June 2026

Research Paper

Managing Geopolitical Cyber Security Risks

by Aude Chocard,
Regulatory Affairs Intern at BIMCO

Abstract

This research paper explores how to develop a **geopolitical strategy in maritime cyber security**. Digitalisation has become complex for the shipping industry, involving many new technologies and external vendors. It may lead to dependencies with the suppliers, making the systems vulnerable to cyber incidents in a context of geopolitical instability. In times of conflict, a shipping company can be targeted through its digital infrastructure and be caught in the middle of competing interests between States. This research paper will provide an overview of current political strategies and help determine whether they present a risk to shipowners.

Contents

Introduction

The purpose of this research paper is to explore aspects of **making the shipping industry more resilient** to cyber risks in a context of geopolitical instability. The research paper will describe a practical strategy for shipowners to identify vulnerabilities in Information Technology (IT) and Operational Technology (OT) systems and anticipate cyber-attacks.

IT systems used in the shipping industry have become complex and interconnected. Today, there are many ways for a company to integrate digital technologies into its activities. A company can choose to develop its own systems or to use existing solutions from external suppliers. This decision is based on whether the company decides to prioritise operational optimisation, cost savings, safety improvements or sustainable development.

Because a single company may have various types of suppliers to maximise cost-effectiveness, flaws in IT systems can arise. Securing computer systems is essential to prevent interruptions in business operations. In the case of a vendor involved in a geopolitical conflict, the company can be targeted or indirectly affected.

This paper will explore a methodology for shipowners to assess the reliability of their systems and whether they can be the target of a cyber-attack. It will be applicable to their own situation, based on the characteristics of their company and the digital tools they use. There is a need to consider geopolitics in the decision-making of cyber security policies, in order to assess the threat. It will also help to react quickly and efficiently in the case of geopolitical incident that involves technology stakeholders.

Cyber risk management is needed through regulations and guidelines. The following document builds on the risk assessment done in the *Guidelines on Cyber Security Onboard Ships version 5*, released in 2024. It goes in line with the same approach, considering also new computer systems and the use of artificial intelligence (AI), and adding a geopolitical perspective. The research paper has been based on the *NIST Framework* and the *IMO Guidelines on Maritime Cyber Risk Management* under the resolution *MSC-FAL.1/Circ.3/Rev.3*.

1. Cyber security and geopolitics in the maritime sector

1.1 A context of digitalisation

Digitalisation has significantly grown in the maritime sector, to improve operations, compliance, and efficiency. Complex technologies in ports and on board may contain vulnerabilities when subject to geopolitical interests, leading to cyber incidents. A strong cyber security policy is essential.

Digitalisation has advanced rapidly in the economy and is transforming the maritime industry. It has become essential to integrate various technologies in port facilities and onboard vessels to enhance the resilience and competitiveness of the maritime supply chain.

Modern ships are becoming increasingly digitalised. New communication and navigation systems facilitate data exchange, providing real-time reporting and coordinated data analytics. Automated systems using satellite and radio technology are greatly needed in the maritime sector to increase efficiency, as they improve decision-making and reduce the likelihood of errors.

However, digitalisation in the maritime industry has raised complex and new flaws. Automated systems can be diverted from their intended purpose, affecting the company's operations, and the maritime sector is no exception. Hackers can exploit vulnerabilities in these systems, when they are not secured enough and can be accessed easily by outsiders. Cyber security incidents have arisen, based on the *Maritime Cyber Threat White Paper 2026* by CYTUR, noting that the number of maritime cyber incidents in 2025 has surged by 103% compared to 2024. Most are identified as Distributed Denial of Service (DDoS), ransomware, or malware, but they can also manifest as authentication attacks, phishing campaigns, Operational Technology (OT) system intrusions, espionage, or even Global Navigation Satellite System (GNSS) and Automatic Identification Systems (AIS) interference.

It is likely that threats directed against maritime equipment will increase in 2026. According to the *Annual Threat Assessment 2026* from the Norwegian Maritime Cyber Resilience Centre (NORMA Cyber), even though targeted attacks in the maritime sector remain unlikely, weak security architectures and lack of compliance are making IT networks more exposed. Shipowners need to be aware of their systems' vulnerabilities as they are constantly evolving.

More specifically, cyber risks need to be analysed from a geopolitical perspective. Maritime trade has become global, involving various stakeholders, including States as well as non-State actors. Geopolitical instability raises concerns because it can jeopardise the efficient functioning of IT systems. One significant case identified is the NotPetya ransomware attack in 2017, which affected shipping giant Maersk. While the original intent of the Russian hackers Sandworm was to target Ukrainian companies in the context of cyber warfare between Russia and Ukraine, computers from companies worldwide were compromised.

The NotPetya attack and the example of Maersk have shown shipping companies the possible intentions of malicious actors, and the consequences of outdated devices and unpatched systems. Even more recently, the hacker group Lab Dookhtegan has paralysed communications on Iranian vessels in 2025, demonstrating the capacity to penetrate and destroy onboard networks. Finally, the current challenge of GPS interference has become an issue as it can affect the safety of navigation. Since the beginning of the conflict in the Middle East, GPS jamming and spoofing around the Strait of Hormuz continue to impact vessels' AIS and to worry shipping companies about what will happen next.

These examples show that the geopolitical landscape and interstate relations can directly impact IT security and the functioning of a shipping company. In general, the maritime sector continues to be vulnerable due to critical infrastructure at sea, conflicts over strategic maritime routes, and chokepoints. Some regions have become particularly sensitive due to their strategic positions and can be coveted for their energy resources or for military reasons, for example. The industry must integrate geopolitics into its strategy, and the IT department must consider it as well in its decision-making. Cyber security risk management has now become essential to ensure the maintenance of the company's services and anticipate the potential risks.

As the digital sector is now concentrated in a few States and non-State actors, they have the monopoly to decide the future of maritime transportation. This situation creates dependencies and new geopolitical dynamics, depending on capabilities and vulnerabilities of the different actors.

1.2 Competition between US and China as a driver of the maritime sector

The US-China relationship is today the backbone of the maritime trade. The current competition between the two States' strategies can fragilise the reliability of a company's vendors, if they rely on American and Chinese companies. Technology exchanges between the US and China may be confronted with their respective legal decisions.

