

Global Journal of Computer and Internet Security

Volume No. 11

Issue No. 2

May - August 2023



ENRICHED PUBLICATIONS PVT. LTD

**S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006**

Global Journal of Computer and Internet Security

Aims and Scope

The Journal of Computer and Internet Security presents research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems. It also provides a forum for ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community.

Managing Editor

Mr. Amit Prasad

Editorial Board Member

Dr. Sachin Garg
Post Graduate Department of
Computer Science Aggarwal College
Ballabgarh,
Faridabad, HARYANA.
sgarg213@gmail.com

Dr. Ambika Sharma
New Delhi Institute of Management
New Delhi, India
sharmaambika3@gmail.com

Global Journal of Computer and Internet Security

(Volume No. 11, Issue No. 2, May - August 2023)

Contents

Sr. No	Article/ Authors	Pg No
01	The Cyber Bullying Recognition and Literacy of Youth in Thailand - <i>Chatchadaakarasriwornnagaoka, Kritchanatsantawee</i>	43 - 48
02	Technology Revolution Gives Cybercrime A Boost: Cyber- Attacks and Cyber Security - <i>Arpita Singh, Sanjay Singh</i>	49 - 58
03	Usage of Blockchain Technologies and Smart Contracts for Secured Internet Banking - <i>Bhavneet Singh, Bhupinder Kaur</i>	59 - 70
04	Strategy to Countering Cyber Terrorism Activities Via Internet by Proposing Six- Ware Cyber Security Framework (SWCSF) - <i>Tri Legionosuko, Rudy Ag. Gultom, Romie O.bura, Deni Dar, Hipdizah, David H. Hutagaol</i>	71 - 84
05	An Integrated Maritime Cyber Security Policy Proposal - <i>Stergios Oikonomou, Ioannis Filippopoulos, Alexandros Voliotis</i>	85 - 105

The Cyber Bullying Recognition and Literacy of Youth in Thailand

¹Chatchada karasriwornnagaoka, ²Kritchanatsantawee

^{1,2}The College of Social Communication Innovation, Srinakharinwirot University, Thailand.

E-mail: ¹chatchada@g.swu.ac.th, ²good0773@gmail.com

ABSTRACT

This research aimed to study 1) the awareness of cyber bullying and social media behavior 2) the cyber bullying and social media literacy level 3) the factors influencing cyber bullying. The quantitative research was carried out by conducting 400 questionnaires from randomly selected groups of youth in Bangkok. Data were analyzed with descriptive statistics including percentage, mean, standard deviation, and multiple regression analysis. The results revealed that the sample group had a high level of awareness and level of media literacy. The most conspicuous issue was the importance of accessing all information on Facebook or IG (mean = 3.88, S. D.= 0.92) at a high level. Factors that influence cyber bullying is: 1) Posting or sending messages to show the exclusion of individual or groups from online societies, 2) Using email or SMS or line to forward rumors, gossip or news not true. The subject of cyber bullying is: 1) being used by others to harass you about sexual misconduct, such as prostitution, through online chatting; 2) being sent or sent by someone else to hurt; 3) Being posted or forwarded to your personal post that you do not want to publish.

Keywords - Cyber Bullying, Media Literacy, Information Technology

I. INTRODUCTION

The rapid advancement of information technology and borderless communication has had impact on living security of people in the society. In the dimension of communication, message receivers may fail to screen the messages they are receiving or using. That is why online social network is another channel that allows message receivers to freely use violence against one another, either intentionally or unintentionally. And that has paved way for a new form of bullying which happens all the time through electronic devices like computers and mobile phones. That new phenomenon is called cyber bullying. Bullying in the cyber world comes in forms of insulting and mockery messages and dissemination of pictures or video clips that contain private information – either true or fake - about someone via the internet or mobile phones with intention to disturb, intimidate, or humiliate particular targets. Those messages can spread quickly while the bullied targets cannot respond promptly. Such bullying behavior can cause stressful, painful, and discouraged feelings to the victims and could lead to severe emotion problems of individuals or eventually social problems.

Cyber bullying is one of serious problems in the Thai society and the situation is growing increasingly worse. More than 80 percent of children and youth in Thailand have faced online bullying, which is among the top of Asia. One important example was a case of a man who was affected by a Facebook

post of a sky train commuter on December 24, 2014 saying “I don’t know who he is, but he’s such a hi-tech guy. He got a small camera hidden in his left shoe. Girls wearing short skirts should beware @BTS Onnut”. The post went viral within 24 hours and he was denounced by netizens as a pervert. What that happened had acute impact on him and his family (ThaiPBS, 2017). “I feel so stressed. I don’t dare to go out. My mother got me something to eat, but I only had few bites. I keep asking myself am I a pervert, why am I condemned, why does my mother have to deal with this notoriety, why does my mother have to get upset because of me while in fact I hadn’t done anything wrong. I was accused of something I didn’t do. I’m such a bad son to make she upset”, said the man.

The actual reason why Mr. John Doe (alias) had a hole in his shoe was that he was repairing an air conditioner earlier and the shoe was accidentally burned by a fire spark from an acetylene torch he was using. And because of the rumor about the hidden camera, Mr. John Doe said he felt antisocial and wanted to escape from the society.

This particular case showed that the message receivers still lacked media literacy. They received and believed the messages without questioning their genuineness or possibility and the accused person did not have a chance to explain or refuse. Accordingly, studies of communication behavior that leads to cyber bullying and online media literacy are vital to the solving and reduction of adverse impact of online social media.

II. OBJECTIVE

1. To study the recognition of bullying behavior in the cyber world and online social media.
2. To study the influencing factors and literacy on bullying behavior in the cyber world and online social media.

III. FINDINGS

Demographic data

The majority or 63 percent of the sample group were female (252 people) and the remaining 37 percent were male (148 people). Most of the sample group or 54 percent were aged between 19 - 22 (216 people). The majority or 51 percent of the sample group were undergraduates (204 people). In terms of occupations, most of the sample group or 53.30 percent were students (213 people). The majority of the sample group or 38.50 percent spent approximately 301 - 500 baht on online media each month (154 people).

Exposure to online media

Exposure to online news and information of the sample group was categorized as follows.

1) Types of media and device – The majority of the sample group or 32.30 percent were exposed to online news and information through mobile phones with an iOS operating system (129 people) and 32 percent were exposed to online news and information through mobile phones with an Android operating system (128 people).

2) Time of exposure per day – The majority of the sample group or 26.30 percent were exposed to online news and information averagely three to four hours each day (105 people).

3) Frequency and pattern of online media use per day – The majority of the sample group used online media for sending messages via Messenger, Line, and IG the most (mean = 3.95, SD = 1.02), in the „frequently“ level.

Recognition of cyber bullying

The sample group recognized and was aware of their privacy on online media, seeing the importance of creating and protecting their online privacy from view or access by others. The item that received the highest score was „protection of privacy of all personal information on Facebook or IG“ (mean = 3.88; SD = 0.92), in the „high“ level, followed by „protection of privacy of personal photos and video clips on Facebook or IG“ (mean = 3.67; SD = 0.96), in the „high“ level, and „protection of privacy of personal messages posted by others“ (mean = 3.60; SD = 1.03), in the „high“ level, respectively.

Experience of bullying others online

The most found bullying experience of the sample group was posting or forwarding Facebook or LINE messages that were intended to humiliate others (mean = 2.35; SD = 1.44), in a „low“ level, followed by sending or forwarding hatred messages online (mean = 2.25; SD = 1.32), in a „low“ level“, and posting or forwarding private messages or photos of others without their consent (mean = 2.19; SD = 1.24), in a „low“ level, respectively.

Experience of being bullied online

The most found bullied experience of the sample group was their personal information was posted or forwarded without their consent (mean = 2.18; SD = 1.20), in a „low“ level, followed by others posting or forwarding humiliating messages about them online (mean = 2.17; SD = 1.17), in a „low“ level and others sending or forwarding messages that hurt their feelings online (mean = 2.17; SD = 1.14), in a

„low“ level. The third most found bullied experience was others sending rumors or gossips about them via emails, short messages (SMS), or LINE messages (mean = 2.13; SD = 1.16) in a „low“ level.

Self-management after being bullied

The method the sample group used the most for self- management after facing cyber bullying was listening to music (mean = 2.42; SD = 0.85), in a „very high“ level, followed by thinking of what to do next (mean = 4.19; SD = 0.76), in a „high“ level, and trying to do good things in order to feel better (mean = 4.19; SD = 0.7), in a „high“ level, and thinking of it as a good lesson or experience (mean = 4.13; SD = 0.76), in a „high“ level.

Multiple regression analysis of factors influencing literacy on bullying behavior in the cyber world and online social media in the aspect of the bullies.

The models that could best forecast literacy on cyber and online media bullying of the bullies were 1) posting or sending of messages to segregate an individual or group of individuals from online society and 2) using emails, short messages (SMS), or LINE messages to spread rumors or fake information. These two models could forecast the literacy on cyber and online media bullying at a rate of 3.2 percent (R Square = 0.032).

Multiple regression analysis of factors influencing literacy on bullying behavior in the cyber world and online social media in the aspect of the bullied.

The models that could best forecast literacy on cyber and online media bullying of the bullied were 1) others using verbal sexual harassment such as calling them hookers or pimps online, 2) others sending or forwarding messages that hurted their feelings online, and 3) others posting or forwarding messages about their personal information without their consent. These three models could forecast the literacy on cyber and online media bullying at a rate of 3.6 percent (R Square = 0.036).

IV. DISCUSSION

The sample group recognized and was aware of the importance of personal privacy online. They gave the most importance to protecting their online privacy from viewing or accessing by others. The item that received the highest score was „protection of privacy of all personal information on Facebook or IG“, in the „high“ level, followed by „protection of privacy of personal photos and video clips on Facebook or IG“, also in the „high“ level. With particular characteristic of the cyber space, online communication has both advantages and disadvantages. While it allows users to show behavior or

express feelings they cannot do in the real world, the anonymity factor of the internet makes it impossible to find the online culprits or investigate if online messages are true or fake. This is why cyber bullying can spread widely among youth and the cyber space has become a place for insulting, exchanging information about sex, and harassing others without having to be as much cautious as in the real world (Ilene R. Bersohn et al., 2002, as cited in NattharatSamoh, 2013). Two important factors that have led to cyber bullying are that cyber bullying can be done anywhere anytime, at home or school, via mobile phones and computers, so it can happen continuously without the victims seeing it coming, and that the bullies can stay anonymous or can create avatars to do the bullying so they do not have to be afraid of being caught (Faye Mishna, et al., 2009, as cited in NattharatSamoh, 2013).

Multiple regression analysis of factors influencing literacy on bullying behavior in the cyber world and online social media in the aspect of the bullies showed that 1) posting or sending of messages to segregate an individual or group of individuals from online society and 2) using emails, short messages (SMS), or LINE messages to spread rumors or fake information were two important factors that can explain the literacy on cyber and online media bullying. This is consistent with a research by SupawadeeCharoenwanit (2017), which defined cyber bullying as bullying between or among people in the cyber world including defaming, insulting, verbal abusing, or spreading of secret or personal information with an intention to cause online harm or humiliation in forms of text messages, video clips, and emails on websites or applications and to make the bullied victims feel ashamed or mentally hurt. Bullying can be categorized into many forms (Kaspersky Lab, 2015; WittayaDamrongkiattisak, 2015) such as denigration, outing, and trickery. Meanwhile, multiple regression analysis of factors influencing literacy on bullying behavior in the cyber world and online social media in the aspect of the bullied showed that 1) others using verbal sexual harassment such as calling them hookers or pimps online, 2) others sending or forwarding messages that hurt their feelings online, and 3) others posting or forwarding messages about their personal information without their consent were three important factors that can explain the literacy on cyber and online media bullying. This is in line with a research of Wimonthip et al. (as cited in SupawadeeCharoenwanit, 2017), which surveyed cyber bullying behavior of youth in Bangkok and found that 43.9 percent of the sample group admitted to being bullied on the internet. The most found forms of bullying were gossiping and cursing. Likewise, a research of Pimpawun et al. (2012, as cited in SupawadeeCharoenwanit, 2017), which studied cyber bullying among Thai girl teens and found that 45.4 percent of Thai teenage girls used to face bullying. The 41.4 percent of which were threatened and attacked online, 5.3 percent faced sexual harassment online, and 16.3 percent were humiliated by recording and dissemination of defaming information online. These researches showed that cyber bullying is increasing around the world and, even worse, in the eyes of many children and youth, cyber bullying is normal behavior anyone has the right to do.

V. IMPLICATIONS

1. There should be indication of the impact of cyber bullying in various dimensions such as social dimension, economic dimension, and psychological dimension. And youth should be encouraged to realize that cyber space is not a personal space they can do anything without considering the possible consequences.
2. There should be provision of knowledge about laws relating to online media, online society, and social network.

REFERENCE

- [1] ThaiPBS, "Check before Share: Case Study From The hold of man shoes," Online: Retrieved December 1, 2016, From <http://news.thaipbs.or.th/content/254319>, retrieved March 10, 2017
- [2] NattharatSamoh, "Youth Perceptions on Cyberbullying," *Journal of Behavioral Science for Development*, Vol.6, No.1, pp.351-364, 2014.
- [3] SupawadeeCharoenwanit, "Cyber Bullying: Impacts and Preventions in Adolescents," *Journal of Science and Technology Information*, Vol.25, No.4, pp.639-648, 2017.
- [4] Kaspersky Lab, "10 forms of cyber bullying," Online: Retrieved December 1, 2016, from <https://kids.kaspersky.com/10-forms-of-cyber-bullying>
- [5] WittayaDamrongkiattisak, "Cyberbullying2," Online: Retrieved March 15, 2016, from <http://www.infocom-mmju.com/icarticle/images/stories/icarticles/ajwittaya/digital/cyberbullying2.pdf>

Technology Revolution Gives Cybercrime A Boost: Cyber-Attacks and Cyber Security

¹Arpita Singh, ²Sanjay Singh

¹Research Scholar, Amity University, Lucknow, India

²Professor, Amity University, Lucknow, India

E-mail: ¹singharpita999@gmail.com, ²sksingh1@amity.edu

ABSTRACT

We are living in digital era where technologies are retouched and proliferate rapidly day by day because of this whole society in fence with gadgets .Criminals are also encourage by technologies and crime is converted into cybercrime with the assistance of computers (Desktops), laptops, mobile phones, etc. To quest criminals and to get rid of cybercrime, a new branch of forensic science is introduced which Digital forensic science is thus encompassing the investigation, track evidence with the help of electronic media and recovery of materials found on digital devices. The nature of crime is still same but the way has changed completely now criminals are using technology to get close to victims instead of going in victims place. In this paper we will discuss about what is cybercrime, explore different categories of cyber-attacks, the Deep web and who digital forensic helps in detection and controlling in cybercrimes. We conclude our study by analyzing some modification required in present digital forensic model and proposed future actions that should be taken to tackle cyber- crime and harden cyber security.

Keywords - Cybercrime, Cyber-Attacks, The Dark Web, Digital Forensic

I. INTRODUCTION

Technology flourish and freshness making it more challenging to detect cyber-crimes. From last some couple of years, 689 million people in 21 countries experienced cybercrime in their daily lives[1]. It has become so passable that many people equally fear online risks and real-world risks. Most of the people believe it has become more rigorous to stay safe online in the past five years than in the “real world”. Indians are cursorily becoming the largest users of several mobile applications and websites. Various security service providers says this make it more challenging in the field of security. So this is very convenient for cyber criminals to attack online through fake apps by putting them in play store.

“With banking increasingly becoming an integral part of mobile device usage, attackers have begun building more sophisticated capabilities into their mobile banking malware. By staying under the radar, they steal more than just credit card data, and bypass security mechanisms,” notes Nilesh Jain, vice president, South East Asia and India, Trend Micro.

