CENTRE FOR
CYBER SECURITY

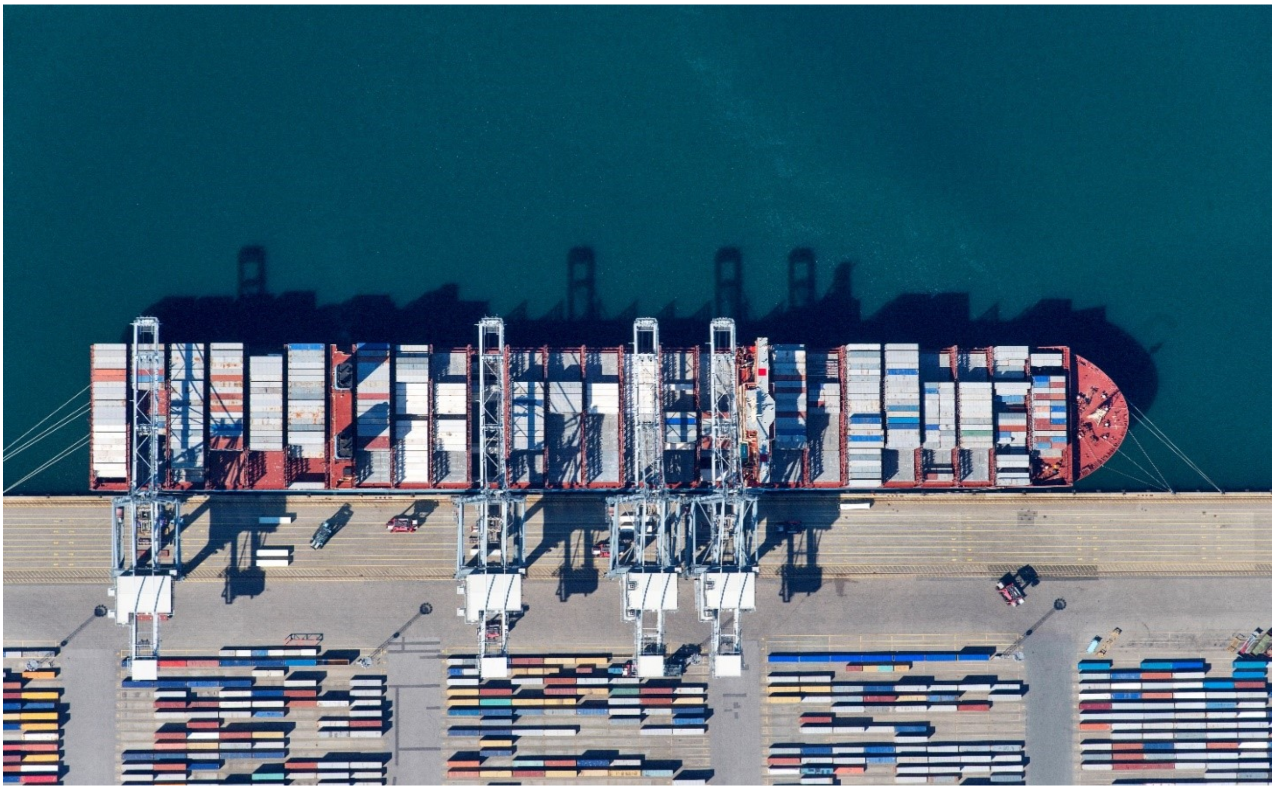


Photo: Mikkel Barker/ Ritzau Scanpix

Threat assessment:

The cyber threat against the Danish maritime industry and ports

Threat assessment: The cyber threat against the Danish maritime industry and ports

This assessment is intended to inform decision-makers within the maritime industry and ports of the cyber threat against the sector. This threat assessment replaces the previous threat assessment against the Danish maritime industry from 2019.

Date: October 2020

Danish Defence Intelligence Service
Kastellet 30
DK-2100 Copenhagen

Tel.: +45 33 32 55 80
E-mail: cfcs@cfcs.dk
https://cfcs.dk

Key assessment

- The threat from cyber crime is **VERY HIGH**. The general threat from cyber crime against private companies and public authorities in Denmark also applies to the maritime industry. Some of the criminals who attack companies across society occasionally also target the maritime industry specifically. In addition, a small number of cyber criminals have even specialized in attacks on the maritime industry.