The US and China are the two world's biggest trading nations. Decisions from their governments shape the maritime industry as they control shipping routes, having the possibility to implement tariffs or blockades that will have consequences for the global economy. Maritime trade has evolved in a bipolar world in which countries align themselves with one of two blocs. The national policies of these two States need to be considered, as other countries often rely on products and services that have been initially developed by American or Chinese companies.

Beyond the respective strategies of these two States, their relation is very important. Whether they decide to cooperate or to act alone, it will have different implications for the shipping companies collaborating with one or both States.

At the moment, the level of economic competitiveness in the maritime sector can seem tense. Both nations want to lead and gain the upper hand over the other. However, it appears that China has become dominant in shipbuilding due to massive investments over the last couple of decades. China's ship building market share surged from a mere 5 percent of the world total in 2000 to over 53 percent

in 2024[1]. China also tries to create alternative routes for its exports to Europe to avoid traditional shipping channels controlled by the US and its allies.

On the other hand, US production capacity remains well below China's. The US Navy is also facing persistent delays and labour shortages. There is a key vulnerability in the US defence industrial base, as it relies on China's industry, along with weaknesses in US port terminals that are run by foreign companies. In response, Trump has called for a revival of the US shipbuilding to counter China's ascendant maritime power. A *Maritime Action Plan* has been announced (February 2026) to increase shipyard construction and make an American cargo fleet on its own more sustainable. This plan aligns with Trump's strategy of *Restoring America's Maritime Dominance*.

In the context of digitalisation, the maritime sector is witnessing a technological competition between the US and China, as both States try to be at the forefront of innovation. Beijing has long promoted a policy known as "Xinchuang" which aims to achieve self-reliance and self-sufficiency in the technology sector. China intends to replace foreign software, hardware, and other IT systems with domestically produced equivalents. In January 2026, Chinese companies have been banned from using cyber security service providers from the US such as Palo Alto Networks, CrowdStrike or McAfee. This demonstrates the defiance between the two States, as these US providers have been considered as a critical national security issue for China's government, claiming they could collect sensitive data.

A directive known as "Delete America" has also been initiated to remove reliance on US technology. This way, China attempts to reduce the possible impact of US sanctions and tariffs on its companies. From the US perspective, the sanctioned Chinese companies are considered a threat because they possess advanced technologies and capabilities.[2]

There is a complex connection between China and the US, as Trump's aggressive strategy aims to become completely independent from China, but US infrastructure still uses digital elements from China. China's digital control is significant, as US seaports continue to rely on Chinese port technology. ZPMC (Shanghai Zhenhua Heavy Industries) operates for the global market and for 80 percent of cranes in US ports. The platform for logistics communication LOGINK is also widely used in the US maritime industry. However, this platform for information exchange can have implications for data privacy, with the Chinese government having access to information about US fleet and operating systems.

1.3 The rise of complex alliances and strategic rivalries

Geopolitical alliances based on the US-China rivalry create multiple dependencies. European companies are in the middle, as they mainly rely on American companies but also trade with Chinese providers when it comes to technology. Geopolitical ambitions and conflicts between jurisdictions could hinder the original US-EU cooperation.

[1] Matthew P. FUNAIOLE, Brian HART, and Aidan POWERS-RIGGS, "Murky Waters, Navigating the Risks of China's Dual-Use Shipyards", Center for Strategic and International Studies, 25 March 2025

[2] Xiaowei LIN, Pengdong ZHANG, Zhihao YANG, Sicen CHEN, "US sanctions and corporate innovation: Evidence from Chinese listed firms", International Review of Economics & Finance, March 2025

Noting a divided maritime sector between American and Chinese national strategies and own interests, two blocs have arisen as countries choose to collaborate with the US or China. As explained before, it has become difficult to use their services without any risk of dependency or data theft. With many stakeholders and other States involved, geopolitical alliances have become complex, creating multiple dependencies.

Considering the Western bloc initially, European countries collaborate with the US and use products and services from American companies. However, the transatlantic relationship can seem tense due to this dependency, since political decisions from the US government could directly impact European countries. The EU now wants to achieve technological independence from the US and develop "sovereign cloud" solutions based in Europe. However, developing its own solutions requires time and coordination within European countries and is costly in the short term.

Moreover, the EU and the US don't have the same regulations and standards. While the US lacks comprehensive digital policy governance on one side, the EU wants to capitalise on security and encryption on the other side. Issues of data privacy and reliable IT networks find themselves in the middle of two different perspectives, which can impact the cooperation between the US and the EU.

As an opposition, China, Russia and Iran have come together as US' adversaries. They cooperate to build digital solutions independently from the US. For instance, Iran provides access to ports and maritime infrastructure to its allies like China, and in return, Chinese companies have helped Iran to develop digital and surveillance capability. They also share common purposes such as China and Russia regarding the Arctic battleground and the Northern Sea Route. Finally, they serve each other's interests when we consider their positions in conflicts, such as in the Iran War and the strategic chokepoint of the Strait of Hormuz.

If the maritime sector is mainly defined by the US and China, Europe has also a role to play. The EU is in the midst of this opposition, trading with both US and Chinese providers for different purposes. However, these different approaches are likely to converge in the IT systems, creating a **double dependence** even more hazardous for European maritime trade. Europe could face supply chain disruptions or sanctions, because of China's control over global supply chains or US' extraterritoriality.

For example, in the case of green technology, "*the US could demand Europe remove Chinese technology from its energy systems or face tariffs, sanctions or reduced security commitments*"[3]. Because Europe is heavily dependent on Chinese green technology and that systems from the US are used in Europe, the US wants to avoid a possible surveillance from China. It forces Europe to support vendors from only one side as the US and China have conflicting requirements, or to develop its own solutions.