One of the very famous cases of cybercrime in virtual world is “The game Blue Whale challenges”, created by, 21 year old Russian Phillip bedecking, which was played by children in the virtual world, had claimed an estimates 130 lives across the world during 2015- 2016 [2].

According to Symantec, 45% of the most popular Android apps and 25% of the most popular iOS apps request location tracking, 46% of popular Android apps and 24% of popular iOS apps request permission to access device's camera, and email addresses are shared with 44% and 48% respectively [3].

Most of the consumers (58%) say they are more likely to experience cybercrime than get the flu, so it's no surprise that 76% of consumers say they are more of the time alarmed than ever about their privacy and 95% believe that it's very important to require companies and organizations to give consumers control of their personal data, including 44% who believe it is absolutely necessary that companies do this, or consequently be fined [4].

As people continue to seek convenience, it's very important to practice simple cyber safety measures:

a. Try to use strong passwords: Try to don't repeat your passwords on different sites and applications. Make them very complex and pick a random combination of words that includes a at least 10 letters, numbers, and symbols.

b. Always keep your software updated: Cyber criminals try to frequently use known exploits, or flaws, in your software to gain access to your application through network. When any software or application gets updated, it also changes its security measures.

c. Use full-service internet security suite: Invest on the security suite that offers real-time protection against existing and emerging malware including viruses and helps protect your private information when you go online.

d. Manage your social media settings on private mode: when you open any account on social media, Keep your personal and private information locked down. Social cybercriminals can often get your personal and financial information with just a few data points, so less share information publicly.

e. Strengthen your home network: A VPN will help encrypt all traffic which can be sent and received from your devices. If cyber criminals can manage to access your network, they will not be able to intercept the data being sent over your network.

f. Adopt necessary course of action to get protect yourself anti-identity theft: When use effectual shopping online, using any secure network, any card reader devices or ATMs any other transaction

online etc. you should always alert on each and every notification. You should always take advantage of protection tools available like ID theft alarms and EMV chip credit/debit card as an extra protection. Cyber- attacks are not sometimes complained by industries and companies because they all are concern about bad publicity. Knowledge plucked from cyber-attacks can be help to analyze method and procedure of cyber-attacks and develop security masseurs [5].

Here we discuss some important and necessary actions for saving one from cyber-attack. Each and every one should follow these steps in their daily life so that they can prevent themself from cyber-crime. There are more course of action for prevention of cyber-crimes but these are necessary one.

II. DEFFERENT CATEGORIES OF CYBER- CRIME

The U.S. Department of Justice explains cybercrime as illegal acts that utilize computer and network for storage of most of the evidence. The U.S. Digital Media copyright Act(DMCA) of 1998 specifies that swap of files of copyright material and content like music and video is an illegal and punishable by law[6]. Now cybercrime effects on network, economy, normal human life, government sectors and private sectors with different ways and it is creation threats to everyone's privacy, economy and social life hence it is duty of cyber experts to create another more secure driveway for normal human being which must convenient as well.

Based on security and technology cybercrime may be categories is many series like-

1. Child pornography: Online pornography which is illegal and involves minors in sexual activities. Some disallowed activities which include trading upon children through pornographic images, cyber-sex, and prostitution, sex slavery of child, video, chats, Webcam Child Sex Tourism (WCST) and sex service.

2. Cyber hate speech: There are many ways of online hate speech that may affects social rights, freedom of expression. Online hatred target religions, nationalities, countries, minorities, migrants, gender identities, individual disabilities, political parties, sports person, youth, old and children.

3. Cyber offenses against Intellectual Property: Some online activities that may transgress the protection of patents, trademarks and copyrights, any online forgery or robbery, disrupt freedom of any individual.

4. Cyberbullying: This includes use of technologies to spoliation of people. Now the days there are a lot of memes running in social sites, cartoon pictures, unlawful messages in order to mock people, and impersonating victims.

5. Cyber spying: Practice of gaining access of any document without permission of holder, government or any group that involve infiltration, interception and acquisition of data. Freelance spies utilize spyware, surveillance methods, key loggers, data traffic interception and communication monitoring.

6. Cyberfraud: Online fraud or forgery exists in many different ways. Victims are tricked through the use of digital technologies. Some examples include online auctions, stock fraud, credit card fraud, telemarketing fraud, false advertising schemes, false damage claims, insider trading, cyber smear campaigns, ad hoc fraud, computer hoaxes, click fraud, Ponzi/pyramid schemes, lottery/sweepstakes and contest scams, get-rich-quick schemes, the Nigerian scam, ringtone scams, missed call scams, text message scams, SMS trivia scams, health scams, emergency scams, dating scams, job scams, small business scams and service scams.

7. Cybergrooming: This is an act of 'befriending' a young and innocent human online by emotional connection and by gaining victim's trust "to facilitate himself with sexual contact and/or physical relation with the victim with target to sexual abuse."

8. Cyberheist: This cybercrime involves a large monetary scale theft conducted through online which is equivalent to real World Bank heist from banks or financial institutions. Malware, hacking or phishing techniques are normally major part of this crime. Cyber criminals often target one financial organization to steal a large amount in a really short period of time. The theft may effect whole organization or a single account with huge amount of cash by e-banking transaction, online payment and stealing money from ATMs.

9. Cybering: This act involves a series of online communications of two partners in a sexual manner. This is also known as 'Cybersex' e.g. among lovers who are apart from each other who exchange texts, images and video clips with each other. Sometime real time videos and chat (images and text) gets viral.

10. Cyberlaundering: In this process comprise commercial transactions using funds from criminal activities. Cyberlaundering is based on e-payments,digital transaction and illegal hard cash that are converted to illegal electronic money.

11. Cyberstalking: Electronic means to monitor people or organization without their consent (stalk) or harass. This illegal activity involves real-time and offline stalking to intimidate, defame and/or blackmail the victims.

12. Cyberterrorism: Cyberterrorists use of technology in terrorist activities that conduct violent acts that result mostly on civilians in metropolitan areas in order to achieve ideological or political gain, religious beliefs or personal reasons.

13. Cybertheft: This act refers financial profit by stealing and selling information from internet in every way possible. The dark web is where most of the stolen information is sold. Cyber theft most include hacking of bank account, commonly sold credit or debit card numbers, online auction credentials and bank account numbers in intension to wrongly sending protected material over the internet.

14. Cybervandalism: Cyber vandalism is act where criminals damages information infrastructures that takes place using computer technology for their own enjoyment and pleasure. The most common attacks are website defacement, using malware to delete data, social media account hijacking and Distributed Denial of Service Attacks (DDoS).

15. Data breach: Revealing of personal information or data that may breaks confidentially. These damage can affect financial loose, physical assets, trade secrets of corporate reputation, lawsuits and intellectual property.

16. Hacking: Hacker is a computer expert with intelligence and a great technical knowledge but when he uses this knowledge in illegal way to cross the threshold of gaining unauthorized access in network through computer system or any other technology it becomes crime.

17. Identity theft: When cybercriminal deliberately use someone else's identity, for obtaining financial benefit or revenge. Here attacker pretend to be another person by using someone else's personal information like their name, identifying number, debit/credit card number, name, date of birth, signature, PIN, electronic signature or fingerprints without their permission to gain benefit from access a person's financial resources.

18. Phishing: Fraudulent act where confidential and sensitive information like user identification number, passwords and credit/debit card detail steals from end user using spam emails and fake

websites. Phishing kit is an active real time URL that interact with a valid website and end user to steal confidential information as man-in-the middle.

19. Religion-related cyber offences: one of the most dangerous forms of terrorism “religious terrorism” in such cyber offences deliver hate speech against other followers of God and other religions.

20. Revenge porn: This cybercrime include the act of distributing sexual images or video of a victim without their knowledge for sake of revenge or search of financial profit

21. Spam: Spam is incredulous junk text message, images and advertisements that are sent by electronic means like email, blogs, search engines, instant messaging (IM) and smart phones.

III. NEED OF CYBER SECURITY MODEL

Cyber security is a important part of information security, this is specifically concentrate on securing and protecting computer systems, computer data and all digital infrastructure from unauthorized access from being hacked, damaged or to be inaccessible. All websites, server, data, programs, accounts etc. can be exploit through cyber-attack so it need to prevent hence cyber security model is extremely needed.

Cyber security model is needed also because-

1. To prevent further activities from assaulting the target again and again.
2. To take the offender behind the bars.
3. With the help of the cyber security models, the action which led is illegal can be traced back so that the perpetrators can be identified and determined.
4. Corporate security professionals and digital forensic experts to make available for security to their respective networks by the helps in improving standards and making them convenient for normal human being.
5. To prevent illegal attacks from eventful again, current detection and prevention mechanisms can be improved with the help of models.

In recent years number of cases from cyber security gets register so cyber security comes under rapid development. Degree of impact on government, organization and individuals of cyber-crime increases day by day hence cyber security model become a critical business issue.

IV. THE DEEP WEB

The deep web content are not indexed by common search engines and standard web browsers cannot access it which is hidden behind HTTP forms and could be used in mailing, online transactions and the real time services for which user must be paid for like online research papers and magazine, video on demand etc. [7] Now Deep web is getting used by online subterranean criminal activities; so its major component converting in Dark Web. Systems like Freenet, TOR and I2P (invisible Internet Project) are part of sophisticated Dark Web where most of owners deliberately keep hidden most of things from view. Here they cyber criminals can sell and buy all illegal things online like illegal drugs, malware, weapons, stolen accounts, identity cards, credit/debit cards, passport, cyber-laundering things.[8]

A new research is definitely required to detect malicious criminal activities, all criminal services and illegal online transaction that occur so frequently now these days in the Dark Web because the Dark Web is providing a safe platform to the cyber criminals.

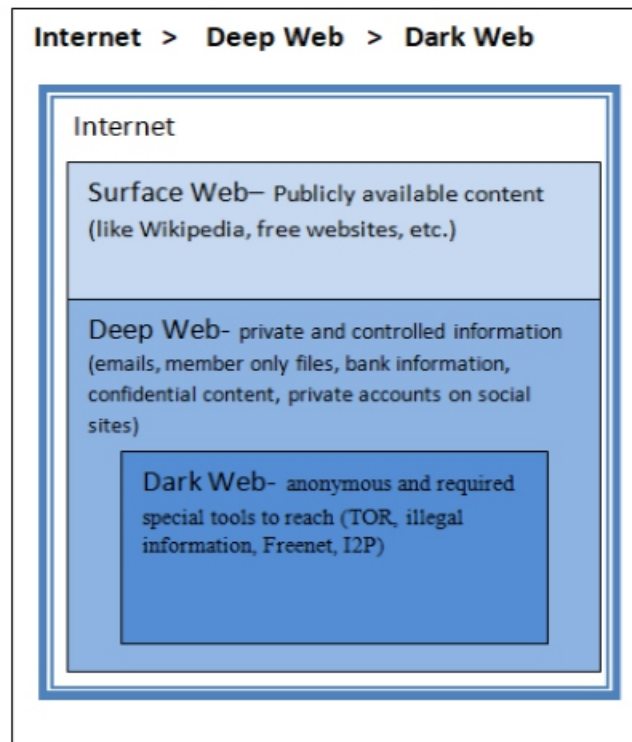


Figure: 1 Three Fold Wave Model of Internet

V. PRESENT ACTION PLAN TO TACKLE CYBER CRIME & PROPOSED FUTURE PLAN TO TACKLE CYBER CRIME

As cybercrime is increasing day by day with a huge ratio but it is very surprising to know about the data that there were no considerable arrests made as compared to the number of cases got registered. Like in 2013, 4356 case got registered under IT Act and persons got arrest were only 2098 which is less than 50%. Similarly 1337 cases reported under IPC sections and persons arrested were only 1203 which is

less than the number of cases got registered. Financial sectors are very often get target, it is more than 60% of total cyber-attacks.[9] When go through the available data it can be conclude that the offenders of cybercrime are likely from 18-30 years age group followed by 30-45 years means most of the young generation involve in cyber-criminal activity.

Present action plan of digital forensic investigation with modified standard procedure as given below [10]:

- **Step 1:** Observe and capture things and generate a report on possible tool and set of actions suitable for digital evidence retrieval in digital forensic.
- **STEP 2:** Generate evidence based on real time- relevance matter like when one got ill on 1-oct- 2018 started taking medicines from that day doctor will start observing him/her from that day not earlier not later.
- **STEP 3:** Inspect all collected data carefully and decide whether digital forensic investigation procedure is required or not.
- **STEP 4:** Enlist the required digital evidence for the process and also produce backup copies of all evidence for further analysis.
- **STEP 5:** Based on digital forensic analysis result which gets produced, the seizure for devices and it should be conditioned to serious case for further process on zone 1.
- **STEP 6:** Based on digital forensic analysis result generate on zone 1, approach zone 2 digital forensic if required and it must be highly restricted for very first degree criminal activity like terrorism.
- **STEP 7:** Generate the end final report and update all protection measures to avoid such cases in future.

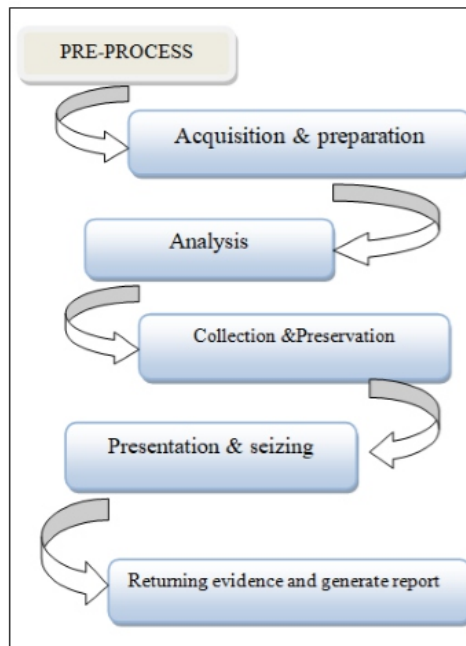


Figure 2: Basic Digital Forensic Investigation Model

The new proposed encapsulated model is analytical, logistic, interpretative and accurate which renounce no errors in case study. Based on analysis done by experts digital forensic seems very challenging, effective and interesting. This study initiated with some old theories and model which are on practice and day to day experiences of experts and researchers. Now it has revealed many more aspects of this field are still untouched even today. Gathering and analyzing of data has never been easy, it is still a tough task. Concept of gathering and analyzing data for generate result has been revolutionized in process of digital forensic which are based on facts and authentic always. [11]

V. CONCLUSION

Cybercrimes are spreading his arms all over the network which is costing users and institutions billions of dollars. Each and Every user should be very careful while surfing online and must read every instruction about security. With more sophisticated methods and technologies future of cybercrime is very horrible. Organization should use every possible protection against cybercriminals and hackers. With the help of anti-virus software, firewalls, biometrics, updated version of software's..etc everyone must try to protect himself from cybercrime. Countries and international organizations should make more powerful laws against cybercrime. Security agencies could try to find many more ways to stop cyber- attacks and provide security to internet consumers. Finally, internet users must educate and informed about cyber problems and security features and how to deal with it.

