Miss the piece of Europe Multilateral Cooperation

Shu-Jui Chang[1], Jen-Fu Wang[2], Tim Waton[1] and Iain Phillips[1]
[1]Loughborough University, UK
[2]Yuan-Ze University, Taoyuan, Taiwan

s.chang@lboro.ac.uk
Fisher2023@saturn.yzu.edu.tw
tim.watson@lboro.ac.uk
i.w.phillips@lboro.ac.uk

Abstract: The research emphasises the importance of European multinational cooperation in addressing cyber threats. Countries cannot combat these threats in isolation; instead, they must engage in collaborative efforts that leverage shared resources, intelligence, and expertise. The study highlights the unique challenges and opportunities Asian countries face, frequently targeted by sophisticated cyber threats, particularly from state actors like China. Despite these challenges, many Asian countries have developed substantial expertise in cyber threat response and mitigation. By participating in multinational cyber exercises and sharing their knowledge, these countries can contribute significantly to the collective resilience of the global cyber defence network. This integration would not only enhance the security capabilities of the individual countries but also foster stronger international relationships, building trust and cooperation that are essential in the fight against cyber adversaries. In conclusion, this study underscores the imperative of multinational cooperation in Europe and beyond, with Asian countries playing a crucial role in enhancing global cybersecurity through their expertise and strategic positions.

Keywords: Cyber Conflict, Cyber Resilience, Multinational Cooperation, Cyber Exercise.

1. Introduction

China's cyber threat approach is more strategic and long-term oriented. China's academic discussion of cyber warfare started in the 1990s when it was called "information warfare"(Jinghua, 2019). They view cyberspace as a critical domain for national power and are actively working to dominate the digital infrastructure and information flow. Since 2004, Hu Jintao has advocated for a "warfare with information principle" due to his deep understanding of how information played an essential role in wars like the Kosovo War (1999), the Afghan War (2001) and the Iraq War (2003). Xi Jinping, the current President of the People's Republic of China, still adheres to the "information-oriented principle" today (中央网安全和信息化委, 2021). Furthermore, realising how information can get an advantage at the initial stage, President Xi applies the intelligence systems to manage and control the flow of information effectively (防研究所, 2021) and the purpose of "accelerating the transformation towards in- formationised warfare, with the beginnings of intelligent warfare." mentioned in the 2019 National Defence white paper (丁, 2019).

Under General Secretary Xi Jinping, China's strategic vision for cyberspace is viewed as the strategic warfare of the information age by Chinese military analysts, paralleling the role of nuclear warfare in the 20th century (Jinghua, 2019). Xi's emphasis on the interconnectedness of cybersecurity and informatisation reflects China's ambition to become a "cyber superpower" (Kania et al., 2017). This ambition focuses on technological advancement and strategically leverages cyber capabilities for information operations and espionage.

Cyber espionage, orchestrated by state-sponsored actors, including government agencies, military units, and affiliated hacker groups, is a critical tool for China. These actors gather intelligence, steal intellectual property, and pursue economic, military, and political objectives (Rugina, 2023). Their activities are designed to give China a competitive edge in various domains, reinforcing its position as a rising global power in cyberspace.

China's cyber espionage or information collection efforts have increasingly become a global concern, with operations targeting various countries across different continents for a long time. These operations often involve state-sponsored hackers or cybercriminal groups with ties to the Chinese government. Below are several case studies detailing China's cyber espionage activities targeting countries around the world (Center for Strategic & International Studies, 2024):

- United States: China's cyber espionage action could be traced back to 2003 when Naval Air Weapons Station China Lake was exfiltrated, including nuclear weapons information and aircraft data. Later, companies like Google and Adobe were compromised without saying that a wide

range of U.S. industries, including aerospace, energy, and technology, are also in China's target list.

