Kettani, H., & Cannistra, R. (2018). On cyber threats to digital smart environments. *Proceedings of the International Conference on Smart Digital Environment (ICSDE'18),* Rabat, Morocco, 183-188. New York, NY: ACM. https://doi.org/10.1145/3289100.3289130

On Cyber Threats to Smart Digital Environments

Houssain Kettani[1] and Robert M. Cannistra[1, 2]
[1]Beacom College of Computer and Cyber Sciences, Dakota State University, Madison, South Dakota, USA
[2]School of Computer Science and Mathematics, Marist College, Poughkeepsie, New York, USA

ABSTRACT
Cyber threats and attacks have significantly increased in complexity and quantity throughout this past year. In this paper, the top fifteen cyber threats and trends are articulated in detail to provide awareness throughout the community and raising awareness. Specific attack vectors, mitigation techniques, kill chain and threat agents addressing Smart Digital Environments (SDE), including Internet of Things (IoT), are discussed. Due to the rising number of IoT and embedded firmware devices within ubiquitous computing environments such as smart homes, smart businesses and smart cities, the top fifteen cyber threats are being used in a comprehensive manner to take advantage of vulnerabilities and launch cyber operations using multiple attack vectors. What began as ubiquitous, or pervasive, computing is now matured to smart environments where the vulnerabilities and threats are widespread.

CCS Concepts
• Security and Privacy → Intrusion/anomaly detection and malware mitigation • Security and Privacy → Systems Security • Security and Privacy → Network Security.

Keywords
Threat Landscape; Cyber Threat Intelligence; CTI; Cyber Security; Cyber Issues; Threat Agents; Threat Vectors.

1. INTRODUCTION
Over the past few years, there has been a radical shift toward a new paradigm where IoT has become integrated within our daily lives and virtually accessible by all ages in various applications from smart homes, smart healthcare solutions, to smart cities; however, these ubiquitous computing applications are vulnerable to cyber threats. Pervasive computing, used interchangeably with ubiquitous computing, adheres to three primary designs: smart devices such as mobile, wireless and service, smart environments referring to embedded system devices, and smart interaction for peer-to-peer device communication [16]. These ubiquitous IoT smart environments possess the potential to improve efficiency with energy consumption, home automation and control, automated healthcare monitoring and active response, as well as seamless smart city integration [13]. With a wide array of cyber interactions occurring between IoT embedded firmware devices and people, cyber security is a real threat to society.

ICSDE'18, October 18-20, 2018, Rabat, Morocco

ACM ISBN 978-1-4503-6507-9/18/10 …$15.00.
https://doi.org/10.1145/3289100.3289130

During the past six years, the European Union Agency for Network and Information Security (ENISA) has published an annual Cyber Threat Landscape (CTL) report articulating cyber security trends based on cyber threat information, data collection and analysis found throughout publicly available resources, where the primary resource is Open Source Intelligence (OSINT) [3]. The ENISA Threat Landscape (ETL) Report 2017 was published in January 2018 and covers information and data ascertained over a time period of twelve months from December 2016 through December 2017. By correlating the data and information articulated within the ETL 2017 report and the ubiquitous computing paradigm shift occurring, the top cyber threats, attack vectors, and overall landscape provide cyber security awareness.

Cyber Threat Intelligence (CTI) is defined as strategic or tactical analyzed actionable information related to "computers, networks and information technology" [8]. Over 50% of security professionals believe the CTI landscape evolves at a faster rate than the organization, or the professional, can "strategically or tactically assess it" [3]. Smart Digital Environments (SDE) are prone to cyber threats and attacks due to their infancy [11]. According to ENISA, the CTI interest areas are CTI information sharing, active defense, and automation methods of CTI, effectively embedding CTI within the organization, and CTI capabilities and skills.