REFERENCES

- [1] 2016 Norton Cyber Security Insights Report <https://us.norton.com/cyber-security-insights-2016>
- [2] <https://www.thehindubusinessline.com/specials/india-file/cyber-crime-cops-and-the-law/article26502097.ece> [Online]
- [3] "The new Indian Express" 2019 [Online] <http://www.newindianexpress.com/lifestyle/tech/2019/mar/23/mobile-revolution-gives-cyber-crime-a-boost-1954534.html>
- [4] 2018 Norton LifeLock Cyber Safety Insights Report <https://us.norton.com/cyber-security-insights-2018>
- [5] Marilyn Wolf "Computer Security as Civil Defense" Available at <https://ieeexplore.ieee.org/document/8666652>
- [6] Priyanka Dhaka ; Rahul Johari "CRIB: Cyber crime investigation, data archival and analysis using big data tool" Published in: 2016 International Conference on Computing, Communication and Automation (ICCCA) Electronic ISBN: 978-1-5090-1666-2 Print on Demand (PoD) ISBN: 978-1-5090-1667-9
- [7] Regner Sabillon, Victor Cavaller, Jeimy Cano, Jordi Serra- Ruiz "Cybercriminals, Cyberattacks and Cybercrime Privacy, security and control" 978-1-5090-6096-2/16/\$31.00 ©2016 IEEE
- [8] Trend Micro (2015). "Below the Surface: Exploring the Deep Web". Forward-Looking Threat Research Team. TrendLabs. <https://www.trendmicro.com/cloud-content/us/pdfs/securityintelligence/white-papers/wp_below_the_surface.pdf>
- [9] P. N. Vijaya Kumar "Growing cyber crimes in India: A survey" Published in: 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE) Electronic ISBN: 978-1-4673-8594-7 Print on Demand (PoD) ISBN: 978-1-4673-8595-4
- [10] Malek Harbawi ; Asaf Varol "An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework" Published in: 2017 5th International Symposium on Digital Forensic and Security (ISDFS) Electronic ISBN: 978-1-5090-5835-8 Print on Demand (PoD) ISBN: 978-1-5090-5836-5
- [11] Gulshan Shrivastava ; B. B. Gupta "An Encapsulated Approach of Forensic Model for digital investigation" Published in: 2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE) ISBN: 978-1-4799-5145-1

Usage of Blockchain Technologies and Smart Contracts for Secured Internet Banking

¹Bhavneet Singh, ²Bhupinder Kaur

¹Yes Bank YamunanagarIndia,

²Meshed GroupSydney Australia

E-mail: ¹sbhavneet13@gmail.com, ²kaurb2605@gmail.com

ABSTRACT

With the increasing number of devices and gadgets using network based communication, the vulnerabilities are elevating to a huge levels. There is need to work out on the secured mechanisms so that the transactions in the network channels can be made secured. To cope with such scenarios, the usage of block chain technology is quite prominent so that the peer to peer based secured communication can be done. In current scenario, the block chain technology is more focused towards crypto currencies in which the distributed ledger is maintained for the transactions. The distributed ledger refers to the replicated, synchronized and shared digital asset to multiple locations and devices so that the third party manipulation cannot be possible. For example, if a bank follows the distributed database ledger with block chain technology can enforce higher degree of security. If that bank is having one million customers then the records of the transactions will be stored on those one million devices. It refers to the fact that the hacker will have to hack one million devices in real time rather than a single server. This is the major advantage of using the decentralized block chain technology. In case of centralized application, if hacker penetrates the server of a bank, then all the details and records of all the customers can be copied. That is the main reason because of which the government agencies should focus on decentralizing their web based applications.

Keywords - Block chain Security, Data Security, High Availability Data, Secured Databases.

I. INTRODUCTION

In the present period, Blockchain Technology is one of the key zones of research just as execution explicitly in the space of Cryptocurrency. Presently days, various computerized digital currencies are very conspicuous and shared all through the world regardless of enormous analysis and contentions [1, 2]. These cryptographic forms of money incorporate BitCoin, Ethereum, LiteCoin, PeerCoin, GridCoin, PrimeCoin, Ripple, Nxt, DogeCoin, NameCoin, AuroraCoin, Dash, Neo, NEM, PotCoin, TitCoin, Verge, Stellar, VertCoin, Tether, Zcash and numerous others. These blockchain based digital currencies don't have any halfway bank or installment door to record the log of the exchanges [3, 4, 5]. That is the principle reason as a result of which numerous nations are not permitting the digital forms of money as legitimate cash exchange [6, 7, 8]. All things considered, these blockchain based digital currencies are celebrated and utilized as a result of immense security highlights [9, 10, 11]. The blockchain organize is having a square of records in which every single record is related with the dynamic cryptography so every one of the exchanges can be encoded with no likelihood of sniffing or hacking endeavors [12, 13, 14].

Using blockchain technology, the servers of government for land registry, citizen information, Permanent Account Number (PAN) and many others can be made secured using decentralized apps [15, 16, 17].

The blockchain based decentralized application can be used for following

- Digital Identity Management in of Government Documents
- (Birth, Marriage and Death) Certificates
- Asset and Land Registry
- Notarized Documents
- Incorporation Services
- Taxation and Financial Records
- Personalized Government Services
- Polling / Voting / Assembly Elections Social Welfare and Benefits

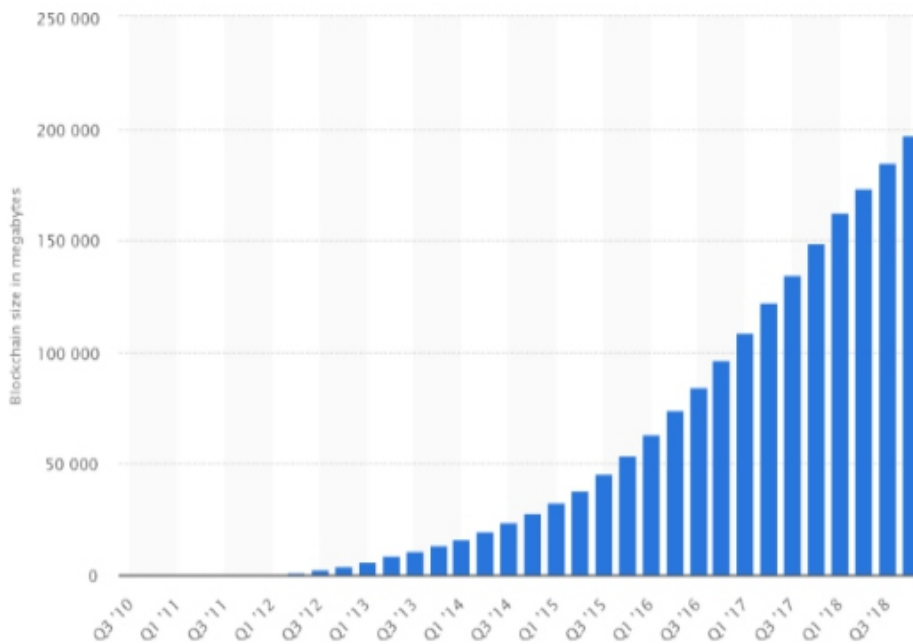


Figure 1: Block chain Size from 2010 to 2019

As per the research analytics and reports from Statista.com, the size of BitCoin blockchain from year 2010 to current year 2019 and that is having enormous use throughout the globe.

II. DECENTRALIZED APPLICATIONS (DAPP) WITH SECURED BLOCKCHAIN

The decentralized application (dApp) refers to the software application that executes on the distributed channels so that the hacking of application will be near to impossible. In traditional centralized application, the application is deployed on a single server [18, 19, 20]. The main limitation with

centralized approach is that if that centralized server is hacked then everything can be damaged or copied from that server. In case of decentralized application, there is no single server rather storage is done on all the client devices so that the replication of the transaction can be done with maximum availability of transaction records.

In the scenario of decentralized application, the hacker will have to crack all the devices associated with that application and that will be very difficult in real time using smart contracts. In smart contracts based dApp, the dynamic token sharing is implemented so that the transactions will have maximum security measures [21, 22].

2.1. Smart Contracts

The smart contract programming is required for the globalization based transactions. It means that the transactions can be done across the people who can't communicate because of different continents, languages and traditions. Smart Contracts automatically validate the transactions and business dealings between the people who can't understand the language of each other.

The smart contract programming is required for the globalization based transactions. It means that the transactions can be done across the people who can't communicate because of different continents, languages and traditions. Smart Contracts automatically validate the transactions and business dealings between the people who can't understand the language of each other [23, 24].

Free and Open Source Tools for Blockchain Development

Hydrachain

URL: <https://github.com/HydraChain/hydrachain>

- Creation of Permissioned Distributed Ledgers
- Setup of Private Chain
- Fully Compatible with Ethereum Protocol

Multichain

URL: <https://www.multichain.com/>

- Compatible with Bitcoin
- Fully Customizable
- Fine-Grained Managed Permissions
- Rapid Creation and Deployment of New Blockchain
- Powerful Data Sharing and Encryption

OpenChain

URL: <https://www.openchain.org/>

- Digitally Signed transactions
- Custom rule definitions for ledgers
- Robustness and Fine Validation
- Client Server Architecture
- Module Design with Real Time Validations
- Immutability with Security

Ethereum

URL: <https://www.ethereum.org/>

- Smart Wallets and Smart Money
- Creation of Own Cryptocurrency Development
- Security against third party intervention or downtime
- Execution of Smart Contracts
- Virtual Shares with Crowd Fund and Crowd Sale

Corda

URL: <https://www.corda.net/>

- Platform for Blockchain and Distributed Ledger
- Smart Contracts
- Development of Distributed Apps
- Notary Infrastructure for Sequencing and Validation of Transactions
- Flow based Framework for Negotiation and Communication in the participants

Credits

URL: <https://credits.com/>

- Smart Contract Programming
- Real Time Monitoring of Network Transactions
- Web Wallet with Security using Private and Public Keys

BigChainDB

URL: <https://www.bigchaindb.com/>

- Big Data enabled Blockchain Database
- Decentralized Management and Control

-
- Dynamic Management of Digital Assets
 - Byzantine Fault Tolerant (BFT) for high performance computing applications
 - Rich Permissioning at each Transaction
 - Integration with MongoDB NoSQL for fast transaction processing with unstructured data
 - Resistance to Tamper and Faults for Security

Quorum

<https://www.jpmorgan.com/global/Quorum>

- Enterprise Level Smart Contract and Distributed Ledger Platform
- Peer Permissioning
- High Performance using Raft based Consensus
- Exchange of Private Messages with Secured Contracts
- Fully Customizable for Large Scale Business and Corporate Applications
- Integration with CakeShop Software Development Kit (SDK) for Graphical User Interface (GUI) enabled Smart Contracts, Quorum Networks and APIs.

Symbiont Assembly

URL: <https://symbiont.io/>

- Byzantine Fault-Tolerance
- Handling Thousands or more Transactions Per Second
- Elimination of data loss with storage of real time critical documents on network
- Sharing of data with advanced encryption and dynamic cryptography
- Maintenance of transaction logs and lifetime without third party intervention

Embark

URL: <https://embark.status.im/>

- Peer to Peer Secured Messaging
- Development and Distribution of Decentralized Apps with Decentralized Communication with Orbit and Whisper
- Integration with Web Technologies including Foundation, React, Angular and others
- Custom Framework Development
- Association with Simulated Blockchains including Ganache
- Automatic Smart Contract deployment
- Integration with Ethereum Blockchains
- Testing Environment for Smart Contracts using Web3

Solidity

URL: <https://github.com/ethereum/solidity>

- High Level Programming Language for Smart Contracts
- Contract Oriented Statically Typed Programming Language
- Object Oriented with support to multiple blockchain platforms
- Compatible with Ethereum, Tendermint, Counterparty and ErisDB
- Creation of Smart Contracts for Crowdfunding, Multi-Signature Wallets, Voting, Blind Auctions and many others

Truffle

URL: <https://truffleframework.com/>

- Platform for Smart Contract Programming with compilation, linking and binary management
- Development Environment with Framework for Testing
- Testing of Contracts using Chai library and Mocha Framework
- NodeJS support for Mocha and Chai integration for unit testing

Solidity is one of the powerful and high performance programming language for writing smart contracts. It follows object oriented programming paradigm with higher degree of security and performance which can be integrated with assorted blockchain platforms.

The code of solidity is compiled and transformed to bytecode which is executed on Ethereum Virtual Machine (EVM). Solidity Programming is having the key base of multiple programming languages and scripts including Python, JavaScript, C++ so that it can be integrated to multiple environments and platforms for integration with blockchains. To work with Solidity Programming, there are many Integrated Development Environments (IDEs) and Editors which can be used including Remix, EthFiddle, JetBrains and many others [25, 26, 27].

To start with Solidity Programming, Remix is one of the powerful IDEs that is open source and also provides the web based interface. The web based interface of Remix IDE is easy for the developers to create the Smart Contracts with Blockchain Programming [28, 29, 30].

The URL of Web Based Remix IDE is remix.ethereum.org that can be accessed directly on the web browsers for writing, compiling and executing the smart contracts.

Following is the scenario of Blockchain integrated currency with the Internet Banking Transactions so that the overall communication and financial transaction will be secured and sniffers free.

```
pragma solidity ^0.4.18; contract NewCryptoCurrency {
string public name = 'NewCryptoCurrency';
// Name of the New Currency
string public currencyName = 'Currency1.0';
// Select Currency
mapping (address =>uint) EBankingBalance;
// Key-Value Pair for Address-Account
event Transfer(address _sender, address _receiver, uint256 _value);
// Log Recording constructor() public {
// Constructor on Creating the Contract EBankingBalance[msg.sender] = 100000;
// Balance Confirmation
}
function sendAmount(address _receiver, uint _amount) public returns(bool sufficient)
{
if(EBankingBalance[msg.sender] < _amount) return false;
// Authentication of the Transfer EBankingBalance[msg.sender] -= _amount; EBankingBalance
[_receiver] += _amount;
emit Transfer(msg.sender, _receiver, _amount);
// Commit of Payment Transfer with Transaction Recording return true;
}
function getBalance(address _addr) public view returns(uint) {
// Checking the Balance return EBankingBalance[_addr];
}
}
```

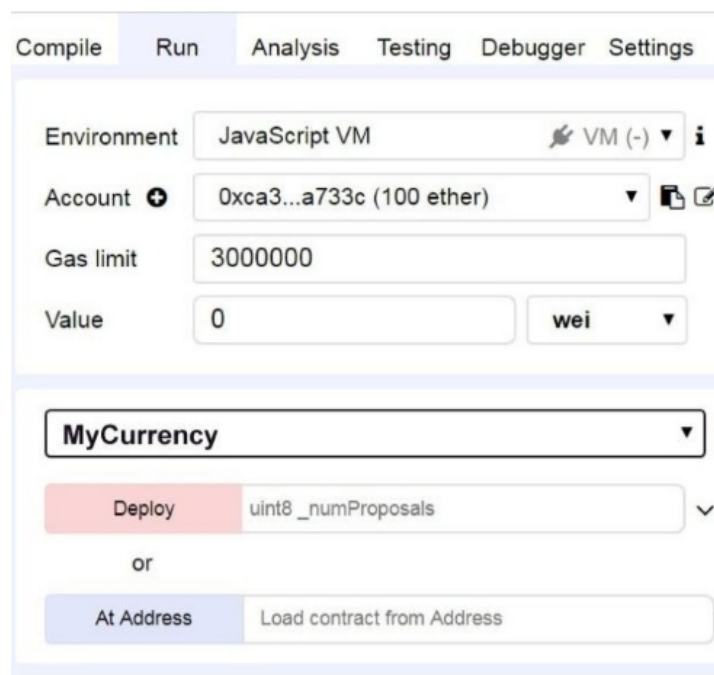
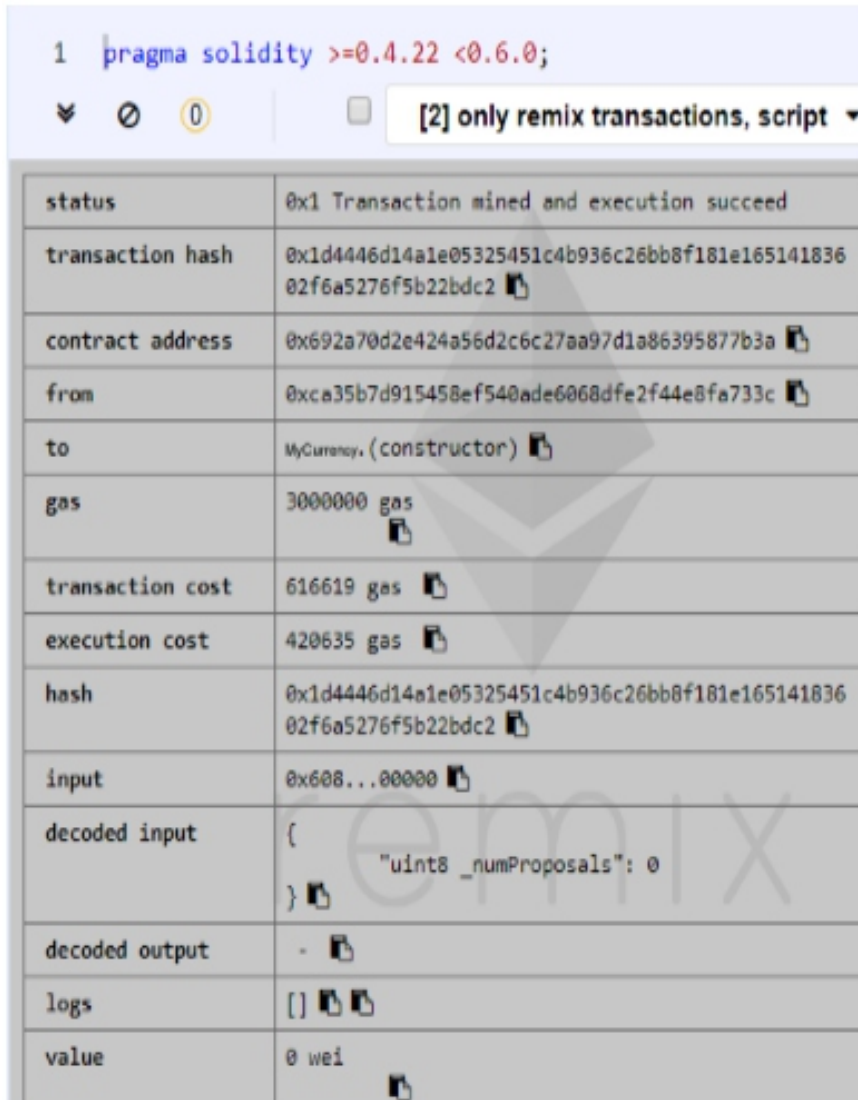


Figure 2: Compile and Run Code in Remix IDE

On click of Deploy option in Remix IDE, the code is executed and detailed logs of the transaction can be viewed.



