Journal of Computer Science

Original Research Paper

Advanced Persistent Threats Attribution-Extending MICTIC Framework

[1]Pedro Ramos Brandao, [2]Henrique São Mamede and [3]Miguel Pupo Correia

[1]Department of Computer Science, Instituto Superior de Tecnologias Avançadas-ISTEC, Portugal
[2]Department of Computer Science, INESC TEC, Universidade Aberta, Portugal
[3]Department of Computer Science, Instituto Superior Técnico, Universidade de Lisboa, Portugal

Article history
Received: 10-12-2023
Revised: 08-03-2024
Accepted: 28-03-2024

Corresponding Author:
Pedro Ramos Brandao
Department of Computer Science, Instituto Superior de Tecnologias Avançadas-ISTEC, Portugal
Email: pb@pbrandao.net

Abstract: This research is inserted in the context of cybersecurity and specifically in the attribution of Advanced Persistent Threats (APT). The investigation that gave rise to the article studies the MICTIC Framework, validating it and proposing an extension to facilitate the assignment of APTs. In this research, we present the motivation for this proposal and its validation. Also, the MICTIC is presented layer by layer and the extended version is submitted for validation through a survey of around 50 university professors and researchers. Due to the fact the MICTIC by itself has not been validated, we decided to do that in conjunction with the extension proposal. Attribution is very important because lets you know who promoted or who carried out an APT-type attack. On the other hand, just the fact that there are sophisticated Attribution mechanisms can act as a deterrent to future attacks. This research contributes to greater ease in obtaining the Assignment of APTs and consequently in understanding how this type of cybercrime works. so much so that there are few studies on the Assignment of APTs. This study objectively contributes to achieving the APT attribution by combining technological and non-technological techniques. It contributes to achieving computer security environments since an APT Attribution is a high deterrent to an APT group getting uncovered and an Attribution being assigned to it. Typically, cybercriminals who have been identified have stopped operating, whereas the opposite is not true; unidentified actors persist with attacks for a long time. Thus, this study also contributes to the overall maintenance of cybersecurity.

Keywords: Advanced Persistent Threat, MICTIC, APT Assignment, APT Attribution

Introduction

Cyber adversaries have moved from conventional cyber threats to advanced, complex, targeted, and well-coordinated attacks. These players started using Advanced Persistent Threat (APT) vectors to penetrate the networks of large corporate and classified organizations through various evasive cyber techniques (Hussain *et al*., 2020).

More recently, attacks have grown in sophistication, exhibiting "big target" and "long term" characteristics. These long-term attacks, sometimes sponsored by nation-state governments, are often referred to as Advanced Persistent Threats (APT) (Hussain *et al*., 2020). An APT consists of a combination of widely known and sophisticated techniques to reach a specific and precious goal and is not limited to being a sophisticated attack. Currently, no technology can ensure the blocking of an APT attack; more significantly, it is already too late by the time the attack is detected (Daly, 2009). New technologies applied to computer networks, such as virtualization and cloud computing, being of great value, present, on the other hand, an excellent challenge for their cybersecurity protection, both traditional and non-traditional, such as security regarding APTs (Hussain *et al*., 2020).

Protection from APT attacks is challenging, requiring techniques that combine technologies from different areas and, their effective integration.

Even more challenging is the attribution of the APTs, that is, knowing who requested and sponsored the APT. It

is a complex combination of operations, many of them non-technological, whose positive results are always challenging to obtain, as explained in the Introduction of this research work.

The purpose of this study provide a guide on how to implement adequate security in a segment of APT called attribution.

The proposed MICTI Framework with extension aims to facilitate the APT Attribution by adding two new layers; this framework has the particularity of mixing technological and non-technological systems to achieve the goal. As such, it is intended to scientifically develop this extension to present a more comprehensive solution to the APT attribution step. Therefore, this study and research have the primary purpose of contributing to the achievement of more straightforward APT attribution through the creation of two new layers in the MICTIC framework, as well as the technical and scientific validation of this framework.

This article is structured through the following topics, topic number two for the research background, where the issue of APT is considered, as well as the literature review, as well as the discussion of the problem under analysis; topic three explains the methodology used in the research; topic four refers directly to the framework extension proposal, layer by layer; topic five refers to the validation of the framework and results are analyzed; and finally, the conclusion.

An APT attacker, according to the National Institute of Standards and Technology (NIST) (NIST, 2024): (i) Repeatedly pursues its goals over a long period; (ii) Adapts to the efforts of defenders to resist; and (iii) Is committed to maintaining the necessary degree of interaction to achieve its goals. These goals are to exfiltrate information or to hinder or prevent critical elements of a program or mission via various attack vectors.

To achieve their objectives, attackers have to go through several steps of undetected attacks (Chen *et al*., 2018).

APT attacks are well-planned and highly organized, so the probability of the attack's success is increased. To be successful, attacks are carried out in several stages. To show how an APT attack is performed, we use the APT attack tree (Schneier, 1999).

Mandiant (2024), Mandiant discussed the life-cycle model of APT attacks, which consists of seven steps (i) Initial commitment, (ii) Establish support point, (iii) Escalate privileges, (iv) Internal reconnaissance, (v) Move laterally, (vi) Maintain presence and (vii) Mission Complete, where steps 3-6 can occur in any order. Ussath and colleagues (Ussath *et al*., 2016) have investigated a three-stage life cycle model of an APT attack, with a focus on only those characteristics that are representative of an APT attack. The authors discussed the following three stages: (i) Initial commitment, (ii) Lateral movement, and (iii) Command and control activity. Although all these attack models are similar as far as the operations involved in APT attacks are concerned, these are either very generalized or specific.

The systematic review of the literature was carried out according to the work and model of Barbara Kitchenham (Kitchenham *et al*., 2009).

In terms of research questions to be answered by the literature review, the following were defined, which we seek to answer with this systematic review:

- Q1: Are there any differences between an APT and a conventional cybersecurity attack?
- Q2: Is there any method to defend against APT?
- Q3: Does an Advanced Persistent Security (APS) have any importance for the defense against APT?
- Q4: Does the MICTIC Framework fit into the APT assignment? Can it be improved?

The following search phrase was obtained to be used in search engines.

("APT" OR "Advanced Persistent Threat" OR "cybersecurity" OR "cyber security" OR "internet security") and ("MICTIC" OR "APT" OR "attribution") AND ("attribution" OR "APT").

The search was carried out in the following databases:

- EBSCO (https://www.ebsco.com)
- IEEE XPLORE (https://ieeexplore.ieee.org)
- IEEE Xplore extended div (https://ieeexplore.ieee.org/), in this database, and for this particular search the search string was divided
- SCOPUS (http://www.scopus.com)
- Science@Direct (http://www.sciencedirect.com)

While carrying out the protocol, it was possible to conclude that there are few peer-reviewed articles about the Attribution of advanced persistent threats. In fact, no more than eight articles were found specifically on the APT Attribution, two of which were the fundamental motivation for developing this study, as explained in the introduction. Thus, it is extremely important for the present work to make use of documents considered ‘gray literature’. However, to guarantee the validity of the documents used, a selection and quality attribution method was followed. For the use of gray literature in this research work, we used the model proposed by Garousi *et al*. (2019).

According to the study by Garousi *et al*. (2019), the quality and consequent credibility of gray literature can be expressed in three layers, each of these “grey” layers represents a level of credibility. The first level of credibility is represented by layer one and the lowest level of credibility is represented by layer three. We can exemplify this terminological conception as follows:

a) Tier 1 (high credibility): Books, magazines, government reports, white papers
b) Tier 2 (moderate credibility): Annual reports, news articles, presentations, videos, etc.
c) Tier 3 (low credibility): Blogs, emails, Tweets, etc.

The following are the terminology components that the USAF has defined: (i) Advanced: The adversary is experienced with intrusion techniques and tools, capable of developing custom exploits, (ii) Persistent: The adversary has the intent to fulfill a purpose, take orders and attack particular targets, (iii) Threat: The adversary is motivated, coordinated and supported.

APTs pose a serious threat to private and public entities worldwide and will remain so in the future (Swisscom, 2019). These attacks represent an imminent menace, with the major issue being the challenge of early detection, as attackers employ a variety of strategies to remain undetected as long as possible and evade efficiently.

An APT differs significantly from an ordinary cyber attack-for instance, in the amount of resources of all types needed to execute the assault.

A typical cyber-attack can target entities or organizations with weak cybersecurity policies to steal client data or a company's financial activities (Chen *et al*., 2014). Such attacks are generally detectable and the harm is usually not critical. Nonetheless, an APT can focus on big organizations and industrial sectors and cause serious damage, such as stealing intellectual property, disrupting essential services, and destroying vital infrastructures. Such assaults are usually not detected and the resulting damage can be severe.

The number of reported cases of APTs has risen considerably in recent years (FireEye, 2014; Lemay *et al*., 2018); APT attackers' main objective is to remain undetected.

An APT constitutes a selective attack to obtain information or damage a government organization, a company, or an industry (Quintero-Bonilla and Martín Del Rey, 2020). Ever since Stuxnet (Falliere *et al*., 2011) emerged, APT attacks have become more careful and more harmful, demonstrating how easy it is to penetrate leading systems while evading most of the more advanced defense systems employed to safeguard the IT environment. Many of these attacks currently go undetected. Once detected, they appear again with modified features to reach their goal; FIN6, APT10, and APT41 (Quintero-Bonilla and Martín Del Rey, 2020) are all attacks that have resulted in substantial losses of money, intellectual property, and confidential data.

