Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems

Mohammed Nasser Al-Mhiqani, Rabiah Ahmad, Warusia Yassin, Aslinda Hassan,
Zaheera Zainal Abidin, Nabeel Salih Ali, Karrar Hameed Abdulkareem
Information Security and Networking Research Group (InFORSNET),
Center for Advanced Computing Technology,
Faculty of Information Communication Technology,
Universiti Teknikal Malaysia Melaka
Melaka, Malaysia

***Abstract*—Cyber-Physical Systems refer to systems that have an interaction between computers, communication channels and physical devices to solve a real-world problem. Towards industry 4.0 revolution, Cyber-Physical Systems currently become one of the main targets of hackers and any damage to them lead to high losses to a nation. According to valid resources, several cases reported involved security breaches on Cyber-Physical Systems. Understanding fundamental and theoretical concept of security in the digital world was discussed worldwide. Yet, security cases in regard to the cyber-physical system are still remaining less explored. In addition, limited tools were introduced to overcome security problems in Cyber-Physical System. To improve understanding and introduce a lot more security solutions for the cyber-physical system, the study on this matter is highly on demand. In this paper, we investigate the current threats on Cyber-Physical Systems and propose a classification and matrix for these threats, and conduct a simple statistical analysis of the collected data using a quantitative approach. We confirmed four components i.e., (the type of attack, impact, intention and incident categories) main contributor to threat taxonomy of Cyber-Physical Systems.**

***Keywords*—Cyber-Physical Systems; threats; incidents; security; cybersecurity; taxonomies; matrix; threats analysis**

I. Introduction

The world accepted that Cyber-Physical Systems (CPSs) connect computers, communication devices, sensors and actuators of the physical substratum, either in heterogeneous, open, systems-of-systems or hybrid. Systems become more interconnected, thereby more complex [1]. Computer networks currently have joined water, food, transportation, and energy as the critical resource for the function of the nationals' economy. Application of CPS can be seen in many forms of industries. The common sector is oil and gas, the power grid manufacturing, defense and public infrastructures are fully relying on the advancement of CPS. Therefore, cyber-physical systems security has become a matter for societal, infrastructures and economic to every country in the world due to the tremendous number of electronic devices that are interconnected via networks communication [2]-[4]. Latest reports have shown that cyber-attacks are aimed to destroy nation's systems that used for country development. CPS starts with by not simply disrupt a single enterprise or damage an isolated machine, but a target to damage infrastructures via modern dynamics threats [5], [6]. Those types of attacks are able to provide destruction to critical infrastructures system which used in sectors such as defense, finance, health, and the public [7]. To accomplish their goals criminals, activists, or terrorists are mostly looking for new and innovative techniques and targets, so cyber-physical systems currently one of the important targets for the hackers [3]. Increased security risk awareness and appropriately security relevant information management provide an equally important role in the trusted infrastructure maintenance [8]-[10]. This paper discusses some instances of attacks on cyber-physical systems that have occurred in the Organization of Islamic Cooperation (OIC) countries. The diversity of the attacks will be covered and analyzed based on their types and targets. The analysis will allow researchers to clearly understand the nature of the attacks and how they were carried out. A proposed matrix for threats verification and threats taxonomy will be discussed using a modified version of many taxonomies presented in [11]-[14] to classify the threats based on certain factors to enable researchers to analyze them along with their types and targets. The different matrices include types of attack, target sector, intention, impact, and incident categories. This article is structured into seven sections describe cyber-physical system threats from fundamental concept to threats categorization and impact. The following section will provide related work on the issue discussed. The remainder of the paper is structured as follows: In Section 2 reviews and discusses several taxonomies that have been presented to classify the threats based on certain factors. Section 3 provides a clear description of the proposed taxonomy to classify the CPS attacks based on types of attacks, target sector, intention, impact, and incident categories. Also, presents a comprehensive detail regarding the proposed matrix in Section 4. In addition, different CPS incidents surveyed from various sources in Section 5. Section 6 discusses and analyses the incidents by the modified taxonomy. Finally, Section 7 concludes this study.

II. Related Work

In [12], the author discusses and classifies incidents of cyber-physical attacks based on the sources, sectors, and impact of the incidents. The research paper provides an example of how the standardization of the cyber incidents information collection can be useful for attack victims and aids in understanding the cyber incidents threats towards different

targets. Four dimensions taxonomy proposed in [13] to provides a holistic taxonomy to enable the researchers to deal with inherent problems in the computer and network attack field. The first dimension of the taxonomy covers the attack's vector and the main attack behavior. The second dimension categorizes the attacks based on their targets. The third and fourth taxonomy dimensions categorized the vulnerabilities and payloads, respectively. The framework in [14] describes core components in cyber terrorism. The data is analyzed using a grounded theory approach in which the framework is drawn. The framework defined the cyber terrorism from six perspectives: target, motivation, domain, attack method, perpetrator action, and the impact of the attack. In addition, the proposed framework provided a dynamic method for defining cyber terrorism and describing its influential considerations. Incident analysis security ontology research is presented in [15] and provides a taxonomy which has some similarities to the framework presented in [14], but some aspects have been added in their classification such as action and unauthorized results. In their taxonomy Giraldo et al. [16] categorized cyber-physical systems by focusing on some of the CPS characteristics such as its domains, defenses, attacks, network security, research trends, security-level implementation, and computational strategies.

