New Approaches to the Investigations and Classification of Cyber Threats Challenged by the Application of Artificial Intelligence Methods

Roumen Trifonov, Ognian Nakov, Slavcho Manolov, Georgi Tsochev and Galya Pavlova

Technical University of Sofia, Sofia 1000, Bulgaria

r_trifonov@tu-sofia.bg

Abstract. The investigations of Cyber Threats on a global scale has, in recent years, taken on a new dimension related to the unprecedented growth of Cyber Crime, Cyber Terrorism and Cyber war, as well as the introduction of Artificial Intelligence methods in the field of Cyber Defense. The research and practice of this implementation shows that there is no universal method effective enough to protect against various types of Cyber Attacks. It turns out that the choice of Artificial Intelligence methods that are best suited to counteract certain classes of threats depends on the systematization, unification and classification of Cyber Security Threats and the sources of those threats. This paper examines the new approaches for identification and analysis of Cyber Threats, as well as the tools used by the various so-called "Threat Agents". These analyses and classification schemes can serve to create criteria for selecting appropriate Artificial Intelligence methods to counteract concrete classes of Cyber Threats.

Keywords: cyber threats, taxonomy, threat agents, threat vector, threat matrix, kill chain, cyber threat intelligence.

1 Introduction

The Special Publication SP 800-30 Revision 1 of the National Institute of Standards and Technology (NIST) [1] in USA defined the Cyber Threats as
"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."

The investigations of Cyber Threats have been going on for many years [10, 11]. The first attempt for their classification was implemented in the

International Standard ISO / IEC TR 13335-1:1996 [2]. Nevertheless, in recent years, this activity has acquired entirely new goals and characteristics, due to two fundamental factors triggered by the unprecedented rise in cybercrime and the emergence of elements of cyber terrorism and cyber war. These factors are as follows:

a) The adoption in Cyber Defense of important military technologies and methods, such as the Cyber Intelligence (Strategic, Operational and Tactical) and the concept of the so-called “Kill Chain”;

b) The widespread introduction into the practice of Cyber Defense of Artificial Intelligence methods.

Thus, on the one hand, different aspects of Cyber Threats are essential for the different phases and varieties of military methods; on the other hand, the research and practice of the implementation of Artificial Intelligence methods shows that there is no universal method effective enough to protect against various types of Cyber Attacks.

The motivation of the present research is based on the belief that the new approaches to identification, classification and analysis of Cyber Security Threats and the sources of those threats will be useful in choosing the appropriate method for counteraction to certain classes of threats.

Research by the team from Computer Systems and Technology Faculty at the Technical University - Sofia in the field of application of Artificial Intelligence methods in different phases of Cyber Defense (Operational Cyber Intelligence, Tactical Cyber Intelligence, Incident Handling) shows that the typification, unification and classification of Cyber Threats play an important role in achieving the specific objectives for each phase. Thus, in Operational Cyber Intelligence, where the primary task is to identify the behavior of a potential adversary, it is important, among the vast information on the network activity of the alleged adversary, to extract so-called “features” - characteristics that make it highly likely to determine its behavior. Moreover, in the case of Incident Handling, it is essential that the incident relate to a high degree of likelihood of a particular element of the Cyber-Threat Classification scheme, for which a remedial procedure has been developed, i.e. to solve a classification problem.

It should be noted that the present work is not just a “literature review” of sources related to the analysis and classification of cyber threats, but also an attempt to show how these classifications can influence the creation of criteria for adequate choice of methods of Artificial Intelligence for different areas of application in Cyber Security.

2 A New Generation of Cyber-Security Threats

The most adequate analysis of the radical changes in Cyber Security in the last few years has been carried out in the report of the European Network and

Information Security Agency (ENISA) "Threat Landscape Report 2016" [3]. ENISA and other leading Cyber Security players have identified and formulated the two main directions of these changes:

a) fifth-generation Cyber-Criminality, where threats are becoming more complex and automated. Major Cybercrime schemes integrate into several tools that perform different functions. One of the features of the fifth generation is called "Advanced Persistent Threats" (APT) as the definition of targeted attacks against specific organizations by some well-coordinated cybercriminals [4]. In addition, such popular cloud computing services as SaaS (Software as a Service), IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and so on in the Cyber-Criminality world has been developed so called "Crimeware as a Service (CaaS)" - a modern model that provides easy access to the tools and services needed to commit Cyber Attacks [5]. This allows even novice Cyber Criminals to perform attacks on a scale that disproportionate to their technical capacity.

b) the transition from the Cyber-Criminality phase to the Cyber-War phase, where the most serious destructive effects are those of a hybrid nature - a combination of cyberattack and physical attack, i.e. Cyber-attacks affecting communications and information systems and violating physical, personal and communication security. The complexity and extent of the impact can affect all spheres of society and turn into a hybrid war against a state or group of states.