- The threat from cyber espionage is **VERY HIGH**. Several foreign states conduct cyber espionage against the maritime industry across the world. The foreign states do this among other things to promote its own industry and economy. States also do it to gain access to security policy relevant information.

- The threat from destructive cyber attacks is **LOW**. It is less likely that foreign states will launch destructive cyber attacks on Denmark. Private companies and public authorities operating in conflict areas are more exposed to the threat from destructive cyber attacks, though.

- The threat from cyber activism is **LOW**. Globally, recent years have seen a drop in the number of cyber activist attacks. However, the threat from simple attacks may suddenly rise should Danish public authorities or private companies find themselves in the crosshairs of cyber activists.

- The threat from cyber terrorism is **NONE**. Serious cyber attacks aiming to create the affect as conventional terrorism presuppose technical capabilities and organizational resources currently unavailable to militant extremists. In addition, the intention among these groups is limited.

Introduction

This threat assessment describes the cyber threat against the so called Blue Denmark, which consists of shipping companies, equipment suppliers, authorities, ports, etc. The assessment applies to organizations in Denmark as well as to their international activities.

The threat assessment covers regular IT systems and sector-specific systems such as Operational Technology (OT) systems on board ships and at port facilities. The assessment describes the current threat landscape and operates with a warning horizon of two years. As cyber threats are dynamic, the threat landscape may change without warning.

The threat assessment is divided into threats from cyber attacks that facilitate crime, espionage, activism and terrorism plus destructive cyber attacks.

The maritime sector is important to Denmark

Denmark is the world’s fifth-largest shipping nation measured in operated tonnage. More than 700 merchant ships operate under Danish flag, and close to 2,000 ships are operated from Denmark. Shipping is Denmark’s largest export business, and most activities take place outside of Denmark.

In addition, the Blue Denmark comprises a number of globally cutting-edge and often high-tech equipment suppliers.

Shipping ties Denmark together and provides connections to our neighbouring countries. Denmark has more than 50 domestic and 15 external ferry routes. Danish island communities and businesses depend on stable ferry services.

With more than 100,000 port calls each year, commercial ports around Denmark ensure supplies to the country. More than three quarters of Danish imports are carried through these ports.

More than 70,000 ships a year navigate the Danish straits, many of them tankers to and from the Baltic Sea, making Danish waters some of the busiest in the world.

Cyber security is important for the maritime industry

Ships, shipowners, equipment suppliers and ports all use sophisticated IT and OT systems increasingly. Cyber attacks against these systems could potentially disrupt operations and damage business. At worst, cyber attacks against ships, shipowners and ports may affect physical safety. Therefore robust cyber security practices are important to the sector.

More information on the potential impact from the cyber threat on physical safety can be found in the threat assessment from March 2020, ”The cyber threat against operational systems on ships”. The publication is available on the CFCS website.

Cyber crime

Cyber criminals threaten the Danish maritime sector
The threat from cyber crime is **VERY HIGH**. This means, that it is highly likely that organizations within the Danish maritime industry will be targets of attempted cyber crime in the next two years.

Economic motivated criminals hack private companies and public authorities across society, including maritime companies. These criminals pose the greatest cyber threat to the Danish maritime industry. In addition, criminal hackers launch isolated campaigns against the Danish maritime industry or specialize in attacks on the industry.

The threat is primarily directed at regular business systems such as non-sector specific administrative systems. However, attacks may also affect or spread to operational systems and, at worst, affect the operation of the systems.

Multiple types of cyber crime pose a threat
Criminal hackers use a wide range of techniques and options to make money. Individual hacker groups often specialize in a particular attack technique. But criminals have also been known to cooperate. They trade accesses to compromised companies and tools used for cyber attack, etc.

Maritime companies in Denmark and across the world have fallen victim to all of the different types of cyber crime. Below is an outline of some of the different attack techniques and examples of criminal income sources.

Serious ransomware attacks have become common
Cyber criminals use ransomware to encrypt computers and networks, demanding a ransom in exchange for decryption. The past years have seen a rise in the number of targeted ransomware attacks to the point where such attacks have become fairly common in Denmark.