- United Kingdom: The earliest reported case indicating China's cyber espionage activities targeting the UK dates back to September 2007. British authorities reported that hackers believed to be associated with China's People's Liberation Army had penetrated the network of the UK's Foreign Office and other key government departments. This incident highlights China's initiation of cyber espionage activities against the UK, at least by this time.
- Europe: While the US and UK have long faced Chinese cyber espionage, Europe emerged as a later target. Evidence suggests China's European focus began around 2007, with France's Secretary General of National Defence uncovering Chinese infiltration attempts. This was followed by accusations of direct network breaches in Belgium just months later, highlighting a more aggressive approach. Suspicions of Chinese collaboration also arose during this period, with some speculating that German intelligence may have been involved in hacking Afghanistan while potentially aiding China. These incidents showcase the breadth of China's European cyber espionage, targeting diverse sectors and government institutions and solidifying China's persistent threat to European security.
- Asia: China's cyber espionage activities extend beyond Europe to target Asian countries. In May 2008, China mapped India's official networks, indicating an interest in disrupting networks during potential conflicts. Additionally, South Korean officials reported Chinese attempts to hack into Korean Embassy and military networks in January 2008.
- Africa: China's attention towards Africa has developed more recently than in other areas. It is reported that Chinese cyber operatives began espionage against African telecom companies in 2023. However, some experts believe this group has been active since approximately 2014, focusing on pro-democracy individuals and groups. Their operations might include gathering various data types, from capturing keystrokes to recording audio.

In summary, China's strategy to become a cyber superpower is multifaceted, leveraging its cyber capabilities in the grey zone. The strategy includes developing a comprehensive framework encompassing awareness, modelling, response, mitigation phases, and general governance to maintain control. Analysing China's tactics and techniques can enhance awareness and modelling efforts.

2. Literature Review

The definition of cyberspace has been hotly debated since 1982 when the first term of cyberspace was coined by a science fiction author, Wiliam Gibson. It has been discussed over decades without a clear conclusion because it encompasses abstract and concrete elements and engages academics, practitioners, and governments, complicating efforts to arrive at a precise, scientific definition (Garvey, 2021).

Starodubtsev et al. (2020) highlight the heterogeneous interpretations of the concept of cyberspace despite the large number of research works dedicated to it. In the paper, definitions of cyberspace are listed, demonstrating that till in recent years, cyberspace is still hard to define, and it is hard to have an efficient basis for theoretical and practical development in politics, economics, social status and society (Starodubtsev et al., 2020).

The diverse concept of cyberspace has been defined and interpreted by various scholars. Ning et al. (2018) introduce the concept of reshaped General Cyberspace, emphasising the interconnectedness of physical, social, and thinking spaces through ubiquitous convergence. In the AJP-3.20, the NATO document defines cyberspace as the global domain consisting of all interconnected communications, information technology and other electronic systems, networks and their data, including those separated or independent, which process, store or transmit data (ORGANISATION, 2020). This perspective extends beyond traditional notions of physical or virtual domains to encompass the integration of cyber elements into various aspects of human activity, including cognitive processes (Ning et al., 2018). Conversely, Ormrod et al. (2016) propose a definition within the Cyber Conceptual Framework, emphasising the complexity of cyberspace and its integration into existing military doctrine. Their model, nested within the National Security Domain, delineates cyberspace into physical and virtual domains, highlighting its significance across political, economic, and military spheres. This comprehensive approach underscores the multifaceted nature of cyberspace and its evolving role in contemporary security landscapes (Ormrod and Turnbull, 2016). The two perspectives of viewing cyberspace are like an analogy of "Cyber 9/11" and "Cyber Pearl Harbor". The nature of adversaries is non-state versus

state, and the target is civilian in the former. Adversaries are the military versus military, and the target is the military in the latter (Council et al., 2010).

On top of the US-led cyberspace definition, Russia assumes it differently as the information-centred area considers the Information Sphere, which is a set of information objects of information, information systems and websites in the information and telecommunication network, etc., whose activities affect the formation and information processing, from individual to public relations mechanisms (publication of legal acts, unknown).

The key takeaway for cyberspace is that it is multi-dimensional beyond the logical but physical aspect. It even transcends the psychological aspect with the golden thread of data and information flow connecting and interacting virtual and reality, digit and physical. There are other characteristics of this space, such as the private sector having more control in this area as its usage and ownership, the offence has more dominated than the defence, and it is fraught with uncertainty (Council et al., 2010).