The CTI information sharing refers to establishing an efficient method to create, disseminate, and consume threat intelligence in a standardized, usable, and legal way. This will ensure the relevant communities possess the information they need in order to address their cyber security policies and procedures to provide better cyber security protection against future cyber threats [1]. Active defense refers to a strategic cyber defense method utilizing asymmetric defense mechanisms by increasing the cyber adversary's cost and decreasing their overall efficiency of the active cyber operation. An example of an active defense strategy for data protection occurs when dynamic data distribution, data movement, and recurring encryption is used and ensures the data is harder to obtain, attack or destroy [20]. Automation methods of CTI is an important aspect to the CTL where a secure, automated method of rapidly sharing and analyzing data, information, and taxonomies is a necessity to integrate CTI to business workflow, governance, and structure control is essential to understanding and preventing cyber threats [1, 3]. By effectively embedding CTI within the organization, the organization is providing a cyber resilience defensive plan to cyber threats by tailoring CTI to the organization's framework, governance, and overall business. Lastly, CTI capabilities and skills ensure the knowledge gained from obtaining this information is proportionate to the related employee skill sets and knowledge presented for CTI awareness [3].

The European Union Agency for Network and Information Security (ENISA) identified areas that will require further clarification, known as CTI issues. The CTI issues are CTI adoption, strategic and tactical automated support, CTI creation and consumption within the organization, lack of CTI skilled resources, specificity of the organization's CTI, CTI type, and simplicity of supply-chain CTI. These issues require resources, education, and active support to adopt the strategic and tactical mission of CTI. One approach ENISA adopted during the 2017 reporting period was the development of an ETL web application located at https://etl.enisa.europa.eu where CTI can be easily obtained in reference to the current report [2].

When assessing SDEs risks, three primary elements are defined that should be taken seriously. These elements are asset (vulnerabilities and controls), threat (threat agent profile and likelihood), and impact. All three elements adhere to the standard ISO 270005: "Threats abuse vulnerabilities of assets to generate harm for the organization" [3]. A subset of the cyber security risk model elements are referenced in the ENISA report, namely: threats, threat agents, and attack vectors. These following sections will discuss these elements in depth.

This paper provides an overview of the current state of CTL pertaining to SDEs and is organized into six parts. Following the introduction, the top fifteen cyber threats are articulated based on the findings from the ETL 2017. Once the foundation is established for each of the top cyber threats, the cyber kill chain is articulated, followed by threat agents and attack vectors founded and used within SDEs. The paper concludes with a short critique of the ETL report findings followed by potential future cyber threat research.

2. TOP FIFTEEN CYBER THREATS

The Oxford Dictionary defines a cyber threat as "the possibility of a malicious attempt to damage or disrupt a computer network or system" [19]. One of the primary reasons for publishing the ETL Report is to analyze, assess and document the top cyber threats in the world that have occurred during the reporting period. Fifteen cyber threats are articulated within the most recent ETL report listed in order based on a ranking system pertaining to quantity of incidents occurred, their role and impact, from highest to lowest. The top fifteen cyber threats are malware, web-based attacks, web application attacks, phishing, spam, denial of service, ransomware, botnets, insider threats, physical manipulation or damage/theft/loss, data breaches, identity theft, information leakage, exploit kits, and cyber espionage.

The top fifteen threats recorded in ETL 2017 have been the same top fifteen threats since 2014, although some order and trending have changed [2-7]. The top three threats however, have remained consistent for the last six years (Malware, Web-based and Web Application Attacks). It is noticeable that Insider Threat was not recognized as a distinct type of threat until 2013 while Cyber Espionage was not included in such list until 2014. The ranking was based on the number of incidents, impact, and relationship to other threats. An increase in trend indicates an increase in incidents but not necessarily an increase in rank. Table 1 presents the top cyber threats articulated within the ETL Report from years 2012 through 2017. The Table shows the increased ranks of phishing and spam attacks as well as the decreased rank of exploit kit attacks. The analyzed threat data are in the public domain, specifically from the Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing [14].

In 2017, the number one cyber threat that was most frequently encountered was malware whereas the cyber threat that was least encountered is cyber espionage. In the following subsections we describe each of these threats presented in the ETL 2017 in the ranking order, where the highest rank is listed first, and the lowest rank is listed last [3].