In targeted ransomware attacks, hackers use considerable time and resources to select and encrypt vital parts of compromised victim networks. Once the systems are locked, hackers often demand ransom equivalent of several million Danish kroner to unlock them. Since late 2019, hackers behind targeted ransomware attacks have started threatening to leak sensitive data stolen from infected systems unless ransom is paid.

Targeted ransomware are used against companies across all sectors worldwide, including the maritime sector. Hackers primarily target general IT systems. But criminal hackers often try to target systems that are most critical to their victims. Hereby the likelihood that the victim pays the ransom is increased.

Consequently, the CFCS assesses that after gaining access, hackers are willing to encrypt OT systems on board ships and at ports. A case in point is the December 2019 attack against a US maritime facility with the Ryuk ransomware. The attack disrupted the network, forcing the facility to shut down its operations for 30 hours.

Blue Denmark companies affected by ransomware
In December 2019, Danish shipping and logistics company DFDS became the target of a ransomware attack against one of its acquisitions abroad. The systems of the foreign subsidiary were in the process of being phased out and transferred to the parent company. However, criminal hackers managed to find a weakness in the subsidiary's systems, allowing them to install a ransomware known as Zeppelin. However, the attack did not reach parent company DFDS, and only the systems of the subsidiary were locked. The DFDS was able to avert the most significant fallout of the attack by using backups and speeding up the transition to new systems.

Danish industrial pump manufacturer DESMI suffered a targeted ransomware attack in April 2020. The hackers initially gained access to DESMI's IT systems via an email containing an infected file. Once inside the system, the hackers spent a week preparing the ransomware attack before locking the systems and sending a ransom note, which DESMI refused to pay.

The attack affected DESMI's communication systems, which were inoperable. The systems had to be restored, and the main systems only became re-accessible four days later. The rest of the systems were restored over a 30-day period.

" I thought we were well protected. On 3 April, I informed the executive board that there were no security holes." On 8 April, hackers locked the company's systems. From interview with Henrik Sørensen, CEO DESMI in Shippingwatch 14 April 2020

A widespread threat from more simple ransomware attacks has persisted for a number of years. Simple ransomware attacks are typically distributed via phishing emails. If the recipient clicks on links in the email or opens infected files, ransomware is installed that automatically locks the computer as well as connected systems and devices. This type of attack is often detected by updated virus protection. However, if the email recipient is on a vulnerable network, an attack could carry serious consequences. Several such examples have been seen on board ships. Technicians and business partners regularly update ship systems via USB-ports, when the ships are at port around the world. On one such occasion ransomware spread from a shipmaster's computer to the ship's OT systems, cutting the power supply on the ship for three days.

BEC – Business Email Compromise
Fraud, in which criminals trick victims into wiring money to foreign accounts, constitutes another source of income for criminals. Some fraudsters use cyber attacks in their scams. In so-called Business Email Compromise (BEC), scammers typically compromise and monitor the victims' emails. Criminals also hit the maritime industry with this type of fraud.

The threat emanates both from fraudsters targeting companies across society and from groups specializing in targeting the maritime industry.

Gold Galleon – cyber fraudsters focusing on the maritime industry
In 2018, an IT security company exposed a criminal group from Nigeria called Gold Galleon. The group specializes in compromising emails exchanged between maritime partners. They monitor the dialogue and modify bank account numbers when money is transferred to agents, ports, etc.

Danish companies have likely also been targeted by Gold Galleon. In 2019, an employee from the Danish shipowner Clipper received an email from a US partner that aroused suspicion. The employee therefore chooses to contact the partner. However, the fraudsters had also compromised the phone connection and returned the call using the partner's phone number. Instead of speaking with his normal accent, the partner now spoke with a Caribbean-sounding accent.

Clipper thus saw through the scam, preventing the criminals from succeeding in their attack. However, Gold Galleon has managed to steal amounts corresponding to millions of Danish kroner from other victims by using the same approach.

Hackers exploit computing power
Hackers also compromise computers and other digital devices to exploit their computing power for illicit profit. The computing power can among others be used to generate cryptocurrency by infecting devices with so-called crypto miners. Hackers also misuse compromised units as a platform for overload attacks, so-called DDoS attacks, or to distribute spam emails.

Maritime companies are among the victims of this type of exploit. It applies both to the misuse of their regular IT systems and units, including routers and servers, as well as systems that are unique to the maritime industry.