III. Proposed Taxonomy

The proposed taxonomy in this paper uses a modified versions of those presented taxonomies in [12]-[15] to classify the attack based on types of attacks, target sector, intention, impact, and incident categories. Each part of the attack will be broken down to the terms shown in Fig. 1 and explained.

A. Types of Attacks

Worm: in their propagation worm is like viruses with no direction by the network from the attackers. However, unlike viruses, in worms, no interaction is needed from the user for activating their attempt to spread.

Trojan: is a type of a program where subversive functionality is added to associate with the existing program.

Virus: virus may be defined as a piece of codes that usually attaches itself to another program, and when the program runs it will run with them.

DDoS: represents the coordinated attacks on the target system service availability that has been given or a network that is indirectly launched through a number of compromised computing systems.

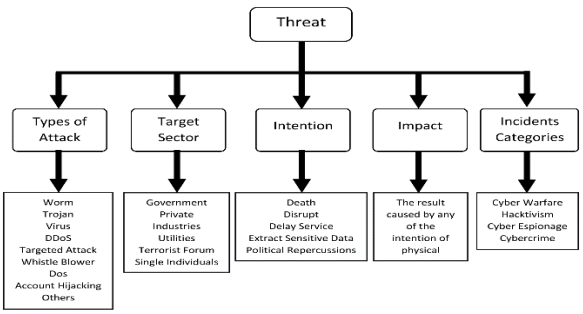

Fig. 1. Threats taxonomy.

Targeted Attack: refers to malicious attack which is targeted to a particular individual, software, systems, or company. It might be used to extract information, disrupt operations, or destroy a certain type of data on the target machine.

Whistleblower: indicates the disclosure of the information for perceived wrongdoing within the organization, or the risk to individuals or entities that have the ability to effect action.

Denial of Service: is defined as an attack that design to disable a network or computer from providing normal services. It is considered to occur only when access to a network or computer resource is intentionally degraded or blocked as a result of malicious action by another user.

Account Hijacking: is defined as a process where a particular individual's computer, email, or other account associated with service or a computing device is hijacked or stolen by hackers.

B. Target Sector

Government: is denoting local or national governments including buildings/housing, emergency services, public benefits, and social services, federal and state governments, tribal governments, military, protection of workers, and environment [16].

Private: refer to the part of a country's organization run by individuals and companies, rather than the government.

Industries: are the sectors that consist of all equipment and facilities used for producing, processing, or assembling goods [17].

Utilities: The utility sector comprises companies such as electric, water, gas, and integrated utility providers [18].

Terrorist forum: is the target sector which relates to any terrorist group such as ISIS or Al Qaeda.

Single Individuals: is the sector in which the attacker aims to affect the individual users.

C. Intention

Death: is the loss of human life.

Disrupt: change of access, removal access to information or to a victim. Manipulate the permission, e.g., Trojan horse or Denial of Service (DoS) attack. Disruption could be the least invasive of the attack [16].

Service Delay: where organizations or companies delay providing services on time due to the problems in the system.

Extract sensitive data: where unauthorized or hackers entities secure access to particular data and extract private information [19].

Political Repercussions: refer to events whose impact affects the government or the people leading the country.

Others: cases that not falling under any of the abovementioned categories.

D. Impact

The impact of the incident describes the incident effect. The impact description requires addressing all the entities affected which include the computer systems, the physical systems which the cyber-physical system interacts with, and the broader impacts on the community and organization [20].

E. Incident Categories

Cyberwarfare (CW): "using cyberspace (by operating within or through it) to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability" [21].

Hacktivism (H): "is the convergence of the hacking process and activism where hacking refers to the operations that exploit computers in ways that are unusual or often illegal, normally with the help of certain software" [22].

Cyber Espionage (CE): is the arm of the corporate high-tech crime. It mainly involves attacks on companies and institutions and not individuals. Cyber espionage does not always necessarily occur on a large scale [23].

Cyber Crime (CC): Involves the all criminal act which deals with the networks and computers (hacking). Additionally, traditional crimes that are conducted through the Internet are included in cybercrime [24].

IV. Proposed Matrix

The proposed matrix in this study uses two separated matrices i.e., threat matrix analysis and target matrix analysis to collect information that is required in cyber-physical system incidents analysis. The threat matrix analysis (see Table I) contains the associations between the intention and the type of attack, while the target matrix analysis (see Table II) contains the association between the attack target sector and the incident category. When the incidents analysis is initially conducted, threats and target are generated then added to the particular table. The matrix is then populated by adding data which correlates the column of the matrix with the row of the matrix. Finally, the threat matrix data is aggregated using (1) and then presented in Table I. Similarly, the Target analysis matrix data are aggregated using (2) and presented in Table II.