[3] Attracta MOONEY, "Chinese green technology poses national security problem for Europe, report warns", Financial Times, 29 April 2026

Given the complex relationship between US and China, we can assess whether a State, like China or the US, represents a threat for others and could engage cyber-attacks. It refers to the situation in which a State causes disruptions for others by using cyber means, causing political instability, economic pressure or security and military risks. In this scenario, the threat is determined by a set of variables: the intent, the capability and the opportunity of conducting cyber operations. (See more about these variables in 3.2)

Table: Description of China's threat assessment

China's threat assessment	
Intent	Targeting the US and its critical infrastructure - Hack of telecommunications companies (2024) - Cyber espionage of the Treasury Department (seeking information, not stealing funds) - Targeting the phones of powerful individuals (D. Trump, K. Harris) - Collecting data that could benefit the Chinese government Cyber espionage activities: South China Sea and Taiwan (leverage point for China and the US)
Capability	Means and skills - System of "military-civil fusion" - Expansion of private sector involvement in supply chains - China's layered defences: the Great Firewall
Opportunity	Economic alliances and dependencies with Russia and Iran Trade agreements with Greece, Canada, due to geopolitical uncertainty and higher tariffs with the US Proxy groups and State-sponsored advanced persistent threats (APTs): Volt Typhoon, Salt Typhoon and APT31

Table: Description of US' threat assessment

US' threat assessment	
Intent	Trump's strategy: "defend forward" approach - Targeting "enemies" with a focus on China, Iran, Russia and North Korea - Leading "offensive cyber operations" - Shaping adversary behaviour (National Security Strategy)
Capability	Reducing investments in countering Russian cyber threats - Strategy to pause all "offensive operations against Russia" and "de-escalate" tensions with Russia - Increase of cyber-attacks in Europe as a direct consequence Limiting regulatory frameworks - CISA's budget reduced - Job cuts in cyber defence agencies and transition to the private sector: Concerns about information sharing and declassification by CISA
Opportunity	US dependence on Chinese electronics and components creates major national security risks Public-private partnerships: less barriers to threat information sharing between government and the private sector 45% of US cloud databases are publicly accessible due to incorrect configuration or missing access controls

2. Identify key IT / OT systems components

Digital systems used by shipping companies can be compromised and are vulnerable to cyber-attacks. Identifying digital tools is necessary to ensure they are reasonably and sufficiently secured to then ensure business continuity despite a cyber incident. Critical IT and OT systems include software and hardware elements that are connected to the Internet, as well as data storage related to online and cloud solutions, and new AI platforms.

Shipowners should focus on the third parties they negotiate and work with to obtain these systems, because the nature and the origin of the supplier can influence whether the digital product or service is reliable or not. States do indeed have different models, jurisdictions and constraints, which a shipping company must consider before committing to a supplier.

Why securing IT / OT systems

Unreliable IT and OT systems can affect a business in two main aspects. The first one is **data surveillance** and data theft. When IT systems lack of security, they could be subject to breaches. If the systems can be easily hacked or accessed by an outsider, the data from the company could be stolen or used for malicious purposes. Workers and customers can be affected, and it can also undermine the company's reputation and trust in it.

On the other hand, lack of security may result in **supply chain disruption**, even though it remains unlikely. When the activity relies on the delivery of a product or service from one or several vendors, the company becomes dependent on their ability and willingness to provide that product or service. If a vendor is deficient or if the company didn't anticipate their decision to no longer wish to do business with its supplier, the activity could be possibly interrupted.

2.1 Software and hardware elements

Software and hardware systems are often intertwined and may be considered at risk if their operation is unreliable. Three things need to be identified to be aware of dependencies: the origin of the system supplier and the jurisdictions it follows, the potential external dependencies related to the supplier, and finally, the person responsible for the control of IT systems. Creating a personal and "neutral" solutions can help reduce dependencies.

Software and hardware systems manufacturers are widespread around the world. Software systems refer to computer programs, and are used as a platform between hardware, the physical part of the system, and the user. Using software and hardware from different companies has become common to maximise technical gains. However, it is important to consider the characteristics from the systems used to make sure they are compatible and can function together.

To identify the main geopolitical vulnerabilities of software and hardware systems, the first question to raise relates to **the origin of the system supplier and the regulatory framework they**

operate under. Depending on the country that the company you work with is based, standards are not the same. Every country has its own jurisdictions, and these jurisdictions apply to IT and OT systems.

As an example, US jurisdictions require certain practices that can prevent dealing with other suppliers. It is necessary to follow these requirements if based in the US or working with US vendors. The Federal Communications Commission (FCC) regularly updates its *Covered List* of communications equipment and services that the US government has determined pose an "unacceptable risk to US national security" and so could be forbidden to use. From this list, it appears that telecommunications equipment produced by Huawei Technologies Company and ZTE Corporation, both Chinese companies, have been banned[4].

Because Trump's administration has recently emphasised a policy aimed at strengthening national security (see National Cybersecurity Strategy), this list is subject to change and may include additional equipment, that will be prohibited from use according to US laws. In March 2026, the FCC added to its list "all consumer-grade routers produced in foreign countries"[5]. Since April 30, Chinese labs are also preventing from testing electronic devices for use in the United States. A proposal could soon add restrictions regarding the connection between Chinese and American companies. Regarding software, Donald Trump tried to ban the Chinese application TikTok over national security concerns.

Then, it is necessary to **be aware of any external supplier dependencies**. The user must know to which other companies the supplier refers, because if multiple vendors are involved in one system, it can require different conditions. If the system supplier relies itself on other vendors and jurisdictions, it means that the company relies on multiple dependencies. This situation makes also the company vulnerable, as the default is more likely to happen, and creates more costs, as it will need to verify compliance with more regulations to ensure the security of the entire IT architecture.

Moreover, if any actor that can have a strategic interest in hacking or destroying systems is involved with the vendor's activity, a threat arises regarding the possibility of a cyber-attack. Dependencies make the systems unreliable and prone to malfunctions.

Because Software and Hardware systems have become interdependent, vendors working together tend to be based in the same country and rely on the same regulations. As an example, the collaboration of Google and NVIDIA has been chosen as these two companies both come from the US. It is easier to merge the work culture and requirements from only one country.

It is finally important to consider the people in control of the system. To use the software efficiently, information is needed about who is in charge of updating and maintaining it. It helps to target those responsible in case of a default and know who decides and can actually react. Different people can be recalled depending on the needs and current issues, and it is important that the main person who uses the system can have full control on it. Additionally, managing access on software and

[4] "List of Equipment and Services Covered By Section 2 of The Secure Networks Act", Federal Communications Commission, 15 June 2026

[5] "FACT SHEET: FCC Updates Covered List to Include Foreign-Made Consumer Routers, Prohibiting Approval of New Models", Federal Communications Commission, 23 March 2026

hardware systems is very important to avoid interferences, so that an external user won't be able to reach the system and exploit its vulnerabilities.