The screenshot shows the Remix IDE interface. At the top, a code editor contains the Solidity pragma statement: `1 pragma solidity >=0.4.22 <0.6.0;`. Below the code editor, there is a dropdown menu showing "[2] only remix transactions, script". The main part of the screenshot is a table displaying transaction details.

status	0x1 Transaction mined and execution succeed
transaction hash	0x1d4446d14a1e05325451c4b936c26bb8f181e16514183602f6a5276f5b22bdc2
contract address	0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	MyCurrency. (constructor)
gas	3000000 gas
transaction cost	616619 gas
execution cost	420635 gas
hash	0x1d4446d14a1e05325451c4b936c26bb8f181e16514183602f6a5276f5b22bdc2
input	0x608...00000
decoded input	{ "uint8 _numProposals": 0 }
decoded output	-
logs	[]
value	0 wei

Figure 3: View Logs and Transaction Details

The detailed logs of the Blockchain Transaction can be analyzed associated with the transaction. There are multiple parameters in the transaction log including Gas Limit. The Gas Limit in Smart Contract Programming refers to the amount of work or throughput associated with the transaction [31].

2.2 NodeJS and Web3JS

NodeJS is a cross-platform open source platform for JavaScript based programming. It can be used for the development of multiple applications including Blockchain Development, Smartphone Applications, Distributed Web Applications, NoSQL Processing, Big Data Analytics, Machine Learning, Internet of Things (IoT) and many others related to advanced computing.

For blockchain programming, NodeJS is integrated with Web3JS. Web3JS refers to the set of libraries and tools for interaction with blockchain based connections [32].

The Web3JS Platform for blockchains and dApp can be integrated with following instructions

npm: npm install web3

purejs: link the dist/web3.min.js meteor: meteor add ethereum:web3

After installation, the code in JavaScript and Server Side Scripts is written with the smart contracts and deployment for the secured applications.

Truffle is another programming suite for the development of blockchain based smart contracts that can be installed with NodeJS and can be executed on Ethereum Virtual Machine (EVM).

With the execution of following instruction, the Truffle Suite is associated with NPM

npm install -g truffle

After installation of Truffle, the versions of installed version can be checked in the terminal truffle version The new project EffBlockchain in Truffle can be mapped as

mkdirEffBlockchain cdEffBlockchain truffleEffBlockchain

In Truffle, the following directory structure is followed to code the application

- contracts/: Source Code for the Smart Contracts
- migrations/: Migration System and Handlers for the Smart Contracts
- test/: Tests and JavaScript Code
- truffle.js: Configuration File for Truffle
- EffBlockchain: Additional Folders and Files required for coding the blockchain

A new file <filename.sol> is created in contracts/ directory for the base coding of smart contracts in the following format

```
pragma solidity ^0.5.0; contract Mysmartcontract {  
}
```

Sending Values

```
function adopt(uintMyVar) public returns (uint) { require(MyVar>= 0 &&MyVar<= 15);  
adopters[MyVar] = msg.sender;  
returnMyVar;  
}
```

The compilation of Truffle Code is done as follows: `truffle compile`

The framework of Embark provides the tools and libraries for development of decentralized apps so that blockchain based implementation can be done. Embark can be used as an alternate to Truffle. To work with Embark, there is need to integrate Node Version Manager (NVM) having multiple versions of NodeJS.

Using "`embark run`", the dashboard of Embark is invoked

The token generation can be further written in code

```
pragma solidity ^0.4.25;
import "openzeppelin-
solidity/contracts/token/ERC20/ERC20.sol"; contract CurrencyToken is ERC20 {
string public name = "CurrencyToken";
string public SymbolCurrency = "SYMBOLCURRENCYCURRENCY";
uint256 public decimals = 18; constructor() public {
}
}
```

As in the above example, the new currency can be mapped with the transaction with the secured communication with network based transactions. It can be anything as per the requirements of the smart contract associated with the blockchain.

III. CONCLUSIONS

Now days, the blockchain based implementations are used in many international banks and the related transactions so that the communication can be made secured. As blockchain based development is the emerging domain of research, there is need to work out different issues related to privacy and resource optimization. In blockchain and decentralized applications, the data is replicated to enormous devices and the issues of security and integrity arise. With the development and deployment of advanced algorithms, the performance of blockchain based implementations can be elevated.

REFERENCES

- [1] Bogner, A., Chanson, M., & Meeuw, A. (2016, November). *A decentralised sharing app running a smart contract on the ethereum blockchain*. In *Proceedings of the 6th International Conference on the Internet of Things* (pp. 177-178). ACM.
- [2] Bahga, A., & Madisetti, V. K. (2016). *Blockchain platform for industrial internet of things*. *Journal of Software Engineering and Applications*, 9(10), 533.
- [3] Yuan, Y., & Wang, F. Y. (2016, November). *Towards blockchain-based intelligent transportation systems*. In *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)* (pp. 2663-2668). IEEE.
- [4] Warren, W., & Bandeali, A. (2017). *0x: An open protocol for decentralized exchange on the Ethereum blockchain*. URL: <https://github.com/0xProject/whitepaper>.

-
- [5] Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2017, October). Metrics for assessing blockchain-based healthcare decentralized apps. In *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)* (pp. 1-4). IEEE.
- [6] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, 42(7), 130.
- [7] Sreehari, P., Nandakishore, M., Krishna, G., Jacob, J., & Shibu, V. S. (2017, July). Smart will converting the legal testament into a smart contract. In *2017 International Conference on Networks & Advances in Computational Technologies (NetACT)* (pp. 203-207). IEEE.
- [8] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*.
- [9] Asharaf, S., & Adarsh, S. (Eds.). (2017). *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities: Emerging Research and Opportunities*. IGI Global.
- [10] Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain and shared economy applications. *Procedia computer science*, 98, 461-466.
- [11] Swan, M. (2015). *Blockchain: Blueprint for a new economy*.
- [12] "O'Reilly Media, Inc."
- [13] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). Fhircain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal*, 16, 267-278.
- [14] Rodrigues, B., Bocek, T., & Stiller, B. (2017). Enabling a cooperative, multi-domain DDoS defense by a blockchain signaling system (BloSS). In *Proceedings of the 42nd IEEE Conference on Local Computer Networks*.
- [15] Karamitsos, I., Papadaki, M., & Al Barghuthi, N. B. (2018). Design of the blockchain smart contract: A Use Case for Real Estate. *Journal of Information Security*, 9(03), 177.
- [16] Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In *Advances in Computers* (Vol. 111, pp. 1-41). Elsevier.
- [17] Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2017). Applying software patterns to address interoperability in blockchain-based healthcare apps. *arXiv preprint arXiv:1706.03700*.
- [18] Swan, M. (2016, July). Blockchain temporality: smart contract time specifiability with blocktime. In *International symposium on rules and rule markup languages for the semantic web* (pp. 184-196). Springer, Cham.
- [19] Bahga, A., & Madiseti, V. (2017). *Blockchain Applications: A Hands-On Approach*. VPT.
- [20] Yuan, Y., & Wang, F. Y. (2018). Blockchain and cryptocurrencies: Model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(9), 1421-1428.
- [21] Wohrer, M., & Zdun, U. (2018, March). Smart contracts: Security patterns in the ethereum ecosystem and solidity. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* (pp. 2-8). IEEE.
- [22] Swan, M. (2015, March). Blockchain thinking: The brain as a dac (decentralized autonomous organization). In *Texas Bitcoin Conference* (pp. 27-29). Chicago.
- [23] McCorry, P., Shahandashti, S. F., & Hao, F. (2017, April). A smart contract for boardroom voting with maximum voter privacy. In *International Conference on Financial Cryptography and Data Security* (pp. 357-375). Springer, Cham.
- [24] Voshmgir, S. (2016). *Blockchains, Smart Contracts und das Dezentrale Web*. Technologiestiftung Berlin, *Blockchains, Smart Contracts und das Dezentrale Web*, 17-35.
- [25] Swan, M. (2015). Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]. *IEEE Technology and Society Magazine*, 34(4), 41-52.
- [26] Walsh, C., O'Reilly, P., Gleasure, R., Feller, J., Li, S., & Cristoforo, J. (2016). New kid on the block: a strategic archetypes approach to understanding the Blockchain.
- [27] Dai, P., Mahi, N., Earls, J., & Norta, A. (2017). Smart- contract value-transfer protocols on a distributed mobile application platform. URL: <https://qtum.org/uploads/files/cf6d69348ca50dd985b60425ccf282f3.pdf>.
- [28] Bashir, I. (2017). *Mastering blockchain*. Packt Publishing Ltd.
- [29] Egbertsen, W., Hardeman, G., van den Hoven, M., van der Kolk, G., & van Rijsewijk, A. (2016). Replacing paper contracts with Ethereum smart contracts.
-

-
- [30] Kounelis, I., Steri, G., Giuliani, R., Geneiatakis, D., Neisse, R., & Nai-Fovino, I. (2017, July). *Fostering consumers' energy market through smart contracts*. In *2017 International Conference in Energy and Sustainability in Small Developing Economies (ES2DE)* (pp. 1-6). IEEE.
- [31] Filipova, N. (2018). *Blockchain—An Opportunity For Developing New Business Models*.
- [32] Sylim, P., Liu, F., Marcelo, A., & Fontelo, P. (2018). *Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention*. *JMIR research protocols*, 7(9).
- [33] Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017, October). *Towards using blockchain technology for eHealth data access management*. In *2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)* (pp. 1-4). IEEE.

Strategy to Countering Cyber Terrorism Activities Via Internet by Proposing Six- Ware Cyber Security Framework (SWCSF)

¹Tri Legionosuko, ²Rudy Ag. Gultom, ³Romie O. Bura, ⁴Deni Dar, ⁵Hipdizah, ⁶David H. Hutagaol

¹Indonesia Defense University (IDU), Indonesia

E-mail: ¹rektor@idu.ac.id, ²rudygultom@idu.ac.id, ³dekanftp@idu.ac.id,

⁴wadekftp@idu.ac.id, ⁵dekanfsp@idu.ac.id, ⁶davidhutagaol@idu.ac.id

ABSTRACT

Nowadays, the terrorist groups have taken advantages the use of Internet access to support their activities, i.e, member recruitment, propaganda, fundraising, cyber attack actions against their targets, etc. This is one of the issues of cyber security as a negative impact of internet utilization especially by the terrorist groups or so called cyber terrorism. They know the benefits of the internet services and social media can be used to facilitate the control of information in their organizational command and control system. In order to tackle this cyber security issue, the internet users should get more understanding as well as protection from their government against the danger of cyber terrorism, cyber radicalism or cyber extremism activities over the Internet. Therefore this paper tries to explain the need of a cyber security strategy to countering cyber terrorism activities via Internet by proposing the concept of Six-ware Cyber Security Framework (SWCSF).

Keywords - Cyber Security, Internet, Cyber Terrorism, Six-ware Cyber Security Framework.

I. INTRODUCTION

In the current era of information globalization, the strength, sovereignty and resilience of a country is not only measured by the magnitude of military or economic power it has, but also depends on many aspects of mastery, use and empowerment of the Cyberspace and Internet access. Nowadays, many countries are highly dependent on the utilization of the Cyberspace and the Internet especially in economic, business, academic, social, political, governmental, defense and security aspects. Through the utilization of constructive cyberspace, nations social relations can be organized directly in a relatively short period of time without space and time constraints, whether in peacetime, crisis or war. The cyberspace phenomenon illustrates the reality that activities in the modern society are interconnected throughout cyberspace. From the perspective of cyber security, the purpose of the use of internet might also be covering the misused for negative or destructive purposes by individuals with bad intention, non-state or/and state actors, including terrorist groups, in fact. As we may know, various facilities (tools) available on the Internet can be used to disrupt, damage, and paralyze critical infrastructure or to threaten the national interests of a country, even to influence radicalism ideology or extremism/ terrorism action, massively and continuously. In the midst of advances in information and communication technology today the various cyber threats or attacks conducted throughout the

cyberspace (Internet) is greatly organized by either a state actor or non-state actors to the national interest of one other country would have the potential to become a form of cyberattack is serious. Various cyber security challenges via cyberspace such as web defacing, cyber propaganda, cyber radicalism, cyber terrorism, cyber warfare, child pornography, black propaganda, character assassination, hate speech, hoax and so on cause many countries to then establish a National Cyber Agency with the single purpose to protect their national interests and resilience. Some of those institutions known are: US Cyber Command, China PLA Blue Army, Korea KISA, Israel Unit 8200 IDF or Indonesia BSSN (National Cyber Agency). In fact, the United States through the National Institute of Standards and Technology (NIST) has defined Cybersecurity as the ability to protect or defend the use of cyberspace from cyberattacks including Cyberterrorism action.

According to The National Conference of State Legislatures definition, “Cyberterrorism is the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terroristic threats made via electronic communication.”. NATO defines cyberterrorism as, “a cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal.”

In Indonesia, 19 May 2017, the President of Indonesia, Mr. Joko Widodo, has signed establishment of the National Cyber and Encryption Agency (BSSN) in charge of implementing national cyber security effectively and efficiently by utilizing, developing and consolidating all elements related to cyber security. The BSSN become the leading sector of the national cyberspace affairs through the issuance of Presidential Decree No. 53 of 2017. Structurally, the BSSN organization is directly under the president and become the leading sector in the National Cybersecurity endeavour.

As we may know that Indonesia is currently ranks 5 countries the largest Internet users in the world after China, India, the United States and Brazil with the number of Indonesian Internet users who reached 132.7 million users or about half of the population of Indonesia. Therefore, the utilization of internet access services by the people of Indonesia becomes an important and strategic issue.