According to an IT security company, the antenna control unit of a ship-borne satellite system was infected by the Mirai malware in 2018. The Mirai malware is used to build so-called botnets comprising thousands of units. The control unit was likely compromised because the shipping company used a standard password.

In December 2019, information about a vulnerability in a yacht control web application was made public. A few days later, hackers exploited the vulnerability to install Mirai malware on the remote-control systems.

Hackers have been known to inadvertently disturb units in a botnet because they were oblivious to the consequences of their hacking. In 2016, for instance, a hacker exploited 900,000 home routers from a Mirai botnet to launch a DDoS attack. The attack was directed at a telecom provider in Liberia. However, it ended up by mistake preventing 900,000 Deutsche Telekom customers from accessing the Internet for two days.

Hackers target personal data

Another source of income for hackers is stealing and selling personal data that could be exploited by other criminals. Organizations in the maritime industry have access to different types of data that could prove interesting to criminals. Passenger ship shipowners, for example, have a lot of data on passengers, partners and employees.

In recent years, Stena Lines, Norwegian Cruise Line and Carnival Cruises have all had hacked systems with sensitive information. For instance, login data relating to some 30,000 travel agents from Norwegian Cruise Line's travel agent portal was offered for sale on criminal Internet forums in March 2020.

Maritime-themed attacks

The greatest cyber criminal threat against the maritime industry emanates from opportunistic attacks directed at victims across society. However, some criminals, such as Gold Galleon, specialize in attacks against the maritime industry. Likewise, some hackers who generally launch attacks against companies across society occasionally also target the maritime industry specifically.

Recent years have seen several phishing attacks against the maritime industry. For example, in 2018, hackers posing as the trade organization Danish Shipping sent emails to its member companies. The criminals asked for login credentials to the member section of the trade organization's website.

In 2019, the US Coast Guard issued a warning on an ongoing campaign. Ships on route to US ports received emails in which attackers posed as port authorities. In the emails the hackers asked for sensitive information, including Notice of Arrival (NOA).

Similarly, in 2019, ships navigating the North Sea likely received phishing messages through the ships' telex systems. The telex messages targeted the communication channels and were maritime themed.

Finally, there are examples of strong maritime brands such as A.P. Moller - Maersk being exploited in phishing attacks to create a false sense of trust that the sender is genuine.

Cyber espionage

Foreign states spy against the Danish maritime sector
The threat from cyber espionage is **VERY HIGH**. This means, that it is highly likely that organizations in the Danish maritime industry will be the targets of attempted cyber espionage within the next two years.

Hackers employed by states and state-affiliated hacker groups conduct cyber espionage. The states motive for espionage against the maritime industry can be divided into two main categories. Firstly, states spy in order to promote their own industries and economy. Secondly advantages and to gain access to information that is the states to obtain relevant information in a security policy context, ranging from overall strategic information to information relevant to military planning.

Worldwide, there has been a long range of attacks on the maritime industry resembling cyber espionage. The victims have come from a wide range of maritime organizations, ranging from research institutions over equipment suppliers to shipyards and shipowners.

Being a strong maritime nation, Denmark has many potential victims. Danish organizations in the industry are regularly hit by hacking attacks that are likely aimed at facilitating cyber espionage.

The threat is particularly targeted at high-tech equipment suppliers, maritime authorities, large international shipping companies, and ports and port terminals that are part of the critical infrastructure in Denmark and abroad.

State hackers steal information for their own industry
Some foreign states use hackers to compromise companies abroad to steal valuable information on technology and intellectual property. Foreign states may also be interested in other commercial business secrets. That can for example be information in connection with tenders or contracts.

Foreign states may use stolen information to promote the development of their own national industries. With theft of the right information, national companies may skip several steps in their innovation and development processes.

Both Russia and China have established very strong cyber capabilities, which both countries use actively on a global scale.

In its Made in China 2025 strategy, China has identified ocean engineering and high-tech ships as one out of ten prioritized industrial areas. China aims to lead the field by 2025.

Special interest in dual-use technology

The threat against the maritime industry is linked to the threat from cyber espionage against the defence industry, which is also **VERY HIGH**. This is rooted in the circumstance that the maritime industry employs technology and equipment that can both be used both for civilian and military purposes, so-called dual-use technology.