The classification of activities in cyberspace, whether as cyber conflict, cyber operations, or the US-led term cyber war, has been the subject of extensive debate, with no clear-cut consensus reached. However, one undeniable fact is the inclusion of cyberspace in military doctrine, signalling the increasing military engagement in this domain. Consequently, this has led to a dominance of military involvement in cyberspace exercises and cooperation initiatives. The shift towards military dominance underscores modern warfare's evolving nature and cyberspace's growing significance as a theatre of conflict and cooperation.

3. Methodology

This paper is divided into two main parts. The first part involves participation in the Locked Shields exercise and a subjective analysis of the exercise itself. The second part comprises objective feedback from Taiwan subject matter experts (SMEs).

Based on Taiwan's Cybersecurity National Security Strategy Version 2, the cybersecurity ecosystem is established around six key organisations: the National Security Council coordinates cybersecurity matters, offering strategic guidance in policy development, international cooperation, and incident response, Ministry of Digital Affairs tasks with propelling Taiwan's digital progress, this ministry fosters connectivity between citizens and technology, enhances industry and security, and addresses evolving threats, National Security Bureau is responsible for collecting and analysing intelligence related to cyber threats from diverse sources, including human intelligence, signals intelligence, and open-source intelligence, Ministry of National Defence supports safeguarding critical information infrastructures and military networks from cyberattacks while developing counter-cyber capabilities to deter and neutralise cyber threats against Taiwan's military, Ministry of Justice investigates cybercrimes, encompassing tasks such as identifying and apprehending cybercriminals, collecting evidence, and prosecuting offenders, and Ministry of Investigation Bureau conducts criminal investigations nationwide, with the 9th Division specifically handling cybercrime investigations.

Six SMEs from the organisation mentioned above were interviewed to gather diverse perspectives. Each interviewee held management or high-administrative positions within government-related sectors. Their invaluable insights contributed significantly to identifying the challenges and opportunities of integrating Asian countries into the NATO-dominated Locked Shields exercise. These insights are crucial for this research, providing real-world perspectives on bridging the gap between Asia and the NATO member-dominated cyber exercises.

The combination of direct participation in the exercise and in-depth interviews with key experts ensures a comprehensive understanding of the current landscape and future possibilities. This methodology captures the experiential aspects of Locked Shields. It grounds the analysis in practical, expert-driven viewpoints, offering a holistic view of the potential for broader international cooperation in cyber defence exercises.

4. Multinational Cooperation in Cyberspace

Among those cyber exercises, the NATO CCDCOE takes the lead in hosting prominent Locked Shields (LS), which focuses on offensive tactics, while LS emphasises defensive capabilities. LS typically takes place at the end of April and is the larger of the two exercises, involving over 4000 participants from 40 nations. Initiated in 2010, it was a small European exercise with experimental scenario-building. It pioneered the investigation of the nature of cyber conflict (Smeets, 2022), and the exercise has grown both in scope and participation.

The exercises operate under the scenario around two fictional islands: Berylia (BER) and Crimson (CRI), long-standing regional adversaries in the northern Atlantic Ocean and revolves nations. Although both BER and CRI are members of the UN, neither belongs to NATO. BER is portrayed as a democracy, while CRI is depicted as a weak parliamentary democracy. To simulate real-world dynamics and foster meaningful discussions, a neutral role, Revalia (REV), is introduced in LS but not CS. Under these actors' settings, the exercise focuses on realistic cyber incident scenarios, leveraging cutting-edge technologies to simulate real-world cases by taking the piece of new trends of the form of conflict into the following year's scenario within a cyber range. This platform has evolved to enable strategic decision-makers, legal experts, and technical professionals to hone their skills.

In the LS scenario, participants primarily take on the role of Blue Teams (BT), embodying the defenders from the BER responsible for thwarting and addressing attacks instigated by the CRI. While both technical and non-technical tracks exist within the same framework to receive new incidents or tasks, there is a disconnect in information sharing. Specifically, the situational reports generated at the technical level by the BT do not adequately inform discussions at the legal and strategic levels despite all being part of the same exercise framework. In short, there is a gap between the technical and strategy levels.

In a nutshell, the annual event brings countries together, pooling their resources and manpower for a united exercise, thus fostering collaboration at the technical level, facilitating legal and strategic responses, promoting learning, strengthening trust networks within the security community, and enhancing skills and cyber situational awareness annually.