The military concept related to the structure of the attack and aimed at creating effective prevention or counter-attack at the various stages of the attack, known as the "Kill Chain", was adapted to the Cyber Defense by IT experts at Lockheed-Martin Corporation [6]. Gradually, this concept was accepted by the expert community as a Cyber Defense tool that defines the stages of Cyber-attacks and the respective counteraction at each stage. The "Lockheed-Martin" model (Fig. 1) [7] includes the following seven steps:

Fig. 1. "Lockheed-Martin" model of the Cyber Kill Chain.

a) Intelligence: selection of the target by attacker selects a target, examination of resources and attempts to identify vulnerabilities in the target network;

b) Creation of the weapon: respective creates weapons for remote access, such as a virus, adapted to specific vulnerabilities;

c) Delivery: dispatch of the weapon to the victim (via e-mail attachments, websites, USB devices, etc.):

d) Exploitation: activation of the weapon program code aiming to exploit the vulnerability;

e) Installation: implementation of unregulated access point (for example, a "back door") usable by the offender;

f) Command and control: obtaining so called "keyboard hands" - constant access to the target network;

g) Action on the target: realization of malicious action, such as fishing, data destruction, or ransom encryption.

The "Kill Chain" model can be used in the analysis of the most common and important threats, differentiating them into the relevant phases of the chain. The analysis should focus on the dynamic development of Cyber Threat assessments and aim to integrate different types of information and provide stakeholders with interactive assessments of threats and related instruments.

By assessing the impact on asset groups at different stages of the chain, it can be determined, which security measures are most appropriate for the different phases, including the intelligence to prevent asset abuse?

3 Classifications of Cyber Threats and Their Important Attributes

In order to build a rational and consistent approach to the choice of Artificial Intelligence methods best suited to counteract certain classes of threats, it is necessary to enable systematization, unification and classification of Cyber-Security Threats and the sources of these threats. The first step in this way can be the identification and analysis of the new concepts in the classifications of Cyber Threats.

A. Currently, the most authoritative classification is so called „Cyber Threats Taxonomy“ [8] published by ENISA on the basis of an analysis of about 40 taxonomies developed by world-leading organizations (including NIST and the US Department of Defense (USA), BSI (BRD), TERENA (Netherlands), etc.).

This information structure is not just a classification by any selected attribute, but a starting point for analysis, providing opportunities for combining, sorting, modifying and refining the definitions of threats. Threat taxonomy is a living structure that is used to maintain a consistent view of threats based on updated information.

ENISA‘s taxonomy consists of the following sections:

a) threat category (including threat families);

b) the individual threats included in a category;

c) threat parameters - such as: specific type, method of attack, targeting a specific IT asset, etc.;

d) additional features such as affected assets, threat agents, related sources, URLs, etc.

B. The systematization of the sources of Cyber Threats is an important element of their systematic analysis.

The mentioned above report of ENISA explained formation of groups of sources with similar characteristics (motivations, level of capabilities, focus, level of preparedness, striking power, etc.) and called „threat agents”:

a) Cyber-Criminals are the most active threat agent group in Cyber-space, being responsible for at least two third of the registered incidents. This group has set up networks to exchange tools for malicious action and hire assistants for the various stages of the attack;

b) Insiders are also the cause of a significant number of incidents. In addition to malicious acts of all kinds, there are widespread violations of existing security policies through negligence and user errors;

c) Hacktivists usually protest against environmental policy, discrimination, corruption, pacifism, public health issues, support of minorities, etc. In the majority of cases they cooperate on a group basis without any leadership schemes;

d) State-sponsored agents (including the cyber-spies) are the fourth most active Threat Agent group. Due to the early maturity of military cyber-capabilities it is not perfectly clear where is the differentiation between cyber-spying and cyber-combating;

e) Others: cyber-fighters, cyber-terrorists, script-kiddies, etc. - their role is less important.

Advanced intruders also use Cyber-Intelligence methods (mainly to look for vulnerabilities and apply anonymization techniques). They are investing significant amounts of their profits to improve and mature their infrastructure. In addition, they use the dark web to exchange information between them.