On a general note, **it is highly recommended to use various and independent IT systems**, that can be easily substituted and considered as "neutral" for other parties you may work with. It is important to find the right balance, having vendors from different places as it is likely that companies from a same place won't work at the same time, but ensuring they are compatible.

It is also better for a company to develop its own solutions, as a way to have full control over their installation, maintenance, and repair, which generally makes them last longer. As explained before, it is possible that the ship's operational continuity is tied to US ecosystems, which is why it is necessary to have backups and other solutions to not be affected by US government's decisions. Otherwise, when reaching out to another vendor, it can cost a lot to start over and transition to entire new systems.

An overview of the main Software Manufacturers

The table below indicates the origin of some main software manufacturers regarding different types of software (operating systems, web applications…). This table helps to identify under which national laws a company operates. Access to a software system from US, the EU or China, as well as compatibility between these systems, may vary depending on national constraints.

The most widely used software systems come from the US, as they offer advanced and high-performance technology thanks to US companies based in innovation hubs (Silicon Valley...). This way, the Internet technology giants GAMAM, that refer to Google, Amazon, Meta (formerly Facebook), Apple and Microsoft, have hold a hegemonic position in software systems. Google Chrome has become for example the most widely used web browser in the world, with approximately 71% of the global market share.[6] As these types of companies operate together, using software from a company in the US often entails reliance on the whole software system from the US.

However, some systems such as cyber security protections from the US have been forbidden in China (see 1.2). The same way, Chinese software systems are widespread in China and Southeast Asia but remain less common, as some are only available in China but also because the US has designated some systems from China as a "US national-security risk"[7]. European countries are still in the middle and mainly rely on US systems, as no European company really stands out.

[6] Robert A. LEE, "Web Browser Usage Statistics 2026: Market Shifts Now", SQ magazine, 11 February 2026
[7] Heather SOMERVILLE, "US Expands List of Chinese Tech Companies It Says Assist Beijing's Military", The Wall Street Journal, 9 June 2026

Table: Description of the various software systems by country of origin

SOFTWARE SYSTEMS			
System software (operating systems…)	Microsoft Windows, Apple macOS, Android	Ubuntu (UK), SUSE (Germany)	HarmoneyOS from Huawei, Deepin OS
Consumer applications (web browsers, social media, media players…)	Google Chrome, Amazon, Mozilla Firefox, Instagram	Vivaldi Browser (Norway), Spotify (Sweden)	QQ Browser from Tencent, UC Browser from Alibaba, TikTok
Productivity Software	Microsoft Office Suite, Google Workspace	LibreOffice (Germany)	WPS Office, Tencent Docs
Communication Software	Slack, Zoom, Microsoft Teams, Discord	Wire (Germany), Element (UK)	WeChat
Security Software	Norton Security, Malwarebytes, McAfee	BitDefender (Romania), Avast (Czech Republic), Eset (Slovakia)	Qihoo 360, Tencent security

An overview of the main Hardware Manufacturers

Hardware systems refer to the physical components of a computer network, as opposed to software systems. The table below indicates the origin of some main hardware manufacturers regarding different types of hardware.

As is the case with software systems, there are many American companies that specialise in hardware systems. We can also find hardware manufacturers based in Japan and South Korea, both collaborating to lead the tech sector, for example with semiconductor partnerships. Additionally, China rapidly advances in high-tech, and their products stand out from American products. "*Chinese developers are increasingly relying on local hardware, with companies like Huawei, Cambricon, Moore Threads, and MetaX*"[8].

Table: Description of the various hardware systems by country of origin

HARDWARE SYSTEMS				
Processing Devices	Apple, Dell, HP	Atos (France), Medion (Germany)	Lenovo, Huawei, Xiaomi	Fujitsu, Panasonic, LG, ASUS, Acer
Internal components (Central Processing Units, Random Access Memory)	Intel, AMD, Apple, NVIDIA, IBM, Micron Technology	ARM (UK), NXP Semiconductors (Netherlands)	HiSilicon Huawei, Loogson	Samsung Electronics, SK Hynix,
Input devices (Keyboard, Mouse, Image scanner)	Corsair, Microsoft, Razer	Logitech (Switzerland), Steelseries (Denmark)	Rapoo, Redragon, Ajazz	Canon, Fujitsu
Output devices (Printer, Headphones)	HP, Bose	Sennheiser (Germany), Barco (Belgium), Philips (Netherlands)	BOE Technology	Canon, Sony
Networks (Routers, Switches)	Netgear, Starlink	Nokia (Finland), Siemens (Germany)	Huawei, ZTE	Panasonic

[8] Anton SHILOV, "Jensen says Nvidia now has 'zero percent' market share in China — says US export policy 'has already largely backfired'", Tom's Hardware, 3 May 2026

2.2 Data storage solutions

Online data storage presents vulnerabilities. The data storage solution used by a company actually relies on jurisdictions in which the cloud service provider is established, and not where the physical servers are based. It is necessary to identify the potential conflicts between the rules the company operates under and those applied to the vendor. In times of opposing geopolitical interests, business operations could be threatened if the cloud solution is interrupted.

The way a company stores its data can influence the capacity for a company to ensure business continuity. By relying on external vendors, and especially cloud solutions, the company relies on a digital platform it cannot control. However, the data from the company needs to be secured against intrusions and to be easily accessible for employees.

Surely, when using a cloud solution, it is possible to identify the location of the physical servers that store the company's data. Because data storage can be materialised, it appears to be secure. A cloud storage provider could ensure that the servers are based in Europe when it deals with a European company, showing proximity and a facilitated access to the data. That means that there is a sense of trust that the data meets high standards in terms of confidentiality, integrity and availability.

However, data fall under jurisdictions in which the cloud service provider is established, according to the US Cloud Act passed in 2018.[9] It means that the regulations that apply are tied to the origin of the cloud service provider and not the location of the servers. In this sense, knowing the location of the data doesn't mean knowing the legal system governing. Monitoring data residency and the geographical location of data is different from ensuring data sovereignty.