The derived equations 1 for the threat analysis are shown below:

$$\text{ThreatVal}_{ti} = \text{likelihood}_t \times \text{Rate}_i \quad (1)$$

$$\text{Total Score}_t = \sum_{i=6}^{6} \text{ThreatVal}_{ti} \quad (2)$$

$$\text{Total Score}_t = \sum_{i=6}^{6} (\text{likelihood}_t \times \text{Rate}_i) \quad (3)$$

$$\text{Total score}_t = \text{likelihood}_t \times \sum_{i=1}^{6} (\text{Rate}_i) \quad (4)$$

Where:

t: *Represent the Types of Attacks*

i: *Represents the Intention*

The derived equations 2 for the target analysis are shown as below:

$$\text{ThreatVal}_{ti} = \text{likelihood}_t * \text{Rate}_i \quad (1)$$

$$\text{Total Score}_t = \sum_{i=1}^{5} \text{ThreatVal}_{ti} \quad (2)$$

$$\text{Total score}_t = \sum_{i=1}^{5} (\text{likelihood}_t * \text{Rate}_i) \quad (3)$$

$$\text{Total score}_t = \text{likelihood}_t * \sum_{i=1}^{5} (\text{Rate}_i) \quad (4)$$

Where:

t: *represents the incidents Categories*

i *represents the Target Sector*

TABLE I. Threats Analysis (Correlation between Types of Attack and Intention)

THREAT ANALYSIS								
INTENTION / TYPES OF ATTACK	**Likelihood**	Death	Disrupt	Delay Service	Extract sensitive data	Political Repercussions	Others	**Total score**
Rate of Impact		6	6	3	6	3	3	
Worm	1							
Trojan	1							
Virus	6							
DDoS	1							
Targeted attack	3							
Whistleblower	1							
Denial of Service	1							
Account Hijacking	6							
Others	3							

TABLE II. Target Analysis (Correlation between Incidents Categories and Target Sector)

TARGET ANALYSIS							
TARGET SECTOR / INCIDENTS CATEGORIES	**Likelihood**	Government (Gov)	Private	Utilities	Terrorist forum	Single individuals (SI)	**Total score**
Rate of Impact		6	3	6	3	3	
Cyberwarfare	6						
Hacktivism	6						
Cyber Espionage	3						
Cyber Crime	3						

A. Rate the Matrix

In this part of the analysis, we have a list of types of attack that apply to a particular intention and the incidents category

that relates to the target sector. From our litterer review, we can rate the threats based on their impact level and the attack likelihood having occurred. This eases the addressing of the threats by presenting the high-risk ones first and then resolving the other threats.

This method indicates that the threats posed by specific types of attacks are similar to the probability of the threats occurring multiplied by the intention which indicates the consequences to CPS system if the attacks were to occur.

A 0–6 scales can be used for probability where 0 represents the types of attacks that are unlikely to occur and 6 representing those that are mostly occurring. Similarly, a 0–6 scale is used for intention with 0 indicating the intention that has no impact and 6 the intention that causes the highest impact. The same method is applied to the second matrix for the incidents category and the target sector.

V. Survey of Incidents

We surveyed many different CPS incidents from various sources and provide details of each one to examine how it was conducted. Some of the cyber incidents are explored in this study due to their high impact on daily life. Table III provides a summary of the incidents.

A. Stuxnet

In 2010, a worm named Stuxnet hit the Iranian nuclear facilities at Natanz. Stuxnet utilized 4 'zero-day vulnerabilities' (vulnerabilities were previously unknown, so there was no time to distribute and develop patches). The worms employed default passwords of Siemens to access the operating systems of Windows that run PCS7 and WinCC programs. They sought out frequency-converter drives manufactured by FararoPaya in Vacon in Finland and Iran. To power centrifuges, these drives were used to be utilized in the uranium 235 isotope concentration. The current electrical frequency to the drivers was altered by the Stuxnet which modified them between low and high speeds that they weren't designed for [25].

Type of Attack: Root, Worm, Trojan

Target Sector: Military (nuclear industry)

Intention: Disrupt

Incident Categories: CW

B. Iranian Infrastructure Attack

Cyber attackers disrupted the Internet network in Iran by attacking the country's infrastructure and communications companies and forcing the Internet to be limited due to the heavy attack. All the attacks were arranged systematically and included nuclear, oil, and information networks [26].

Type of Attack: unknown

Target Sector: Gov

Intention: Disrupt

Incident Categories: CW

C. Iran Hijacking of US Drone

Iranian specialists in electronic warfare were able to bring down an American bat-wing RQ-170 Sentinel by cutting off its communications links according to an Iranian Engineer working for an Iranian team attempting to unravel the stealth and intelligence secrets of the drones.

Iranians used the "spoofing" technique which considers landing altitudes, longitudinal and latitudinal data accurately causing the drone to land to the wanted location, without needing to crack the remote-control signal and communications from the control center [27].

Types of Attack: spoofing

Target Sector: Military

Intention: captured drone's systems

Incident Categories: CW

D. Iranian Oil Terminal 'offline'

A malware attack forced Iran to disconnect its key oil facilities. It is believed that the computer virus targeted the Iranian oil ministry and the national oil company by attacking their internal computer system. As prevention, the equipment at many Iranian different plants such as on the Island of Kharg was disconnected from the internet [11].

Type of Attack: Virus

Target Sector: Gov (Oil Company)

Intention: Disrupt

Incident Categories: CE

E. Saudi Aramco Attacks

The external source-originated virus targeted the Saudi Aramco Company and infected around 30,000 of its workstations. The company suspected the attack to be the outcome of a virus that had infected individual workstations without influencing the main parts of the network [28]. To prevent further attacks, Aramco was forced to cut off the electronic system from outside access.

Type of Attack: virus

Target Sector: Gov (Oil Company)

Intention: Disrupt

Incident Categories: H

F. Egypt Maritime Transport Sector

The attacked list comprised the websites of the Presidency, the Armed Forces, the Maritime Transport Sector, the Parliament, the Egyptian Accreditation Council, the Large Taxpayer Center, Ministry of Interior and many others. The attack affected the websites of the Egyptian government [30].