We can summarize the differences between APT attacks and conventional threats in a straightforward way, Table (1).

Jiageng uses the definition given by the National Institute of Standards and Technology; APT is defined as someone who has a high sophistication and specialization of potential resources, by which they can obtain opportunities for success through various attack possibilities, such as information infrastructure, data mining, organization, or reserve these possibilities for future attacks (Chen *et al.*, 2018).

Table 1: APT attacks and conventional threats

Feature	APT attacks	Typical malware attacks
Definition	An APT is a targeted, sophisticated and very organized attack. (e.g., Stuxnet)	Malware that is a malicious program used for attacking and disabling a system (e.g., ransomware)
Attack	Organized crime and government players' groups	A cracker (a hacker in illegal activities)
Target	Diplomatic organizations, the information technology industry and other sectors	Any personal or business computer
Purpose	Filter sensitive data or harm a specific target	Personal acknowledgment
Attack lifecycle	Keeps possible persistence using different mechanisms	Ends when detected by the security system (e.g., anti-virus software)

Ussath reports that the number of detected and disclosed APT campaigns has recently increased significantly. Most of these campaigns use sophisticated methods, tactics, and procedures to compromise their targets. Typically, the main goal of APT campaigns is to exfiltrate confidential data or intellectual property. Due to such attacks' sophistication, most security systems cannot detect or prevent these types of attacks (Ussath *et al*., 2016).

Also, according to this author Huang and Zhu (2020), timely detection of APT (i.e., before attackers reach the final stage) is effective (i.e., with a low rate of false alarms and missed detections) still an open problem due to its stealthy and deceptive characteristics. As reported in LLC (2018) (Huang and Zhu, 2020), US companies in 2018 took an average of 197 and 69 days to detect and contain a data breach. Stuxnet-type APT attacks can hide in a critical industrial system for years and quietly increase the probability of physical component failure (Huang and Zhu, 2020). Due to insufficient timely and effective detection systems for APT, the defender remains uncertain about the type of user, i.e., legitimate or adversarial, throughout the stages. To prepare for potential APT attacks, the defender must adopt precautions and proactive defense measures, which can also damage the user experience and reduce the usefulness of a legitimate user. Therefore, the defender must strategically balance the tradeoff between security and usability when the user's type remains private (Huang and Zhu, 2020).

Researchers (Alshamrani *et al*., 2019) state the following about APTS. Regarding APTs, "there is a different breed of attacks that have become increasingly prominent in recent decades" (Alshamrani *et al*., 2019). That class of attacks is characterized by the slow, lateral movement of a group of attackers to achieve their goal, which is usually to steal the target's data while remaining undetected (Alshamrani *et al*., 2019). APT attackers may use familiar methods to break into a network, yet the tools they use to penetrate that network are unfamiliar. As the term specifies, the tools used are advanced and have to be so for an attacker to stay on the network for extended

periods. APTs are usually executed by well-funded attackers, provided with the resources necessary to attack as long as the funding organization needs (Alshamrani *et al*., 2019). The attack only ceases when detected or the funding organization gets all the data it needs. In any case, the damage is always caused to the organization that has been the victim of an APT attack, sometimes irreparable damage, which is more common in the case where the attack has not been detected until the organization's data has been extracted (Alshamrani *et al*., 2019).

The term "APT" refers to attacks carried out by nation-states and is an adapted military term for the field of information security. APTs are often carried out by a team of highly skilled and well-funded attackers working for a government or organization with the aim of obtaining vital data about the target. An APT, as its name implies, does not represent a usual attack or an attack by an ordinary hacker (Alshamrani *et al*., 2019).

An APT attacker, according to the National Institute of Standards and Technology (NIST) (NIST, 2024): (i) Repeatedly pursues its goals over a long period; (ii) Adapts to the efforts of defenders to resist; and (iii) Is committed to maintaining the necessary degree of interaction to achieve its goals (NIST, 2024). These goals are to exfiltrate information and hinder or prevent mission-critical aspects of an organization or a company's business through various attack vectors (NIST, 2024).

To achieve their objectives, attackers have to go through several steps of undetected attacks. These various steps consist of creating backup points, scanning the internal network, and moving from one system to another laterally within the network in order to get to the target system and carry out their criminal activity. These various stages usually involve accessing a system on the network, then escalating privileges if needed to get to the victim system, then getting access to sensitive systems and transmitting status/info via an Internet connection to the attackers' command and control center. After the attack is complete, the attackers can choose either to stay and pursue their malicious attacks on other network systems or exit the system after the clean-up, based on the system after the clean-up, based on the requirements of the funding source.

The attacks are carried out in several stages and models to be successful. Attack methodologies change and may be in a separation of several vectors, such as digital and physical, which complicate whatever detection system is in place.

Criminal investigations are commonly deployed to investigate the culprits of traditional criminal acts. However, attribution is generally reserved for APT tracking, i.e., cyber espionage (Steffens, 2020). A crucial principle is that APT groups are directly integrated into intelligence agencies, or at least controlled by them. This is why the expression "state-sponsored attacks" has been popularized and is nowadays more or less used as a synonym for APT attacks (Pernet, 2014).

For many years, most of the statements of public attribution have originated from IT security companies - with differing degrees of objectivity on those attributions. Mandiant's APT1 report was one of the most specific, objective, and politically relevant, even naming individuals and concrete military units. In this case, the government's affiliation with the hackers was obvious. Several other reports also had names and even photos of individuals assumed to be likely perpetrators who worked for the military (Team, 2022). Other reports have limited their traceability to the countries of origin, avoiding objectively indicating the respective government (e.g., (Security Response, 2015; NIST, 2024). This, of course, is primarily a formal technicality of attribution since the assumption is that APT groups are state-sponsored. Another usual aspect of attribution cases is that many companies correlate attribution and specific languages used in APT-related artifacts (Drozhzhin, 2015). However, these particularities in the attribution may be complete and not effectively conducive to correct attribution.

On the other hand, for ethical reasons, some companies avoid naming individuals; others do not name governments for political or legal reasons. Attribution can be performed at different levels of detail-abstractly named individuals, organizations, countries, groups, etc.

Since 2016, government agencies have continuously increased the number of published attribution statements. In particular, the U.S. Department of Justice has unsealed a significant number of charges against Russian, Chinese, Iranian, and North Korean hackers (Nickels, 2019).

The primary difference between attribution by IT security companies and attribution by governments is usually emphasized in public discourse, giving a political connotation, as a rule, to the former. While that may be true, there are at least three obvious methodological differences. Firstly, official statements and indictments deal with particular attacks or incidents, while industry attribution focuses on APT groups and their activities over more extended periods. Secondly, indictments must specify legal entities, although official declarations generally specify a foreign government for political purposes. At the same time, security company reports carry different designations and may be restricted to the granularity of a home country. Finally, official attribution frequently depends on intelligence agency data which cannot be published. Security companies, on the other hand, often clearly indicate their sources and techniques to increase that same transparency and confidence in their attribution and assessments (Pernet, 2014).

Attribution can also be a deterrent mechanism. Computer espionage and specifically APTs, offered states a good risk-benefit ratio. Investing a few million dollars in developing APT tools could be more promising for developing and emerging countries than lengthy and expensive research projects. Stealing technical knowledge

could tremendously boost a nation's development plans. Considering this opportunity, it is not surprising that, according to reports from security firms, several APT groups have been assigned to India, Pakistan, Iran, North Korea, and China (Kopan, 2015).

Plausible denial capability could and can dramatically reduce the reserves against placing implants to sabotage critical infrastructure such as power and telecommunications networks in peacetime. In case of a conflict, these statically placed implants can be used for coercion or even cause considerable harm to the opponent. Therefore, the ability to assign a state before that, the capability of detecting implants before they are employed for sabotage a key impediment. This is why attribution is so important (Kopan, 2015). Without attribution, APT would be a low-risk tool.

Attribution is efficient despite the fact that governments do not employ hackers but recruit cyber mercenaries as agents. The US White House imposed sanctions not only on Russian intelligence agencies and GRU officials but also on two persons after the hacking and leaking attacks on the Democratic National Committee (DNC) (House, 2016). The two persons were not linked explicitly to the Russian government, but imposing sanctions on them could be considered as a means of attacking the hacker market. If a hacker has to contemplate the possibility of being identified, punished, denied entry to certain countries, or even the subject of an international arrest warrant, his or her will to take part in cyber-attacks is likely to decrease (House, 2016). Lastly, attribution can also have an impact on public opinion. During the 2016 and 2017 US and French election campaigns, emails and documents from politicians were stolen and published by hackers. These thefts led to the resignation of DNC Chair Debbie Wasserman Schultz in the United States but had no significant effect on the campaign in France. If attribution can help show that hackers are not altruistic actors but rather imbued with a criminal strategy, then attribution plays a key role here (Kopan, 2015).

Materials and Methods

The scientific research methodology employed is Design Science Research (DSR) (Wikipedia, 2022).