Storing data on cloud storage solutions can present vulnerabilities because the jurisdictions that the provider relies on can be in conflict with the jurisdictions under the company. The same as for software and hardware elements, the cloud storage company can also rely on external vendors, which can imply overlapping jurisdictions.

When looking at the European cloud market, **US providers account for two-thirds of the EU cloud services.** It is very likely that a company based in Europe relies on an American provider, meaning it will follow US jurisdictions primarily. However, the EU and the US don't have the same regulations, especially regarding data privacy. For instance, Amazon Web Services (AWS) is the main supplier in Europe, but there is no evidence that the service complies with the EU Cloud Code of Conduct, an extension of the GDPR[10]. US providers could collect data and interfere because they rely on extra-European laws. Identifying the person in charge of the data storage ensures it is stored in a secure manner.

Additionally, cloud storage can be used as a geopolitical weapon. Access to data storage could be interrupted if the supplier decides or is forced to do so, directly affecting the company. This concern

[9] "White Paper Demystifying the debate on the US CLOUD Act vs European/UK Data Sovereignty in the context of cloud services", CMS law firm, 3 February 2026
[10] General Data Protection Regulation (GDPR) – Legal Text, 2018

has been justified after Microsoft disconnected ICC Chief Prosecutor Karim Khan's Outlook email account, following an executive order from Donald Trump.[11] The US President imposed this sanction after arrest warrants related to Israeli officials over alleged war crimes in Gaza. This case has showed the government's ability to regulate the activities of domestic companies outside their home country. If in principle, the penalty was applied only to that individual, it raises a fear of a **"digital kill switch"**, in which entire departments might be implicated in these sanctions.

Because European companies rely on US vendors and therefore US policies, the US and Trump's administration could leverage this dependency for geopolitical ends. The US have the power to disrupt the business activity of European companies that rely on American providers, which would force Europeans to comply with US demands or be subjected to financial sanctions. For instance, given the ambition to annex Greenland, the US could also threaten Danish companies to block access to cloud service providers from the US. While perhaps less likely because American companies claim to be independent from Trump's political decisions, there has been an increase in public-private partnerships in the US, which could create a real risk in the end.

To limit cyber security vulnerabilities, the company should store its data in multiple ways and backup data on safe and external devices. Creating copies of files help to restart the activity if it has been interrupted without losing information.

An overview of Cloud Storage Solutions

Cloud data storage solutions are mainly based in the US and owned by GAMAM. Main providers are AWS, Microsoft Azure, and Google Cloud, known as the "Big Three", which hold for 63% of cloud share market[12]. Other solutions like Rackspace, DigitalOcean, Tencent Cloud (<1% individually) only represent 30% of market share. China on its side tries to rely only on local players, as Tencent Cloud held around 15% of China's market in Q3 2024.

2.3 Artificial Intelligence platforms

AI platforms also present vulnerabilities. In the context of the US-China AI competition, States invest massively to develop their own AI solutions. Using AI from a vendor based in a different country means it could have control over its functioning. It is essential to be aware whether the AI system is compatible with digital tools used by the company. The company's data could also be analysed using the AI system.

AI platforms can finally present vulnerabilities as they have become widely used by companies. They are strongly connected to existing software, hardware and cloud storage providers. The biggest tech companies try to capitalise on this new AI phenomenon, and there is already a monopoly of a few AI systems. It is then very likely for a company to have even more dependencies with the use of AI.

[11] Sam CLARK, "Microsoft didn't cut services to International Criminal Court, its president says", Politico, 4 June 2025

[12] "Cloud Market Share Trends - Big Three Together Hold 63% while Oracle and the Neoclouds Inch Higher", RENO, NV, Synergy Research Group, 19 November 2025

The tech competition is now focusing on an **"AI race"** between the US and China. The US has lead AI development for the last years, with major firms such as OpenAI, Anthropic and Alphabet. The Generative AI agent Chat GPT was the first mainstream large language model (LLM) ever created. Today, almost one in eight people on the planet uses it[13].

The US is trying to maintain its monopoly in AI, by developing protectionist policies towards China. With the proposed MATCH Act (April 2026), the US is trying to prevent Chinese factories from manufacturing computer chips on their own by restricting exports from US allies. This law would concern the Dutch company ASML[14], a leader in extreme ultraviolet (EUV) and DUV lithography machines. Since China accounted for 33% of ASML's sales in 2025, AI Chinese companies won't be able to operate and will need to find an other supplier. This US law shows how dependencies create vulnerabilities.

On its side, China is trying to close the gap in the AI race with the US, and two AI clusters have been officially established. To reduce dependencies, China has launched its own AI-powered chatbot: DeepSeek. The power struggle in AI software has become more complex, as China is developing cost-effective solutions that could compete with the highly effective tools used in the US. Regarding AI hardware, China is leading the development of semiconductors, robots and autonomous vehicles. By developing local hardware solutions and considering the restrictions from the US, China has become independent from the US. As an example, NVIDIA's market share of AI accelerators in China has now dropped to 0%[15].

China is not the only one to reduce its dependency from the US, as new AI development hubs are also emerging (European Union, African Union, Brazil, Australia). The EU is investing to develop AI capabilities, so that its new AI systems would comply with its own jurisdictions.

Using AI as a company implies relying on multi vendors, and external confidentiality policies. The functioning of an AI platform could be disrupted if it depends on components that the AI company doesn't have the control over. It has been observed that US tech giants such as Google or Microsoft have made massive investments in AI start-ups like Open AI. Additionally, the US Department of State has invested in AI for the military[16].

There is a need to be aware of the various actors involved and the public-private partnerships when using an AI system. The AI system must be compatible with the other IT systems used, ie be compliant with other jurisdictions on which the company relies. Regarding Open AI, there is a possibility of a breach of data privacy and of causing unfair competition in the tech sector. These dependencies in the tech sector are criticised by the EU and the UK, which could threaten the use of AI in these areas.