Type of Attack: DDoS

Target Sector: Gov (Transport)

Intention: Delay service

Incident Categories: H

TABLE III. SUMMARY OF INCIDENTS

Year	Country	Title	Type of Attack	Target Sector	Intention	Incident Category
2010	Iran	Stuxnet	Worm, root, Trojan	Military (Nuclear industry)	Disrupt	CW
2011	Iran	Iranian infrastructure and communications companies	unknown	Gov (infrastructure companies)	Disrupt	CW
2011	Iran	Iran hijacked US drone	spoofing	Military (US drone)	Captured drone's systems	CW
2012	Iran	Iranian oil terminal 'offline'	virus	Gov (Oil company)	Disrupt	CW
2012	Saudi	Saudi Aramco	virus	Gov (Oil Company)	Disrupt	H
2012	Egypt	Maritime transport sector	DDoS	Gov (Transport)	Delay service	H
2012	Syria	Syrian Ministry of Foreign Affairs	unknown	Gov (foreign ministry)	Extract sensitive data	CW
2012	Syria	Secret Assad emails lift lid on life of leader's inner circle	Whistleblowing	Single Individual	Extract sensitive data	H
2012	Qatar	Qatar’s RasGas Attack	virus	Private (Oil Company)	Disrupt	H
2013	Saudi	Saudi Arabian Defense Ministry System Breached	Account Hijacking	Gov (military)	Extract sensitive data	CW
2014	Syria	Syrian Hackers Ramp Up RAT Attacks	Targeted attack	Single Individual	Remote PC	CE
2015	Turkey	Attack on Istanbul Airport passport control system	virus	Gov (Airport)	Delayed service	CC
2015	UAE	Energy companies attacked by Trojan Laziok	Trojan	Gov (Energy)	Extract sensitive data	CC
2016	Turkey	Leaks Turkish Police data	Account Hijacking	Gov (Police data)	Extract sensitive data	CW
2016	Saudi	Shamoon 2	Malware	Gov (Industries)	Disrupt	CC
2016	UAE	The Operation Ghoul in UAE	Targeted attack	Industrial and Engineering companies	Extract sensitive data	CC
2017	Turkey	The source of the widespread electricity cuts across Istanbul	unknown	Gov (Transmission & electricity)	Disrupt	CW
2017	Qatar	Qatar News Agency Hacked	Account Hijacking	Gov (website)	Political Repercussions	CC

G. Syrian Ministry of Foreign Affairs

Around one gigabyte of documents was released by unknown hackers. The documents allegedly represented the internal government emails contents from the Ministry of Foreign Affairs. The publication of the documents was considered as part of the Syria campaign. The published documents comprised all information types, such as scanned copies of Syrian ministers' passports, specifics about an arms transport from Ukraine [30].

Type of Attack: unknown

Target Sector: Gov (foreign ministry)

Intention: Extract sensitive data

Incident Categories: CW

H. Secret Assad Emails Hacked

The attack targeted to sign into emails of nearest helpers of the president of Syria using a simple and straightforward password of numbers from 1 to 4. Israeli Haaretz site published selected documents from the hacked emails. The documents involved emails between Bouthaina Shaaban the president's media adviser and the press attaché in Syria's UN mission. The emails briefed the president before his interview with Barbara Walters in which the president denied responsibility for his governments' troops killing of civilians in Syria [31].

Type of Attack: Whistleblowing

Target Sector: Gov (President's Email)

Intention: Extract sensitive data

Incident Categories: H

I. Qatar's RasGas Attack

These attacks have brought down the computers of the RasGas Company due to a virus that hit the computer systems. Qatar RasGas was forced to close the email system and its website. The company's experts in security warned of hackers efforts to hit the energy and oil industry [32].

Type of Attack: Virus

Target Sector: Gov (Oil Company)

Intention: Disrupt

Incident Categories: H

J. Saudi Arabian Defense Ministry Mail System Breached

A source claimed that Syrian Electronic Army (SEA) received a secret document hacked from the emails of Saudi Arabia's Ministry of Defense involving secret arms deals. The documents were forwarded to the government of Syria [33]. A screenshot was shown to prove the successful attack on the mail system of the ministry.

Type of Attack: Account Hijacking

Target Sector: Gov (military)

Intention: Extract sensitive data

Incident Categories: CW

K. Syrian Hackers Ramp up RAT Attacks

Ramp up RAT attacks were launched through the social network. Hackers from Syria tried to download remote access Trojans (RATs) into the victim's computers. According to security researchers, they also discovered evidence of rising attacks from Syria [34]. The attackers seemed to take advantage of people's fear of government monitoring in the state. They created fake messages or posts on the social network such as in Skype and Facebook warning users about being attacked and where these messages themselves led to fake AV downloads.

Type of Attack: Targeted

Target Sector: Single Individual

Intention: Remote PC

Incident Categories: CE

L. Cyber Attack Hits Istanbul Airport

The cyber-attack targeted Istanbul Ataturk Airport specifically the passport control system at the international departure area, and at another airport in Istanbul. As a result, the passport control system shut down, flights were delayed, and passengers waited in lines for hours at the two airports [29], [35].