II. UNDERSTANDING THE CHALLENGES OF GLOBAL INFORMATION SECURITY

To understand the cybersecurity challenges in the context of the global domain requires an understanding of the development of the global strategic environment. One country must be able to comprehend holistically that cyberspace as a borderless global domain, space-less and time-less that bring new challenges in the current era of globalization of information.

The un-conformed international understanding of the meaning of cyberspace and how to govern it will remain as obstacles, challenges and resistance when one country tries to make a unilateral claim that global cyberspace as part of their country's sovereignty. This is in contrast to the claims of the conventional sovereignty of a country which is governed by the international treaties, such as UNCLOS 1982 (United Nations Convention on Law of the Sea) whereas in UNCLOS 1982 it is clearly and assertively defined the right that a sovereign state and the responsibility of a sovereign state in the use and management of the oceans of the world in which it is entitled (ZEE/ Exclusive Economic Zone) and establishes guidelines for its business, environment and her natural reserves management. Sovereignty in cyberspace today are seen to be non-physical, borderless, stateless and timeless to all.

The terminology of border in cyberspace then explained by the Government of the United States of America through The United States Department of Defense (DoD) as:

“A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers”.

The US DoD then creates a definition derivative for cyberspace operations as “The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace”. When referring to the Tallin Manual document there is a more rigid definition of cyberspace operation, i.e.

“a cyber-operation, whether offensive or defensive, that is reasonably expected cause injury or death to persons or damage or destruction to objects”.

Indonesia, as part of the international community will also face the global challenges of international cybersecurity affairs, cyber security and codes encryption through the almost the same cyberspace it is. This challenge may have the implications as new forms of threat to the state security such as cyberattack, cybercrime, cyber prostitution, cyber propaganda, cyber terrorism to cyber warfare.

Currently more and more emerging cybercrime action conducted by international syndicate actors through Indonesian territory because the legal formality governing cybercrime activities and the capacity of the law enforcement in Indonesia is very limited let alone the public are not too aware with the understanding of Cybersecurity in general.

The properties and characteristics of the borderless, spaceless and timeless cyber spaces make cybercrime as a form of trans national crime or transnational crime. The development of cyber terrorist and cyber propaganda actions by the radical groups in some countries has turned out to utilize cyber space as an effective "media of struggle".

Some of their actions are carried out through cyber space such as member recruitment, control and coordination communication systems, collection of financial resources management, including hiring hackers/ crackers to cyber troops and creating their own cyber weapons.

This condition makes cyberspace as a global domain to become a national crucial issue that needs to be correctly identified, evaluated, anticipated in order to searched for a comprehensive, integral, holistic, effective and efficient solution. Terrorist's use of social media and the Internet to pursue their ideological aims is well documented. This includes terrorist groups such as Isis who are using the Internet and social media sites, as a tool for propaganda via websites, sharing information, data mining, fundraising, communication, and recruitment.

Therefore, a comprehensive understanding of the aspect of cyberspace as a global domain of the international community becomes important to be addressed correctly facing the increasingly complex and dynamic cybersecurity challenges to protect the integrity and sovereignty of the Republic of Indonesia.

III. CYBER SECURITY CASES

It cannot be denied that the digital technologies are great enablers, but they can be misused by actors to conduct criminal actions that may exploit nations, business and individuals. Critical infrastructures, such as government operations, storage and delivery systems, banking and financial markets, as well as military control and command are targets of such cyber security challenges. In the context of cybersecurity issues there are several examples of cyber security cases that have occurred in the world, i.e.:

- In 2014, The ISIS have been using both platforms as magnets that have attracted thousands of views, comments, forums and posts. For example, through the use of videos posted on YouTube,

it began its “one billion” campaign, which called upon Muslims to join ISIS. The videos attracted huge audiences and were accompanied with the words: “Proudly support the Muslim cause” (see Fig. 1).



Figure 1: YouTube videos of the ISIS's one billion campaign

- Furthermore, ISIS had released a free to download application (app) which kept users updated with the latest news from the organization. The application entitled: “The Dawn of Glad Tidings” (see Fig. 2) was promoted online and was available on the google android system, before it was detected and suspended. Most of the content was regulated by Isis’s social media arm. This app shows us how the use of cyber-terrorism and social media have converged in this virtual space for terrorist groups such as ISIS.



Figure 2: The ISIS social media application campaign

- April 2016 in Panama, there is a "leakage" via social media of 11.5 million classified documents (2.6 terabytes files) containing sensitive data from companies around 214,000 companies in a Panama well-known service company, Mossack Fonseca. The “leaked” important secret documents are emails (4,804,618 files), database (3,047,306 files), PDF (2,154,264 files), images (1,117,026 files), texts (320,166 files) and other formats (2242 files). Suspected "leak" of 11.5 million secret documents are done throughhacking by hackers or deliberately leaked / tapped by people in Mossack Fonseca itself.

- October 2016 in USA, The United States government "accused" the Russian of political hacking and wiretapping attacks related to the election of the President of the United States in 2016. According to the CIA Agency intelligence analysis concluded that the activities of Russian hackers who managed to tap the information and information system of the parties directly related to the electronic votes in the United States, although this has been denied by the Russian side. A valuable lesson to be learned from this case is the requirement for special attention to cyber security for the implementation of Presidential election or Regional Head election using the electronic system votes. The role of the coding system (cryptography) is crucial in this aspect to avoid tapping.
- In 2016, a British teenager who "terrorised" some of America's most senior intelligence officials (FBI and CIA senior officials) after tricking his way into their email and phone accounts has been sentenced to two years in youth detention.
- In May 2017, Wannacry Ransomware attack was a worldwide cyberattack by the WannaCry ransomware cryptoworm virus, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency (see Figure 3).

In Indonesia, two national level hospitals in Jakarta, RS. Harapan Kita and RS. Dharmais have been suffered from this fatal cyberattack that paralyzed some health information systems in both hospitals. It shows us that the impact of Ransomware cyberattacks is very harmful and dangerous. It can be imagined if such virus attacks our national critical infrastructure or the state defense system where the impact will be far greater and massive.



Figure 3: The Screenshot of a WannaCry ransomware attack on Windows 8

IV. CASE STUDY: THE NIST CYBER SECURITY FRAMEWORK

In February 2013, the US President issued an Executive Order (EO) 13636, in order to improving national critical infrastructure cybersecurity. The EO states: "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cybersecurity environment that encourages efficiency, innovation and economic prosperity while promoting safety, security, business confidence, privacy and civil liberties". The US President EO 13636 ordered NIST to work with stakeholders to develop a voluntary framework based upon existing standards, guidelines, and practices in order to reduce cyber risks to national critical infrastructure. The NIST 2014 framework (Version 1.0) consists of standards, guidelines, and practices to promote the protection of critical infrastructure. It is composed into five basic cyber security activities:

- Identify, to develop the organization's understanding to manage cyber security risk to systems, assets, data and capabilities.
- Protect, to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect, to develop and implement the appropriate activities to identify the occurrence of cybersecurity events.
- Respond (to develop and implement the appropriate activities to take action regarding a detected cybersecurity event).
- Recover (to develop and implement the appropriate activities to maintain the integrity of the security plan and maintain network resilience while restoring impaired ability or services because of cybersecurity attacks.

The five activities above are then divided into categories in order to determine a more specific security practices and capabilities, i.e. asset management, access control, etc. Categories are further divided into sub-categories to explain in more detail or technical controls needed to meet the goals of each category (see Table 1).

In 16 April 2018, NIST re-publishes the latest revision of its cyber security framework, Version 1.1, "Framework for Improving Critical Infrastructure Cybersecurity" (see Table 2). The newest version of NIST is the results of an ongoing collaborative effort involving industry, academia and government. This NIST version 1.1 was published to refine the previous NIST version 1.0 cybersecurity framework published in 2014. As we may know, the United States is very concern of the risk management for its national critical infrastructure especially from cyber security threats or cyberattacks that can be placing the Nation's security, economy and public safety and health risk

Functions	Categories	Sub-categories	Information References
Identify	<ul style="list-style-type: none"> Asset Management Governance 	<ul style="list-style-type: none"> Inventory devices, systems & software, etc. 	<ul style="list-style-type: none"> NIST 800-53 CM-8, CA-2, etc.
	<ul style="list-style-type: none"> Access Control, etc. 	<ul style="list-style-type: none"> Review access periodically 2 factor authentication 	<ul style="list-style-type: none"> ISO 27001 A6, A9, A11, A13, etc.
Detect	<ul style="list-style-type: none"> Detect & Monitor for anomalies & events 	<ul style="list-style-type: none"> Review logs for suspicious activity, etc. 	<ul style="list-style-type: none"> NIST 800-53 AU-6, CA-7, etc.
Respond	<ul style="list-style-type: none"> Mitigation of security events, etc. 	<ul style="list-style-type: none"> Report suspicious events, etc. 	<ul style="list-style-type: none"> ISO 27001 A6, A16, etc.
Recover	<ul style="list-style-type: none"> Recovery planning, improvements & communication 	<ul style="list-style-type: none"> Recovery plan Manage public relations Repair reputation 	<ul style="list-style-type: none"> NIST 800-53 CP-10, IR-4, IR-8, etc. ISO 27001 A16, etc.

Table 1: The NIST Cyber Security Framework (Ver. 1.0)

The Framework Core elements work together as follows:

- Functions organize basic cybersecurity activities at their highest level. These Functions are “Identify”, “Protect”, “Detect”, “Respond” and “Recover”.
- Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities, i.e. “Asset Management”, “Identity Management and Access Control”, and “Detection Processes”.
- Subcategories further divide a Category into specific outcomes of technical and/or management activities, i.e. “External information systems are catalogued”, “Data-at-rest is protected”, “Notifications from detection systems are investigated”.
- Informative References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory.

FRAMEWORK FUNCTIONS	IDENTIFY ID	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
PROTECT PR	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES	
DETECT DE	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES	
RESPOND RS	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES	
RECOVER RC	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES	

Table 2: The New NIST Cyber Security Framework (Ver. 1.1)The five Framework Core Functions are defined below:

- **Identify** - Develop an organizational understanding to manage cyber security risk to systems, people, assets, data and capabilities, i.e., “Asset Management”, “Business Environment”, “Governance”, “Risk Assessment”, and “Risk Management Strategy”.
- **Protect** - Develop and implement appropriate safeguards to ensure delivery of critical services, i.e., “Identity Management and Access Control”, “Awareness and Training”, “Data Security”, Information Protection Processes and Procedures”, “Maintenance” and “Protective Technology”.
- **Detect** - Develop and implement appropriate activities to identify the occurrence of a cybersecurity event, i.e., “Anomalies and Events”, “Security Continuous Monitoring”, and “Detection Processes”.
- **Respond** - Develop and implement appropriate activities to take action regarding a detected cybersecurity incident, i.e., “Response Planning”, “Communications”, and “Improvements”.
- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident, i.e., “Recovery”, “Planning”, “Improvements”, and “Communications”.

The Framework Core elements work together as follows:

- **Functions** - organize basic cybersecurity activities at their highest level. These Functions are “Identify”, “Protect”, “Detect”, “Respond” and “Recover”.
- **Categories** - are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities, i.e. “Asset Management”, “Identity Management and Access Control”, and “Detection Processes”.
- **Subcategories** - further divide a Category into specific outcomes of technical and/or management activities, i.e. “External information systems are catalogued”, “Data-at-rest is protected”, “Notifications from detection systems are investigated”.
- **Informative References** - are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory.

V. THE SIX-WARE CYBER SECURITY FRAMEWORK (THE SWCF) PROPOSAL

As mentioned above, this academic paper contributes an initial concept proposal of cyber security framework, so called, Six-Ware Cyber Security Framework (SWCSF) as the cyber security strategy to countering cyber terrorism activities over the Internet. The SWCSF proposal is a comprehensive concept for cyber security strategy and solution to enhance computer network security resilience from various threats, attacks and vulnerabilities as well as in countering cyber terrorism activities through the cyberspace. This is an operational-level cyber security strategy that enables to figure out the most efficient and effective actions that may lead to the success of cyber security operation.

The idea behind this new concept was inspired by NIST cyber security platform version 1.0., dated 12 February 2014. The SWCSF concept tries to elaborate NIST cyber security framework to be more practical for the operational level. The security framework discussion can be found also in mashup web data extraction system. The SWCSF concept contributes a common thought to understanding, managing, and expressing network security risks, both internally and externally. The SWCSF concept contributes increased security awareness environment within an organization where it requires internal/external risk assessment and also threat analysis policies. All levels employees in the organization, ranging from highest level to lowest level must be actively involved in the SWF concept implementation. Otherwise, they cannot obtain better understanding of how threats or attacks can be carried out successfully across the entire organization.

II. THE SWCSF ENABLERS

The SWCSF enablers provide a set of activities, which consists of six main variables, sub-variables, indicators and information references (e.g., reference guidance). The SWCSF enablers are not only a set of checklist of actions to perform, but it presents key network security solutions to manage security risk and analysis in an organization computer network. The SWCSF enablers comprises six main aspects, e.g., Brainware, Hardware, Software, Infrastructureware, Firmware, Budgetware (see Table 3).

Aspects	Variables	Sub-variables	Indicators	Information Security References
Brainware	<ul style="list-style-type: none"> CISO, etc. 	<ul style="list-style-type: none"> Security training, etc. 	<ul style="list-style-type: none"> Security Awareness 	<ul style="list-style-type: none"> CISSP, CISA, etc.
Hardware	<ul style="list-style-type: none"> Server Farms 	<ul style="list-style-type: none"> USB, etc. 	<ul style="list-style-type: none"> No compromises 	<ul style="list-style-type: none"> Benchmarking, etc.
Software	<ul style="list-style-type: none"> Application 	<ul style="list-style-type: none"> MS Office, etc. 	<ul style="list-style-type: none"> No pirated Application, etc. 	<ul style="list-style-type: none"> Regular updates, etc.
Infrastructureware	<ul style="list-style-type: none"> Network Infrastructure 	<ul style="list-style-type: none"> Firewalls IDS. DMZ, etc. 	<ul style="list-style-type: none"> No network security breaches, etc. 	<ul style="list-style-type: none"> Self penetration testing, etc.
Firmware	<ul style="list-style-type: none"> Security handbook 	<ul style="list-style-type: none"> Business Continuity Plan (BCP) 	<ul style="list-style-type: none"> Good Business processes 	<ul style="list-style-type: none"> NIST. ISO 27001, etc.
Budgetware	<ul style="list-style-type: none"> Sufficient budget 	<ul style="list-style-type: none"> Buy software licenses, etc. 	<ul style="list-style-type: none"> Licenses always updated, etc. 	<ul style="list-style-type: none"> Allocated budget policy, etc.

Table 3: The SWCSF Concept (Enablers and Components)

- Brainware or Human Factor, is the main aspect in network security environment. This variable becomes top list variable within the SWF concept. From network security perspective, it is commonly known that human is the weakest link in information security environment. Human factor plays a dominant role to enhance or, on the contrary, to disrupt all efforts of existing information security within an organization. Therefore, organizations must have a function or position related to information security, e.g., Chief Information Security Officer (CISO). The

CISO is a company's top executive who is responsible for security of personnel, physical assets, data and information in both physical and digital form. Its position has increased in the era of cyberspace where it becomes easier to steal sensitive company information. One of CISO's responsibilities is to conduct information security certification programs to all level employees. The intention is to produce "information security awareness employees" related to their position and function.

