Deception Planning Models for Cyber Security

Cristiano De Faveri*, Ana Moreira†, and Eric Souza‡

NOVA LINCS, Departamento de Informática
Faculdade de Ciência e Tecnologia - FCT
Universidade NOVA de Lisboa - UNL,
Caparica, Portugal
*c.faveri@campus.fct.unl.pt, †amm@fct.unl.pt, ‡er.souza@campus.fct.unl.pt

Abstract—**Deception-based mechanisms are typically used to enhance overall security by causing misperception on adversaries who take actions in favor of defense. The process of creating deception is complex and demands careful planning to maximize the benefits while mitigating potential risks. Advances in creating deception planning processes for cyber security are generally based on military tactics, where deception has a long history. However, the complexity of computer systems demands deception planning processes that fit the needs of integrating deception into traditional software security mechanisms. This paper presents a survey of existing deception planning processes in military and digital realms. The goal of this review is to identify the scope of deception planning models, which tools have been used to plan deception, and how the planning is integrated into other activities in the software development phases. We identified 20 different features in the studies, which we used to compare them. The outcome of this survey can be used to facilitate the understanding of how deception planning has been conducted and supported while identifying potential gaps to be addressed in future research.**

I. Introduction

Deception is a key aspect of many interplays including business and social interactions, games, warfare, nature and digital security. In the field of psychology, deception represents a deliberate attempt to conceal, fabricate, and manipulate factual or emotional information to create or maintain in others a belief that the communicator herself considers false [1]. In the digital realm, deception is a well-know technique used by mal-actors to entice and manipulate legitimate users on their own benefit. Techniques like phishing and social engineering use deceptive tactics to grab legitimate users attention while stimulating them to perform desired actions. In cyber defense, deception has been investigated since the 90's to build early-warning and advanced security surveillance tools [2], [3], [4].

Deception-based security is typically employed as a second (or third) line of defense to prevent, detect and respond to offensives against a computer system [5]. When associated with traditional security mechanisms, deception offers unique advantages, mostly because adversaries use to assume that systems always operate in the context of honesty. We design systems to respond with the truth, even when the system recognizes it is under attack. As a consequence, adversaries evolve their exploitation strategies in different paths to reach their objectives. Deception tries to change this game by increasing the system's entropy when applying simulation (showing the false) and dissimulation (hiding the real) techniques. The expected results include: *(i)* adversaries wasting time and resources on obtaining and analyzing false information, *(ii)* increase adversaries' perception of the risk of being detected, *(iii)* offensives being break or slowed down, *(iv)* a chance to grasp about attacker tactics, *(v)* detecting unknown attacks that other defensive tools may miss.

Deception requires careful planning and application of multiple methods to be effective [6]. As the number of methods and tactics increases, strategies to coordinate these methods, validate multiple deception channels, and track the effectiveness of the operation by monitoring integrated effects become a challenge. Moreover, deception involves risks that need to be clearly stated early in the development of deception, thus conflicts and trade-offs can be identified and resolved early to attenuate the costs. Examples of such risks include adversaries launching a counter-deception, or sensitive data leakage (as fake data is fabricated using real data), or access to functions in real components of the system, or conflicts between running deception tactics and new added ones, or still false-positive interactions where a real user reaches a deceptive element in the system.

Many methods have been proposed to plan, design and create deceptive strategies. Most of these methods have their roots on the military arena, where deception has a long tradition. The proposed models chiefly fall into four categories: cognitive models, taxonomies of techniques, game-theory models, and planning and execution of deception operations. This paper surveys the existing deception planning and execution models, which are designed for (or are related to) cyber security, and identifies a set of properties that may assist in the evolution and development of systematic approaches for deception-based defenses.

The remainder of this paper is organized as follows: Section II provides the basics of deception-based defense, including a reference model of deception planning and execution. The survey approach is presented in Section III, and the findings are shown in Section IV. We discuss the results and point for potential research directions in Section V, drawing conclusions in Section VI.

