About China's Return to the Global Stage. *Foreign Policy*. https://foreignpolicy.com/2023/04/06/macron-europe-china-von-der-leyen/

Metcalf, M. (2022). The PRC considers military AI ethics: Can autonomy be trusted? *Front. Big Data*. https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2022.991392/full

Moore, S. (2023). Cybersecurity Giants in China: How Fortinet, Cisco, Huawei and Tencent are Shaping the Landscape. *Networkpoppins*. https://www.networkpoppins.com/blog/how-cisco-huawei-tencent-fortinet-china-cybersecurity-giants-shaping-the-landscape

Nagi, A. (2022). The Pitfalls of Saudi Arabia's Security-Centric Strategy in Yemen. *Malcol H. Kerr Carnegie Middle East Center*. https://carnegieendowment.org/research/2023/01/the-pitfalls-of-saudi-arabias-security-centric-strategy-in-yemen?lang=en&center=middle-east

Ndzendze, B., & Marwala, T. (2023). Artificial Intelligence and International Relations. In *Artificial Intelligence and International Relations Theories* (pp. 33-54). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-4877-0_3

OECD AI Principles. (2024). https://oecd.ai/en/ai-principles

Packard, N. (2020). The ARPANET into the Internet: A Tale of Two Networks. *Studies in Media and Communication*, *8*(1), 37. https://researchspace.auckland.ac.nz/handle/2292/62906

Pernot-Leplay, E. (2024). *The AI Regulation in China, EU & US: A Comparion*. https://pernot-leplay.com/ai-regulation-china-eu-us-comparison/

Pleil, H. (2023). *Being a Cyberpower - China's Ambitions in Cyberspace*. https://www.techpolicy.press/being-a-cyberpower-chinas-ambitions-in-cyberspace/

Protection of Civilians in Armed conflict. (2023). https://documents.un.org/doc/undoc/gen/n23/127/10/pdf/n2312710.pdf

Regulation (EU) 2024/1689, (2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

Rynning, S. (2005). Return of the Jedi: Realism and the Study of the European Union. *Politique Européenne*, *17*, 11-34. https://www.jstor.org/stable/45017748

Sacks, S. D. (2023). A framework for Lethal Autonomous Weapons Systems Deterrence. *Joint Force Quarterly*, *110*. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3447193/a-framework-for-lethal-autonomous-weapons-systems-deterrence/

Santoni de Sio, F. V. d. H., J. (2018). Meaningful Human Control over Autonomous Systems: A Philosophical Account. *Front. Robot. AI*, *5*. https://doi.org/10.3389/frobt.2018.00015

Sayler, K. M. (2024). *Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems*. https://crsreports.congress.gov/product/pdf/IF/IF11150

Scharre, P. (2021). Debunking the AI Arms Race Theory. *The Strategist*, *4*(3), 121-132. http://dx.doi.org/10.26153/tsw/13985

Shared Vision, Common Action: A Stronger Europe. (2016). https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

Si, M. (2024). Cybersecurity reshaped by AI-based solutions. *China Daily Hong Kong Edition*. https://lb7.chinadailyhk.com/upload/main/pdf/2024/08/06/5cdd766561fac366ad4c06d9c761f055.pdf

Solomon, T. (2012). Human Nature and the Limits of the Self: Hans Morgenthau on Love and Power. *International Studies Review*, *14*, 201-224. http://ereserve.library.utah.edu/Annual/POLS/6850/Steele/human.pdf

Spara, M. (2020). From Rivalry to Friendship". The European State Systems and the Cultures of Anarchy. *E-International Relations*. https://www.e-ir.info/2020/09/13/from-rivalry-to-friendship-the-european-state-systems-and-the-cultures-of-anarchy/#google_vignette

Starcevic, S. (2024). *Timeline: Europe under cyber siege in 2024*. https://www.politico.eu/article/europe-cyberattacks-russia-china-uk-ministry-of-defence-hacks/

Stokes, J., Sullivan, A. & Greene, N. (2023). U.S.-China Competition and Military AI: How Washington Can Manage Strategic Risks amid Rivalry with Beijing. *Center for a New American Security (CNAS)*. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/FINAL4.pdf

Tang, S. (2010). *The Security Dilemma: A Conceptual Analysis. In: A Theory of Security Strategy for Our Time*. Palgrave Macmillan. https://doi.org/https://doi.org/10.1057/9780230106048_3

Van der Meulen, N., Jo, E. A., Soesanto, S. (2015). *Cybersecurity in the EU and Beyond: Exploring the Threats and Policy Responses*. https://www.rand.org/pubs/research_reports/RR1354.html

Vandermeeren, F. (2024). *Understanding EU-China Economic Exposure*. https://single-market-economy.ec.europa.eu/system/files/2024-01/EconomicBrief_4_ETBD_23_004ENN_V2.pdf

Walt, S. M. (2022). *Does Anyone Still Understand the 'Security Dilemma'?* (Foreign Policy, Issue. https://foreignpolicy.com/2022/07/26/misperception-security-dilemma-ir-theory-russia-ukraine/

Waltz, K. (1979). *The Theory of International Politics*. Addison-Wesley Publishing Company. https://dl1.cuni.cz/pluginfile.php/486328/mod_resource/content/0/Kenneth%20N.%20Waltz%20Theory%20of%20International%20Politics%20Addison-Wesley%20series%20in%20political%20science%20%20%20%201979.pdf

Webster, G., Creemers, R., Kania, E,. Triolo, P. (2017). Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017). *Digichina*. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

Williams, M. C. (2004). Why Ideas Matter in International Relations: Hans Morgenthau, Classical Realism, and the Moral Construction of Power Politics. *International Organisation*(4), 633-665. https://www.jstor.org/stable/3877799

Xinbo, W. (2000). *US Security in Asia: Implications for China-US Relations*. https://www.brookings.edu/articles/u-s-security-policy-in-asia-implications-for-china-u-s-relations/

Xinhua. (2022). *The Taiwan Question and China's Reunification in the New Era*. http://english.scio.gov.cn/whitepapers/2022-08/10/content_78365819_5.htm

Zhang, W., Kaja, A., Luo, Y. & Stein, S. (2024). *Spotlight Series on Global AI Policy - Part III: China's Approach to Artificial Intelligence*. https://www.insideglobaltech.com/2024/02/08/spotlight-series-on-global-ai-policy-part-iii-chinas-policy-approach-to-artificial-intelligence/

Zhu, L. (2024). *Navigating AI's uncharted waters: Insight from China's Model AI Law, EU AI Act*. https://iapp.org/news/a/navigating-ai-s-uncharted-waters-insights-from-china-s-model-ai-law-eu-ai-act