---

[13] Misha GLENNY, Luke MINTZ, "China is winning one AI race, the US another - but either might pull ahead", BBC, 7 April 2026

[14] Toby STERLING, "US targets Chinese chipmaking with proposed export restrictions on ASML and others", Reuters, 3 April 2026

[15] Anton SHILOV, "Jensen says Nvidia now has 'zero percent' market share in China — says US export policy 'has already largely backfired'", Tom's Hardware, 3 May 2026

[16] "United States and Eight Companies Launch the Partnership for Global Inclusivity on AI", Office of the Spokesperson, 23 September 2024

3. Guidance to evaluate the risk for a shipowner

There is a need to consider geopolitical alliances and adapt the business strategy to not rely on external vendors. Shipowners must be aware of the digital technologies used in the company to ensure business continuity and avoid cyber incidents. Cost-effective solutions must be considered on the long run after a risk analysis, because dependencies can create additional costs when the service you rely on is not working and you need a last-minute solution.

The following method will help characterise the business and the possible dependencies according to the chosen organisation. It enables the identification of threat actors and the interstate conflicts that may affect the company, to then know the source of cyber-attacks and the risks they can generate. The geopolitical context makes the threats more complex because States as well as non-State actors interact with each other and can be both responsible. They can have various motives but still find a common interest, which may combine political, economic, and military resources. The purpose is to identify when an actor can be considered a threat.

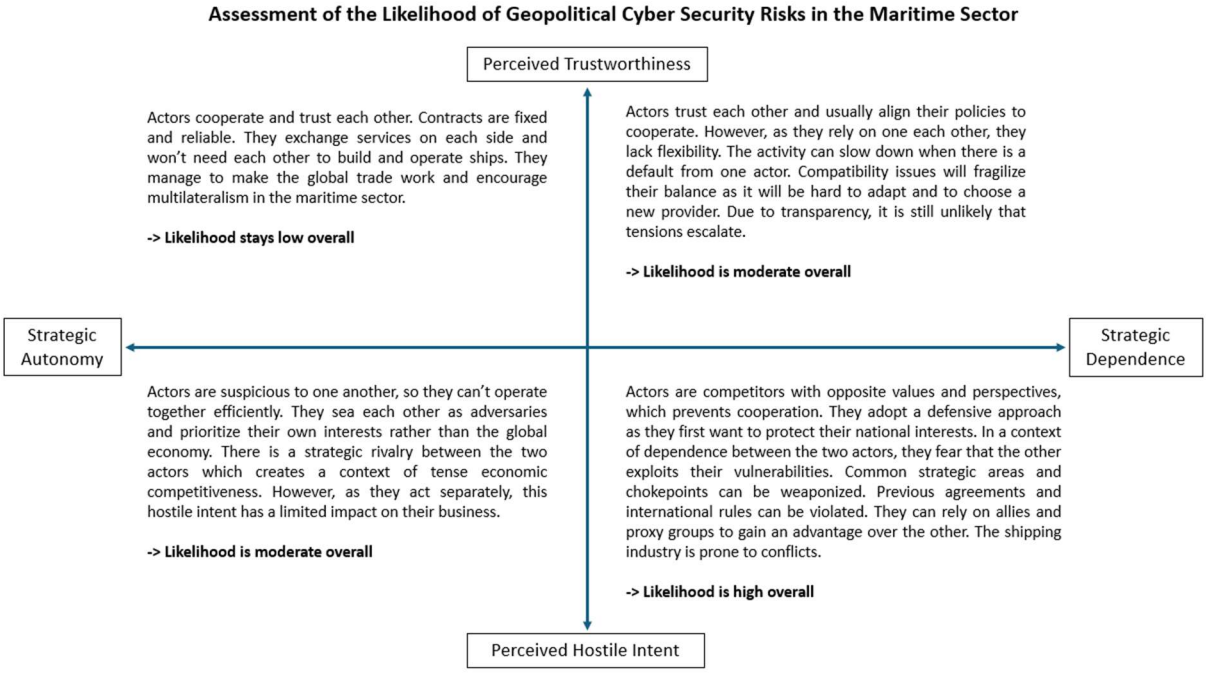
3.1 Methodology to evaluate the Likelihood of a Cyber Geopolitical Incident

Summary of assessing the Likelihood of a Cyber Geopolitical Incident	
1	**Establish the geopolitical profile of the company**
2	**Verify the compliance between the company and its stakeholders (vendors especially)**

First of all, **it is advised to establish the profile of the shipping company** with the characteristics that could involve geopolitics. Because shipping is global, it is important to identify the scope of the company. It can be described based on the head office location, the operational areas and trade routes. It is also essential to consider the Flag State, meaning the country in which the vessel is registered, which is not always the same as the company's home country. Finally, the provenance of the company's customers must be known as it can imply complexities if they are involved in geopolitical conflicts and represent other States' interests.

Secondly, **the shipowner must check compliance between his company and the different stakeholders**, from the vendors they operate with to the customers they serve. IT systems are interconnected and need to be compatible to work together, based on regulations and strategic policies from the different places involved. It is necessary to review the compliance before making an agreement with a vendor and verify that the jurisdictions from the vendor fit with your requirements. It is easier to choose vendors that follow the same standards as the company, to avoid regulatory burden. Both the company and the vendor should refer to States that are on the same side on the geopolitical landscape. As an example, two companies in Europe will both rely on EU laws and policies, which will limit compliance efforts.

The following assessment tool will help identify the nature of stakeholder relationships (third party, State...) based on the company profile and so evaluate how reliable the dynamic is. We consider here two variables: the status of cooperation and the level of dependency.



The **status of cooperation** evaluates the diplomatic links between two actors. If one country trusts the other, based on cultural exchange or similarity of economic models, it can lead to stability and reliability in their relations within the maritime sector. On the contrary, a hostile intent towards an actor creates defiance and can lead more easily to conflicts and direct confrontation in times of crisis.

The **level of dependency** evaluates then to what extent the activity of two actors relies on each other. The status of economic connections is essential because it contributes to facilitate or not the global trade, as countries operate now internationally. It also means that if one of the two actors exclusively relies on one of them, it cannot operate outside of its services, making itself vulnerable.

As a shipowner, you can apply the graph for you and a vendor by scaling these two variables. You can measure the trust you have in each other, based on the States, jurisdictions and partnerships to which you are affiliated, and then the level of dependency, meaning if you only rely on one another.