978-1-5386-3893-4/17/$31.00©2017 European Union

II. Deception-based defense

Deception is the process by which deliberate actions are employed to cause misrepresentation and induce erroneous inferences [7]. Deception is not an exclusively human activity. Common examples of deception can be found in biology, where some animals have distinct characteristics to deceive adversaries [8] (e.g., certain octopi mimic other objects and creatures, chameleons change colors to match the background, pathogens use multiple tactics to deceive the immune system [9]). Deception has also a long history in the military arena, where deceptive tactics are used to create asymmetry and manipulate the enemy to reduce their effectiveness [10], [11]. Much like the conventional warfare, strategic deception in the cyber terrain has been applied in both offensive and defensive purposes.

A. Cognitive aspects of deception

Deception must be targeted to influence the thinking of the adversary. Psychologists have delved into how the perception of the world and of other subjects diverge from reality in patterns that could be detectable and explained. These patterns are generally referenced as "biases", which can influence decision-making, beliefs, and behavior [12]. Thompson et al. [13] discuss three major groups of biases: *(i)* **personal and cultural:** personal biases are constraints arising from individual's past experiences. Cultural biases are thinking constraints acquired during evolution from widely held beliefs, practices, or cognitive styles characterizing one's specific social environment. *(ii)* **organizational:** these are restrictions imposed by local information, traditions, and goals of the individuals' organization. Deception tactics can be designed taking into account insider attackers, such as current and former employees. *(iii)* **cognitive:** these refer to patterns of deviation in judgment, whereby inferences may be drawn in an illogical fashion [14], [15], leading to perceptual distortion, inaccurate judgment, illogical interpretation, or what is broadly called *irrationality* [16]. This can be motivated by various process, including information-processing shortcuts, emotional and moral aspects, social influence, mental noise, and our biological limited capacity in processing information. Cognitive biases crosscut cultures, personalities and organizations.

Deceptive tactics exploiting personal, cultural and organizational biases tend to be more effective as they exploit a particular cognitive vulnerability of one individual (or a group of). However, these tactics are rare due to the difficulty in knowing the opponent in advance. According to [17], exploiting cognitive biases leads to more general but less effective deceptive tactics. The reason why we experience cognitive biases is not due to any intellectual or emotional predisposition during the process of judgment, but simply from the way the mind works. Consequently, cognitive bias may influence how we estimate probabilities, evaluate evidences, and attribute causality [18].

B. Deception as a cyber security strategy

Earlier documented works showing the use of deception include "The cuckoo's egg" [2] and "An Evening with Berferd" [3], in which the authors discuss how they interacted with an attacker by providing fabricated responses. These reports led to the first ideas on *honeypots*, which are resources primarily designed to entice attackers and learn their tactics [19]. Typically, honeypots are categorized into research and production. Research honeypots aim at providing data on the methods used to attack systems, and present little risk of propagating an attack. Production honeypots target the protection of an organization while distracting the attacker, but present more risk of propagating an attack. The deception toolkit released in 1997, is one of the earlier tools applying deceptive techniques for cyber defense [4]. It allows the creation of simulated Linux services configured by a deception-specific finite state-machine language to determine the level of emulation of a service. Honeypots are often grouped in clusters, the *honeynets* [20]. Honeynets are research honeypots using real systems and applications. At the client-side, honeypots have been proposed to identify malicious websites that target client application vulnerabilities [21]. Similarly, mobile honeypots focus on deceptive techniques for threats on mobile devices [22], [23], [24].

Traditional manifestation of honeypots suppose a computer, or some physical resource for the attacker to interact with. This vision targets deceiving network attacks, representing a restricted notion of the honeypots potentialities. Honeypots that are not computers are called *honeytokens* [25], which are any sensitive data in a database (e.g. credit card numbers, passwords and salaries), files (like spreadsheets, presentations), or even a bogus login service. Typical honeytoken techniques include the use of disinformation, excuses, and response delay. Disinformation is the act of planting false information into the system to cause confusion or lead attackers astray. For example, false passwords on a file associated with user accounts [26], [27], decoy files deliberately installed on a server [28], service detecting file misuse [29] methods to generate honeytokens in relational database [30]. Additionally, techniques to generate honeytokens have been proposed, such as the honeygen for relational databases [30], the use of aspect-orientation [31], and the use of personal data [32]. Google Hack Honeypot[1] leverages the purpose of search engines by emulating a vulnerable web application to be indexed by search engines.