5. Asia's Challenges and Opportunities

Russia's threat can potentially unite NATO mainly members for the LS exercise, an efficient platform for multinational collaboration. Through LS, participating nations can strengthen their cyber resilience, build trust among allies, and standardise strategic and operational approaches. Meanwhile, China's increasing cyber threat landscape extends beyond Asia to a global scale.

Despite not having formal diplomatic recognition from European Union member states, Asian countries maintain extensive informal relations and cooperation with Europe across various sectors. However, Asian countries face significant challenges, including identity issues and the need for increased collaboration and development.

However, why does the cyber status of Asian countries matter to European countries? Geopolitically, the strategic locations of Asian countries in key regions highlight the potential global economic consequences of any conflict or blockade. Economically, Asian countries play vital roles in global supply chains and trade networks. Politically, the successful democratisation processes in many Asian countries carry significant implications for regional stability and democracy promotion.

The subsequent section delves into the role of Asian countries in multinational cooperation, examining their challenges and opportunities in light of the evolving cyber threat landscape.

5.1 Challenges

5.1.1 Complicated International Political Issues

Diplomatic coercion and pressure from China are prevalent, particularly concerning countries and international organisations aligned with nations in Asia. While Russia's political influence tactics are less overt, China actively exerts its power to sway nations away from supporting Asian countries.

China's methods of exerting pressure extend beyond diplomatic channels. For instance, it consistently blocks Asian countries' participation in international organisations, denying them access to vital information and resources, especially during global crises. Economic coercion is evident, with China imposing sanctions on these nations after certain political events or policy decisions, targeting various industries and sectors.

The pressure exerted on the international stage significantly impedes Asian countries' participation in multinational cyber exercises. Organisers and participant countries face considerable pressure from China, discouraging them from engaging with other nations. Unlike Russia's pressure tactics, which may focus on geopolitical interests, China's stance on Asian countries is often treated as a binary issue. Establishing friendly relations with them is viewed by China as aligning against its interests, effectively designating their allies as adversaries of China.

Given these circumstances, many international organisations and countries prefer to maintain a friendly facade towards Asian countries, avoiding any explicit recognition or support that could provoke China. The question of their identity becomes a delicate balancing act, where expressing support risks inviting China's ire and potential retaliation. As a result, despite underlying goodwill towards these nations, most nations and international bodies opt to keep a cautious distance when their status is questioned.

5.1.2 Scattered Diplomatic Issues

In NATO, the structure is characterised by a united and multilateral framework where member countries collectively address security issues, coordinate military strategies, and conduct joint exercises under a cohesive organisational umbrella. This unified approach allows for streamlined decision-making processes, shared resources, and strong solidarity among member states. The integrated command structure and common strategic objectives facilitate a coordinated response to global security challenges, exemplifying the strength of a united defence alliance. In contrast, security cooperation in Asia primarily operates on a bilateral basis rather than through a comprehensive multilateral organisation. The US, for instance, maintains separate security alliances with South Korea, Japan, and Taiwan. These alliances are vital for regional stability but lack the overarching framework characterising NATO. Consequently, each bilateral relationship functions independently, with distinct agreements, military commitments, and strategic goals tailored to the specific needs of each partnership.

This bilateral nature of cooperation in Asia presents several challenges. Firstly, there is no unified command structure or formalised mechanism for joint decision-making across these partnerships. This can lead to fragmented responses to regional threats and a lack of cohesion in addressing broader security issues. Secondly, the absence of a multilateral defence organisation means there are limited opportunities for collective training, resource-sharing, and joint military exercises that include all these partners simultaneously. This can result in inefficiencies and missed opportunities to strengthen regional cybersecurity through collaborative efforts. Lastly, lacking a formal multilateral cyber security organisation in Asia can complicate diplomatic efforts. Each bilateral relationship must be managed separately, requiring significant diplomatic resources and often leading to inconsistent policies. Additionally, the absence of a unified Asian security organisation can make it more challenging to present a cohesive front in negotiations with major powers like China.

In summary, while NATO benefits from a united organisational structure that enhances collective security and coordinated action in cyber exercise, Asia's cooperation, predominantly based on bilateral relationships, faces challenges in achieving the same level of cohesion and strategic integration.