Type of Attack: Virus

Target Sector: Gov (Airport)

Intention: Delay of services

Incident Categories: CC

M. Energy Companies Attacked by Trojan Laziok

An Attack called Trojan Laziok attacked the energy sectors. These attacks targeted the Middle East companies especially United Arab Emirates companies, according to Symantec, Trojan Laziok acted as reconnaissance tools that enable the hackers to steal database from the targeted computers. The attacks targeted oil, helium gas and companies through spam emails from the domain money trans.eu. Microsoft Excel files are attached to the emails with an exploit for the Microsoft Windows Common Controls ActiveX Remote Code Execution Vulnerability. By clicking on the attachments it starts up its infection process. Trojan Lazoik hid in the directory: %SystemDrive%\Documents and the other directory Settings\All Users\Application Data\System\Oracle [36].

Type of Attack: Trojan

Target Sector: Gov (Energy sector)

Intention: Extract sensitive data

Incident Categories: CC

N. Leaks of Sensitive Data from Turkish Police Servers

Hackers known as ROR [RG] released a huge amount of sensitive data belonging to the Turkish National Police database. Around 50 million citizen data was leaked and publicly shared online such as first name, surname, citizenship number, sex, address, and date and place of birth [37].

Type of Attack: Account Hijacking

Target Sector: Gov (Police Law Enforcement)

Intention: Extract sensitive data

Incident Categories: CW

O. *Shamoon 2 Malware*

Three new waves of the destructive Shamoon 2 attacked many companies in Saudi Arabia. Bryan Lee and Robert Falcone "determined that the actors conducting the Shamoon 2 attacks use one compromised system as a distribution point to deploy the destructive Disttrack Trojan to other systems on the targeted network, after which the Disttrack malware will seek to propagate itself even further into the network" [38].

Type of Attack: DNS Hijacking

Target Sector: Private (Airlines)

Intention: Delay service

Incident Categories: CC

P. *The Operation Ghoul in UAE*

This is named after the Operation Ghoul group was the source of a multiple cyber-attacks that were reported in the United Arab Emirates. What the cyber-hackers did was to send malicious attachments with phishing emails particularly these emails sent to the top managers and some of the middle-level employee of various companies. The phishing emails are appearing to be coming from a local bank with messages that claiming to offer some advice on the payment from their bank. The email contains SWIFT document attachment which contains a malware [39].

Type of Attack: Targeted attack

Target Sector: Industrial and Engineering companies

Intention: Extract sensitive data

Incident Categories: CC

Q. *The Source of Widespread Electricity Cuts Across Istanbul*

A source from the Ministry of Energy in Turkey claimed that critical cyber-attacks caused widespread electricity cuts in the city. It mentioned that many infiltration attempts which the hacker tried on the controlling systems of electricity and transmission were prevented [40].

Type of Attack: Malware

Target Sector: Gov

Intention: Disrupt

Incident Categories: CC

R. *The Official State News of Qatar Agency Hacked*

Qatar announced that the Qatar News Agency (QNA), its national news agency, was hacked and a few articles about sensitive issues published on the website before it went down. The articles focused on the Palestinian-Israeli conflict, relations between Qatar and the Republic of Iran, remarks on Hamas, and negative perspectives on the relationship between Qatar and President Trump. The articles were attributed to Sheikh Tamim bin Hamad Al-Thani the Emir of the country, leading to Saudi Arabia, the United Arab Emirates, Egypt and Bahrain breaking off all the relations with Qatar in the worst diplomatic crisis to hit Gulf Arab states in decades [41].

Type of Attack: Account Hijacking

Target Sector: Gov (News Agency)

Intention: Political Repercussions

Incident Categories: CC

VI. Analysis of Incidents

A. *Analysis of Incidents by Modified Taxonomy*

Fig. 2 shows that among all the OIC countries, Iran has the highest number of cyber-physical attacks which are mostly related to political issues in the country, followed by Turkey, KSA, and Syria. The other surveyed countries have between one to two cases of CPS attacks.

Fig. 3 represents the incidents by year for the attacks surveyed in this work. As can be seen, 2012 had the highest number of attacks. That was the year following the Arab Spring in the Middle East and the Israeli–Palestinian conflict in Gaza [42] where the number of incidents in cyber-physical systems increased.

Fig. 4 details the attacks by type. Four cases took advantage of a virus, 3 utilized account hijacking, 1 case each of the other methods, which are, targeted attack, Spoofing, DDoS, and DNS Hijacking, and 2 cases where the method of attack is not defined.

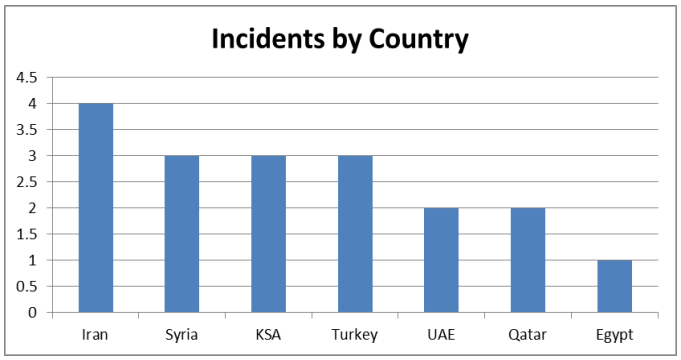

Fig. 2. Incidents by Country.