Table 1. Annual change in ranking of the top fifteen threats according to ETL

Top Threats	Year					
	2017	*2016*	*2015*	*2014*	*2013*	*2012*
Malware	1	1	1	1	2	2
Web-Based Attacks	2	2	2	2	1	1
Web Application Attacks	3	3	3	3	3	3
Phishing	4	6	8	7	9	7
Spam	5	7	9	6	10	10
Denial of Service	6	4	5	5	8	6
Ransomware	7	8	14	15	11	9
Botnets	8	5	4	4	5	5
Insider Threat	9	9	7	11	14	-
Physical Manipulation/ Damage/Theft/Loss	10	10	6	10	6	12
Data Breaches	11	12	11	9	12	8
Identity Theft	12	13	12	13	7	13
Information Leakage	13	14	13	12	13	14
Exploit Kits	14	11	10	8	4	4
Cyber Espionage	15	15	15	14	-	-

2.1 Malware

Malware is the "most frequently encountered cyber threat" [3] and is ranked number one within the top fifteen cyber threats list. The term malware is the culmination of two words: "malicious" and "software"; therefore, malware is software developed for malicious intent to gain control over other systems [10]. Two of the most detrimental examples of malware that used ransomware while exploiting the EternalBlue vulnerability are WannaCry and NotPetya [15].

2.2 Web-based Attacks

Web-based attacks use web-enabled services, as well as systems (e.g. browsers, webpages, and content managers). Attack vectors include browser exploits, malicious URLs, water-holing, and drive-by downloads. Mitigation techniques for these types of attacks include sandboxing, web traffic filtering, and patching vulnerabilities [3].

2.3 Web Application Attacks

Web application attacks are aimed at web applications, services, or mobile apps that take advantage of exposed or vulnerable APIs. Vulnerabilities, such as SQL Injection, Cross-Site Scripting (XSS), and Content Management System (CMS) are among the most prevalent web application attacks. Mitigation techniques include

formulation of security policies, web application firewalling (WAF), web application vulnerability scanning and patching [3].

2.4 Phishing

Phishing usually uses email as its method of transport to target a group of users or an individual user "…posing as a legitimate institution to lure individuals into providing sensitive data…" as described on phishing.org [9]. The type of sensitive data is usually requesting personal information that can be used to steal a person's identity in order to access bank information, or network credentials to gain access to account information or data. Spearfishing is a type of phishing attack targeting people within an organization. Mitigation techniques includes user education identifying fake and malicious emails.

2.5 Spam

Spam is the act of unsolicited advertisements within email or even on social networks [18]. Spam contributes to 55.9% of the overall email traffic in 2017 which correlates to nearly 454 billion emails per day according to ENISA, securelist.com and talosintelligence.com [3]. Roughly 88% of spam originates from botnets. Mitigation techniques include implementing spam filters and anomaly detection techniques as well as user education.

2.6 Denial of Service

Denial of service (DoS) and Distributed Denial of Service (DDOS) attacks occur when a targeted attempt is made to overload a resource on a server using half-open TCP sessions which prevents users from accessing the service on the targeted server [17]. This disrupts the service and effectively makes the service unavailable. "Pulse wave" DDoS attacks occur in short bursts that target multiple servers and services. A large-scale example occurred in 2017 when the Mirai botnet targeted IoT devices across the world. This was the largest DoS attack to date. The attack led to a massive increase in policy and security standards for IoT devices specified by state governing agencies. Mitigation techniques include a reaction plan to detected incidents, implementing DDoS protection at the ISP, firewall-based access control lists (ACLs), as well as intelligent network mitigation systems.

2.7 Ransomware

Ransomware is malware that limits users to gain access to digital information by locking the user's system, screen or files until a ransom is paid [22]. Ransomware as a Service (RaaS) allows a bad actor to use script kiddies and other means to easily and automatically create ransomware attacks. The most frequently and wide spread ransomware attacks that occurred in 2017 are Cerber, Jaff, Sage, GlobeImposter, and Locky. Mitigation techniques include implementing minimal user data access using web filters with anti-malware analysis where attachments or external links are blocked, limiting local user administrative permissions, vulnerability and patch management routines, and policy control for external devices [3].