5.1.3 Complicated Geo-Political Issues

Asia's geo-political terrain is a mosaic of historical legacies, strategic manoeuvres, and economic entanglements, rendering it among the most intricate regions globally.

China's actions in the South China Sea epitomise this complexity. China employs a multifaceted approach by constructing and fortifying artificial islands, establishing administrative frameworks, and deploying coast guard vessels and maritime militia. Furthermore, it enforces fishing regulations and conducts resource extraction, bolstering territorial claims while projecting power without direct military engagement. This assertive stance puts pressure on nations like the Philippines, Vietnam, Malaysia, and Brunei, which are facing encroachments on their territories. Such tactics, distinct from subtler approaches, make uniting Asian nations against Chinese influence a formidable task.

The Taiwan Strait adds another layer of complexity. China's escalating pressure on Taiwan raises the potential military conflict involving the US and its allies. These tensions are exacerbated by the strategic rivalry between global powers like the US and China, extending across economic, technological, and military domains. Consequently, smaller regional players find their policies and alliances influenced by these dynamics.

In this milieu, fostering regional cooperation becomes increasingly challenging, especially for nations directly impacted by China's ambitions.

5.2 Opportunities

5.2.1 Information-Centered Focus

The AJP-3.20 Applied Joint Doctrine outlines three distinct layers for cyberspace operations: the cyber persona layer, logic, and physical layer (Organisation, 2020). China's approach has focused towards the cyber-persona layer, prioritising intelligence and information gathering.

When designing multinational cyber exercises, it is crucial to define the objectives clearly, aims, and scope from the outset (Concepts and Centre, 2023). While EU or US-centric exercises emphasise incident response, particularly in scenarios involving cyber disruptions to critical infrastructure, Asian-focused exercises may prioritise risk management and prevention strategies against social engineering, intelligence collection, and cyber espionage. The evolving tactics of major cyber actors like Russia and China influence this distinction.

The current situation, with ongoing kinetic warfare in Ukraine involving Russia, underscores Russia's focus on traditional warfare methods. Conversely, China's approach appears more information-oriented. Therefore, when designing cyber exercises tailored to the Asian context, it would be apt to emphasise intelligence-gathering and information-centric strategies, reflecting the unique cyber landscape and tactics prevalent in the region.

From insights drawn from LS, it is assumed that there is a lack of sufficient discussion and practice on information sharing and intelligence gathering. LS primarily focuses on preparing for potential threats in the physical and logical layers.

Asia countries stand to benefit from filling the gaps in discussions and practices observed in exercises like LS, particularly given the looming threats from China. While the exercises do not explicitly name potential adversaries, the geopolitical and political context suggests that exercises held in Europe primarily aim to counter threats from Russia. Asian countries participating in these exercises are gearing up to confront threats from China.

5.2.2 Information Sharing

Enhancing collaborative defence efforts and strengthening cyber resilience can be significantly augmented by integrating Information Sharing and Analysis Centers (ISACs) into cybersecurity exercises. ISACs serve as collaborative forums facilitating the sharing of cybersecurity information and best practices among members within specific sectors or industries, thereby promoting information sharing, threat intelligence exchange, and coordinated incident response among organisations, government agencies, and stakeholders. Considering the emphasis on multi-nation cooperation in exercises like LS, incorporating ISACs becomes crucial for effective practice.

In the context of cyber exercises, involving ISACs in scenarios can simulate real-world collaboration and coordination among participants facing common cyber threats. Through ISAC platforms, participants can share real-time threat intelligence, tactics, and mitigation strategies, enhancing situational awareness and enabling more effective response actions.

One of the key benefits of integrating ISACs into exercises is the opportunity to test and refine information-sharing protocols and procedures. Participants can practice exchanging threat intelligence and incident data, evaluate the effectiveness of communication channels and mechanisms, and identify areas for improvement in collaborative information-sharing processes. This iterative approach enables organisations to strengthen their collective defence capabilities, build trust, and improve information-sharing efficiency among members.

Moreover, involving ISACs fosters a culture of collaboration and cooperation among participants, overcoming traditional barriers to information sharing, such as confidentiality concerns and competitive advantage. By focusing on defending against cyber threats and mitigating potential impacts on critical infrastructure and essential services, organisations can work together within the framework of an ISAC.

