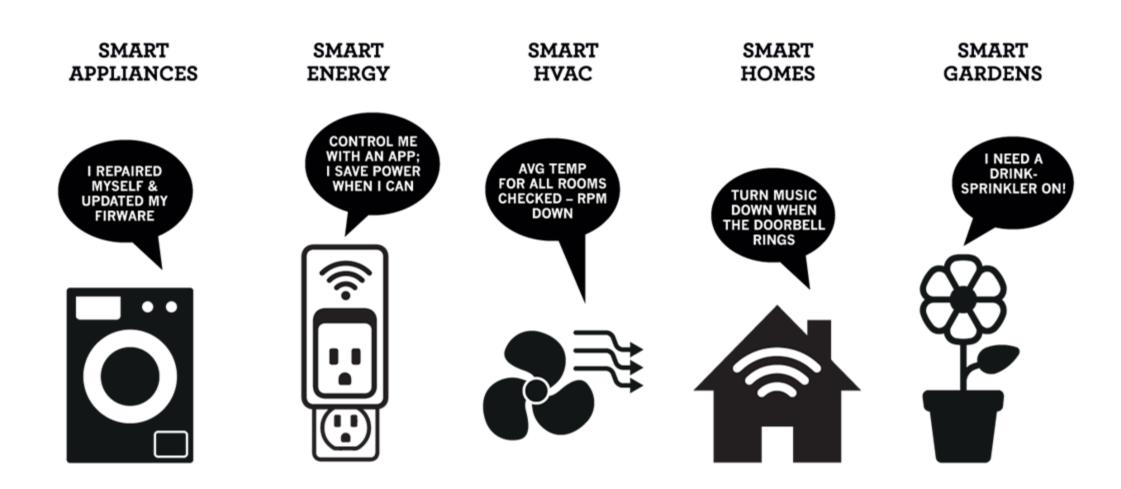
## International Ship and Port facility Code (ISPS)