It is in the DSR methodology that we find the appropriate foundations for the development of the artifacts of this research as the ideal means to produce scientific knowledge, mainly in the epistemological aspect and the framework derived from the work-" The Science of the Artificial"-by Herbert Simon (Wikipedia, 2022), with the adaptations and proposals of (Peffers, 2022). As we know and as referred to by Peffers, the notion of artifact is not restricted to physical objects; it can be something designed abstractly, even an artificiality, that is, abstractions can also be artifacts (Peffers, 2022); in this context, the artifact to be developed in this research and through this scientific method is mainly a framework, that is, a conceptual guide that will support and guide the research objectives.

The method-Design Science Research Methodology-(DSRM) proposed by Peffers *et al*. (2007); Hill (2002) will be followed, through the following steps: (1) Problem definition, (2) Literature review, (3) Presentation of possible solutions, (4) Development, (5) Evaluation, (6) Best solution option, (7) Reflection and learning and (8) Presentation of results. In this research work, we will always bear in mind the model suggested by Peffers in Fig. (1).

DSR commits to two main goals in this study context: First, to solve a practical problem in a high-specificity context through an artifact; on the other hand, to generate new scientific knowledge. There will be two related research cycles in the DSR: One about the design of the artifact, which can be called the "design cycle" (Peffers, 2022), where the purpose is to design the artifact to solve the main goal (the MICTIC framework with extension); the other can be called the "knowledge cycle" (Peffers, 2022), which focuses on the elaboration of conjectural theories related to the human (significantly important in the primary purpose of our study) and organizational aspects.

A global model will be proposed where the MICTIC framework will be inserted with the extension (the MICTIC Framework serves to assign an APT, it had already been mentioned by an author (Steffens, 2020) but has never been scientifically validated, in this study is developed, added new layers and scientifically validated), allowing the attribution engine-or simply attribution must be considered to work better; in this case, directly related to the first layer of the aforementioned framework extension, that is, with the analysis of the general behavior of a sample of a system.

In the background, the second layer of the framework extension will be developed, which is everything related to social engineering. An admittedly complex a priori vector that requires the most objective possible configuration, as well as the establishment of relationships and correlations between artifacts and behaviors in a system where numerous actors can already be considered and where an APT incident is expected to occur.

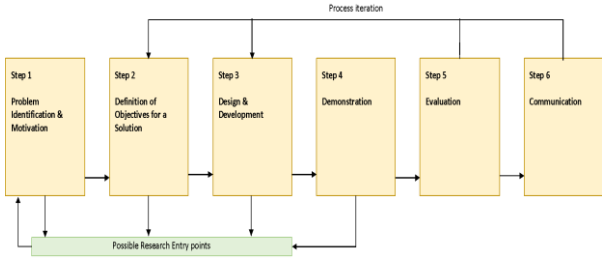

Fig. 1: The Design Science Research Methodology (DSRM) (Adapted from (Peffers *et al*., 2007))

In the second part of the framework extension work, multiple scenarios and multiple components are considered and the issue of social engineering requires the analysis of all possible components involved in a process related to an APT and not exclusively the attribution.

With regard to the qualitative aspect, refers to the development in abstract terms of the two layers of the MICTIC Framework, where there is a direct and dynamic relationship between the objects of study and the real world. The same applies to the conceptualization of the entire APT attribution process, where the interpretation of phenomena and the attribution of meaning are basic in the qualitative research process. The data analysis to be developed will be primarily inductive.

Based on the existing literature, the objective is to conceptually develop two more layers at the level of one of the most recognized frameworks for obtaining APT attribution, on the other hand, these two artifacts will be inserted in a larger model whose objective is the defense and mitigation against APT.

After this conceptualization and contextualization in an anti-APT model with Attribution, the entire model will move to a qualitative analysis phase.

The proposal will be validated with an anonymous survey, to be responded to by a universe of 50 experts.

Framework Extension Proposal

Attribution is a very particular case in the realm of cybersecurity and APTs (Kopan, 2015). Its analysis is not exclusively technological. This is because it makes use of other non-technological systems such as: The analysis of facts (data related to the event, such as the time it took place, code syntax, i.e. the way the code is written, hypothetical motivations, social context of the target, etc.); social engineering (vulnerabilities caused by humans, both inside and outside, behavior analysis, obtaining privileged information about users from third parties, level of security culture on the part of users, relationship of users with other entities and companies, etc.); espionage (it may be necessary to use espionage methods to obtain data about the attackers, i.e., involve intelligence agencies to get facts and data confirmations); specific reasoning in relation to facts (correlation of data and cross-referencing of data, such as possible geolocation of the origin of attacks, similarity of the attack with other attacks, comparison of the tools used in the attack with other tools already used, checking whether there are attacks that have used the same tools, etc.). Thus, Attribution results from using a very complex mix of systems. Moreover, as such, it must be addressed in a specific and detailed way. The sum of all the analysis systems may allow the correct attribution of an APT to be achieved.

Another one is that this is done intentionally and not by accident. These assumptions substantially impact the following explanation: Someone wants to speak to me.

Keep in mind that without premises, it would usually not be possible to find any likely explanation. The premises are essential to abductive reasoning, so they must be true!

Although attribution services are provided by various security companies, government agencies, and non-governmental organizations, no public framework defining the technical process for attribution has yet been established. Agencies and companies may have their internal processes in place, although they have not yet published them. Thomas rid and ben Buchanan's Q model (Rid and Buchanan, 2015), which is heavily focused on political concerns and whether the results of the allocation are to be published, only broadly addresses the technical process to achieve these results.

We do not intend to present a universally valid framework for technical attribution. Yet, for this study's purposes, a framework helps define a common thread that maintains the possibility of attribution. For this purpose, the MICTIC framework and its extension are introduced.

The MICTIC framework has never been published in scientific journals and has never been scientifically verified and validated and we intend to do so within this research. Even at the level of published papers on the subject, we only found one by Brandao (2021), an article with scientific supervision highlighting this framework's importance, proposing the hypothetical advantage of extending it.

This framework is based on the general idea that cyber espionage and sabotage are composed of many distinct components. These components are not phasing as in the cyber chain; rather they are artifacts, activities, and resources of an APT group. The MICTIC acronym comprises the names of the components: Malware, Infrastructure, Control Servers, Telemetry, Intelligence and Cui bono. In a sense, it represents a slimmer form of the Diamond model (Rid and Buchanan, 2015), adjusted to match the specific fields of specialization of Infosec analysts, whilst at the same time following the supposed separation of tasks inside APT groups. Each aspect of MICTIC determines a type or source of valuable information for attribution. Frequently, this translates into duties that can be assigned to either members or sub-teams of an APT group in Table (2).

Table 2: Extended framework mystic

	Aspect	Example
M	Malware	Timestamps, language settings, chains
I	Infrastructure	WHOIS data links to private websites
C	Control server	Hard disk logs or source code
T	Telemetry	source IPs, working hours and malware generation
I	Intelligence	Intercepted communication
C	Cui bono	Geopolitical analysis of strategic motivation
A	Social acceptance	Through incentives
C	International cooperation	Sharing of information on APT identification

The malware component consists of developing and configuring exploits, trojans, and backdoors. This is the duty of the developers on the attacker's side, while malware analysts and inversion engineers are involved on the Infosec side.

The infrastructure includes the rental and operation of servers that are used for malicious code download and data exfiltration. Numerous APT groups are said to have devoted members who look after the infrastructure. In terms of analysis, this is mirrored by researchers tracking and monitoring C and Cs through publicly accessible services. The individual servers and the artifacts that can be found therein constitute the control server aspect. These are the primary resources employed by the operators carrying out actual cyber espionage operations. Telemetry consists of data on the (mainly manual) activities of operators within a target network, which can be analyzed by security firms. Additional sources are available to government agencies and form part of the 'intelligence' component. Lastly, the cui bono aspect refers to the task that the group state sponsors-usually a non-technical department-request. This aspect is covered in the INFOSEC community by the geopolitical analysis according to which the strategic motivations of the country are aligned with the perceived attack activity.

The following topics embody these components (but not necessarily in that particular order) and describe what evidence can be found in each, thus characterizing and defining our framework for attribution.

It should be noted that all the phases of attribution mentioned above involve these components. While the stages structure the process of attribution regarding the sequence of analysis steps, the extended MICTIC framework can be used to ensure that all aspects of a cyber activity are covered and is also helpful for defining work packages for a team of analysts. For instance, for data collection in phase 1, reverse engineers can focus on the malware aspect. At the same time, liaison officers can use law enforcement to seize control servers and policy analysts can focus on the cui bono aspect.

The attribution process should cover as many MICTIC extended aspects as possible. The more aspects the evidence comes from, i.e., the more evidence proven, the more confidence it provides for the attribution hypothesis.

The aspects have no temporal or causal order; instead, they run parallel. They require different skills and resources. Therefore, they can even be operated by different sub-teams of an APT group. In this regard, a framework is a helpful tool for defining the monolithic or self-restraint of an intrusion set or APT group (technically defined). As we will later see, some cyber-attacks can be linked to multiple actors of varying relations. In certain assaults, malware may be acquired from a freelancer by a government agency and then given to a different contractor so that he or she can utilize it to target a particular group of companies. The usage of Winnti malware is possible in such a scenario. The Chinese Ministry of State Security (MSS), according to a US Justice Department indictment, allegedly recruited hackers to utilize Winnti against businesses in order to steal intellectual property related to turbines (York, 2022). If the usage of this malware were the only factor grouping cyberattacks, then assaults on online gaming sites with a financial motivation would also be included in the intrusion set. This intrusion set would be on the basis of a single component (malware). In framework terminology, this set is denominated in the MICTIC-1 intrusion set. If now the difference in motivation espionage versus crime is employed to divide the attacks, two distinct sets of intrusions are identified, every MICTIC-2 (using cui bono and malware). Further refinement of the analysis can be done, for instance, by looking at differences in manual activity as covered in the telemetry component. According to FireEye, this results in a reasonably well-defined set of intrusions or APT groups, at least MICTIC-3 such as APT41 (Williams, 2016).