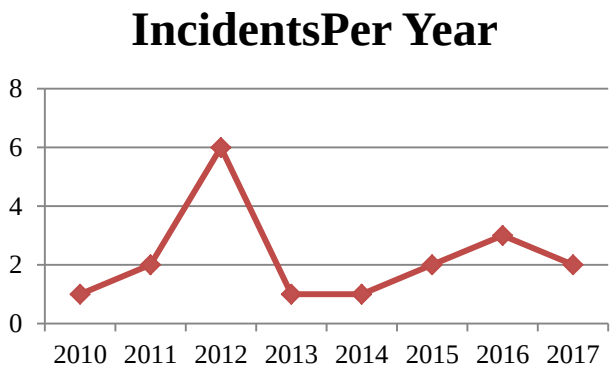

Fig. 3. Incidents by Year.

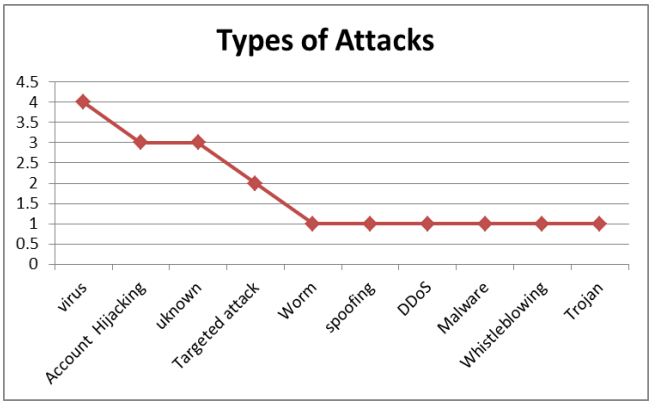

Fig. 4. Types of Attacks.

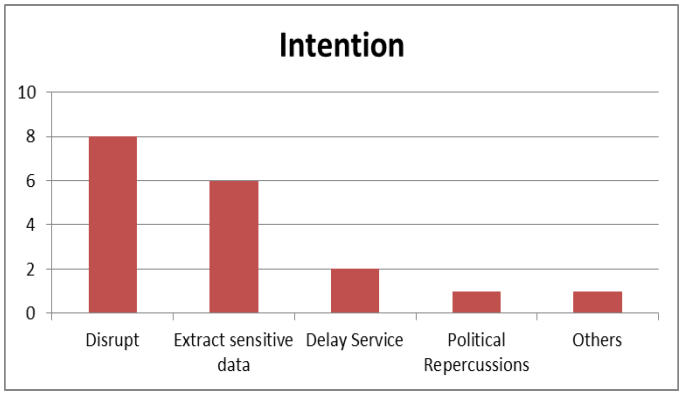

Fig. 5. Intention.

We next look at the intention of these attacks. As shown in Fig. 5, most aimed at disruption and extracting sensitive data, 2 at delays in services, and 1 each at political repercussions and for other intentions.

Fig. 6 represents the categories of the incidents. Cyberwarfare with 8 cases formed the highest category, while 5 incidents were cybercrime, 4 involved Hacktivism, and 1 cyber-espionage.

Fig. 7 shows the attacks by sectors. Most attacks were in the government sector involving the oil industry, transport, and other utilities at 44% of surveyed incidents, government websites (17%), the military (17%), and 11% for both private single individuals.

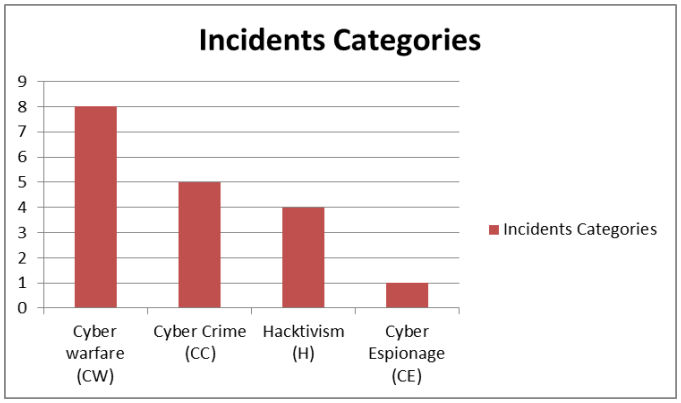

Fig. 6. Intentions categories.

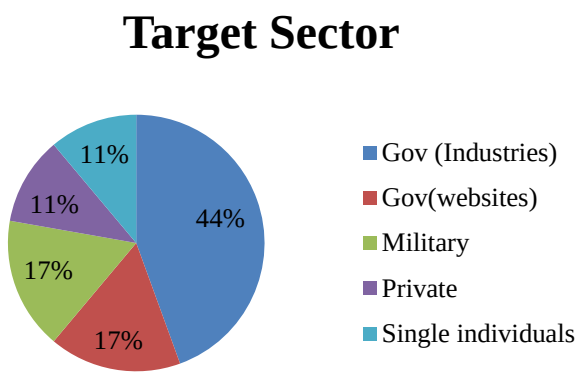

Fig. 7. Target sector.

B. Analysis of Incidents using Matrix

In the threat matrix in Table IV the data is aggregated and then sorted to define the types of attacks and intention relative importance. Since death, disruption, and accessing sensitive information has a strong impact, their ranks are high in the threat matrix especially when the type of attacks have a high probability of occurring many times like virus and account hacking types. The aggregate intention data then added into threat matrix along with the corresponding threat to the types of attacks.

The results of this analysis and the aggregate data in the matrices are used to increase overall awareness of each type of these attacks.