# Cyber security provisions

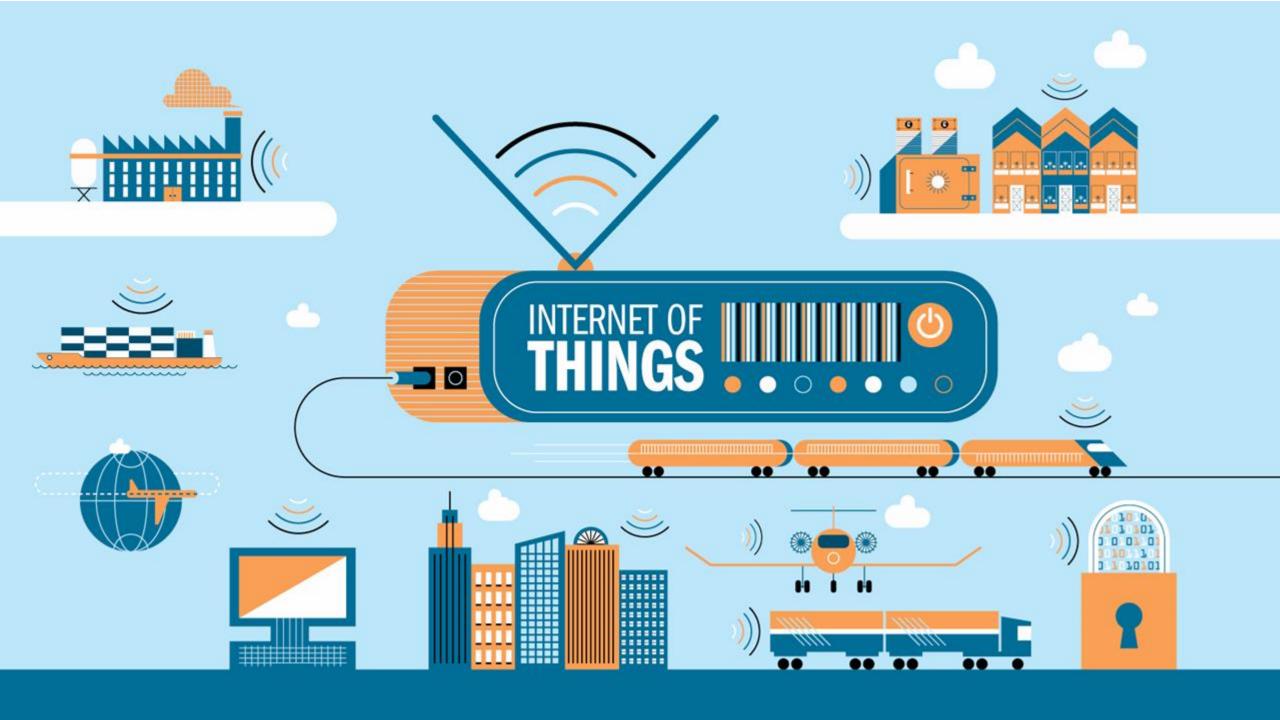
Kim Jeonghun Kim Jinsick Oh sumi



# Day of Mr.Kim



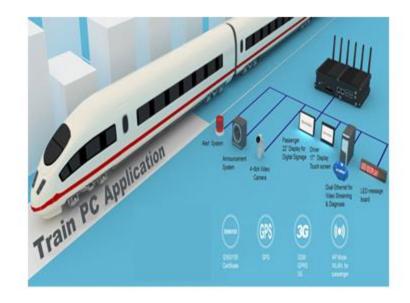
Changes in life with internet development.





# Current state of transportation







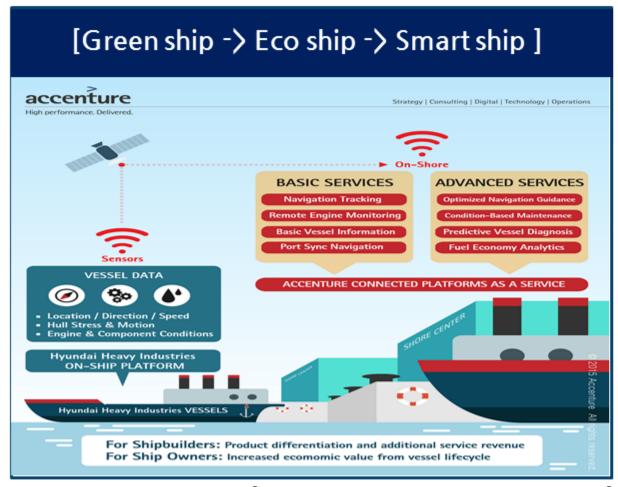
Remotely piloted vehicle

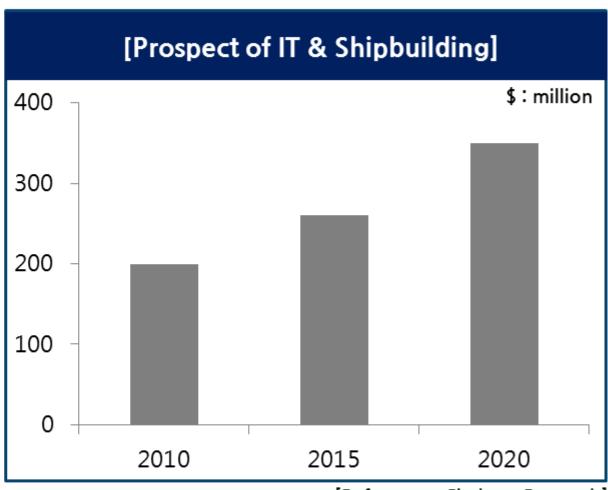
IOT based train Managing system

Auto driving Car

## New trends in maritime industry





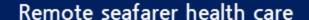


[Reference: Hyundai Heavy Industries Co]

[Reference : Clarkson Research]