The number of aspects covered by a set of intrusions is therefore, at least for the purposes of this book, a rough indicator of the degree of definition of a group. The MICTIC (Steffens, 2020) level also indicates the confidence that the internal configuration, the separation of work, from the group has been perceived. For instance, the definition of a group using Winnti alone doesn't tell you much about its internal configuration. Moreover, the differentiation of motivation results in the hypothesis of parallel operations, or even parallel players. The definition of manual TTPs suggests that the group's day-to-day operations have been understood and described. All layers of the framework MICTIC can be consulted in Steffens's book (Steffens, 2020).

In one of the later topics, extended MICTIC will be used to evaluate the probability of an assumption being based on false alarms. The overall idea is that a hypothesis is more resilient against identifiable attacks the more aspects are involved in the analysis. This is based on the assumption that continuously planting false flags in several aspects needs more work than doing so in a single aspect alone and may call for cooperation between numerous sub-teams.

Along the same line, when reporting the results of the attribution, the number of extended MICTIC aspects covered forms part of the assessment of confidence in the results.

MICTIC Extension Aspect S-Social Acceptance through Incentives

Rational actors behave according to incentives. Today's internet lacks an incentive structure to encourage positive forms of attribution and discourage negative forms of attribution. Positive forms of attribution include methods to identify those responsible for the malicious behavior during and after the act. Negative forms of attribution include attempts to discover the identity of those involved in non-malicious exchanges.

Today's Internet has very few incentives to discourage crime and malicious behavior: The rewards for malicious behavior are high, while the risk of getting caught and getting an attribution is low. Neither are there incentives for users to adopt attribution as something necessary to change the reward structure in favor of non-malicious actions.

The attribution value is not understood by an average user. Most people are told that non-attribution (anonymity, privacy, and repudiation) is what the Internet is all about. This pervasive concept is certainly the key to the free exchange of ideas as well as malicious behavior.

Attribution can be used as a tool to create positive and negative incentives, increasing value for the average user and promoting growth in individual, business, and government use:

- Individuals must find value in reliable financial and business transactions and develop confidence that fraud and theft can be detected, attributed, and prosecuted
- Businesses must have policies, and legal and technical methods in place in a significant amount to manage the risk associated with malicious activities on the Internet that disrupt commercial interests. This would indicate the existence of relatively mature risk models and would allow companies to better manage the risk and, consequently, achieve the attribution more easily
- Governments increasingly depend on Information Technology (IT) and the Internet for routine and emergency operations. For many governments, Internet technologies serve as the backbone for intragovernmental communications, financial transactions, policy announcements, public relations, and emergency operations. They should also have a significant interest in having a mindset on the part of employees regarding the attention to be given to anomalies in the systems that may indicate cybercrime and immediately reporting these occurrences, which consequently would also facilitate the attribution

The significance of the global information infrastructure dictates the need to develop incentives for parties to adopt value-added methods. More importantly, we believed it was essential to start communicating the value of attribution to gain broad understanding and acceptance.

The key to creating positive incentives for Internet users to participate in promoting and attributing and eventually demanding, attribution of online actions is to identify a set of online activities where something of value to the user is at risk.

Examples of such activities may include online banking, online tax preparation, online medical services, and administration of personal information. To illustrate one possible approach, we'll use online banking as an example.

A logical overlay can be built on the internet that allows assignment between a set of customers of an online bank. That is, all significant actions performed by any of the users who choose to be part of the attribution overlay are entirely attributable to that user. This creates an online setting where users are increasingly responsible for the actions they perform. For applications in which transaction accuracy is expected, well-meaning users will find value in a system where online actions can be attributed to a valid user. On the other hand, malicious actions performed by a non-member of the attribution override may not always be attributed to the offender, but the attribution override can make an investigation easier by providing evidence that the action was performed outside the community of members, protecting the user from transactions fraudulent. Additionally, if a user in the assignment overlay repudiates an assigned action, that user's computer can be detached from the assignment overlay and checked for possible compromise.

Defense against Internet threats coming from outside the attribution overlay improved transactional accuracy, and protection of computers within the attribution overlay are all provided to users by the attribution overlay.

The concept of overlapping attribution does not protect from all types of exploitation, however, it constitutes a step in the correct direction. As is generally the case with security services, the implementation will unavoidably introduce unforeseen complexity and vulnerability and therefore will require continual improvement.

One potential implementation of an assignment override is based on a Root of Trust (RoT) provided to individual users through an assignment group administration process. The RoT is in charge of the authentication of the origin of incoming messages and the sealing of the attribution data of outgoing messages through a digital signature technique. Attribution data should include the machine, user, context, and content of the message, as well as the expected destination. Attribution data can also include source routing data, geolocation, a secure two-way handshake, and required responses. To prevent the system from being compromised, the unique keys used to authenticate and seal attribution data should be well protected in a hardware device, such as a smart card or Trusted Platform Module (TPM), that can serve as a RoT.

The goal of this approach is to make the exploitation of the system by a malicious actor using only software more difficult. Outgoing messages that need to be attributed can be submitted to the smart card or TPM for verification of the format of the message and digital signature completion. Incoming messages can be submitted to the TPM or smart card for confirmation of their origin, enabling each system to verify that all messages are from the assignment overlay network prior to their processing. It should be noted that this implementation will enable participants in the assignment overlay to limit the processing of messages to only those messages originating in the assignment overlay. Additionally, it will allow staff responsible for operational security to identify whether a compromise comes from the

assignment overlay or from an external source. Such a simple determination can contribute to protecting members from overlapping attribution of certain fraud classes. On the other hand, in a sense, it creates an automatic mechanism to get the assignment if there is an APT attack that affects this overlapping group.

Besides the use of a RoT at each endpoint, there may be value in embedding the trust system at several network points. Through a similar attribution procedure, these extra points of confidence may attest to the presence of messages on the network at different periods, giving investigators the right information and complete trust in that information. This would be comparable to how physical investigators work, who frequently use recording equipment: Cameras at ATMs, traffic cameras, credit card records, electronic collectors, and Dynamic Host Configuration Protocol (DHCP) data.

Any overlapping assignment should be accompanied by a process for registering and revoking users. There are numerous approximate solutions for the management of public key infrastructures that can form the basis of an assignment override. As new identity management methods are implemented, the attribution override can benefit from them. While the concept of overlapping attribution has several issues in common with the management of digital identity, overlapping attribution has one major advantage: Uniform control. That is, the attribution overlay can be built by a sole entity, such as a bank, and administered according to policy wholly managed by the same entity. Many banks and online service suppliers can build logical assignment overlays using this paradigm. Users have the option of joining numerous assignment overlays, which makes each user responsible for all actions relating to that service supplier. It should be noted that it is also feasible to employ overlay technology to build a network not attributable to simply exchanging ideas freely.

Traditional attempts to create a network overlay require all users to participate fully in the network overlay and believe that it helps with attribution in the event of an attack and have built-in the idea that attribution matters, which of course is linked to a culture of safety in organizations.

The approach suggested above does not require full participation and is aimed at gaining continued acceptance of attribution services by communicating and providing value to a specific community. For example, an online financial services provider might offer value to customers who choose to join the attribution network in the form of account insurance.

That is, this layer of the model is based on the cooperation of users of an organization's network and on training employees or customers that attention to attribution is important.

MICTIC Extension Aspect IC-International Cooperation

With many cyber-attacks traversing multiple jurisdictions and the growing need for fast and accurate attribution capabilities, there is a need for technical cooperation that far exceeds existing in-principle agreements. Such cooperation may indeed be in its infancy in the Computer Emergency Response Teams (CERTs) system development and, while directly beneficial in providing enhanced attribution, would be of great value to cybersecurity in general.