TABLE IV. THREAT ANALYSIS DATA

THREAT ANALYSIS								
INTENTION / **TYPES OF ATTACK**	**Likelihood**	Death	Disrupt	Delay Service	Extract sensitive data	Political Repercussions	Others	**Total score**
		6	**6**	**3**	**6**	**3**	**3**	
Worm	**1**	6	6	3	6	3	3	**27**
Trojan	**1**	6	6	3	6	3	3	**27**
Virus	**6**	36	36	18	36	18	18	**162**
DDoS	**1**	6	6	3	6	3	3	**27**
Targeted attack	**3**	18	18	9	18	9	9	**81**
Whistleblower	**1**	6	6	3	6	3	3	**27**
Account Hijacking	**6**	36	36	18	36	18	18	**162**
Others	**3**	18	18	9	18	9	9	**81**

TABLE V. TARGET ANALYSIS MATRIX

TARGET ANALYSIS							
TARGET SECTOR / INCIDENTS CATEGORIES	Likelihood	Government	Private	Utilities	Terrorist forum	Single individuals (SI)	Total score
		6	3	6	3	3	
Cyberwarfare (CW)	6	36	18	36	18	18	126
Hacktivism (H)	6	36	18	36	18	18	126
Cyber Espionage(CE)	3	18	9	18	9	9	63
Cyber Crime(CC)	3	18	9	18	9	9	63

The data in the target analysis matrix in Table V is similar to the previous matrix which is aggregated and then sorted to define the types of attacks and intention relative importance, while this matrix is aggregated and then sorted to define the incidents category and target sector relative importance. Government services, websites, and utilities have a high impact when their systems are hacked. The likelihood of cyberwarfare and Hacktivism occurring in the target analysis is very high since most of the incidents analyzed in our study fall under these two categories.

VII. CONCLUSIONS

The wide uses of CPS nowadays bring some risks and means for cybercriminals to use in their attacks against governments, organizations, or individuals. In this paper, we classified CPS threats based on modified taxonomies in generating organized information for other academics, experts, and researchers. This paper also provides researchers with matrices for studying the threats and enabling them to rapidly identify and correlate key threats involving CPS systems which, in turn, will lead to increased overall awareness of these incidents. However further work though is needed, the first suggestion is to include the study on how to trace the source of incidents, which cover the study of the groups and single individual hackers where the source of incidents come from, and the second suggestion is to study the cyber-physical security detection mechanisms to detect the attacks whether it comes from outsider or insider.

ACKNOWLEDGEMENTS

This project is funded by the Ministry of Higher Education Malaysia under Transdisciplinary Research Grant Scheme (TRGS) with project Number TRGS/1/2016/UTEM/01/3. And this project referred as TRGS/1/2016/FTMK-CACT/01/D00006 at UNIVERSITI TEKNIKAL MALAYSIA MELAKA

REFERENCES

[1] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, “STPA-SafeSec: Safety and security analysis for cyber-physical systems,” J. Inf. Secur. Appl., vol. 34, pp. 183–196, 2017.

[2] W. Wang and Z. Lu, “Cybersecurity in the Smart Grid: Survey and challenges,” Comput. Networks, vol. 57, no. 5, pp. 1344–1371, 2013.

[3] C. W. Ten, G. Manimaran, and C. C. Liu, “Cybersecurity for critical infrastructures: Attack and defense modeling,” IEEE Trans. Syst. Man, Cybern. Part ASystems Humans, vol. 40, no. 4, pp. 853–865, 2010.

[4] J. Walker, B. J. Williams, and G. W. Skelton, “Cybersecurity for emergency management,” Technol. Homel. Secur. HST 2010 IEEE Int. Conf., pp. 476–480, 2010.

[5] J. J. Walker, T. Jones, M. Mortazavi, and R. Blount, “CyberSecurity Concerns for Ubiquitous/Pervasive Computing Environments,” 2011 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov., pp. 274–278, 2011.

[6] N. S. Ali, “A four-phase methodology for protecting web applications using an effective real-time technique,” Int. J. Internet Technol. Secur. Trans., vol. 6, no. 4, p. 303, 2016.

[7] Al-Mhiqani,M.N., Ahmad R., Abdulkareem K. H., Ali N.S., "Investigation Study of Cyber-Physical Systems: Characteristics, Application Domains, and Security Challenges,"ARPN Journal of Engineering and Applied Sciences, Vol. 12, No. 22, pp. 6557-6567, 2017

[8] Ali, N. S., & Shibghatullah, A. S.,"Protection Web Applications using Real-Time Technique to Detect Structured Query Language Injection Attacks," International Journal of Computer Applications, Vol. 149, No. 6, pp. 0975-8887,2016.

[9] Sridhar, S., Hahn, A., & Govindarasu, M."Cyber–physical system security for the electric power grid". Proceedings of the IEEE, 100(1), 210-224.

[10] Ten, C. W., Liu, C. C., & Manimaran, G. . "Vulnerability assessment of cybersecurity for SCADA systems". IEEE Transactions on Power Systems, 23(4), 1836-1846, 2008.

[11] B. Miller and D. Rowe, “A survey SCADA of and critical infrastructure incidents,” in Proceedings of the 1st Annual conference on Research in information technology - RIIT ’12, 2012, p. 51.

[12] M. Kjaerland, “A taxonomy and comparison of computer security incidents from the commercial and government sectors,” Comput. Secur., vol. 25, no. 7, pp. 522–538, Oct. 2006.