- Hardware, plays dominant role in handling threats, attacks and vulnerabilities. CISO has to teach all level employees how to use and treat organization's hardware devices safely and wisely. It is because a high-level hacker is not just relying on a specific technique, but still combined with the conventional attack, e.g., social engineering attack. Combination of internal risk assessment and threat analysis are extremely needed, e.g., controlling individual access into the organization's premises or facilities, locking systems and removing unnecessary CD-ROM or USB thumb drives, or monitoring and protecting the security perimeter of organization's facilities, etc.
- Software, relates to utilization of software applications security which are used daily in the office, e.g., email, website, social media and other applications. High security awareness is required because a high profile attacker will always kept on trying to infect or inject malicious emails on its attachments or invite to visit malware-infected websites. Hackers are also constantly introducing new threats although various cyber security application tools are available in the market.
- Infrastructure ware, has an important role in facilitating secure organization network infrastructure, e.g., monitoring network from threats, attacks and vulnerabilities. Nowadays, most of organizations have been highly dependent on Internet access. On the other hand, not all of employees have a good level understanding about security risks they might face in the office, where this condition is making the organization's network infrastructure more vulnerable.
- Firmware, includes documentation of an organization security strategy and policy, standard operating procedures (SOPs), business continuity plans (BCPs), network security frameworks or International Organization for Standardization (ISO), i.e. ISO 27001:2013, etc., NIST cyber security framework version 1.0, government security policy and strategy, etc.
- Budgetware, plays important and strategic role in facilitating implementation of the five-ware variables above. It is because an organization is urged to provide big enough money or sufficient budget to purchase e.g., network security application tools, patching systems, software licenses, training and education, certification programs, etc. It is highly recommended top level management must put this matter as a high level priority in order to build information security awareness. Allocating sufficient information security budget could protect the entire network system. Otherwise, they will face organization's significant financial losses, etc.

VII. THE SWCSFCOMPONENTS

The SWCSF components work together as follows:

- Variables, organize network security fundamental aspects as enablers, e.g., brainware, hardware, software, infrastructureware, firmware and budgetware) at highest level. These variables help an organization in managing its security risk and analysis by organizing or clustering data or information, threats and attacks activity. Variables align with security and policy framework to reduced impact to organization quality of services e.g., investments in human resources, planning budgeting exercises or recovery actions, etc.
- Sub-variables, are sub-divisions of a variable closely tied to a particular (for example, brainware variable) security awareness activities e.g., “security awareness”, “socialization and training”, “cyber security certification program”, etc.
- Indicators, are sub-divisions of a sub-variable, divided into technical outcomes. Indicators provide a set of results to achieve outcomes for each sub-variable. Indicators example (like security awareness sub-variable) e.g., “conducting security awareness training program”; “socializing and implementing security awareness culture in the company”; or “notifications from any social engineering attacks or security breaches that are being investigated”, etc.
- Information References (IR), consists of network security standards, guidelines, methods and practices to achieve solutions or outcomes associated with each indicator. IR which presented in the SWF concept are illustrative and not complete, yet. For example, conducting security awareness training program indicator: “certified ethical hacking (CEH) course from EC-council”; “DoD information assurance awareness training”; and “Achieving ISO 27001 Certification”; etc.

The SWCSF component provides a set of activities to achieve specific network security outcomes, and references examples of guidance to achieve those outcomes. The SWCSF component is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by organization as helpful in managing the risk within organization network security environment.

VIII. CONCLUSION

The Internet users in all countries must aware and prepare of the cyber security issues as a negative impact of internet utilization by the terrorism groups, because they know the benefits of the internet services and social media can be used to facilitate the control of information in their organizational command and control system. To countering cyber extremism activities via internet within the region, countries need to cooperate in the use of cyber space. Countries should establish efforts to increase security measures with collaborative efforts in cyber security by including collaborative usage of

critical information infrastructure, conduct of cyber security exercises, collaborative usage of information resource, control of information network infrastructure, control of information flow and conduct of collaborative cyber space defense. The Internet users in all countries need to have a national cyber security framework standard such as Six Ware Cyber Security Framework (SWCSF). At this moment, the SWCSF is just an initial proposal or concept to enhance cyber security environment. In the future, the SWCSF needs to be developed and implemented more in-depth through further research.

REFERENCES

- [1] *Establishing BSSN –Indonesia National Cyber Agency*, https://id.wikipedia.org/wiki/Badan_Siber_dan_Sandi_Negara, last accessed December 19th 2019.
- [2] Chen, J., and Duvall, G., “On Operational-Level Cybersecurity Strategy Formation,” *Journal of Information Warfare: 13.3:* 79-87. SSN 1445-3312 print/ISSN 1445-3347 online, 2014, last accessed January 24th 2019.
- [3] Colonel Dr. Rudy AgusGemilang Gultom, “Cyber Intelligence Overview”, *Materials of Cyber Security Policy & Practice Course, The Naval Postgraduate School (NPS), Monterey, California, USA, May 2015.*, last accessed February 4th 2019.
- [4] Internet, Dr. Conway, M., “What is cyberterrorism? The story so far”, *Journal of Information Warfare*, 2(2), 33–42., 2003, last accessed January 21st 2019.
- [5] Internet sources, “Cyber Attacks: Technique, Tools, Motivation & Impact”, last accessed January 28th 2019.
- [6] Internet, “The Famous Cyber Attacks/Cyber Warfare in the World”, accessed January 16th 2019.
- [7] Internet, Irshaid, F., “How ISIS is spreading its message online”, *BBC news*, Accessed 22 Dec 2014. Available at: <http://www.bbc.co.uk/news/world-middle-east-27912569>”, *Journal of Information Warfare*, 2(2), 33–42., 2003, last accessed February 2nd 2019.
- [8] Internet, Sueddeutsche, “Panama Papers (the Secrets of Dirty Money)”, <http://panamapapers.sueddeutsche.de/articles/56febff0a1bb8d3c3495adf4/>, last accessed January 24th 2019.
- [9] Internet, Independent, “Vladimir Putin says Russians accused of hacking US election ‘do not represent’ the country)”, <https://www.independent.co.uk/news/world/americas/us-politics/vladimir-putin-internet-research-agency-troll-farm-robert-mueller-indictment-13-russians-a8239386.html>, last accessed January 25th 2019.
- [10] Internet, Independent, “British teenager who ‘cyber- terrorized’ US intelligence officials gets two years detention”, <https://www.independent.co.uk/news/uk/british-teen-hacker-kane-gamble-us-intelligence-officials-jailed-cia-fbi-a8315126.html>, last accessed February 4th 2019.
- [11] Internet, The US White House, Executive Order, “Improving Critical Infrastructure Cybersecurity”, 12 February 2013, <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>, last accessed February 14th 2019.
- [12] Internet, The NIST, Version 1.1, “Framework for Improving Critical Infrastructure Cybersecurity”, 16 April 2018, https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without_markup.pdf, last accessed January 19th 2019.
- [13] Internet, Wikipedia, The National Conference of State Legislatures, “Cyberterrorism”, <https://en.wikipedia.org/wiki/Cyberterrorism>, last accessed January 19th 2019.
- [14] Internet, Wikipedia, NATO, “Cyberterrorism”, <https://en.wikipedia.org/wiki/Cyberterrorism>, last accessed February 9th 2019.
- [15] President Obama’s International Strategy for Cyberspace, “Prosperity, Security, and Openness in a Networked World”, May 2011, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, last accessed January 22nd 2019.

An Integrated Maritime Cyber Security Policy Proposal

¹**Stergios Oikonomou**, ²**Ioannis Filippopoulos**, ³**Alexandros Voliotis**

^{1,3}Dept. of Biochemistry and Biotechnology, University of Thessaly, Volos, Greece,

²Department of Computer Science, University of Thessaly, Lamia, Greece & Department of Informatics and Engineering, Hellenic American University, 436 Amherst Street, Nashua, New Hampshire 03063, USA

E-mail: ¹stergios.oikonomou@gmail.com, ²yf@outlook.com.gr, ³abwasp2000@yahoo.gr

ABSTRACT

The security environment of the twenty-first century has changed. There is no 100% security. The maritime industry as a part of the cyber domain is a very competitive and complex industry. Increasingly dependent on complex critical communication and information systems make this industry one of the most susceptible to cybersecurity attacks. Cyber threats and cyber-attacks are becoming more frequent and more sophisticated every day. As these attacks have been happening more frequently with serious consequences, cybersecurity has become a primary focus for the maritime industry. The cyber threats cannot be eliminated completely, but the risk can be greatly reduced to a level that allows maritime community to continue to prosper, and benefit from the huge opportunities that digital technology brings. Therefore, appropriate Cyber Defense measures and capabilities have to be in place to face and counter the threats from cyberspace. This will require having effective tools, a well-trained workforce and proper processes in place to detect, analyze, counter, and mitigate cyber threats and vulnerabilities. To help understand the risks, this paper attempts to analyze the common cyber threats, the possible actors behind a cyber-attack as well as its anatomy. Furthermore, there is a report about the vulnerabilities in ship systems but the main purpose of this paper is to propose a cyber-security policy and its components for the maritime sector.

Keywords - Maritime, Cyber Defense Policy, Cyber Attacks, Vessels, Information Security, Cyber Security Policy, Cyber Attack, Integrity, Confidentiality, Availability.

I. CYBER SECURITY

A. What is cyber security?

One of the most appropriate short definition as given by Techtargget.com is: «Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access». In an organization, people, processes, and technology must all complement one another to create an effective defense from cyber-attacks. People can be the weakest link or the strongest defence in an organization. As more than 80% of all reported information security and cyber incidents at sea are related to human error, the human element is one of the biggest vulnerabilities of the industry and must be a core part of the solution. Processes are crucial in defining how the organization's activities, roles and documentation are used to mitigate the risks to the

organization's information and last IT systems can be deployed to prevent or reduce the impact of cyber risks. Last but not least, cyber security is everybody's responsibility.

B. The Importance of Cyber Security in Maritime The global shipping industry is undergoing a technological revolution. Crews becoming smaller, ships becoming larger, and a growing reliance on automation all significantly worsen the risks from hackers. Modern maritime ships are often monitored and controlled remotely from shore-based facilities thousands of miles away to ensure efficiency. There are many different classes of vessels which tend to have different computer systems built into them. Many of those systems are designed to last more than three decades. Placed in another context, many ships operate outdated and unsupported operating systems. All this creates a new platform for hackers to conduct targeted cyber-attacks. Why to hack shipping companies? What are the motivations? A few may be:

- stealing money;
- stealing information;
- causing disruption or loss.

About stealing money: An attacker could trick a company to transfer money directly to him using the method "man-in-the-middle" through which the attacker establishes communication with the victims who think that they exchange messages between them, when in fact the entire conversation is controlled by the attacker and direct the companies' monies directly to him. Another way is by using ransomware (described in more details at subparagraph III.B.2), where the victim's computer or database is encrypted by the attackers. The victim then has to pay a ransom in order to get the key to decrypt data. According to a report published by the United Nations Office on Drugs and Crime, the World Bank and Interpol, «pirates of Somalia managed to claim some 3-400 million USD in ransom from 2005 to 2012. Out of 179 hijacked vessels in this period, ransom was paid for 152 vessels». **Stealing information:** In shipping there is a large number and many different types of information with a great deal of value.

For example an attacker can steal information about shipping containers and the type of their content and the route they will follow. Such information may be sold to a competitive company or for investment purposes.

If we speak about the motivation causing disruption or loss we refer to the target to make systems and resources unavailable. Such attacks may be: cyber- attacks on port systems that may cause ports' shutdown, violation or even deletion of data that are used in a cargo terminal and may lead to terminal suspension until all the data restored.

II. CYBER THREATS

A Cyber Threat is any unauthorized attempt to gain access in a computer network. Nowadays there are many different kinds of cyber threats and the most important of these are presented below. Common Cyber threats are Phishing and Spear Phishing, Malware, Denial of Service (Dos), Inside Threat, Advance Persistent Threat (APT), Password Attacks.

III. CYBER ATTACK

A. Actors behind a cyber-attack

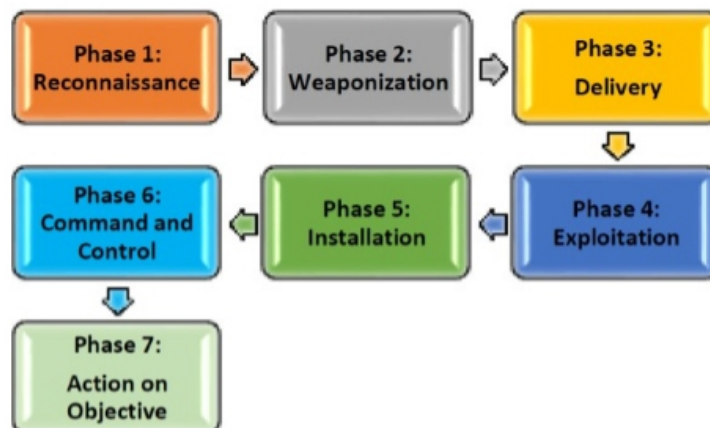
There are various kinds of actors who are conducting cyber operations directly or indirectly against the maritime organizations, such operations can cause disruptive effect on the functioning of these organizations.



Picture 1: Cyber-attack actors

- 1) Espionage
- 2) Hacktivism
- 3) Criminal
- 4) Terrorism
- 5) Business competitors

B. Anatomy of a cyber-attack



Picture 2: Cyber-attack phases

1) Phase 1: Reconnaissance

Cyber attackers first identify the target, the vulnerabilities included, the best ways to exploit them in order to launch a cyber-attack. They only need a single point of entrance to get started, as anyone in an organization would suffice as a target.

2) Phase 2: Weaponization

The information that any cyber attacker gathers is used in order to change something that he discovered causing a favorable result for him.

3) Phase 3: Delivery

Following weaponization phase, it's time for the attackers to start their attack.

4) Phase 4: Exploitation

During the exploitation phase, the attacker takes advantage of discovered vulnerabilities.

5) Phase 5: Installation

Once the attacker gains access to the organization's network, he must ensure that he will continue to have that access as long he wishes.

6) Phase 6: Command and control

In this phase the attacker has unlimited access to the network. He can move deeper into the network. He can exfiltrate data, conduct DoS operations and anything malicious that he wants.

7) Phase 7: Action on objective

This is when the attacker comes to his real objectives and goes on to act on them. The objective could be anything such as stealing data, messing around with the operations of the company, cause mischief with the order-taking system and get things shipped to customers based on fake orders, shut down equipment, disable alarms etc.

C. Vulnerabilities in Ship Systems

Till recently, there was a belief that distance and isolation of vessels was a security barrier against cyber-attacks. However, this is wrong. Ships nowadays are using more and more onboard Information Technology (IT) and Operational Technology (OT) systems which are interconnected and connected to the internet. This interconnectivity increases the risk of exposure to internet-based and insider cyber-threats. There should always be a distinction between IT and OT systems. IT is an often-used and fitting

term to describe business enterprise systems that move necessary data in order to support business-level operations including software, hardware and communication technologies. OT is a domain complementary to IT that consists of hardware and software components and systems that directly monitors/controls physical devices and processes. Both IT and OT might be vulnerable to cyber threats. At maritime industry there are a number of onboard systems which may be exposed to cyber risks. Vessels do not need to be attacked directly because an attack can happen via the company's shore-based IT systems and very easily penetrate the ship's critical OT systems. Maritime companies should make sure that they understand how shipboard systems might be connected to uncontrolled networks.

IV. CYBER POLICY

A. Scope

Cyber Security Policy serves a lot of purposes. The main purpose for a well-thought-out policy is to describe all the procedures to be followed in order to guard all the critical assets, equipment and data against cyber-attacks. Furthermore, policy describes the user's roles, responsibilities and privileges. What is considered acceptable use? What are the security rules to be applied? The policy answers these questions and describes the user limitations. It contains procedures for responding to incidents that threaten the security of the company computer systems and network. Ideally, a cyber security policy should be documented, reviewed, and maintained on a regular basis.