This multi-stakeholder technical research, engineering, and consulting capability would fill some important gaps through:

- Research and recommendation of the best attribution techniques
- Providing ongoing support for a multilateral allocation capability
- Providing continuous awareness and training so that teams around the world cooperate in incident response as well as investigations
- Making suggestions for the improvement of protocol and the development of standards to meet the demands of member countries for the tracking of attackers to international engineering bodies (such as the IETF)
- Interacting with those developing cybercrime policy and legislation to make sure that non-technical and technical methods are complementary and mutually supportive
- Help ensure interoperability of attribution infrastructures and technologies used by collaborating entities
- Evaluating the outcomes of the cooperation that has already been implemented by the technical bodies and law enforcement agencies with the aim of providing feedback for continuous improvement
- Ideally, such cooperation would involve information sharing and cooperation on
- Vulnerability information
- Incident data
- New methodologies and techniques for attribution and tracking, including hardware and software tools
- Best practices
- Intelligence on the latest hacking capabilities and trends (including means to prevent attempts to establish attribution)

Other desirable features of a technical cooperation system include:

- Stability and continuity of the technical team to develop and maintain world-class experience, mainly due to the fact that technical information about attacker-defender resources and other technologies

has a very short shelf life. Informal cooperation will likely be inappropriate in this regard
- A worldwide incident response capability (a multilateral incident response team). Such a team would be fully involved in daily operations of incident response, possibly raising issues of jurisdiction or control from the perspective of individual nation-states or other participating entities

To achieve these TPA allocation objectives there is a need to formalize the collaboration and cooperation needed to provide allocation across national, jurisdictional, and administrative borders. This formalized structure should consider:

- The organizations covered by the framework. It may be natural to think of policy structures as lying between nation-states, but questions of entitlement involve the interests of corporations and other organizations as well as nation-states
- The amount of information to be collected. Technological issues may limit the amount of information collected to aid attribution, but policy choices need to be clarified as to the circumstances under which tracking data may be collected, retained, and used
- The amount of information to be shared, including the speed with which the information will be shared (a significantly important aspect because the information must be shared as quickly as possible, to cross-check data to be capable of making the attribution) and the equipment and processes to be employed. This will become increasingly important as attribution processes are automated. Policy choices regarding the extent of information sharing will need to be incorporated into technical approaches. Likewise, the ephemeral nature of evidence in cyberspace makes rapid response essential; therefore, an effective policy framework will need to incorporate elements of a multilateral technical assistance function
- Period of retention of data that can be employed to track evidence of an APT that is a crime, treaty violation, or other offense. There has, for example, been a lot of worry that the Cybercrime Convention defines too broadly the tracking data that can be collected by Internet service providers, posing a threat to privacy
- Types of incidents for which information will be shared; for example, an instance (which occurred during the release of the "I Love You" virus) where the act is a crime in a victim's country but not in the country of origin
- Extraterritorial evidentiary seizure. An agreement should be proposed that allows for the extraterritorial electronic seizure of data necessary to establish attribution, but under explicitly defined conditions, and circumstances and with safeguards that will help prevent abuse. This may include placing evidence in escrow until the appropriate legal authorities are provided for its access; if these are not provided, evidence may be destroyed or access withheld
- Appropriate ranges of responses to an attack once the assignment has been established. While this issue may seem to be outside the scope of the attribution problem, the appropriate attribution, as discussed earlier, depends on the possible range of responses. Conflicts can arise if, for example, Party A can use evidence of attribution as a basis for actions that Party B, which has information essential to the attribution, considers inappropriate. The response interval also needs to consider the deadline. Extraterritorial retaliatory or defensive action by the target of a cyber-attack may be justified (by, among other things, the UN Charter's Article 51, which confirms the inherent right of a nation to self-defense) while a cyber-attack is ongoing. When an attack appears to be over, it is less clear how to respond; the severity of the attack, the risk of further attacks, and other considerations are important. These are issues for which a pre-existing framework would be of value
- Cost-sharing agreements. Maintaining resources for proper attribution is not free, nor are special actions required to provide attribution for a specific event
- Procedures for dealing with non-participants in the policy framework and with unreliable jurisdictions. The Cybercrime Convention is not a global agreement, nor is any policy framework for assignment likely to include all relevant entities. Non-participation or unreliable entities obviously make attribution difficult; there may be a need for a process to reach mutually agreed understandings (by participants in the proposed policy framework) on what constitutes proper attribution based on information from unreliable sources
- Adjudication in case of erroneous assignment. Errors can occur; actions taken to respond to cyberattacks attributed to a particular source may later prove to be based on incorrect assessments. An established process is needed to deal with this matter; there exist several international procedures for resolving disputes, so it may not be necessary to create new institutions. The key point is that these procedures must be worked out in advance

Attribution is necessary to properly handle malicious activity on the Internet, regardless of the nature of that activity, particularly the most sophisticated APT attacks. The required focus and confidence of the attribution depends on the severity of the malicious activity and the parties involved or affected. Sufficient allocation can be achieved through a series of gradual steps, but it cannot be

achieved simply by introducing new technologies or policies. Attribution requires a system of acceptance, cooperation, technology, and traditional research supported by specific policies, laws treaties, and methodologies, being the result of the sum of all of these.

Designing such a system is complicated by indecision over what constitutes malicious Internet activity, the tension between necessary attribution and non-necessary attribution, and the fact that there must be widespread international participation in any useful implementation of attribution.

A key step in developing an attribution system is gaining user acceptance and awareness. Well-meaning parties must be encouraged, through incentives, to accept and value the assignment, so that they can collaborate around whatever system we can create. For an attribution system to work, good citizenship must be the norm and an incentive structure must reinforce desirable behavior. While attribution is necessary to discourage and punish malicious behavior, selective non-attribution is a critical feature of the Internet and must be preserved and even strengthened to facilitate the free exchange of ideas and protect individuals from oppressive regimes.

As developed countries have become highly dependent on the Internet for business and government operations, Internet infrastructure has become the target of military-style attacks. Perhaps the biggest challenge for an attribution system is identifying nation-states that choose to engage in cyber warfare-like activities, as these unreliable parties have no interest in supporting effective attribution. This challenge can only be overcome through a comprehensive approach, such as the system that is adopted for global nuclear non-proliferation, which develops technical and non-technical multilateral approaches in an environment of mutual distrust.

Attribution is a complex issue and investment structuring is a significant challenge. Designing and implementing a working attribution system will require continual refinement, balancing many social, political, and technical requirements.

As we have already mentioned, APT Assignment is a slow discipline and can only provide step-by-step information, being the result of a complex sum of techniques and procedures, both technological and non-technological.

Validation

In this section, we present the validation work that has been accomplished. The validation is achieved using a survey.

This survey aims to carry out the technical and scientific validation of the Framework and its extension. The questions were prepared in such a way as not to allow misunderstandings and to form a heterogeneous and objective body on the validation of the artifact. All questions in this survey were validated in the Pre-Test.

We followed a two-step approach for the survey, as illustrated by Fig. (2).

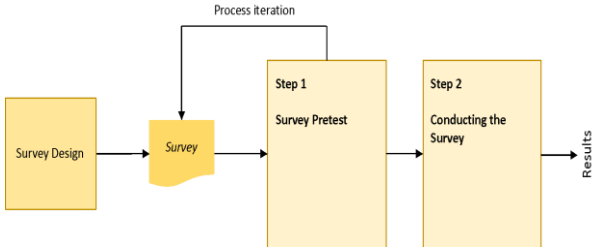

Fig. 2: Using the survey for validation

Table 3: Question areas for proposal validation

Analysis vector	Description
Relevance	To what extent is the proposed framework relevant and/or important
Utility	The proposed framework will be useful
Completeness	Classifying the framework in terms of completeness
Generic	Any other comments on the proposed framework

The survey questions were elaborated following the principle of enabling the validation of the survey. The objective was to find out if the pairs agreed that the questions would allow, in the end, to obtain a reliable result of a validation, or not. Thus, the questions are limited to the intrinsic aspect of the validation survey questions. It was also intended to know if the questions were sufficiently objective to be able to use the binary method.

The questions were prepared in such a way as to result in an opinion of each of the layers of the Framework and result in a global perspective of its viability.

After defining the survey, it has been pre-tested and the results of that step would have to be reflected on the survey. After that, it is pretested again until it is considered to be ok. In such cases, step 2 is performed, conducting the survey and getting the results.

Survey Design

For the design of the survey, we considered six analysis vectors, as listed in Table (3).

Based on those analysis areas, the following questions have been designed:

- Question 1: Do you know what an Advanced Persistent Threat (APT) is?
  Question one is intended to find out if the respondents know the concept of APT because if they do not know the concept, they could not answer the following questions. On the other hand, it also aims to establish a proportionality perspective of the lack of knowledge of this type of attack by respondents who work in one way or another in the area of information sciences
- Question 2: Do you know what the APT Attribution phase is?

It is intended to ascertain whether the respondents who knew the meaning of APT knew one of its phases, in this case, the attribution

- Question 3: Is the information submitted regarding the MICTIC extended framework clear and sufficient to draw conclusions about it?
  This question ensures that the material sent for analysis allows conclusions to be drawn objectively. That is, the information submitted was sufficiently complete and unambiguous for analysis
- Question 4: Do you agree with the analysis carried out on layer 1 of the framework: Malware analysis?
  Layer 1 of the Framework reports to malware analysis, as described in section 5.3. It is intended with this question to validate the options presented for how malware should be analyzed to draw some conclusions on attribution
- Question 5: Do you agree with the analysis carried out on layer 2 of the framework: Attack infrastructure?
  It aims at validating the options presented for layer 2 of the Framework, i.e., the Attack Infrastructure was presented from the attacker's perspective, public information and tools, and active tracking, all as ways to integrate an attribution analysis
- Question 6: Do you agree with the analysis carried out on layer 3 of the framework: Control server analysis?
  This question is about the operation and analysis of control servers used by attackers and the ways to analyze them. Whenever possible, the analysis of these servers may allow a conclusive approximation of the attack's attribution
- Question 7: Do you agree with the analysis carried out on layer 4 of the framework: Telemetry?
  This question refers to the proposed existence of a layer intended for telemetry analysis to consolidate data obtained in analysis and add it to the remaining data from the other layers allowing the attribution
- Question 8: Do you agree with the analysis on layer 5 of the Intelligence framework?
  Question 8 refers to the role of intelligence and espionage services. Valuing this type of information acquisition's key role for attribution and in many cases, it is one of the main tools for attribution
- Question 9: Do you agree with the analysis done on layer 6 of the framework (framework extension): Social acceptance through incentives?
  As for social acceptance through incentives, since these are a set of tools of subjective character, they could bring some uncertainties. This part was already part of the MICTIC framework extension
- Question 10: Do you agree with the analysis done on layer 7 of the framework (framework extension): international cooperation?
  Regarding the proposal of an extra layer, it is proposed to use integrated international cooperation to obtain information to create a model that can build the attribution of an APT attack
- Question 11: To achieve an APT Attribution, do you consider adding the two layers of the MICTIC framework extension relevant?
  It is intended to know if the respondents consider it important to create two extra layers in the MICTIC Framework to achieve the attribution more easily
- Question 12: Do you consider the extended MICTIC Framework and how it was built/presented a critical tool to achieve an APT attribution?
  It is unambiguously intended to know whether or not the extent of the framework is significant for an APT attribution
- Question 13: Do you consider this study on APT Attribution scientifically relevant?
  This question is intended to provide an overall opinion on the entire development of the framework with its extent and scientific validity
- Question 14: Do you consider this study on the APT Attribution relevant in social and political terms?
  This is a more subjective question, as are, in fact, many attribution questions about whether the work is considered relevant in social and political terms. That is because questions of attribution can raise many political issues, even diplomatic problems between countries
- Question 15: Generally, do you consider the Framework with all the proposed layers well designed?
  This is also a final global issue. It is also intended to obtain an overall opinion on all the work presented, including whether the proposal is well structured in terms of architecture