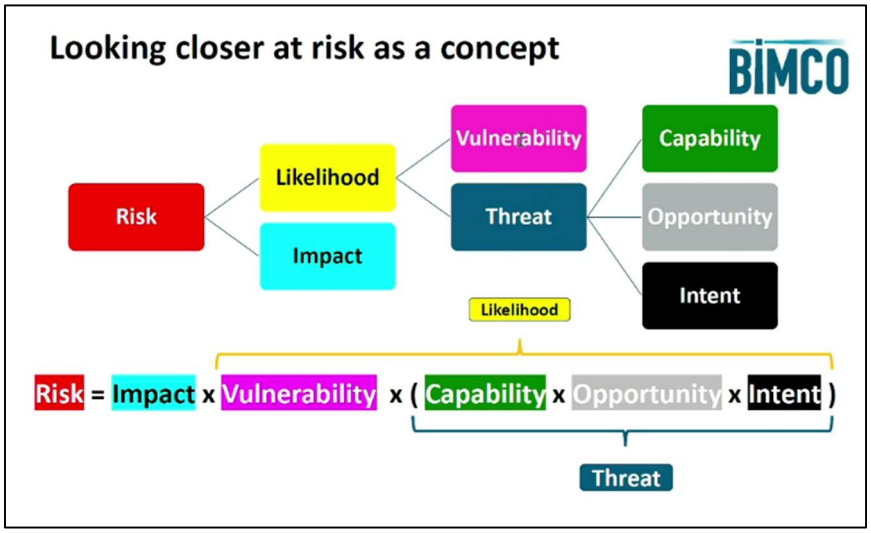
Assessment of the likelihood of a cyber geopolitical incident	Perceived Trustworthiness	Perceived Hostile Intent
Strategic Autonomy	**Low Likelihood**	**Moderate Likelihood**
Strategic Dependence	**Moderate Likelihood**	**High Likelihood**

In the end, these two variables can determine the likelihood of a risk materialising. The likelihood that a risk will materialise is high when a company is dependent on services and products of a third party, because it increases its vulnerability, and when it is seen as hostile from an actor, as it creates a threat. The company is indeed vulnerable because it cannot control its activity if it is interrupted and is also threatened when there is an intent to disrupt the business.

The more trust and the less dependence you have with a vendor, the healthier and more sustainable the dynamic is.

3.2 Recalling and adapting the risk concept

Risk management is essential regarding cyber security incidents in a geopolitical context. The risk management process includes factors such as impact, likelihood, vulnerability, threat, capability, opportunity and intent of malicious actors to conduct cyber-attacks. They are all related (see figure below) and relevant when calculating risk. It follows that if either of the factors is low or even zero, the same will eventually apply to the risk. It is important to emphasise that risk assessment is not a one-time activity. It must be repeated at regular intervals to assess whether threats, vulnerabilities, likelihoods, impacts and risks have changed, and if the control measures are still appropriate.



Assessing the threat depends on the characteristics of a malicious actor. From a geopolitical perspective, it **is directly linked to assessing the intent** (see 3.1). A hostile intent can emerge when you are seen as an adversary due to territorial, economic or military conflicts. Related to digitalisation, the technological competition can increase the hostile intent. On the other hand, when the relation between two actors is based on trust, cooperation and good faith, it is less likely than one considers the other as a threat, because actions are reliable and predictable. This intent relies on how one actor is perceived by the other. It can be identified in the national strategy, based on specific goals and targets indicated by a State or a non-State actor.

Capability then addresses the resources and technical skills from a cyber security aspect. The more a State or non-State actor invests in cyber security means, the most likely they can be efficient and used to serve the intent. Capability also refers to policies, regulations and standards implemented to govern strategic actions in cyber space. **Opportunity** finally relates to the conditions that can favour the threat of an attack. Capability and Opportunity are the reasons a threat can be effective and must be considered seriously. However, they primarily depend on whether there is an intent from the malicious actor.

Assessing the vulnerability is important because it relates to what can make an attack less feasible and attractive. If there is no vulnerability and in this case no dependence, the **likelihood** of an incident occurring is zero. Even if the threat is high, it must be put into perspective as the lack of vulnerability prevents the threat from occurring in the end. However, this assessment of the likelihood can often vary and must be done regularly. Depending on whether the threat is seen as more real and factual, the degree of vulnerability may differ. Geopolitical alliances and the stability of proxy groups, but also the cyber infrastructure, with ships connected to the Internet or with an insufficient network segregation, can represent weaknesses and reasons for an actor to target another one.

The impact factor finally relates to the potential material and human consequences, the individuals involved, and the ultimate shock on the company's operations. This variable will determine whether there is a risk for a specific company or ship. After doing an assessment of the likelihood, the shipowner needs to consider the impact of the risk to evaluate if it needs to be considered.

A risk acceptance profile of the company must be made at this point to calculate to what extent a risk is acceptable.

Conclusion

We have seen that digitalisation has impacted the shipping industry in many ways that have led to an increase in cyber-attacks. The implication of interstate relations and national jurisdictions need to be considered as they have made cyber-attacks more complex. Dependencies between shipping companies and their suppliers need to be verified regarding digital tools they may use on software, hardware, cloud storage solutions and AI platforms. It is likely that the situation may evolve toward more frequent geopolitical threats, which will also be harder to anticipate. Cyber security risk management policy should include geopolitics analysis as weaponizing digital technologies has become an integral part of competing States' strategies. The risk concept as described in 3.2 can be recognised as a basis to identify whether a company is at risk and should have better cyber security protections, also depending on how much risk your company is willing to take.

As BIMCO has recently launched a **Cyber Security Survey** updated with current topics of 2026 such as geopolitics and AI, this analysis is strongly connected. Results have shown an increase of interests in these issues since they are having an increasing impact on shipping companies' operations.

We recommend a greater focus on the close link between cyber security and geopolitics.