2.8 Botnets

Botnets consist of several internet connected devices referred to as bots; where each bot performs one task in a repetitive manner working together with a command and control server and a botmaster [12]. In 2017, IoT botnets were the second most important cyber threat in relation to a large-scale DoS attack. When an embedded firmware device such an IoT sensor is compromised, it becomes one device within the botnet. Mitigation techniques include implementation of firewalls, traffic filtering, and botnet sinkholing.

2.9 Insider Threats

Insider threats stem from users who use their authorization to gain access to confidential information to cause harm to the security of the organization. The healthcare industry is known for having a high percentage of insider threats occur where 59.2% of breached protected health information (PHI) have been the direct result of insider threats. Mitigation techniques include user awareness as well as limiting authorized access and segregation of duties [3].

2.10 Physical Manipulation, Damage, Theft or Loss

Physical manipulation, damage, theft and loss of digital assets such as computer equipment is a direct correlation and cause of data breaches. Mitigation techniques include encryption in all information storage, current asset tracking and inventory, limited physical access and maintaining a sound security policy where good practice is upheld.

2.11 Data Breaches

Data breaches are incidents that have occurred in the past and have only been found after the data or information is stolen. The data breach itself is not necessarily the threat; however, it is the result of a successful attack that already happened. A high number of breaches result from stolen or weak passwords. A few of the top data breaches that have been reported are from NetEase, River City Media, Deep Root Analytics, Edmodo, EmailCar, Yahoo Japan, and Equifax. Mitigation techniques include data classification, implementing a data loss prevention solution, encryption and access rights, privileges or permissions reduction.

2.12 Identity Theft

Identity theft is a cyber threat where the attacker's objective is to obtain confidential information to identify an individual or computer system for the purpose of impersonating their identity. Identity theft is the result of a successful attack. Personal information such as credit card data is available on the black market for $10 - $20 [3]. The top five identity threats include skimmers, dumpster divers, phishers, hackers, and telephone impersonators. Mitigation techniques include protecting privacy settings and identity documents, password protecting all digital devices and implementing a content filter for unwanted attachments.

2.13 Information Leakage

Information leakage occurs in a variety of ways stemming from collection of personal data to business data obtained from internet resources, online services or a company's Information Technology infrastructure. This is truly a breach caused from unsecured data. With the inception of mobile devices, information leakage has risen. Mitigation techniques include avoiding information in clear text, analyzing application code for vulnerabilities and exploits, as well as implementing encryption.

2.14 Exploit Kits

Exploit kits are a collection of pre-assembled exploits contained within compromised web resources and can also be part of a malicious advertising campaign. The exploits kits possess the ability to identify vulnerabilities within web pages automatically. One example of an exploit kit payload is ransomware. The top ten exploit kits are Neutrino, RIG, Empire Pack, Sundown, Bizarro Sundown, Magnitude, Terror, Nebula, KaiXin, and CK. Mitigation

techniques include vulnerability patch management orchestration, and malware detection configured for inbound and outbound channels.

2.15 Cyber Espionage

Cyber Espionage occurs when computer networks are used to acquire unlawful access to confidential information. Attack targets include government and commercial organizations for political reasons. The actors involved in Cyber Espionage include nation states, as well as organized crime. Advanced Persistent Threats (APTs) are used as a grouping of processes, tools, and resources to infiltrate networks without detection over a long period [3]. Examples of Cyber Espionage include CopyKittens, APT33, APT32, APT28, APT29, and APT17. Cyber Espionage mitigation techniques include security policy creation, vulnerability assessment, patch and vulnerability management, and a comprehensive plan due to the nature of Cyber Espionage [21].