C. Identifying a particular attacker's affiliation with a respective group of Threat Agents is too useful for Cyber Defense, as analyses show that each group is distinguished by a specific set of instruments for Cyber Attacks. The Table 1 visualize which threat agent groups are involving in which threats.

This information might be useful for all interested stakeholders in order to identify the capability level can be assumed behind the top threats and thus support in decisions concerning the strength of the security controls that are implemented to protect valuable assets.

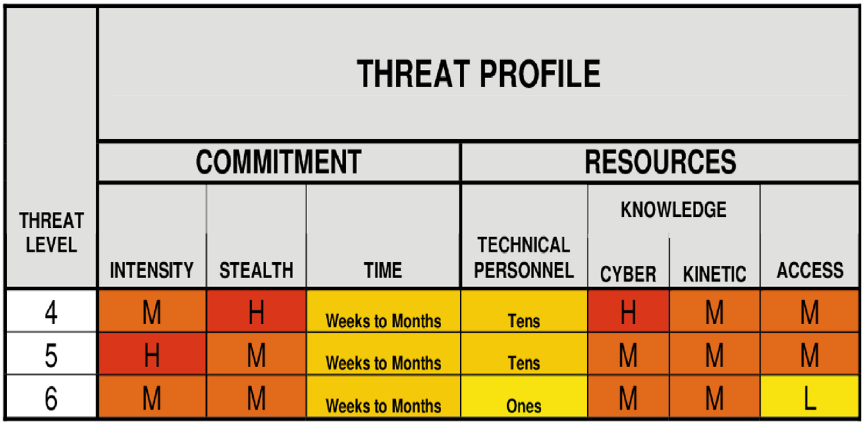
D. One of the new defined attributes of the Cyber Threats is so-called "Attack Vector", charactering methods and tools applied by the concrete Threat Agent. A threat agent can abuse of weaknesses or vulnerabilities on assets (including human) to achieve a specific outcome by this means. In the correct context, the study of the different steps performed on an attack vectors can provide valuable information about how Cyber Threats can be materialized.

The description of the workflow of the attacks based on the „kill chain" model, also has quite similar features within a particular group of Threat Agents. This understanding creates additional opportunities for adequate planning of Cyber Defense.

Table 1. Threat agents in the deployment of the identified top cyber-threats.

	Threat agents							
	Cyber criminals	Insiders	Nation states	Corporations	Hacktivists	Cyber-fighters	Cyber-terrorists	Script kiddies
Malware	●	♦	●	●	♦	♦	♦	♦
Web-based attacks	●		●	●	●	●	●	●
Web application attacks	●		●	●	●	●	♦	♦
Denial of service	●		♦	♦	●	●	●	●
Botnets	●		●	●	♦	●	●	●
Phishing	♦	●	●	●	●	●	♦	
Spam	♦	●	♦	♦				
Ransomware	●	♦	●	●		♦		♦
Insider treats	●					♦	♦	
Physical manipulation/damage/ theft/loss	●	●	●	●	♦		♦	♦
Exploit kits	●		●	●		●		
Data breaches	●	●	●	●	●	●	●	♦
Identity theft	●	●	●	●	●	●	♦	♦
Information leakage	●		●	●	♦	♦	🔴	♦

E. One of the results of the newest Cyber Threat analyses is the so-called “threat matrix” [8], which describes the identification of the adversary’s abilities, the patterns of past and current behavior, and his specific tasks, techniques and procedures. This matrix (Fig. 2) [8] is focused to those who have already shown intent and ability to attack. It contain qualitative and quantitative evaluation criteria. The matrix can be used for priority allocation of resources to most likely opponents.



THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
					KNOWLEDGE		
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	CYBER	KINETIC	ACCESS
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L

Fig. 2 The “threat matrix”.

F. The threat modelling [9] as another useful tool for the systematic analysis of Cyber Threats realizes an iterative process consisting of five major steps (Fig. 3) [9]:

a) identification / verification of security objectives – threat modelling aimed at determining of the activities in subsequent steps;

b) creation of application overview - attempt to extract essential features and identify the threat agent;

c) decomposition of application - a detailed description of the mechanics of malicious action;