References

Articles

- Robert A. LEE, “Web Browser Usage Statistics 2026: Market Shifts Now”, SQ magazine, 11 February 2026 https://sqmagazine.co.uk/web-browser-usage-statistics/

- Clotilde BÔMONT, Tim RÜHLIG, “Challenging US dominance: China's DeepSeek model and the pluralisation of AI development”, European Union Institute for Security Studies, 28 July 2025 https://www.iss.europa.eu/publications/briefs/challenging-us-dominance-chinas-deepseek-model-and-pluralisation-ai-development

- Sam CLARK, “Microsoft didn’t cut services to International Criminal Court, its president says”, Politico, 4 June 2025 https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/

- Peter DOHR, “China’s Weaponization of Global Cyber Supply Chains”, Center for Strategic and International Studies, 1 December 2025 https://www.csis.org/blogs/strategic-technologies-blog/chinas-weaponization-global-cyber-supply-chains

- Matthew FERREN, “The Trump Administration’s Cyber Strategy Fundamentally Misunderstands China’s Threat”, Council on Foreign Relations, 26 January 2026 https://www.cfr.org/articles/the-trump-administrations-cyber-strategy-fundamentally-misunderstands-chinas-threat

- Clara FONG, “The U.S.-China Trade Relationship: What’s Behind the Competition?”, Council on Foreign Relations, 15 May 2026

- Michael FROMAN, “China, the United States, and the AI Race”, Council on Foreign Relations, 10 October 2025 https://www.cfr.org/articles/china-united-states-and-ai-race

- Misha GLENNY, Luke MINTZ, “China is winning one AI race, the US another - but either might pull ahead”, BBC, 7 April 2026 https://www.bbc.com/news/articles/c145enxln0go

- Clete JOHNSON, “Spies, Saboteurs, and Access to U.S. Connected Devices”, Liberty Bell Project, 14 July 2025 https://libertybellproject.us/reports/spies-saboteurs-and-access-to-u-s-connected-devices/

- Mark KENNEDY, Christa BRZOZOWSKI, “America’s Maritime Blind Spot: How China is Gaining the Upper Hand on the High Seas”, Wilson Center, 5 March 2025 https://acrosskarman.wilsoncenter.org/article/americas-maritime-blind-spot-how-china-gaining-upper-hand-high-seas

- Xiaowei LIN, Pengdong ZHANG, Zhihao YANG, Sicen CHEN, “US sanctions and corporate innovation: Evidence from Chinese listed firms”, International Review of Economics & Finance, March 2025 https://www.sciencedirect.com/science/article/pii/S105905602500098X

- Charles MILLON, “Digital geopolitics and the rise of cyberwarfare”, GIS, 3 May 2024 https://www.gisreportsonline.com/r/digital-geopolitics-cyberwarfare/

- Attracta MOONEY, “Chinese green technology poses national security problem for Europe, report warns”, Financial Times, 29 April 2026 https://www.ft.com/content/c9cd5751-8d2d-4f24-b676-7c3ec349e404?syn-25a6b1a6=1

- Ismet OZALP, “Maritime Cybersecurity in 2026: What Ship Managers Actually Need to Know”, NAVATOM, 3 April 2026 https://navatom.com/blog/maritime-cybersecurity-2026-ship-managers-guide

- Matthew P. FUNAIOLE, Brian HART, and Aidan POWERS-RIGGS, “Murky Waters, Navigating the Risks of China’s Dual-Use Shipyards”, Center for Strategic and International Studies, 25 March 2025 https://features.csis.org/hiddenreach/china-shipyard-tiers/

- Anton SHILOV, “Jensen says Nvidia now has 'zero percent' market share in China — says US export policy 'has already largely backfired'”, Tom's Hardware, 3 May 2026 https://www.tomshardware.com/tech-industry/artificial-intelligence/jensen-says-nvidia-now-has-zero-percent-market-share-in-china-says-us-export-policy-has-already-largely-backfired

- Heather SOMERVILLE, “US Expands List of Chinese Tech Companies It Says Assist Beijing’s Military”, The Wall Street Journal, 9 June 2026 https://www.wsj.com/politics/national-security/u-s-expands-list-of-chinese-tech-companies-it-says-assists-beijings-military-a2c6c6b9?eafs_enabled=false

- Toby STERLING, “US targets Chinese chipmaking with proposed export restrictions on ASML and others”, Reuters, 3 April 2026 https://www.reuters.com/world/china/us-targets-chinese-chipmaking-with-proposed-export-restrictions-asml-others-2026-04-03/

- Frank UMBACH, “US cybersecurity policy under Trump”, GIS, 26 November 2025 https://www.gisreportsonline.com/r/trump-cyber/

Reports

- “Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025”, US Department of Defense, 23 December 2025 https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF

- “Annual Threat Assessment of the US Intelligence Community”, Office of the Director of National Intelligence, March 2026 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf

- “Cloud Market Share Trends - Big Three Together Hold 63% while Oracle and the Neoclouds Inch Higher”, RENO, NV, Synergy Research Group, 19 November 2025 https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher

- “FACT SHEET: FCC Updates Covered List to Include Foreign-Made Consumer Routers, Prohibiting Approval of New Models”, Federal Communications Commission, 23 March 2026 https://docs.fcc.gov/public/attachments/DOC-420034A1.pdf

- “Guidelines on cyber security onboard ships”, version 5, BIMCO, Class NK…, 2024 https://www.maritimeglobalsecurity.org/media/g3qlxdaw/2024-11-14-guidelines_on_cyber_security-v5-final.pdf

- “Guidelines on Maritime Cyber Risk Management”, MSC-FAL.1/Circ.3/Rev.3, IMO, 4 April 2025 https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf

- “List of Equipment and Services Covered By Section 2 of The Secure Networks Act”, Federal Communications Commission, 15 June 2026 https://www.fcc.gov/supplychain/coveredlist

- “Maritime Industry Security Threat Overview (MISTO)”, BIMCO, ICS, INTERTANKO…, 26 November 2025 https://www.maritimeglobalsecurity.org/media/hjcjxkcn/2025-03-31-misto-final.pdf

- “United States and Eight Companies Launch the Partnership for Global Inclusivity on AI”, Office of the Spokesperson, 23 September 2024 https://2021-2025.state.gov/united-states-and-eight-companies-launch-the-partnership-for-global-inclusivity-on-ai/

- “White Paper Demystifying the debate on the US CLOUD Act vs European/UK Data Sovereignty in the context of cloud services”, CMS law firm, 3 February 2026 https://cms.law/en/aut/legal-updates/white-paper-demystifying-the-debate-on-the-us-cloud-act-vs-european-uk-data-sovereignty-in-the-context-of-cloud-services