3. CYBER KILL CHAIN

Each cyber threat articulated within the ETL 2017 report specifies a description, interesting points, trends and statistics, top threats throughout the reporting period, specific attack vectors, mitigation actions, and the position of the cyber threat within the kill chain along with references used for articulation. SDEs are highly sought after targets due to the scaled down kernel used within the IoT sensors' embedded firmware. The position in the kill chain will typically span multiple workflow steps depending upon the cyber threat defined. The Cyber Threat Kill Chain Workflow Steps are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control and Actions on Objectives. Reconnaissance refers to passively discovering information about the target. Weaponization occurs when a specific tool or utility is developed, or crafted, to attack the specific target using the information gained through reconnaissance.

Delivery is actually using the crafted utility to attack the target. It is important to note that delivery could be used in tandem with exploitation. Exploitation refers to exposing a specific vulnerability that the target possesses for malicious reasons. Installation occurs when the attack installs an agent or other software, on the target possibly through a phishing attack. Command and Control (C&C) is used once the cyber threat is installed within the target system or network and can be activated remotely or simply reports back to an external entity outside of where the targeted network is located. This is also referred to as the checking in phase. Actions on Objectives refers to adhering to the initial goals of the targeted attack or cyber threat. Table 2 displays the cyber threat kill chain attack workflow steps correlated to each of the top fifteen cyber threats. It is important to note that the cyber threat kill chain does not apply to the fifteenth cyber threat of cyber espionage since it is considered a composite threat [3].

4. THREAT AGENTS

A threat agent is defined as an individual, group, or organization that can "manifest a threat" [4]. A classification system of individual and group threat agents is used to disseminate the data and information [3, 4]. Threat agent identification is a continuous process as these the attributes can change over time, as well as the classification. An example of attributes used in classifying the threat agent include whether the agent is hostile or non-hostile. A hostile threat agent could be crackers, amateurs, employees, nations, organized crime, or terrorists [4]. A non-hostile threat agent could be hackers, amateurs, employees, or partner organizations. It's important to note there is overlap and the threat agent would need further attributes defined to successfully classify the threat agent.

After trend analysis, the ETL report describes threat agents as using masquerading techniques, such as: "imitating origin, imitating intention, smokescreens", using tools of espionage, and various code segments to falsify their identity as a genuine part of the organization. The top threat agents are: cyber criminals, insiders, cyber spies, hacktivists, cyber offenders, cyber fighters, cyber terrorists, and script kiddies. The ETL report further defines the involvement of each threat agent according to the top cyber threats within Table 3 [3].

Table 2. Top fifteen cyber threats to kill chain workflow step correlation

Top Threats	Cyber Threat Kill Chain Attack Workflow Steps						
	Reconnaissance	*Weaponization*	*Delivery*	*Exploitation*	*Installation*	*Command & Control*	*Actions on Objectives*
Malware					✓	✓	✓
Web-Based Attacks		✓	✓	✓			
Web Application Attacks	✓			✓	✓		
Phishing	✓	✓	✓				
Spam		✓	✓				
Denial of Service	✓	✓				✓	✓
Ransomware					✓	✓	✓
Botnets						✓	
Insider Threat	✓	✓	✓	✓	✓	✓	✓
Physical Manipulation/ Damage/Theft/Loss				✓			✓
Data Breaches							
Identity Theft	✓	✓	✓				✓
Information Leakage	✓	✓	✓	✓			✓
Exploit Kits		✓	✓	✓	✓		
Cyber Espionage							

5. ATTACK VECTORS

An attack vector is defined as "a means by which a threat agent can abuse a weakness or vulnerability on assets to achieve a specific outcome" [2]. In order to fully comprehend cyber threats, along with the tactics, techniques and procedures (TTPs) used, an attack vector taxonomy is defined and categorized by the vector used. TTPs refer to how the cyber threat agents are used to orchestrate, manage, and monitor the cyber-attack which aid in the analysis of security intelligence.