B. Cyber Security Policy Contents

1) Roles and Responsibilities

a) Security Operation Centre (SOC)

A Security Operation Centre (SOC) is a centralized facility with a dedicated security team inside, that has to exist in every maritime organization, in order to monitor, analyze and assess its network and IT-services against cyber threats. The required capabilities for SOC are: security monitoring, vulnerability analysis and pretesting, configuration test and security templates application, security inspection and risk analysis, malware, forensic analysis, audit and source code security support, conducting mitigation and counter-measures, incident management and coordination, systems and networks security assessment and Intruder detection. A SOC should be also able to organize Incident Handling Teams capable to react to incidents or attacks.

b) **Company Cyber Security Officer (CCySO)** Every company should designate a Company Cyber Security Officer. A person designated as the CCySO may act as the supervisor of the Incident Handling Team. The CCySO is shore-based personnel and should have knowledge, in some or all, of the following:

- Networks and operating system;
- System evaluations;
- System security penetration testing;
- Security operations/network monitoring;
- Security information and event management;
- Network mapping;
- Configuration of firewalls, routers and other security tools;
- Encryption systems;

The duties and responsibilities of the CCySO should also include, but not limited to:

- Analyze existing and future systems across the company, review security architectures, and develop solutions that integrate information security requirements to proactively protect information;
- Incident handling capability by monitoring, analyzing and responding to incidents;
- Conduct forensic analysis and review and assessment of security events and logs via sophisticated cyber security/event management tools;
- Conduct security risk assessments, and make recommendations of countermeasures to address risks, vulnerabilities and threats;
- Review and validate security documentation;
- Order the activation of the Contingency Plan and select the appropriate recovery strategy;
- Determine who should be notified if a cyber incident occurs.

c) Ship Cyber Security Officer (SCySO)

The SCySO is responsible for all security aspects of cyberenabled systems on the ship, i.e. both the IT, OT and communications systems. The SCySO should have knowledge of, in some or all of the following:

- How to inspect ship security measures;
- Emergency procedures contingency plan and other security plans;
- Proper management of security and communication sensitive information;
- Current cyber security threats;
- Recognition and detection of dangerous devices;

-
- Different types of techniques that are likely to be used to bypass security measures;
 - The layout of the ship installed equipment;
 - Monitor reports on incidents;
 - Secure communications;
 - How to recognize persons who are likely to threaten security.

The SCySO should also be responsible for:

- Ensuring that security measures are implemented, maintained and that all security incidents reported to the CCySO;
- Implementing and supporting network defense, access control, data protection and data transfer mechanisms;
- Taking backups from the system and implementation of the recovery plan;
- Training shipboard personnel and increase security awareness;
- Ensuring that ship security equipment is properly operated, tested, calibrated and maintained.

d) Ship Security Officer (SSO)

The SSO (master and ship duty officers with specific security duties) is responsible to ensure ship security. The SSO should have knowledge of:

- Facility security measures and operations from ships and ports;
- Undertaking regular security inspections of the ship;
- Backup plans in cooperation with SCySO;
- Ways to control and manage the crew ;
- Techniques used to circumvent security measures;

The SSO should also be responsible for:

- Reporting all security incidents to the SCySO;
- Ensuring that all shipboard personnel has the required security training and awareness;
- Conducting security inspections with SCySO at regular intervals;

e) Shipboard Personnel

Shipboard personnel should have sufficient knowledge and ability to:

- Recognizes characteristics and behavioral patterns of persons who are likely to threaten security;
- Uses communications with safety;
- Applies emergency procedures and contingency plans;
- Search (physical) persons, baggage, cargo, and ship's stores.

Finally, it should be noted that all crew members regardless of position and responsibility should be constantly vigilant.

2) Procedures

a) Physical Security and Access Control

Every ship should have specific security areas and security measures to control access. Efforts to control electronic and physical access of information systems are essential to ensure that sensitive data is retrieved or altered for legitimate and approved purposes only, otherwise the malicious actors could steal or alter important information, take control of the ship or damage critical systems. Physical access of spaces containing IT/OT assets must be controlled by physical barriers and devices (doors, locks) with security cameras (CCTV) and only accessed by authorized personnel. Access Control Lists (ACLs) for physical possession or contact with system assets (devices, systems, workstations, servers, network connections, etc.) must be kept up to date. Each employee must have a unique user credential. Disable automatic saving passwords for all applications. Define clearly all the equipment which requires remote access and disable remote management for simple users.

b) Identification and Authentication

USER LOGON IDS

Every user shall have unique logon id and password. An access control system should identify each user and prevent unauthorized users from entering or using information resources. Users shall be responsible for the proper use or misuse of their logon ID. All user login IDs must be audited at least twice yearly and should be removed when they are no longer in use. Logon IDs should also not be passed on from one user to another. Users who desire to obtain access to workstations or networks must have a completed and signed a Network Access Form. This form must be signed by the SCySO or department head of each user requesting access.

PASSWORDS

Passwords are required to gain access to networks and workstations. Every user should select a unique password to obtain access to any electronic information both at the server and/or the workstation level. Passwords must be locked after a maximum of three (3) unsuccessful logon attempts and SCySO should be the only responsible person to reset passwords. When passwords are reset, the system must automatically ask for it to be changed.

All passwords must comply with the following restrictions in be difficult to guess and intercept them:

- Must be at least eight characters long;
- Must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.
- Must be changed every 90 days. Compromised passwords shall be changed immediately.
- The previous five passwords cannot be reused.
- Shall not be shared, or written down on paper, or stored within a file or database on a workstation, and must be kept confidential.

CONFIDENTIALITY AGREEMENT

Users of information resources shall sign, as a prerequisite for employment, an appropriate confidentiality agreement via which they will declare that they «understand that any unauthorized use or disclosure of information residing on the information resource systems may result in disciplinary action, consistent to the policies and procedures of federal, state, and local agencies». All the temporary staff and third-party staff not already covered by a confidentiality agreement shall sign such a document before accessing into information resource systems.

c) Network Security

Network security is crucial for a ship. There must be measures to secure the networks of a ship like the following:

- Unused ports from all network devices should be closed;
- Servers and other equipment containing sensitive data must be maintained in a secure location;
- Several types of perimeter security appliances like firewalls, IDS/IPS systems, must be used with secure configurations on them and changing all the default passwords;
- Access to network areas can be restricted by isolating them or by implementing firewalls, smart switches and routers;

d) Satellite and Radio Communication Systems The most secure network is self-contained, with no access to the outside world, but this is not possible for most maritime transportation organizations. Communications with multiple organizations including port administrations, ships, marine facilities, trucking companies as well as within organizations is necessary. The satellite link provider is responsible for providing a secure satellite connection and, in cooperation with the shipping company, will have to decide on the measures taken to ensure that it is safe. It must prevent illegitimate connections gaining access to the onboard systems. It must use interfaces with security control software provided from the communication equipment. If using a VPN, the data traffic

Ensure that available Wi-Fi signals do not permit access to sensitive data or functions. At last, in front of the servers and computers connected to the network there should be deployed a firewall.

e) Printers and External Devices

Transferring data from uncontrolled to controlled systems is a major risk. Nowadays the use of removable media with malicious content, is perhaps the main way to gain illegal access to networks and devices. Companies must ensure that external devices are not used to transfer information between uncontrolled and controlled systems. The best is to prevent all employees to use their own devices. If so authorized, the external devices should be password-protected and encrypted. All external devices must to be scanned in a computer that is not connected to the ship's controlled networks. SCySO should perform periodic scans of the system and should do real-time scans of files derived from external sources as files are downloaded, opened, or executed. If it is not possible to scan the removable media on board, then the scan could be done prior to boarding.

f) Social Media and Internet Usage

Nowadays the use of social media is very popular and becoming an integral part of business. Companies use social media as means to advertise and keep in touch with clients. Personal use of social media in the workplace must be permitted, subject to certain conditions, as follows:

- It must not be overused but must be minimal and take place substantially outside of normal working hours and the company should withdraw the use permission at any time;
- Do not post material in breach of company copyrights;
- Employees must never disclose commercially sensitive or confidential information because social media activity of the employees in the target company will be monitored to extract information about the systems and any technology vulnerabilities assessed;
- Employees should avoid social media communications that might be misconstrued in a way that could damage the business reputation, even indirectly;
- Employees online profiles must not contain the company name;
- If employees see social media content that disparages or reflects poorly on company, they should contact SCySO immediately;
- Be aware though that even if you make it clear that your views on some topics do not represent those of the organization, comments could still damage the company's reputation;
- All users personally are responsible for what they communicate on social media sites outside the workplace, for example at home, using their own equipment. Users must always be mindful of contributions and what they disclose about the company;

Limited personal use of the internet or email at work is acceptable if it doesn't interfere with users' normal duties. Such use should take place substantially outside of normal working hours, for example, breaks, lunchtime. Users can access nonbusiness related sites, but are personally responsible for what they view. They must not use company's equipment to access the internet either from within or from outside the company network and they may not upload, download, use, any images, text, or software which:

- Are not permitted from the SCySO through the «whitelist»;
- Make employees not to work productively (like games);
- Encourage or promote activities which would, if conducted, be illegal or unlawful;
- Involve activities outside the scope of user's responsibilities - for example, unauthorized selling/advertising of goods and services;
- Might affect or have the potential to affect the performance of, damage or overload the system, network and/or external communications in any way;
- Might be defamatory or adversely impact on the image of company.

Additionally, users must not include anything in an email which they cannot or are not prepared to account for. Care should be taken when adding attachments to emails. It is better not to use attachments, but if this is necessary, no attachment should exceed 20Mb in size. The auto-forwarding facility within the company's email system should not be used to forward work emails to private accounts (e.g. Gmail or Yahoo). Large files should be compressed. Users must not download through their email, any software, executable files or image files (GIFs and JPGs) unless they have obtained prior permission from SCySO.

g) Monitoring of Log Files and Alerts

If a maritime company wants to identify early and successfully address cyber-attacks, must have a good log files monitoring policy. Reviewing security reports, log files and alerts is a specialized ability which require a cyber security analyst in order to be most effective. Companies must create and implement a log retention policy that specifies how long log data should be maintained. This will be extremely helpful for the analysis, because older log entries may show reconnaissance activity or previous instances of similar attacks because incidents may not be discovered until days, weeks, or even months later. Every hardware system in the company's network generates some type of log file. All the systems using either Microsoft or Unix software produce logs. Event Log Management is a key component of compliance initiatives, since it can be monitored, audited, and reported on file access, unauthorized activity by users, and policy changes. The best options is to place an IDS or IPS sensor behind the firewall, to monitor and filter traffic between the internet and the internal network and alert SCySO for any cyber incident.

h) Antivirus Updates and Software Patches

Many maritime organizations don't apply patches often and timely, to fix vulnerabilities and protect their systems. Patching is one of the most important steps that a maritime organization can take to reduce exploitations from cyber threats in software and computer-based systems.

First, companies should only use authorized software on their systems. For this purpose, it's better for the company to have a list (whitelist) with all the software which is permitted to be used. Then, it is important for antivirus updates and software patches to be distributed to ships on a timely basis. In each software, application or operating system, there are potential vulnerabilities which could be exploited by malicious cyber actors. Patching is the process of adding software code to eliminate a vulnerability and ensure the integrity of data residing on an IT/OT system. However, patch management can be a tough process. Vulnerabilities and fixes must be identified, analyzed, and tested before patches can be deployed and implemented. A tool that scans automatically all the systems for vulnerabilities is essential. Assigning a person to be responsible for the updates and reporting completion to the CCySO. Functional systems which are essential for the operation of the vessel may be updated on company's ashore facilities.

i) Intrusion Detection and Response

Having (and practicing) an incident response plan is probably one of the most crucial steps that any company must take. Every company should have systems like IDSs in place, to detect intrusions and respond to them. A clear and concise plan of action will help neutralize any intrusion into a network and mitigate potential damage. This plan should be tested continuously with exercises, examining its effectiveness in dealing with the cyber incidents. The incident response and the damages assessment should be also considered.

j) User Awareness and Training

Continuous training and awareness of both crew members and simple workers of a shipping company are essential elements to mitigate and effectively address cyber risks. Training should be tailored for all the staff, onboard and onshore, according to each one's duties. SCySO is responsible for training the shipboard personnel and increasing their security awareness and SSO must ensure that every one of them has the required security training and cyber awareness. Continuous exercises should be carried out to simulate possible incidents and their outcomes must to be considered for future exercises, but also to all participants, in order to see how their actions could affect the ship or the entire company. Finally, all crew members in accordance to the cyber security policy should at least be aware of:

-
- How to use the secure personal and other external devices (removable media, etc.) before connecting them to vessel's systems;
 - The risks related to emails and how to utilize email in a safe manner;
 - How to use social media and internet with safety;
 - How to install and maintain software on vessel hardware with safety;
 - How to safeguard user information, passwords, etc.;
 - Recognize cyber risks in relation to the physical presence of non-authorized personnel;
 - How to detect suspicious activity and how to report a possible cyber incident;
 - The consequences of cyber-attacks on the safety of the vessel;

k) Recovery

Taking steps to put backups in place, allows the organization to continue its operations despite a successful cyber-attack. The frequency of backups depends on the frequency that new data was introduced and how critical these are. SCySO should take backups regularly, using different storage media and he is responsible to do periodic recovery tests from backup site. External media such as dedicated external drives, recordableCD or DVD, should be available to the crew for data backup. Ensure that hardware is up-to-date and capable of recovering data. Since the portable backup drive can potentially contain sensitive information it should be protected by encryption and kept in designated secure locked location. Recovery plan should be implemented from the SCySO. Another good practice is to store backed- up data offsite. In this case, data is backed up at the company's facility and then labeled, packed, and transported to the storage facility. If the data is required for recovery or testing purposes, the company contacts the storage facility requesting specific data to be transported to the organization or to an alternate facility.

3) Cyber Security Risk Assessment

Risk assessment is the process which collects information and assigns values to risks for informing priorities, defining the needs for critical system protection, and developing courses of action. It doesn't provide permanent information and it needs to be updated on a regular basis.

Risk assessment includes the following:

- Mapping all the system assets (hardware, connections) that are at risk. This can be done for example with an automated discovery tool;
- Identification of the cyber threats in the systems. As mentioned above, these threats could be malware, phishing, spear phishing, social engineering, DoS, inside threats, APTs, or actors like espionage, hacktivists, criminals, terrorists, business competitors etc.

-
- Identification of the vulnerabilities in the systems. Here are mentioned specific vulnerabilities that exist and could compromise the IT and OT equipment and ship network;
 - Analyze the impacts of the vulnerabilities. The analysis of the impacts resulting from each vulnerability determines to which degree the security state of the system affects;
 - Determination of the risks. Here assesses the level of risks to the system associated with vulnerabilities mentioned above;
 - Documentation. Any findings should be documented for further and future use.

4) Cyber Security Contingency Plan

What is Cyber Contingency Plan?

A cyber security contingency plan helps a maritime company to respond effectively to cyber incidents. Contingency planning is a necessary component for the business continuity and disaster recovery. It should be based on a cyber security policy that describes the actions and the steps to be taken when a cyber incident has occurred or is likely to occur.

According to the NIST Special Publication 800-34, there are some steps for a cyber security contingency plan:

- Develop the cyber security contingency planning policy statement;
- Conduct the business impact analysis (BIA);
- Identify preventive controls;
- Develop recovery strategies;
- Develop a contingency plan;
- Testing, training and exercises;
- Plan maintenance.

b) Develop the Cyber Security Contingency Planning Policy Statement

Cyber Security Contingency Policy Statement should give all necessary elements to achieve the policy purpose and should assign specific responsibilities to specific staff. For a maritime organization, the contingency policy should be developed not only for the ships but also for offshore installations and should evaluate the IT/OT equipment and systems, mention the kinds of disasters, operations of the systems, staff training requirements and estimated time to restore the IT/OT systems. The basic elements of the policy should be known to all employees onboard and onshore, according to each one's duties. The responsible person to start the activation of the Contingency Plan is the CCySO.

c) Conduct the Business Impact Analysis (BIA) BIA is the process by which a maritime organization collects information and identifies the critical components about its system, as well as the threats that the system may face, the risks that these threats can cause and how they can affect the organization. According to the NIST Special Publication 800- 34 the BIA has the following phases:

- **Identify Critical IT Resources.**

In this phase, CCySO finds all the critical system components, identifies the required resources to operate them, and finds all the persons that use the system network in any way

- **Identify Disruption Impacts and Allowable Outage Times**

In this phase, CCySO analyzes the previous critical resources and determines the impacts on IT operations if a given resource is disrupted or damaged. Allowable outage times indicates the maximum time that an IT system can be unavailable before it causes a significant impact on the system.