### Representative Case







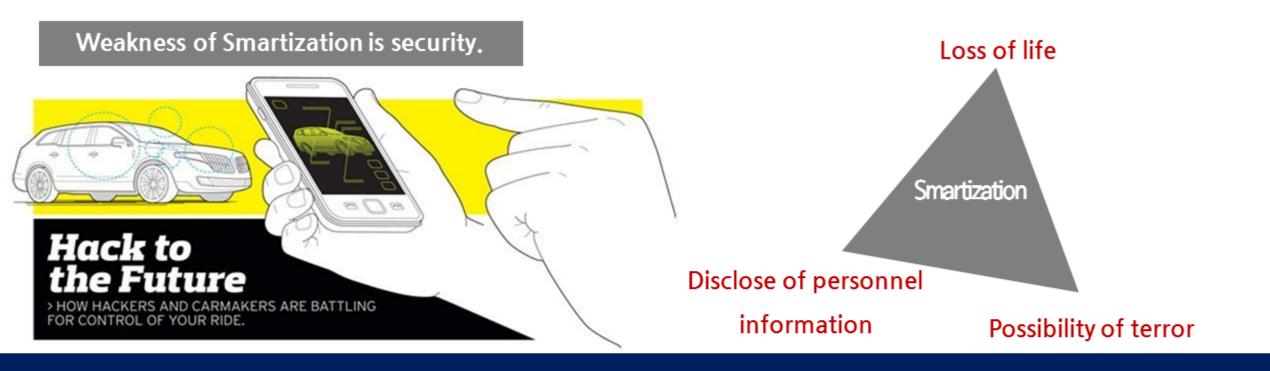
#### **Summary**

Connection between vessels and marine medical center for a regular health consultation



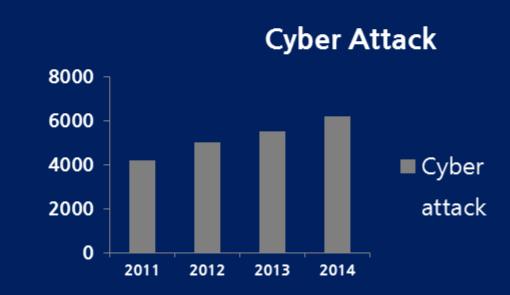


But we have to be ware of the imminent danger of cyber crime.



#### Growing numbers of cyber attack

According to SISCO number of cyber attacks has increased 14% from last year. This is the most number of attacks since 2000, cyber attacks are growing. Nowadays the attacks are more organized and sophisticated causing severe damages.







Part A.

# Mandatory requirements

SSA ship security assessments

SSP ship security plan

PFSA port facility security assessment

PFSP port facility security plan

Part B.

# Guidance on implementing part A

SSA ship security assessments

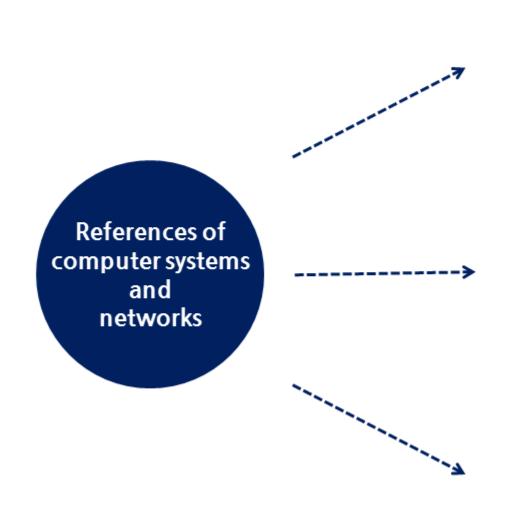
SSP ship security plan

PFSA port facility security assessment

PFSP port facility security plan







#### B/8.3, B/15.3 B/8.4 B/15.4

Radio and telecommunication systems, including computer systems and networks.



#### B/15.7

Systems such as electrical distribution systems radio and telecommunication systems and computer systems and networks.



#### B/15.16

Measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks..



### B/8.3 B/15.3 B/8.4 B/15.4

### Radio and telecommunication systems, including computer systems and networks

This may suggest that computer systems and networks are a subtype of cyber security

Which could lead to an interpretation that only the computer systems and networks operating radio and telecommunication systems are of importance when conducting security plan

This interpretation could exclude several important types of systems such as e-navigation systems, supervisory control and data acquisition (SCADA) systems, security systems, VTS systems





### B/15.7

Systems such as electrical distribution systems radio and telecommunication systems and computer systems and networks

This time it can be interpret as computer systems and networks are an independent systems with radio and telecommunication systems

This is the most extensive definition on clause relating to computer systems and networks in the ISPS Code.