The five most common attack vectors categorized within the ETL report are: "attacking the human element, web and browser based attack vectors, internet exposed assets, exploitation of

vulnerabilities or misconfigurations and cryptographic, network or security protocol flaws, and supply chain attacks" [3]. Attacking the human element is one of the most prevalent attack vectors since the purpose is to exploit people through social engineering, phishing, or social media attacks. Web and browser-based attack vectors utilize compromised, or fake, websites to deliver exploits or malicious code. Internet exposed assets are an attack vector where services that are not sufficiently protected are exposed and used to deliver malware or perform ransomware attacks. Exploitation of vulnerabilities and misconfigurations are attack vectors used to gain access into an organization, system, or network. A widespread example of this attack vector is the ransomware attack known as Wannacry [3]. Supply chain attack vectors refer to an indirect attack to damage the target such as the software or hardware infrastructure.

Table 3. Threat agent involvement to the top cyber threats: primary threat group (P) and secondary threat group (S)

Top Threats	Threat Agents							
	Cyber Criminals	*Insiders*	*Nation States*	*Corporations*	*Hacktivists*	*Cyber Fighters*	*Cyber Terrorists*	*Script Kiddies*
Malware	P	S	P	P	S	S	S	S
Web-Based Attacks	P		P	P	P	P	P	S
Web Application Attacks	P		P	P	P	P	S	S
Phishing	P	P	P	P	P	P		
Spam	P	P	S	S				
Denial of Service	P				P	P		P
Ransomware	P	S	P	P		S		S
Botnets	P		P	P	S	P		
Insider Threat	P		S	P		S	S	
Physical Manipulation/ Damage/Theft/Loss	P	P	P	P	S		S	S
Data Breaches	P	P	P	P	P	P		S
Identity Theft	P	P	P	P	P	P	S	S
Information Leakage	P		P	P	S	S	S	S
Exploit Kits	P		P	P		S		
Cyber Espionage		S	P	P		S		

6. CONCLUSION

Smart Digital Environments (SDE) are utilizing ubiquitous computing where IoT devices are being used in a variety of industry verticals such as homes, healthcare, enterprises, and cities enabling these entities to become more efficient in numerous ways; however, due to the number of cyber threats taking advantage of the vulnerabilities within these devices, we need to be proactive through cyber security awareness. While the 2017 ETL Report articulates the top fifteen cyber threats found within the public domain, there is considerable research and evidence that lend itself to the conclusion that SDEs are a highly sought-after target. The Mirai botnet is an early example of what can occur if an SDE is vulnerable and exploited. The cyber threats, threat agents, attack vectors presented are considered real and should be monitored, investigated, and continuously analyzed by each state agency and each individual organization; however, the way each entity should address these cyber threats will vary significantly based upon the organizational entity and dynamics.

In this article, an overview of the top fifteen cyber threats presented by ENISA were articulated providing a high level of detail contained within the report and reinforced through additional research. Standardization will be an essential element in preparing the ETL in the future, as well as other state agency reports of similar nature, and the data gathered should be based on multiple creditable sources gathered from real time analytics, businesses, government, and educational entities.

7. FUTURE RESEARCH

Further research could be conducted to explore other state agency reports while comparing and contrasting reports for data modeling and analysis. If other state agency reports are generated, combining the reports within a relational database would help articulate, query, and automate the reporting of the highest ranking cyber threats. Further reports could be classified and analyzed for cyber threat origin relating to region of potential source and cyber threat and attack target, further defining and clarifying difference threat matrices. Specific SDEs could also be articulated and used as case studies to determine the increase or potential decrease in cyber threats. The cyber threat agent classification system could be further developed to continually update the attributes used as well.

8. REFERENCES

[1] CryptoMove (2018). Available at https://www.cryptomove.com/

[2] European Union Agency for Network and Information Security (ENISA). (2018). *ENISA Threat Landscape Web Portal*. Retrieved from https://etl.enisa.europa.eu/

[3] European Union Agency for Network and Information Security (ENISA). (2018). *ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends*. Heraklion: ENISA. https://doi.org/10.2824/967192

[4] European Union Agency for Network and Information Security (ENISA). (2017). *ENISA Threat Landscape Report 2016: 15 Top Cyber-Threats and Trends*. Heraklion: ENISA. https://doi.org/10.2824/92184