Much of the maritime operational equipment such as navigation and communication equipment can be used by commercial ships as well as by naval vessels. Illicit acquisition of information on dual-use technology may potentially be effective in meeting both commercial and security policy needs of foreign states.

For some countries with extensive cyber capabilities, dual-use technology has even become a defence policy focus. For example, as part of the modernization of its armed forces, China has a declared goal of "civilian and military fusion" (" junmin ronghe"), whose focus includes dual-use technologies. In Russia, the development of dual-use technologies is a declared goal of the country's military development organization, the Russian Foundation for Advanced Research Projects (FPI).

States spy on partners

Some foreign states use cyber espionage as a means to gain insight into foreign partners' strategic intentions. Such partners may include authorities in other countries and foreign companies with substantial activities in the intelligence service's home country.

Because the Danish maritime industry holds a strong position in the global market, Danish maritime companies and authorities may become targets of attacks from hackers with this motivation. In the textbox below, there is a subset of examples of Danish activities in Russia and China that can motivate cyberespionage.

Examples of Danish maritime activities in Russia and China
In 2018, assisted by a Russian nuclear-powered icebreaker, Maersk Line's ship Venta Maersk was the first ever container ship to complete a trial transit of the North East Passage. The transit attracted a lot of attention, and the North East Passage is a top priority to President Putin. In general, the Arctic is an area of great interest to several great powers, including Russia and China.

In collaboration with local partners, APM Terminals owns and operates port terminals across the world. Of these seven are located in China and five in Russia. The ports are strategically located and are part of the countries' critical infrastructure.

Danish ships are among the operators carrying most containers out of China. Thus, Danish shipping lines play a vital role to China's export of goods. At the same time, 73 out of 100 ships that were ordered by Danish shipowners in 2018 were built at Chinese shipyards.

Surveillance of ship traffic and logistics

State hackers are also responsible for compromising IT systems on board ships. This allows them insight into for example the ships' location and their cargo. Shipments of military supplies may be of particular interest to foreign countries. Ship systems can also be used as an entry point to gain access to the shipping company's central systems.

Ports, logistics and shipping companies can in the same way also be targets of cyber espionage. In connection with military conflicts, civilian companies may come to play a different role to ensure the security of supply as well as support for the military operations. Ships, ports and logistics companies can become critical, not only to society as a whole but also to the military. One motivation behind cyber espionage against such companies could be the development of destructive cyber attack capacity. Access and experience of hacking could be exploited in connection with a conflict.

Suppliers as stepping stones

Suppliers and partners to key public authorities and private companies may also become victims of cyber espionage attempts without being the main target themselves. Hackers attack organizations in order to use them as a stepping stone to compromise customers and partners that may be of interest to foreign states.

The scope of the individual cyber attack may thus fall beyond the procurement of specific knowledge. It can also include procurement of specific access. Some sub-suppliers or partners may not hold knowledge of interest to foreign states. However, they may have accesses or credibility that hackers can exploit to compromise their intended targets.

Destructive cyber attacks

The threat from destructive cyber attacks is **LOW**. This means, that it is less likely that Danish maritime companies and authorities will be the targets of attempts at destructive cyber attacks within the next two years.

It is less likely that foreign states are intent on launching destructive cyber attacks against Denmark. States are behind the vast majority of destructive cyber attacks.

The CFCS defines destructive cyber attacks as attacks where the expected affect is death, personal injury or property damage. The definition also covers destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken.

The majority of destructive cyber attacks launched so far have destroyed data. Either the hackers have deleted or encrypted data without the possibility of restoration. Even within this wide definition, destructive cyber attacks are relatively rare.

Activities in conflict areas may heighten the threat

In conflict areas where states use destructive cyber attacks against civilian targets, the threat from destructive cyber attacks may be higher. As Danish maritime activity is global, Danish maritime companies are thus at risk of becoming victims of attacks that are not directed against Denmark but at companies operating in conflict areas.

During the conflict between Ukraine and Russia, there have been several incidents of destructive cyber attacks in Ukraine. The 2017 NotPetya attack, which affected A.P. Moller - Maersk, among others, was directed at companies with activities in Ukraine. Hackers deployed the NotPetya malware to companies by hijacking a software update for a tax application.