### B/15.16

measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks

This clause is also misleading

This is incomprehensive

It does not clearly state if computer systems and networks are related to radio and

telecommunication, or port services and utilities.







## There are two potential threats regarding cyber security in the clauses

- 1. Each states the duties and the assessments regarding the security plan of each officers which does not specify the threat of cyber security
  - 2. There is no specific requirement or standard regulations regarding the designation of the officers which brings the possibility of lack of expertise in the officers



## **Analysis 1**

Practical application could result inconsistent treatments of computer systems and networks

The three clauses interpretations are interrupting one another

Therefore the committee should consider an consistent clauses regarding cyber security

## **Analysis 2**

The clauses of security officers have potential threats in lack of expertise

No specific standard of requirements of the security officers

Which brings a underling vulnerability of officer personnel's lack of integrated expertise in both maritime science and cyber security

Therefore the committee should consider a reliable system that gives credibility for the officers.

## **Proposal 1**

Strongly recommend to change the regarding computer systems and network in to one comprehensive clause that will contain all the systems in general

- B/8.3 , B/8.4 B/15.3 , B/15.4 radio and telecommunication systems, including computer systems and networks
- B/15.7 systems such as electrical distribution systems radio and telecommunication systems and computer systems and networks
- B/15.16 measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks

Change the given clauses above in to (or can be discussed)

Computer systems and networks conducting all operations in and out of the vessel, and ports.

## Proposal 2

Given the underling vulnerability of security due to the possible lack of expertise in officer personnel We strongly advise to set a standard of requirements of the security officers. There fore we advise the committee to discuss

- 1. Initiating a bar exam which will include expertise in vessel structural, cyber security provisions. Issuing a specific certificate of qualification (ex. Maritime Cyber Security Officer) the given new state of importance of cyber security.
- 2. Initiating a guideline of training program for the existing security officers in cyber security. (ex. Maritime Cyber Security Academy)



## **Proposal 2**

#### Insert the clause A11.1 company security officer

The Company or a third party shall designate a company security officer. A person designated
as the company security officer should possess a specific certificate
(ex. maritime cyber security officer)

#### Insert the clause A/12.1 ship security officer

A ship security officer shall be designated on each ship by the company or a third party. A
person designated as the ship security officer should possess a specific certificate
(ex. maritime cyber security officer)

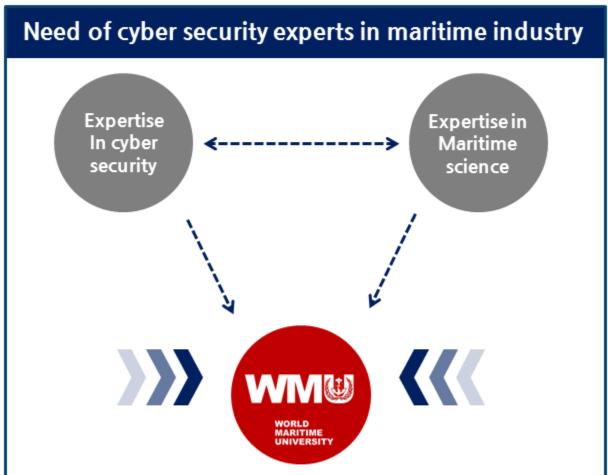
#### Insert the clause A.17.1 Port facility security officer

 A port facility security officer shall be designated for each port by the port authority or a third party. A person designate as the port facility officer should possess a specific certificate (ex. Maritime cyber security officer)









Reference: Symantec

## Maritime Cyber Security Officer initiation policy roadmap



	2017	2018		2019	2020		2021				
Development of Maritime Cyber Security officer education program based on Maritime universities											
Establishment of administration committee	Off-line, On- program dev	Maritime Cyber Security Academy ( total management and supervision of education)									
Re education / qualification program	Promotion of qualification program		Re education of current security officers Alternation program for the new security officer personnel								
Security officer certification system				Ultimately issuing a qualification exam from Maritime cyber security academy							