Additionally, integrating ISACs into cyber exercises provides valuable cross-sector learning and knowledge exchange opportunities. Participants from different industries can share insights, lessons learned, and best practices, enriching their understanding of emerging threats and effective defence strategies. This collaborative approach enables organisations to leverage the collective expertise and experiences of the broader cybersecurity community, enhancing their ability to adapt and respond to evolving cyber threats.

Asia countries have practised a great success of ISAC systems. Take Taiwan's National Cyber Security Program (2021-2024) exemplifies the effectiveness of integrated defence systems through the establishment of Security Operation Centers (SOCs), Computer Emergency Response Teams (CERTs), and ISACs across multiple critical infrastructure domains. Coordinated by the Executive Yuan, these domains connect with CI providers to ensure cybersecurity protection and conduct united defence efforts across different sectors, contributing to national security through robust information-sharing practices and standard intelligence exchange formats.

In conclusion, including ISACs in cybersecurity exercises like LS offers numerous benefits for enhancing collaborative defence, information sharing, and incident response capabilities. Taiwan's expertise in implementing information-sharing systems serves as a valuable example for other nations, highlighting the pivotal role of ISACs in strengthening cyber resilience and mitigating the impact of cyber threats on critical infrastructure and organisations.

5.2.3 *Joining Existing Fraternity or Establishing a New One*

Under China's influence, Asian countries face challenges in joining existing multinational cyber cooperation organisations or establishing platforms to attract NATO members. Despite this pressure, there has been some progress in fostering multinational cooperation.

For instance, in the 2024 LS, Asia countries such as Korea, Japan, and Singapore successfully collaborated with NATO member states, participating in the BT. Moreover, their efforts in supporting Red Team operations, White Team coordination, and Green Team infrastructure setup have been commendable, showcasing practical cooperation.

However, nations like Taiwan, which are confronting more acute challenges, encounter political and diplomatic hurdles in participating in exercises dominated by NATO members. In response, Taiwan is exploring alternative avenues, such as hosting its exercises and inviting NATO members to participate.

The Taiwan Administration for Cyber Security, MODA, hosted Cyber offensive and Defensive Exercises for years to promote global cooperation in cyber security defence. In 2023, the event attracted participation from 18 international cybersecurity organisations working in one of the critical infrastructures - water resources sectors to build a simulated cyber range. Unlike the rule in the LS, in which all BTs are representative of BER, Taiwan's water company served as the BT. At the same time, the RT consisted of countries like the US and the Czech Republic, joint teams from government agencies, and award-winning participants from Taiwan in international hacking competitions.

In addition to the technical-level exercise, the non-technical part is hosted in the conference format - The Advanced Cybersecurity Exploration Conference (ACE), which brought together scholars, industry representatives, and government officials worldwide to focus on two major cybersecurity issues: critical infrastructure security and risk management for emerging technologies. The ACE conducted an in-depth analysis of recent cyber security threats to Taiwan and corresponding strategies. Other speakers from Estonia, Australia, Albania, and other countries in the field of cyber security shared insights on topics such as geopolitical dynamics and emerging threats, the importance of cyber security, and risk management policies (李昱緯, 2023).

In conclusion, Japan, Korea, and Singapore, among others, strive to integrate into the Western sphere of cyber activities and cooperation, a pursuit that has yielded good progress. Their dedication to aligning with Western standards and practices reflects their commitment to global cybersecurity efforts. Meanwhile, Taiwan's endeavours to participate in NATO-led initiatives have faced obstacles, yet it has proactively engaged in alternative strategies, such as hosting exercises and inviting Western participation. These approaches demonstrate innovative thinking and determination in bridging gaps and fostering collaboration with strengths.

6. Conclusion

Europe has established a robust framework for multinational cooperation in cybersecurity, marked by regular exercises and strategic partnerships, significantly bolstering the collective cyber defence capabilities of nations across the continent. Key exercises like NATO's CMX and Cyber Coalition have played pivotal roles in cultivating trust, improving communication, and nurturing a sense of camaraderie among participating countries.