- **Develop Recovery Priorities**

The impact and allowable outage times from the previous step enables the CCySO to develop recovery priorities that will be implemented during cyber contingency plan activation that will allow the maritime organization to determine the order that systems should be restored or recovered.

d) Identify Preventive Controls

Armed with the results of the BIA, a maritime organization can begin to take preventive measures to reduce the effects of system disruptions, increase system availability and to reduce contingency life cycle costs. Some common measures are firewalls, UPS, antivirus software, frequent backups, offsite storage of backup media, least-privilege access controls etc.

e) Develop Recovery Strategies

Recovery strategies help the organization to recover from an incident. The strategies should always prioritize critical functions, address the impacts identified in the BIA, take into account factors like allowable outage time and security. Furthermore, these strategies should include a combination of methods as mentioned in subparagraph V.B.2.k.

f) Develop a Contingency Plan

The development of the contingency plan is the main phase in implementing a comprehensive contingency planning program. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.

Contains detailed roles, responsibilities, teams, and procedures and includes technical information designed to support contingency operations that are tailored to the organization, information system, and its requirements. There are three phases that govern actions to be taken following a system disruption:

- Activation/Notification Phase describes the process of activating the plan based on outage impacts and notifying recovery personnel
- Recovery Phase details a suggested course of action for responsible staff to restore system operations at an alternate site or using contingency capabilities
- Reconstitution Phase includes activities to test and validate system capability and functionality and outlines actions that can be taken to return the system to normal operating condition and prepare the system against future outages

g) Testing, Training and Exercises

Contingency plan can be very complex. Testing this plan is necessary if the maritime organization wants to be sure that it is effective. Organizations need to take many decisions such as who does what and where, and what to do if it doesn't work. No one ever wants to find out that the plan was poor during a crisis. Each contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The company should conduct training classes and exercises to ensure that the plan is effective.

Test results and lessons learned should be documented and reviewed by test participants and other personnel as appropriate. Important players should understand what their role is. Simulating a cyber disaster or performing testing to validate plan's effectiveness is necessary. Anything anyone can learn in a non-stress situation will be invaluable when the real thing happens.

h) Plan Maintenance

Nothing is ever static when dealing with cyber security. The plan should be a living document. Companies will need to reevaluate their cyber contingency plans on a regular (preferably scheduled) basis, especially if there are relevant technological, operational, and personnel changes, to ensure that it is consistent with the risks the organization is facing. Every modification of the plan should be coordinated through the CCySO and should be recorded. The contingency plan contains sensitive operational and personnel information, therefore its distribution should be marked accordingly and controlled.

5) Cyber Incident Handling Process in the Maritime

Cyber defence requires mechanisms and procedures on the base of ongoing preparation in order to prevent, detect, respond, mitigate and recover from attacks affecting the confidentiality, integrity and availability of information and of supporting system services and resources. Having an established and rehearsed plan of action which a maritime organization executes after identifying a cybersecurity attack is crucial to limiting the damages. An effective plan should be comprehensive, covering every aspect of the incident.

Mechanisms may be seen in a circle with four phases, as below:

- Preparation
- Detection & Analysis
- Containment Eradication & Recovery
- Post-Incident Activity

a) Preparation

The main aim of this phase is to prevent incidents by building up resilience and by using security controls measures. A good preparation is the key to success. Not preparing for a cyberincident increases the risks impacting maritime operations. First step to be prepared for a cyber incident is to do an impact assessment.

The next step is to determine the kind of equipment and the cost of it in order to protect the assets that are critical to port and maritime operations. Maritime organizations must keep in mind that it may not make sense to spend a lot of money protecting a device unless the value of the information and data it stores or processes is operationally critical. The cost of protecting the file server for example is not just the cost of replacement or repair or the cost of backup, but also the cost to the organization if the information and data that stored on it will lost. Another important part of this phase is to train the personnel to raise their cyber awareness. Every person in a maritime organization must have a basic training in cyber awareness focusing on impacts of cyber incidents and cyber-attacks. This is the best protection. In addition, ensure that users are made aware of the lessons learned following a cyber incident. A small investment in user training can turn into significant savings for the organization when a threat is avoided by a trained user. Users should also know the responsible person to which they will report any suspicious activity. Maritime organizations must create an incident handling team led by CCySO to be prepared to respond if an event occurs. Companies should decide who is in charge if an event happens. Maritime organizations should also take part in risk assessment. Frequent risk assessments of systems and applications help to identify vital resources and the way to prioritize them during a cyber incident.

b) Detection & Analysis

The most challenging and also the most important part is to detect and analyze possible incidents. Early detection of an incident allows the maritime organizations to respond before it escalates any further. When an unusual action or network behavior is noticed, it should be reported immediately by the users. People have to be trained for being suspicious and for recognizing abnormal behavior of their systems. This abnormal behavior may not only relate to incidents that have already occurred or are occurring at that time, but may also relate to incidents that indicate that they may happen in the future. All these different categories of incidents should be perceived and identified using many different sources, like IDS or IPS systems, log files, publicly available information, and people. Different types of security software systems should be used (not all systems detect all incidents), as well as third party monitoring. When an incident occurs, the incident handling team should immediately start recording all facts regarding the incident. Then, the team should perform an initial analysis to determine for example which system or application is affected, who is responsible, what tools are being used etc. After this, the team must ensure a fast and coordinate reaction and report the incident to the public. In particular when more than one incident occurs, handling should not be handled on a first-come, firstserved basis. Ultimately, detecting and analyzing a cyber incident is the main key to quick return to normal operations with minimal disruption.

c) Containment Eradication & Recovery

When an incident occurs, it must be contained to gain valuable time for reaction and prevent further damage. The key is to have a strategy already in place, based on known threats. This strategy should support rapid decision-making, also define acceptable risks in dealing with incidents, identify the different kinds of attacking hosts and consider the specifics and individual aspects of each incident type. If an incident is only contained without eliminating the problems it has created, it will most likely continue to create more and more problems. This is the eradication phase, where all the "faults" created by the incident are detected and eliminated. Then follows the recovery phase. At this phase, all necessary steps are taken in order to restore systems to its normal operations such as use of backups, patches installations etc. or in large-scale incidents maybe even rebuild the all system from beginning.

d) Post-Incident Activity

This phase aims to learning from incidents, reflecting and reviewing what happened, how the incident was managed and what can be improved. The key to a proper lessons learned regime is holding a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically after smaller incidents. As incidents performed through new attack methods, they are of widespread concern and interest. Respective information on this as well as on the incident handling, should be

shared as well as reported to other organizations. Prepared documentation should be updated as a result of the lessons learned meeting.

Because of the changing nature of information technology and changes in personnel, the incident handling team should review all related documentation and procedures for handling incidents at designated intervals. At the end, an important post-incident activity creates a followup report for each incident, which can be used as «best practice» for future incident handling and data collection on incident handling (resources, time, and number) in order to justify future organizational changes as well as funding issues.

V. CONCLUSION

Although at the past the cyber security was something that didn't concern the maritime industry, the last few years fortunately there has been a gradual change in the mindset of the industry, and cyber security is now perceived as genuine threat and is a necessary element for the safe and efficient operation of all maritime organizations. Cybersecurity risks continue to grow exponentially around the world and greatly influence the maritime which uses complex critical IT and OT systems which have several vulnerabilities and should be protected against cyber threats. Taking into account the modern trends of shipping that lead it to fully autonomous vessels then it is understood that cyber security becomes even more important. The aim of this paper is to analyze the common cyber threats, the possible actors behind a cyber-attack as well as its anatomy. Furthermore, give a short report about the vulnerabilities in ship systems but the main purpose is to give a cyber security policy and its components for the maritime sector. The creation of a cyber security policy with: specific roles and responsibilities for the users, secure procedures, and the existence of plans to deal with the different cyber risks are essential elements in order to tackle and reduce the number of cyber-attacks more effectively in order to allow maritime community to continue to prosper.

REFERENCE

- [1] Trend Micro (2014). *A security evaluation of automatic identification systems*, Available at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais>
- [2] *Understanding Cyber risk: Best practices for Canada's Maritime sector*, Transport Canada.
- [3] SANS Institute (2017), *Reply to Request for Information (RFI), Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development*.
- [4] Safety4Sea (2018). *The seven phases of a cyber attack*. Available at <https://safety4sea.com/the-seven-phases-of-a-cyber-attack>
- [5] Safety4Sea (2018). *10 steps to maritime cyber security*. Available at <https://safety4sea.com/10-steps-to-maritime-cyber-security>
- [6] Safety4Sea (2018). *Understanding the cyber risk at sea*. Available at <https://safety4sea.com/understanding-the-cyber-risk-at-sea>.
- [7] *The Maritime Executive* (2018), *The Seven Phases of a Cyber Attack*, Available at: <https://www.maritime->

-
- [8] *The Guidelines on Cyber Security Onboard Ships, version 3, Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI and WORLD SHIPPING COUNCIL*
- [9] *MTI Network, Maritime Cyber Security, January 2016, Available at: <https://www.flipsnack.com/mtinetwork/mti-network-cyber-securityreport-2016.html>*
- [10] *National Institute of Standards and Technology (NIST), Contingency Planning Guide for Information Technology Systems, Special Publication 800-34, (June 2002).*
- [11] *National Institute of Standards and Technology (NIST), Computer Security Incident Handling Guide, Special Publication 800-61 Revision 2, (August 2012).*
- [12] *SOPHOS, Threatsaurus, The A-Z of computer and data security threats, (2013).*
- [13] *SBIR-STTR, America's seed fund, Introduction to cyberthreats, course10-tutorial2, Available at <https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial2.pdf>*
- [14] *Rapid7, Common Types of Cybersecurity Attacks. Available at <https://www.rapid7.com/fundamentals/types-of-attacks>, (2018)*
- [15] *Gnostech Inc (2018), Cyber Incident Response in the Maritime Environment, Available at <https://www.gnostech.com/maritimeblog/cyber-incident-response-maritime-environment-part-1,2,3,4>.*
- [16] *HM Government, National Cyber Security Strategy 2016-2021, (2016).*
- [17] *National Cyber Security Center, Cyber Attacks White Papers, Common Cyber attacks: Reducing the impact, (2016).*
- [18] *Institution of Engineering and Technology (IET), Hugh Boyes and Roy Isbell, Code of Practice - Cyber security for Ships.*
- [19] *UCSB Information Security (2015), Inventories. Available at <https://security.ucsb.edu/faculty-staff/inventories>.*
- [20] *Central Intelligence Agency (CIA), Careers & Internships, Available at <https://www.cia.gov/careers/opportunities/supportprofessional/information-assurance.html#job-details-tab2>*
- [21] *Bunkerspot, Limassol based shipping company victim of cyber fraud, Available at <https://www.bunkerspot.com/latest-news/40447-globallimassol-based-shipping-company-victim-of-cyber-fraud>*
- [22] *FutureDirections (21 August 2018), The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges, Available at <http://www.futuredirections.org.au/publication/the-global-maritimeindustry-remains-unprepared-for-future-cybersecurity-challenges/>*
- [23] *Dejan Kosutic, 9 Steps to Cybersecurity, (2012).*
- [24] *Edith Cowan University, A critical analysis of security vulnerabilities and countermeasures in a smart ship system, Dennis Bothur, Guanglou Zheng, Craig Valli, (2017)*
- [25] *Techopedia, definitions, Available at <https://www.techopedia.com>*
- [26] *Agence Nationale De la Securite Des Systemes d'Information, Thierry COQUIL, Guillaume POUPARD, Best Practices For Cyber Security On- Board Ships, (2016)*
- [27] *Blank Rome Maritime, Maritime Cybersecurity: A Growing Threat Goes Unanswered, Kate B. Belmont, (2015)*
- [28] *National Cyber Security Center, The cyber threat to UK business, (2016/1017) report.*
- [29] *JRCS Corporation, Engine Control Console, Available at <https://www.jrcs.co.jp/en/products/detail/engine-control-console>*
- [30] *The North of England P&I Association, Cyber Risks in Shipping, (June 2016)*
- [31] *Safety4Sea (2017). Inmarsat takes mature approach to maritime cyber security Available at <https://safety4sea.com/inmarsat-takes-matureapproach-maritime-cyber-security/>*
- [32] *Maritime Security Review (14 June 2018), The maritime cyber threat, Why 50.000 ships are so vulnerable to cyberattacks, Available at <http://www.marsecreview.com/2018/06/the-maritime-cyber-threat>.*
- [33] *CyberKeel, Copenhagen, Denmark, Maritime Cyber Risks, (pages: 16- 19), Available at www.cyberkeel.com, (2014)*
- [34] *International Armour Co, Defence and Security, Maritime Cyber Security, Available at <https://www.armour.gr/catalogues/pdf/CyberSecurityOnBoard.pdf>*
- [35] *National Institute of Standards and Technology (NIST), Guide for Conducting Risk Assessments, Special Publication 800-30 Revision 1, (September 2012).*
- [36] *Royal Belgian Institute of Marine Engineers, The ship's electrical network, engine control and automation, Kari Valkeejärvi, Marine Technology, Wärtsilä Corporation*
- [37] *Marineinsight, What Are The Duties Of Ship Security Officer (SSO)? Available at <https://www.marineinsight.com/marine-safety/what-are-the-duties-of-ship-security-officer-sso/>*
- [38] *Wikipedia, AIS, Available at https://en.wikipedia.org/wiki/Automatic_identification_system*
-

-
- [39] MarineInsight, *What is Ship Security Alert System (SSAS)?*, Available at <https://www.marineinsight.com/marine-piracy-marine/what-is-shipsecurity-alert-system-ssas/>, (2018) I Filippopoulos et al, (2018), *Transferring Structured Data and applying business processes in remote Vessel's environments using the " InfoNet" Platform*, 2018 IEEE South-Eastern European Design Automation, Computer Engineering, Computer Networks and Society Media Conference (SEEDA_CECNSM).
- [40] Wikipedia, *Dynamic Positioning*, Available: https://en.wikipedia.org/wiki/Dynamic_positioning
- [41] Wikipedia, *Global Maritime Distress and Safety System*, Available at https://en.wikipedia.org/wiki/Global_Maritime_Distress_and_Safety_System
- [42] MarineInsight, *Marine Radars and Their Use in the Shipping Industry*, Available at <https://www.marineinsight.com/marine-navigation/marineradars-and-their-use-in-the-shipping-industry>, (2017)
- [43] Wikipedia, *Voyage Data Recorder*, Available at: https://en.wikipedia.org/wiki/Voyage_data_recorder
- [44] Wikipedia, *Bridge Navigational Watch Alarm System*, Available at: https://en.wikipedia.org/wiki/Bridge_navigational_watch_alarm_system
- [45] I Filippopoulos et al, (2017), *Collecting and using vessel's live data from on board equipment using "Internet of Vessels (IoV) platform"*, 2017 IEEE South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM).
- [46] Wikipedia, *Advanced Persistent Threat*, Available at https://en.wikipedia.org/wiki/Advanced_persistent_threat
- [47] Gnostech Inc (2017), *Maritime Cyber Vulnerabilities and Hacking in the News*, Available at <https://www.gnostech.com/maritime-blog/maritimecyber-vulnerabilities-hackings-news/>
- [48] International Maritime Organization (IMO), *Measures to Enhance Maritime Security*, (17 May 2016)

Instructions for Authors

Essentials for Publishing in this Journal

- 1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.
- 2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.
- 3 All our articles are refereed through a double-blind process.
- 4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. <http://enrichedpub.com/> . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd.** The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).
2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);
3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);
4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.

The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005