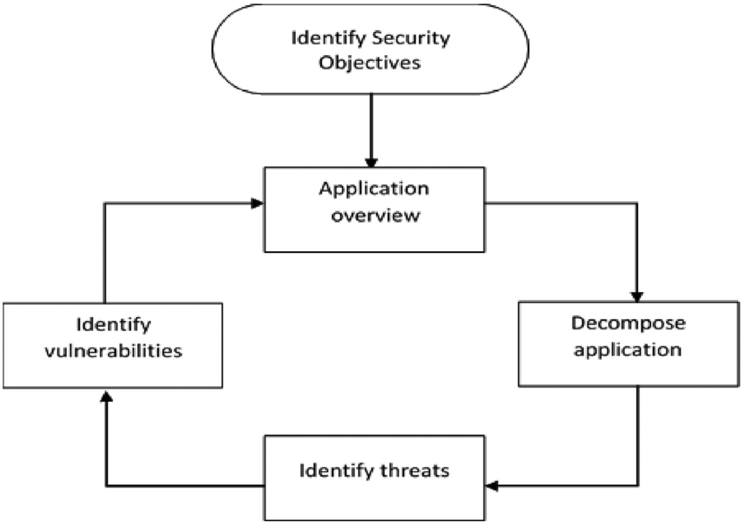


Fig. 3. The steps of threat modeling.

d) threats identification - threat analysis such as so called "STRIDE - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege", attack trees and a generic risk model;

e) vulnerabilities identification – reviewing the layers of application for searching weaknesses related to these threats and using vulnerability categories to focus on those areas where mistakes are most often made.

To adapt the model to specific needs, the key resources identified in threat modelling need to be updated as research progresses.

4 Conclusions

As mentioned above, a comprehensive analysis of the most up-to-date approaches to Cyber Threat investigations has been carried out by the team in order to solve the problem of creating criteria for selection of the most suitable Artificial Intelligence methods for the different phases of Cyber-Defense.

With the methods described above over 40 types of threats (some with several subspecies) were examined in terms of their evolution, level of impact and complexity, sophistication, availability, attribution, etc.

This analysis of the threats gives opportunity to evaluate possibility for potential attack pattern recognition and to develop models for active Cyber Defence. The process of modelling, experiments and selection of criteria is described on the official website of the project [11] and in published articles that are referenced on this website. In short, the results of this choice are formulated in the project as follows:

a) *basic criteria*: maximum performance (i.e. detection efficiency coupled with performance level) and a minimum percentage of false alarms;

b) *additional criteria*: flexibility for use in different environments; generic methodology; the processing speed needed to analyze the contents of packets to exclude lost packets.

The application of these criteria led to the following choice of Artificial Intelligence methods:

a) in the case of Tactical Cyber Intelligence - a network of Self-Learning Multi-Agent systems;

b) in the case of Operational Cyber Intelligence, the Echo State Network (ESN) method with Reservoir Computing for training;

c) in the case of Incident Handling - so called Reinforcement Learning.

Acknowledgments

This research is realized under the national science program "Information and Communication Technologies for common digital market in science, education and security" financed by Ministry of Education and Science in Bulgaria

References

1. NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessment September 2012
2. ISO/IEC TR 13335-1:1996 Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for IT Security
3. Threat Landscape Report 2016 ENISA, 2017
4. State of Cybersecurity An ISACA and RSA Conference Survey ISACA, 2016
5. TrustWave Global Security Report TrustWave, 2016
6. www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/ LM-White-Paper-Intel-Driven-Defense.pdf
7. Gaining the Advantage Applying Cyber Kill Chain Methodology to a Network Defense Lockheed Martin Corporation, 2013
8. ENISA Threat Taxonomy A tool for structuring threat information Version1.0 January 2016
9. Duggan, D. P., Thomas, S. R., Veitch, C. K., & Woodard, L. Categorizing Threat: Building and Using Generic Threat Matrix http://www.idart.sandia.gov/methodology/materials/Adversary_Modeling/SAND2007-5791.pdf
10. Shostack, A. Threat Modelling designed for security, John Wiley & Sons, Inc., 2014.
11. Project Web site https://npict.bg/
12. Dimitrov, V., Semantics of Vulnerabilities and Intelligent Search, Computer and Communications Engineering, Vol. 13, No. 2/2019, pp. 20-25, Workshop on Information Security 2019, 9th Balkan Conference in Informatics, 26-28 September 2019, Sofia, Bulgaria
13. Kaloyanova, K., Exploring Cybersecurity Curricula Designation Requirements, Computer and Communications Engineering, Vol. 13, No. 2/2019, pp. 64-68, WS on Information Security 2019, 9th Balkan Conference in Informatics, 26-28 September 2019, Sofia, Bulgaria