[5] European Union Agency for Network and Information Security (ENISA). (2015). *ENISA Threat Landscape Report 2014: Overview of Current and Emerging Cyber-Threats*. Heraklion: ENISA. https://doi.org/10.2824/061861

[6] European Union Agency for Network and Information Security (ENISA). 2013. *ENISA Threat Landscape Report 2013: Overview of Current and Emerging Cyber-Threats*. Heraklion: ENISA. https://doi.org/10.2824/022950

[7] European Union Agency for Network and Information Security (ENISA). 2013. *ENISA Threat Landscape Report 2012: Responding to the Evolving Threat Environment*. Heraklion: ENISA. Retrieved from: http://www.enisa.europa.eu/

[8] Hansen, A., Staggs, J., & Shenoi S. (2017). Security analysis of an advanced metering infrastructure. *International Journal*

of Critical Infrastructure Protection, 18, 3-19. https://doi.org/10.1016/j.ijcip.2017.03.004

[9] Hayati, P., Potdar, V., Talevski, A., Firoozeh, N., Sarenche, S., & Yeganeh, E.A. (2010, April). Definition of Spam 2.0: New spamming boom. *Proceedings of the 4th IEEE International Conference of Digital Ecosystems and Technologies (ICDET)*, Dubai, UAE, 580–584. Piscataway, NJ: IEEE. https://doi.org/10.1109/DEST.2010.5610590

[10] Hern, A. (2017, December 30). WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017. *The Guardian*. Retrieved from: http://www.theguardian.com

[11] Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. *National Institute of Standards and Technology Special Publication 800-150.* Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.SP.800-150

[12] Libicki, M. (2017, June). The coming of cyber espionage norms. *Proceedings of the 9th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia*, 1–17. Piscataway, NJ: IEEE. https://doi.org/10.23919/CYCON.2017.8240325

[13] Lin, H., & Bergmann, N.W. (2016). IoT privacy and security challenges for smart home environments. *Information, 7*(3), 44. https://doi.org/10.3390/info7030044

[14] Malware Information Sharing Platform (MISP) Project. (2018). *The Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing*. Retrieved from http://www.misp-project.org/

[15] PHISHING. (2018). What is Phishing?. *PHISHING.org*. Retrieved from https://www.phishing.org/what-is-phishing

[16] Poslad, S. (2011). *Ubiquitous computing: Smart devices, environments and interactions*. Hoboken, NJ: John Wiley & Sons.

[17] Sajjan, R.S., & Ghorpade, V.R. (2017, March). Ransomware attacks: Radical menace for cloud computing. *Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),* Chennai, India, 1640–1646. Piscataway, NJ: IEEE. https://doi.org/10.1109/WiSPNET.2017.8300039

[18] Saleh, M.A., & Manaf, A.A. (2014, August). Optimal specifications for a protective framework against HTTP-based DoS and DDoS attacks. *Proceedings of the International Symposium on Biometrics and Security Technologies (ISBAST),* Kuala Lumpur, Malaysia, 263–267. Piscataway, NJ: IEEE. https://doi.org/10.1109/ISBAST.2014.7013132

[19] SANS SECURITY AWARENESS. (2016, March). What is Malware?. *OUCH! Newsletter*. Retrieved from https://www.sans.org/security-awareness-training/ouch-newsletter/2016/what-malware

[20] SECUREWORKS. (2017, May 12). Cyber threat basics, types of threats, intelligence & best practices. *SECUREWORKS.* Retrieved from https://www.secureworks.com/blog/cyber-threat-basics

[21] Vidalis, S., & Jones, A. (2005, January). Analyzing threat agents and their attributes. *Proceedings of the 4th European Conference on Information Warfare and Security (*ECIW), Glamorgan, UK, 369–379. Reading: Academic Conferences Limited.

[22] Vormayr, G., Zseby, T., & Fabini, J. (2017). Botnet communication patterns. IEEE Communications Surveys & Tutorials, 19(4), 2768–2796. https://doi.org/10.1109/COMST.2017.2749442