These questions were drawn up with the principle of enabling validation of the survey. The aim was to determine whether the peers agreed that the questions would allow a reliable validation result to be obtained in the end. It was also intended to find out whether the questions were sufficiently objective to be able to use the binary method. Thus, the questions were limited to the intrinsic aspect of the validation survey questions.

In Table (4), the survey questions are listed, with an indication of the analysis vector they correspond to.

Survey Pre-Test

The pre-test for the Framework validation survey and respective extension was prepared according to the good practices recommended by Ruel *et al*. (2016); Hill (2002). Following the recommendations, they provide, the questions that were used are presented in Table (5).

The characterization of the respondents of the pretest is presented in Table (6). For this pretest of the survey, a

group of 10 individuals (these ten individuals were all PhDs in computer science, higher education professors, and all had over 20 years of professional experience) was also conducted to validate the clarity and scientific objectivity of the questions applied in the main survey.

All respondents answered 'yes' to all the pretest questions. So, it was possible to conclude that the survey was valid and appropriate.

Conducting the Survey

Having validated the survey and following the steps considered appropriate in this approach, we carried out the survey. It has been carried out among 53 individuals, all with a PhD in the field of information technology.

Table (7) characterizes the universe of respondents in the framework validation survey with extension.

Table 4: Survey questions

Question no.	Analysis vector	Question
Q1	Generic	Do you know what an Advanced Persistent Threat (APT) is?
Q2	Utility	Do you know what the APT Attribution phase is?
Q3	Completeness	Is the information submitted regarding the MICTIC extended framework clear and sufficient to draw conclusions about it?
Q4	Relevance	Do you agree with the analysis carried out on layer 1 of the framework: Malware analysis?
Q5	Relevance	Do you agree with the analysis carried out on layer 2 of the framework: Attack infrastructure?
Q6	Relevance	Do you agree with the analysis carried out on layer 3 of the framework: Control server analysis?
Q7	Relevance	Do you agree with the analysis carried out on layer 4 of the Framework: Telemetry?
Q8	Relevance	Do you agree with the analysis on layer 5 of the intelligence framework?
Q9	Relevance	Do you agree with the analysis done on layer 6 of the framework (framework extension): Social Acceptance through Incentives?
Q10	Relevance	Do you agree with the analysis done on layer 7 of the framework (framework extension): International Cooperation?
Q11	Relevance	To achieve an APT Attribution, do you consider adding the two layers of the MICTIC Is framework extension relevant?
Q12	Completeness/utility	Do you consider the extended MICTIC Framework and how it was built/presented a critical tool to achieve an APT Attribution?
Q13	Relevance	Do you consider the proposal on APT Attribution scientifically relevant?
Q14	Relevance	Do you consider the proposal on the APT Attribution relevant in social and political terms?
Q15	Utility/completeness	In general, do you consider the Framework with all the proposed layers well designed?

Table 5: Pretest questions

Question no.	Question
Q1	Was the information submitted on the framework sufficient to be analyzed in a way that could be evaluated??
Q2	The Framework information sent was clear and objective
Q3	Is the number of questions sufficient to conclude on the importance, or not, of the framework?
Q4	The information for each question is clear and unambiguous
Q5	Are the questions logically well-ordered?
Q6	Are the questions direct and concise?
Q7	Do the questions measure what is intended to be measured?
Q8	Are the questions free of unnecessary expressions and jargon?
Q9	Are the questions impartial?
Q10	Are the results obtained from the answers formulated mutually exclusive and exhaustive?
Q11	Do you consider the survey technically correct?

Table 6: Characterization of the respondents of pretest

Academic degree	Profession/institution	Teaching area (T = Tecnol./O = Other)	Years of professional practice
PhD	University professor/ISTEC Lisboa	T	30
PhD	University professor/ISTEC Lisboa	T	25
PhD	University professor/ISTEC Lisboa	T	15
PhD	University professor/ISTEC Lisboa	T	10
PhD	University professor/Univ. Nova de Lisboa	T	13
PhD	University professor/Univ. Évora	T	32
PhD	University professor/Univ. Évora	T	31
PhD	University professor/Univ. Lusíada	T	29
PhD	University professor/Univ. Lusíada	T	14
PhD	University professor /IP Luso Lisboa	T	16

Table 7: Characterization of the respondents of the validation survey

Academic degree	Profession/place (country)	Number of respondents	Teaching area (T = Tecnol./O = Other)	Years of professional practice
PhD	University Professor/ISTE (Portugal)	10	T, T, T, T, T, T, T, T, T, T	30, 22, 25, 10, 12, 14, 15, 9, 10, 16
PhD	University Professor / University Rey Juan Carlos, (Spain)	6	T, T, T, T, T, T	25, 27, 25, 24, 26, 12
PhD	University Professor / Universidad Politéncica de Madrid, (Spain)	6	T, T, T, T, T, T	15, 12, 10, 23, 24, 13
PhD	University professor / Universidad de extremadura, (Spain)	6	T, T, T, T, T, T	10, 12, 14, 12, 18, 12
PhD	University professor / Univ. Nova, (Portugal)	2	T, T	13, 15
PhD	University Professor / Univ. Évora, (Portugal)	2	T, T	32, 12
PhD	University professor / Faculdade de Ciências da Universidade de Lisboa, (Portugal)	2	T, T	31, 11
PhD	University professor / Instituto Superior de Educação e Ciências Portugal)	6	O, T, O, O, O, T	29, 22, 12, 9, 12, 15
PhD	Professor University / Univ. Lusíada, (Portugal)	2	T, T	14, 20
PhD	University Professor / IP Luso Lisboa, (Portugal)	4	T, T, O, O	16, 8, 7, 9
PhD	University Professor / ISCTE, (Portugal)	2	T, T	12, 14
PhD	University Professor / Universidade Autónoma de Lisboa, (Portugal)	2	T, T	17, 9
PhD	University professor / Faculdade de Ciências e Tecnologia da Universidade de Coimbra, (Portugal)	2	T, T	8, 15
PhD	University professor / Faculdade de Ciências da Universidade do Porto, (Porutgal)	2	T, T	9, 16

Results

In this topic, we present the results of the analysis of the answers to the validation survey Table (8).

Attribution is an abductive reasoning process that tries to find the best suitable explanation for observations. In this study we submit for validation, we have outlined that this approach is used to generate hypotheses about the people, organizations, or countries likely to be behind cyber-operations. The whole principle behind what is presented for validation is that an APT is considered an attack by a particular group, not an isolated individual. The same general concept can be applied to the reason for the organizational structure of an APT group will have an impact on the evidence and traces it leaves behind. If the malicious software is bought from an international supplier, similar family samples will be detected in disparate networks of victims, which cannot be explained by coherent cui bono. Suppose various units use infrastructures run by the same "quartermaster" type entity. In that case, intrusion sets will be different in terms of TTP and malware, but similar in terms of infrastructure configuration. If a client recruits several freelancers, a wide range of TTPs and malware will target the same organizations, with malware being highly correlated with some TTPs.

Analysts are able to choose from a range of group patterns to best match the data available, just as programmers choose from a variety of software design patterns to best suit a task.

The exact structure of the inner group will ultimately only be disclosed by law enforcement agencies and intelligence methods. Threat intelligence consumers and information security analysts will need to approximately determine the most probable group structures on the basis of technical data. These results will unfortunately only be made public in detail in rare situations.

Theoretically, group configurations can be determined by any subset of the MICTIC aspects: Sponsors (cui bono), telemetry (operators), control servers (administrators), infrastructure (acquisition manager), and malware (developers). We only cover here those configurations that either match the results in the reports and indictments or that are in line with the current tradition in Infosec.