[13] S. Hansman and R. Hunt, “A taxonomy of network and computer attacks,” Comput. Secur., vol. 24, no. 1, pp. 31–43, Feb. 2005.

[14] A. Rabiah, Y. Zahari, “A Dynamic Cyber Terrorism Framework,” Int. J. Comput. Sci. Inf. Secur., vol. 10, no. Xxx, 2012.

[15] C. Blackwell, “A security ontology for incident analysis,” in Proceedings of the Sixth Annual Workshop on CyberSecurity and Information Intelligence Research - CSIIRW ’10, p. 1, 2010.

[16] J. Giraldo, E. Sarkar, et al., "Security and privacy in cyber-physical systems: A survey of surveys," IEEE Design & Test, 2017.

[17] EIA, “Fuel Oil and Kerosene Sales - Energy Information Administration,” Office of Petroleum and Biofuels Statistics, Office of Energy Statistics, 2013.

[18] J. R. Klinefelter and T. A. Klinefelter, Minimalist Investor Maximum Profits, 1st editio. Page Publishing Inc, 2015.

[19] Y. G. B, P. C. Bhaskar, and R. K. Kamat, “Assessing the Guilt Probability in Intentional Data Leakage,” Int. J. Comput. Sci. Inf. Technol., vol. 3, no. 3, pp. 4075, 2012.

[20] W. B. Miller, D. C. Rowe, and R. Woodside, “A Comprehensive and Open Framework for Classifying Incidents Involving Cyber-Physical Systems,” in IAJC/ISAM Joint International Conference, 2014.

[21] K. B. K. B. L. G. Alexander, “Warfighting in Cyberspace,” JFQ NDU Press, vol. 35, no. 46, pp. 58–61, 2007.

[22] D. E. Denning, “Activism, Hacktivism, And Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy,” in Networks and Netwars: The Future of Terror, Crime, and Militancy, 1999.

[23] P. Warren and M. Streeter, Cyber Crime & Warfare: All That Matters. Hodder & Stoughton, 2013.

[24] T. Critchley, High Availability IT Services. Taylor & Francis, 2014.

[25] S. D. Applegate, “The Dawn of Kinetic Cyber,” in Cyber Conflict (CyCon), 2013 5th Int. Conference, 2013.

[26] S. Aryan, H. Aryan, and J. A. Halderman, “Internet censorship in Iran : A First look,” 3rd USENIX Work. Free Open Commun. Internet, no. August, p. 8, 2013.

[27] B. W. O’Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, “Real-time GPS spoofing detection via correlation of encrypted signals,” Navigation, vol. 60, no. 4, pp. 267–278, 2013.

[28] B. van N. Barend Pretorius, “Cybersecurity and Governance for ICS/SCADA in South Africa" - The Proceedings of the 10th International Conference on Cyberwarfare and Security, in The Proceedings of the 10th International Conference on Cyber, 2015, p. 558.

[29] Urban, J., "Not Your Grandaddy’s Aviation Industry: The Need to Implement Cybersecurity Standards and Best Practices Within the International Aviation Industry". Albany Law Journal of Science & Technology, 2017.

[30] W. S. PENDERGRASS, “What is Anonymous?: A case study of an information systems hacker activist collective movement,” 2013.

[31] J E. Grohe, “The Cyber Dimensions of the Syrian Civil War Implications for FutureConflict,” 2015.

[32] S. K. Venkatachary, J. Prasad, and R. Samikannu, “Economic Impacts of CyberSecurity in Energy Sector : A Review,” Int. J. Energy Econ. Policy, vol. 7, no. 5, pp. 250–262, 2017.

[33] P. Bradshaw and P. Bradshaw, Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation, vol. 2017.12. University of Oxford, 2017.

[34] W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson, “When Governments Hack Opponents : A Look at Actors and Technology,” Proc. 23rd USENIX Secur. Symp., pp. 511–525, 2014.

[35] E. Livanis, “Financial Aspects of Cyber Risks and Taxonomy for the Efficient Handling of These Risks,” in 14thInternational Scientific Conference on Economic and Social Development, 2016, no. May, pp. 80–87.

[36] R. de Oliveira Albuquerque, L. J. GarcÃ-a Villalba, A. L. Sandoval Orozco, R. T. de Sousa JÃonior, and T. H. Kim, “Leveraging information security and computational trust for cybersecurity,” J. Supercomput., vol. 72, no. 10, pp. 3729–3763, 2016.

[37] D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, “Targeted Online Password Guessing,” Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS’16, pp. 1242–1254, 2016.

[38] F. O. H. and M. Sulmeyer, “Getting beyond Norms (New Approaches to International CyberSecurity Challenges),” 2017].

[39] Q. Tao, M. Jiang, X. Wang, and B. Deng, “A cloud-based experimental platform for networked industrial control systems,” Int. J. Model. Simulation, Sci. Comput., vol. 9, no. 4, p. 1850024, 2017.

[40] Y. Biran, J. Dubow, S. Pasricha, G. Collins, and J. M. Borky, “Considerations for Planning a Multi-Platform Energy Utility System,” Energy Power Eng., vol. 9, no. 12, pp. 723–749, 2017.

[41] J. Cordy, “The Social Media Revolution: Political and Security Implications,” NATO Parliam. Assem., no. August, p. 10, 2017.

[42] M. Khalid, " Cyber Attacks: The Electronic Battlefield" ,Doha, QatarArab Center for Research and Policy Studies2013.