Given the persistent cyber threats faced by various Asian countries, their integration into the European cyber

community could yield substantial benefits. Drawing upon their extensive experience in dealing with cyber threats, these Asian nations could offer valuable insights, enriching the resilience of the European cyber defence network. By actively participating in European cyber-security exercises and sharing their expertise, countries stand to contribute to and gain from the collective strength of these partnerships.

Furthermore, becoming part of the European cyber community would enable Asian countries to forge stronger international relationships, fostering trust and cooperation on a global scale. This integration could facilitate the development of joint strategies, shared resources, and a unified approach to countering cyber threats. In an increasingly interconnected world where cyber threats transcend geographical boundaries, the participation of Asian countries in European cybersecurity initiatives would not only bolster their defences but also contribute to the broader global endeavour to uphold secure and resilient cyberspace.

Acknowledgements

I want to express my sincere gratitude to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) for their invaluable support. The expertise, resources, and guidance provided by CCDCOE were instrumental in completing this work.

References

CSIS Center for Strategic & International Studies. Significant cyber incidents, 2024.

The Development Concepts and Doctrine Centre. Influence Wargaming Handbook. UK Ministry of Defence, 2023.

National Research Council, Global Affairs, Division on Engineering, Physical Sciences, Computer Science, Telecommunications Board, Committee on Deterring Cyberattacks, Informing Strategies, and Developing Options for US Policy. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy. National Academies Press, 2010.

Myles D Garvey. A philosophical examination on the definition of cyberspace. In Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions, pages 1–11. World Scientific, 2021.

Lyu Jinghua. What are China's cyber capabilities and intentions?, 2019. URL https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intention [Accessed:19/04/2024].

Elsa Kania, Samm Sacks, Paul Triolo, and Graham Webster. China's strategic thinking on building power in cyberspace, 2017. URL
https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-buildin
Accessed: 19/04/2024.

Huansheng Ning, Xiaozhen Ye, Mohammed Amine Bouras, Dawei Wei, and Mahmoud Daneshmand. General cyberspace: Cyberspace and cyber-enabled spaces. IEEE Internet of Things Journal, 5(3):1843–1856, 2018.

North Atlantic Treaty Organisation. Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations. UK Ministry of Defence, 2020.

NORTH ATLANTIC TREATY ORGANISATION. AJP-3.20 ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS. NATO STANDARDISA- TION OFFICE (NSO), 2020.

David Ormrod and Benjamin Turnbull. The cyber conceptual framework for developing military doctrine. Defence Studies, 16(3):270–298, 2016.

Official publication of legal acts. Presidential decree of 12.5.2016 number 646 "on approval of the doctrine of the russian federation information security, unknown. URL
http://publication.pravo.gov.ru/Document/GetFile/0001201612060002?type=pdf [Accessed:25/05/2024].

Juma Mdimu Rugina. Economic cyber espionage: The us-china dilemma. Ulus- lararası I˙li¸skiler C¸ alı¸smaları Dergisi, 3(2):77–90, 2023.

Max Smeets. The role of military cyber exercises: A case study of locked shields. In 2022 14th International Conference on Cyber Conflict: Keep Mov- ing!(CyCon), volume 700, pages 9–25. IEEE, 2022.

Yu I Starodubtsev, EG Balenko, EV Vershennik, and VH Fedorov. Cyberspace: terminology, properties, problems of operation. In 2020 International Multi- Conference on Industrial Engineering and Modern Technologies (FarEast-Con), pages 1–3. IEEE, 2020.

丁. 《新代的中防》白皮全文, 2019. http://www.mod.gov.cn/gfbw/fgwx/bps/4846424.html [Accessed: 20/09/2023].

中央网安全和信息化委. "十四五"家信息化划, 2021. URL ttps://www.gov.cn/xinwen/2021-12/28/5664873/files/1760823a103e4d75ac681564fe481af4.pdf [Accessed: 08/04/2024].

李昱緯. 18國資安專家匯聚code 2023活動展現台灣資安戰力, 2023. URL https://moda.gov.tw/ACS/press/news/press/8583 [Accessed: 7/5/2024].

防研究所. Nids china security report 中安全略告2021 新代的中事略. Technical report, 防研究所, 2021.