Table 8: Results analysis

Question no.	Analysis
Question 1	We have noticed seven respondents didn't know the concept, which is a significant percentage. Of these seven respondents who didn't know the APT concept, it is inferred that they were the ones who didn't answer the following questions
Question 2	They know what an APT is and what Attribution means in the context of this threat. Therefore, they can understand the following questions as they relate directly to Attribution, i.e., knowing who the promoter is of the APT type attack
Question 3	The result of the survey regarding this question has proven that the information provided was sufficient for the respective intended analysis
Question 4	The answers to the survey regarding this question were all affirmative, thus validating the options presented
Question 5	The answers were all affirmative; the respondents agreed with the formulations presented
Question 6	The answers to the question were all positive, thus allowing this layer of the Framework to be validated
Question 7	The answers to this question were all positive, thus allowing us to validate the proposed layer
Question 8	All the respondents' answers to this question were positive, which validates the proposals outlined in this Framework layer
Question 9	The answers to this one were all positive; that is, the relevance of this additional layer of the Framework was validated
Question 10	The answers were all positive, which validates this proposal for the extra layer of the Framework
Question 11	All the answers to this question were positive. This means that respondents consider the creation of these two layers both relevant and important
Question 12	All responses were positive, meaning that the respondents validated the importance of the Framework extension
Question 13	All the answers were positive. This means that the respondents consider the work relevant and scientifically valid
Question 14	All the answers were positive. This means that the respondents consider that the model presented could be important in both political and social terms if it allows an allocation to be more easily achieved
Question 15	All respondents answered positively. This means they considered the work well-integrated and well structured

In this context, the framework presented and its extension can facilitate the pursuit of the attribution and this study has been submitted for validation.

Considering the answers collected from the survey, we can draw the following conclusions: Regarding the Framework and its extension, the proposals on malware analysis and the proposed mechanisms are validated; as is the issue of the attack infrastructure and the tools used in it; the analysis to be done on the control servers; the utilization of telemetry techniques, as is the importance of the work of intelligence organizations, including espionage methods. The two additional layers to the Framework have also been validated, i.e., social acceptance through incentives and international cooperation to obtain information on APT attacks. The architecture of the Framework was validated and the work's relevance was validated to make it easier to obtain the award, which can have added value in both political and social terms. The general and scientific importance of the work presented has been given as valid.

Discussion

Based on the analysis of articles selected for RSL, we can conclude that an Advanced Persistent Threat (APT) is a highly sophisticated and dangerous threat. One of the main dangers in relation to this type of threat is the fact that it is very difficult to make an early detection of the APT attack.

In principle, this is mainly due to the use of purpose-built tools for this type of attack or the use of zero-day vulnerabilities, therefore undetectable by conventional security systems.

In this sense, an APT is a very selective attack obtaining unauthorized access to certain systems whose main objective is to exfiltrate intellectual property data and in some cases make certain systems inoperative.

It can also be deduced that the number of APT-type campaigns and attacks has increased exponentially. There has been a sophistication of the means used and an increasing differentiation in relation to conventional computer security attacks. This increasing sophistication of the means used, technological and non-technological, translates into an increasing inability for conventional security systems to be able to identify this kind of attack.

Especially because this kind of attack and threat has the characteristic of moving laterally, that is, without being considered by the systems as something anomalous or intrusive, and also with the additional characteristic of remaining in the systems for long periods of time without being detected. Especially because known methods can be employed to invade a network or a system, while the tools that will be utilized to proceed with penetration are, as a rule, completely unknown. This is another big difference from conventional attacks.

In this sense, we can say that the APTs are normally executed by groups. Attackers with very advanced knowledge, usually well-funded, either through organizations or through governments, whose main objective is to obtain crucial information about a certain organization or State. Thus, APTs can also in most cases be carried out by nation-states.

This type of attack according to the opinion of all the referenced and analyzed authors, can be categorized into five stages: (i) Recognition, (ii) Establishment of a support point, iii) Lateral movement, (iv) Exfiltration, (v) Post-exfiltration.

One aspect systematically mentioned by the analyzed authors is that this kind of attack uses zero-day exploits in a very systematic way, a relevant aspect because this characteristic alone differentiates this kind of attack from traditional ones and avoids its detection by conventional security systems. security. Therefore, an APT does not trigger a single-step attack, it is an attack made up of several stages that differ greatly from one another and for each of the stages, as a rule, well-differentiated tools are used between each of these stages, as well as hacking very different between the aforementioned steps. Unlike traditional attacks, APTs follow a sophisticated profile in order to achieve their goals.

APTs are described by the authors as threats with malicious and/or anomalous behavior that almost always manage to overcome security blocks and whose main objectives are cyber espionage, theft, and manipulation of private and confidential information from various organizations or States.

In this context, there is also a unanimous opinion that attack methods are diverse and very sophisticated and their choice is based on the typology and characteristics of the targets. The tools that are commonly used include, among many others, social engineering, cryptography, binary command and control code, rootkits, and all types of advanced malware produced specifically for each of the attacks.

Compared to traditional attacks, APT has at least two major distinct characteristics: (i) The attacker is very well organized and has very sophisticated resources, with the objective of stealing as much data as possible or inactivating an installation or system; (ii) Based on a highly meticulous and methodical reconnaissance phase, the attacker will previously launch a social engineering attack against some users, then gain access to the data in a stealthy and slow manner.

As a result of what was mentioned above, it can also be concluded that it is very difficult to devise a defense method for APT. It is also for this reason that defending against APT has become one of the main issues in the cybersecurity domain. This implies the awareness of the complexity of the APT and consequently, due to its design characteristics, the protection of the systems imposes extreme challenges.

One of the ways to carry out defense in depth is through network monitoring measures such as log analysis, and verification. From file integrity, monitoring logs, and detecting rootkits, they can all provide an indication of a hypothetical intrusion. On the other hand, the proper configuration of the logs and their analysis, including those of firewalls, detection systems for network intrusions, web servers, and databases, become essential. Thus, organizations should establish baselines for security and compare log data against them. It should be noted that to detect an APT it is essential to analyze the outgoing traffic, as the objective is usually to exfiltrate data from within the network.

In addition to these techniques, there are other mitigating methods presented by other authors, such as anomaly detection, whitelists, black lists, detection systems for network intrusions, awareness, cryptography, traffic analysis, pattern recognition, and multilayer security.

Attribution, according to the few authors consulted and analyzed, is a fundamental element to act against APT, mainly because a positive attribution execution generates a deterrent effect among criminal groups.

The attribution to be more effective requires, in the future, a simultaneous concentration on the actors and the context.

The MICTIC framework and its possible extension may be one of the mechanisms that will facilitate the allocation of APT.

However, any solution goes through an integrated set of techniques, all of them in a layered process.

We verified through the RSL that there are practically no known Frameworks, that is, public ones, to be used in the APT assignment. This is one of the facts that justifies the development of new methodologies to achieve the allocation of APT.

In addition to issues strictly in the field of security, it is crucial to consider and highlight the fact that at the diplomatic level, a well-founded attribution is an important prerequisite for exerting pressure on governments that sponsor APT attacks.

From another perspective, attribution can help to show that hackers are not altruistic actors, but on the contrary, have very real and pragmatic objectives with a criminal strategic base.

Another important aspect in creating a framework for allocation is to establish how APTs after discoveries are designated, there should be a universal procedure for the designation of APTs. Currently, the various companies that assign APTs assign their own names to sets of APTs. Thus, the same threat actor can be referred to by different abstract names, which in the first instance soon creates some confusion between researchers and companies and between companies and official bodies.

Findings Summary

We can now provide answers to the research questions, as follows:

Q1: An APT and a conventional cybersecurity assault?
From the consulted literature it is concluded in a very objective way that there is a huge difference between an APT and a conventional cybersecurity attack

Q2: Is there any method to defend against APT?
From the literature consulted it is concluded that it is extremely difficult to have a security system that can detect an APT at the beginning of the assault because APTs use tools created for this purpose and do not use signatures that are already known

Q3: Does an APS have any importance for the defense against APT?
There is very little literature on APS applied to APT, however, it is concluded that a well-implemented APS can be positive for the prevention of APT because it performs behavior analysis and not merely signature analysis.

Q4: Does the MICTIC Framework fit into the APT Assignment? Can it be Improved?
Regarding APT Assignments, the available literature is even more limited. There is a huge deficit of literature on this topic. Even so, what exists indicates that the MICTIC Framework is one of the few methods, known, that can facilitate the assignment. It is possible to improve it by adding layers to the framework

In summary, we can conclude from the entire RSL that APTs are the most complex cyber threats today, with extreme difficulty in being detected. This attack is very different from the traditional attacks. APT uses techniques and technologies to purposely create attacks.

The allocation of APT does not have any public and scientifically validated Framework to proceed with it.

It justifies the development of a framework, being able to start from the MICTIC framework and create an extension after the creation of that artifact to proceed to its scientific validation.

Conclusion

As for the main objective of this study, to contribute to the achievement of more straightforward APT attribution through the creation of two new layers in the MICTIC framework and the validation of this Framework, procedures were developed and described for each of the Framework's layers and two new layers were created.

How malware analysis and functionality can indict the attack perpetrators has been specified. In the malware analysis layer, malware's development for attribution was described as how malware can help identify a cybercriminal group, all while considering its specificity. It described how malware could be a source for analysts and the importance of analyzing the evidence obtained from the particularities of the environment of tool developments that serve the attack.

At the attack infrastructure layer, we have shown the importance and functionality of managing the control server and how imperative it can be to find that same server. The importance of getting public information and tools was described and developed. The importance of active screening was developed and demonstrated.