The threat may also increase if the maritime company works for companies or states that are targets of destructive cyber attacks. In 2018, Iranian oil and gas company Saipem, which operates a number of special-purpose vessels, fell victim to a targeted destructive cyber attack. Saipem is a sub-contractor of Saudi oil company Saudi Aramco, and the attack took place using variants of the same malware that was used in previous attacks against Saudi Aramco. The destructive cyber attack that hit Saipem deleted data on several hundreds of Saipem’s computers worldwide.

The maritime industry may also become collateral victims of a destructive cyber attack. Over the spring and summer of 2020, critical infrastructure in Israel and Iran became the target of cyber attacks. Each country has accused the other of the attacks. One of the attacks hit the port in Bandar Abbas, Iran, in May 2020. The attack affected the operation of the port, causing delays to the ships using the port.

Maritime equipment suppliers are as mentioned particularly exposed to cyber espionage. Hackers may potentially use compromised equipment suppliers as stepping stones to launch destructive cyber attacks on OT systems on board ships. It can for example be attacks disguised as legitimate system updates.

The fallout of this type of attack may be quite significant if, for example, it takes place through an engine manufacturer, a supplier of navigation equipment or other critical equipment.

Cyber activism

The threat from cyber activism is **LOW**. This means, that it is less likely that organizations within the Danish maritime industry will be exposed to of attempts of cyber activism within the next two years.

Globally, the number of cyber activist attacks has dropped over the past few years. Cyber activists rarely focus their attention on Danish public authorities and private companies.

The purpose of cyber activism is to draw the largest possible attention to a specific cause. To this end, cyber activists use different attack techniques that differ in complexity – ranging from relatively simple overload attacks, so-called DDoS attacks, to resource-heavy hacks and leaks of sensitive information from public authorities and private companies.

Thus, cyber activist attacks cover a multitude of activities ranging from opportunistic attacks to organized campaigns. However, a common denominator seems to be that while the attacks are often launched in response to specific events, there appears to be continuity in the topics pursued by the different activists, including climate and animal welfare.

The threat from simple attacks may become a reality if Danish public authorities or private companies find themselves in the crosshairs of cyber activists. The text box below describes a DDoS attack on A.P. Moller - Maersk in May 2020. It serves as an example of how a low-level threat may quickly be translated into action using relatively simple means.

COVID-19 pushes climate change activists to launch cyber attacks
The spring 2020 Corona virus shutdown also affected environmental activists. On 10 March 2020, the environmental campaign group Extinction Rebellion launched a protest action in the Danish Parliament Hall the day before Denmark went into lockdown. However, during the lockdown, the group decided to launch virtual protests in the form of cyber attacks instead.

According to the group's own newsletter, it carried out simple DDoS attack against a number of companies in May 2020. The companies including A.P. Moller - Maersk, was targeted because the activists felt that the companies CO2 emissions were too high.

The activists used a relatively simple tool. They used their home computers to send thousands of messages containing excerpts from the UN climate report to the company websites. The activists aim was to overload the websites causing them to shut down.

Cyber terrorism

The threat from cyber terrorism is **NONE**. This means, that it is highly unlikely that organizations in the Danish maritime industry will be exposed to cyber terrorism attempts within the next two years.

The CFCS defines cyber terrorism as cyber attacks aimed at creating effects similar to those of conventional terrorism, including cyber attacks causing personal injury or major disruptions in critical infrastructure.

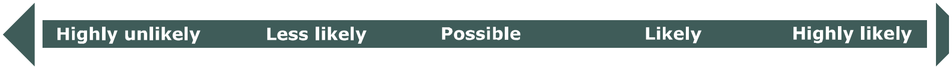
Cyber attacks of such serious magnitude presuppose technical skills and organizational resources that militant extremists currently do not possess. At the same time, the intent to conduct cyber terrorism is extremely limited.

Definition of threat levels

The Danish Defence Intelligence Service uses the following threat levels.

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are not likely.
MEDIUM	A general threat exists. Capacity and/or intent to attack and possible planning. Attacks/harmful activities are possible.
HIGH	An acknowledged threat exists. Capacity and intent to carry out attacks and planning. Attacks/harmful activities are likely.
VERY HIGH	A specific threat exists. Capacity, intent to attack, planning and possible execution. Attacks/harmful activities are very likely.

The DDIS applies the below scale of probability


Highly unlikely
Less likely
Possible
Likely
Highly likely