### **FIRST STEP**

Establishment of administration committee
Development of training program

### **SECOND STEP**

Organizing a Security Officer Qualification exam / program

### THIRD STEP

Securing Maritime Cyber Security Officer

## Maritime Cyber Security Officer initiation policy roadmap



Basic training

Research process

Applied studies

#### **Vessel System Training**

- Marine engineering
- Maritime law

- Applied electronic
- Marine engineering
- Vessel engine automation system

#### **Cyber Security Training**

- C- programing applies
- Introduction to hacking
- Understanding of security
- Applied information security
- Hacking security
- Understanding of network attack

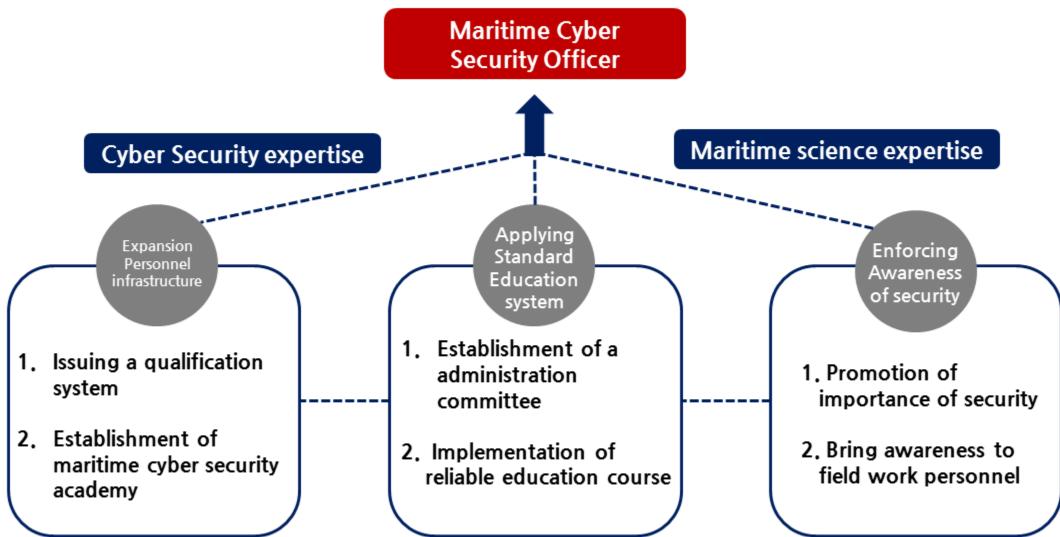
- Electronic navigation system
- Marine information system
- Smart vessel engineering

- Applied system hacking
- Cryptology programing
- Wireless sensor network

		Education Roadmap								
Studies	Study	Basic training						Applied		
	subjects	1 Quarter 2 Quarter			3 Quarter			studies 4 Quarter	Hours	Training form
		C programing apply							10h	e - learning
Technical education	Cyber Security training	Introductio	n to hacking						10h	e - learning
			Applied information						20h	e - learning
			security						201	Class
			Hacking security						20h	
					Understanding	of			20h	Class
					Network attac	c				I
						Applied syst	em hacking		30h	Field
						Cryptology	programing		30h	Class
							Wireless Senso	r Network	30h	Class
		Marine engineering							30h	Class
		Mariti						40h	e - learning	
			Applied electronic						20h	Field
			Marine engineerin	9					30h	Field
	Vessel System training		V	essel engine					30h	Class
			auto	omation system						I
					Elec	tronic navigation	system		40h	Class
					Ма	ine information	system		40h	Class
							Smart vessel er	ngineering	45h	Class
Awarness training	Cyber security	Understanding of secu	rity						10h	e - learning
training	awareness	Security pla	anning and appliance						20h	e - learning

## Maritime Cyber Security Officer education plan







#### Re-establishment of ISPS CODE

The clauses and guidelines regarding cyber security is misleading

Advise the committee to change the clause of ISPS Code regarding software systems and networks.

#### Training of maritime cyber security officer

Initiating a guideline of training program for the new security officers.









Secure Voyage.



Efficient Voyage.