In the layer on control servers, we refer to the techniques used in APT and the importance of obtaining information on these machines to achieve attribution.

In the telemetry layer, we refer to how telemetry is essential for analysts. Within the MICTIC framework, telemetry is related to the operators' manual activities, such as sending spear-phishing emails, installing malware, or even making lateral moves. In this respect, the aspect overlaps with operators working with control servers. However, the typology of data is quite different from that obtained with C and C, resulting in various tools and workflows for analysts.

The intelligence layer has been developed and shown how the issue of organized information is of utmost importance. These factors can be vital in achieving an APT Award, whether espionage, counterintelligence, signals intelligence, cyber activity, human intelligence, or hacking back. A direct and intrinsic relationship has also been established between this layer and cui bono, as these are espionage operations through which Attribution information can be obtained.

From here, two more layers were created that were completely new so that an APT Attribution could be more easily obtained in a summation with the previous ones.

We have created a layer of social acceptance through incentives, where the primary assumption is that rational actors behave according to incentives. So incentives can provoke the obtaining of information. The importance of the global information infrastructure dictates the need to develop incentives for parties to adopt value-added attribution methods. More importantly, it is crucial to start communicating the value of Attribution to gain broad understanding and acceptance. We have developed a mechanism whereby the key to creating positive incentives for Internet users to participate in promoting obtaining and eventually demanding online share attribution is to identify a set of online activities in which something of value to the user is at risk.

The second layer proposed was international cooperation. International cooperation between all interested structures and not exclusively between official agencies is key to achieving the Attribution, perhaps even one of the key layers of the whole model. International sharing outside government agencies is critical and of total value in obtaining the APT Award.

After this model was developed, it was submitted for validation by a universe of highly qualified individuals with PhDs in information technology or related fields. This validation was achieved through a survey described and presented in Chapter VIII of this study.

The Framework developed was fully validated by the survey results, as was the importance of the work to the issue of obtaining the Attribution.

This study objectively contributes to achieving the APT attribution by combining technological and non-technological techniques. It contributes to achieving

computer security environments since an APT Attribution is a high deterrent to an APT group getting uncovered and an Attribution being assigned to it. Typically, cybercriminals who have been identified have stopped operating, whereas the opposite is not true; unidentified actors persist with attacks for a long time. Thus, this study also contributes to the overall maintenance of cybersecurity.

In future work, the issue of APS as a tool for detecting and mitigating APT attacks should be further explored. The APS covers secure network design and implementation, including authentication, authorization, data and access integrity, network monitoring, and risk assessment, as well as concepts such as malicious versus malicious threats, adversarial mindset, motivation, the economics of cybercrime, criminal infrastructure, dark web and the criminal types that organizations face nowadays. Creating new mechanisms to deal with this highly sophisticated threat is critical. Therefore, the development of APS frameworks concurrently with Attribution is a path that we believe should be followed.

Finally, it must be highlighted that the subject in question is relatively new and that there are practically no scientific papers on APT Attribution until the present moment. Such a situation has generated difficulty in obtaining peer-reviewed scientific papers on APT attribution.

Therefore, the present research work significantly contributes to the problematic scientific dissemination of APT Attribution.

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the effort.

Funding Information

This study was supported by National Funds through the Portuguese funding agency, FCT - Fundação para a Ciência e a Tecnologia, within project LA/P/0063/2020.

Author's Contributions

Pedro Ramos Brandao: Engaged in all experimental procedures, conceptualized and structured the research plan, organized the study, oversaw data analysis, and contributed to manuscript writing.

Henrique São Mamede: Supervised the mouse-related work, reviewed the research plan, organized the study, and provided critical review of the manuscript.

Miguel Pupo Correia: Conducted critical reviews and made significant contributions to multiple versions of the manuscript.

Ethics

This manuscript is original and contains unpublished material. The corresponding author certifies that all co-authors have reviewed and approved the manuscript, and confirms that no ethical issues are involved.

Data Availability Statement

Data included in article/supp. material/referenced in the article.

References

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851-1877. https://doi.org/10.1109/comst.2019.2891891

Brandao, P. R. (2021). Advanced Persistent Threats (APT) Attribution-MICTIC Framework Extension. *Journal of Computer Science*, *17*(5), 470-479. https://doi.org/10.3844/jcssp.2021.470.479

Chen, J., Su, C., Yeh, K. H., & Yung, M. (2018). Special Issue on Advanced Persistent Threat. *Future Generation Computer Systems*, *79*, 243-246. https://doi.org/10.1016/j.future.2017.11.005

Chen, P., Desmet, L., & Huygens, C. (2014). A Study on Advanced Persistent Threats. *Springer Link*, 63-72. https://doi.org/10.1007/978-3-662-44885-4_5

Daly, M. (2009). The Advanced Persistent Threat (or Informa onized Force Opera ons). *Usenix*, 2013-2016.

Drozhzhin, A. (2015). *Russian-Speaking Cyber Spies Exploit Satellites*. Kaspersky. https://web.archive.org/web/20170727075548/https://www.kaspersky.com/blog/turla-apt-exploiting-satellites/9771/

Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet Dossier* (1–). Symantec Corporation.

FireEye, (2014). FireEye: Neuer Mandiant Threat Report. *Datenschutz Und Datensicherheit-DuD*, *38*(6), 427. https://doi.org/10.1007/s11623-014-0166-x

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for Including Grey Literature and Conducting Multivocal Literature Reviews in Software Engineering. *Information and Software Technology*, *106*, 101-121. https://doi.org/10.1016/j.infsof.2018.09.006

Hill, M. M. (2002). *Investigação Por Questionário* (2nd Ed.,). Edições Sílabo.

House, T. W. (2016). *FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment*. office of the press secretary. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and

Huang, L., & Zhu, Q. (2020). A Dynamic Games Approach to Proactive Defense Strategies Against Advanced Persistent Threats in Cyber-Physical Systems. *Computers and Security*, *89*, 101660. https://doi.org/10.1016/j.cose.2019.101660

Hussain, S., Ahmad, M. B., & Uddin Ghouri, S. S. (2020). *Advance Persistent Threat-A Systematic Review of Literature and Meta-Analysis of Threat Vectors* (Springer Link). Springer. https://doi.org/10.1007/978-981-15-4409-5_15

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic Literature Reviews in Software Engineering - A Systematic Literature Review. *Information and Software Technology*, *51*(1), 7-15. https://doi.org/10.1016/j.infsof.2008.09.009

Kopan, T. (2015). *White House Readies Cyber Sanctions Against China Ahead of State Visit*. CNN. https://web.archive.org/web/20170718181028/http://edition.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-president-obama/

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of Publicly Available Reports on Advanced Persistent Threat Actors. *Computers & Security*, *72*, 26-59. https://doi.org/10.1016/j.cose.2017.08.005

Mandiant. (2024). *Advanced Persistent Threats (APTs)*. Mandiant. https://www.mandiant.com/resources/apt-groups

Nickels, K. (2019). *Cyber Indictments and Threat Intel: Why You Should Care*. Medium.

NIST. (2024). *National Institute of Standards and Technology*. NIST. https://www.nist.gov/

Peffers, K. (2022). *Ken Peffers*. Google Scholar. https://scholar.google.com/citations?user=zwOdzCgAAAAJ&hl=en

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45-77. https://doi.org/10.2753/mis0742-1222240302

Pernet, C. (2014). *Sécurité Et Espionnage Informatique* (2nd Éd., 1). Eyrolles.

Quintero-Bonilla, S., & Martín Del Rey, A. (2020). A New Proposal on the Advanced Persistent Threat: A Survey. *Applied Sciences*, *10*(11), 3874. https://doi.org/10.3390/app10113874

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *In Journal of Strategic Studies* (1). https://doi.org/10.1080/01402390.2014.977382

Ruel, E., Wagner III, W. E., & Gillespie, B. J. (2016). *The Practice of Survey Research* (1st Ed.,). SAGE. https://doi.org/10.4135/9781483391700

Schneier, B. (1999). Attack Trees. *Dr. Dobb's Journal*, *24*(12), 21-29.

Security Response, S. (2015). *Iran-Based Attackers Use Back Door Threats to Spy on Middle Eastern Targets*. Security Response.

Steffens, T. (2020). *Attribution of Advanced Persistent Threats* (1st Ed.,). Springer Vieweg. https://doi.org/10.1007/978-3-662-61313-9

Swisscom, (2019). *Target Attacks Cyber Security Report 2019* (Targeted Attacks, 1–).

Team, C. G. I. (2022). *CrowdStrike-Intelligence-Report-Putter-Panda*. Putter Panda. Retrieved 2022, from. https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. (2016). Advanced Persistent Threats: Behind the Scenes. *IEEE Xplore*, 181-186. https://doi.org/10.1109/ciss.2016.7460498

Wikipedia. (2022). *Herbert A. Simon*. Wikipedia. https://en.wikipedia.org/wiki/Herbert_A._Simon

Williams, K. Y. (2016). Insider-Threat Detection in Corporate Espionage and Cyber-Espionage. In *National Security and Counterintelligence in the Era of Cyber Espionage* (1–, p. 16). IGI Global. https://doi.org/10.4018/978-1-4666-9661-7.ch004

York, U. S. D. C. S. D. N. (2022). *Unites States of America versus Zhang Zhang-GUI*. Retrieved 2022, from. https://www.justice.gov/opa/pressrelease/file/1106491/download