Useful lies, like "communication with central server is broken", in response to a request can justify resource denial. While general excuses exploit common resources of a system (e.g. communication channels, network issues, authentication methods, and database interaction), domain-specific excuses can offer more realistic excuses. A financial system delivering the excuse "Your account has been locked. Please contact the bank." may cause in the attacker's mind the perception of a successful attack. Well-designed excuses may keep attackers

[1] Despite of the name, the technique is available for any search engine.

confident, while wasting their time. Delay responses are used when the defender requires extra time to assemble a defense. Delaying can be achieved by slowing down a system response, by asking more questions or additional information to read before the attacker can proceed. Delay responses can also be integrated with excuses to advise attackers to wait for some event before moving ahead.

C. Deception Planning Models

The deception planning and execution process involves convoluted adversarial relationships and complex engineering systems. Although the overall process can be intricate, planning is typically part of a deception core process, which involves also deployment activities, target engagement, and a termination phase. Figure 1 illustrates the deception core process.

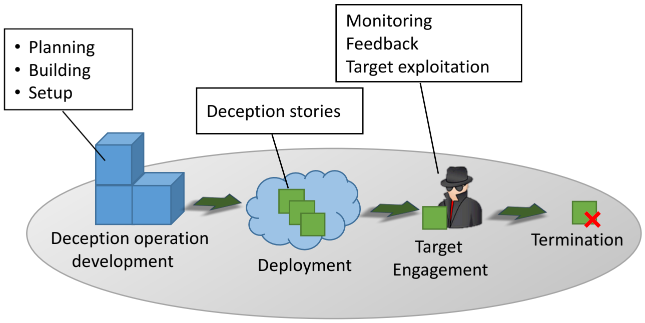

Fig. 1: Deception Core Process, adapted from [33]

Deception-operation development encompasses deception planning, building and the preparation to engage the target. Planning is an interactive process containing activities to describe the different requirements of the operation. During the building phase, a deception story containing an outline of how the computer system will be portrayed is built, the feedback channels are configured, and a termination plan is set. During the setup phase, the exploitation of target actions are identified along with responses for problems and coordination with security operations. Deployment represents the transition between the operation plan to the observation. During deployment, the deception plan is deployed and it is maintained until the deception is received by the target or the deception is aborted for some reason. The target engagement phase is marked by the deception story being received by the target. A successful deception considers the target receives the deception story, accepts it, and, as a consequence, takes the intended action [33]. Feedback channels collect information about the target interaction and the decision to continue the operation or modify it is made. Termination occurs when the deception story is no longer needed due its achievements, or when the target discovers the stratagem. The focus of this paper is to survey deception planning models as part of deception operations development phase.

III. Survey Approach

In order to identify and characterize deception planning models, an evidence-based approach was followed. More specifically, the performed study is grounded on the systematic review (SR) method [34]. SR has been applied by many researchers in an attempt to reach a systematic, replicable, and transparent process to synthesize research results and practices.

- **Research questions (RQ):** the RQs addressed by this survey work are:
  RQ1 - Which are the scope of deception planning models?,
  RQ2 - Which tools have been used to plan deception?,
  RQ3 - How is deception planning integrated into other activities in the development phase?

- **Search process and sources:** for search and selection, three relevant databases were used: IEEE Xplore, ACM Digital Library, and Springer. We use Google scholar to cross-checking our initial findings and to search for deception planning in other areas, such as military and strategic planning, which were not catch in the database. The search was conducted using queries such as:

```
"Deception" AND
("Plan" OR "Planning" OR
 "Model" OR "Process");
"Deceptive" AND ("Plan" OR
"Planning" OR "Model" OR "Process");
```

  The strings were adjusted for each search engine, since they differ on query formulation. Also, they were executed against the metadata of the documents.

- **Inclusion and Exclusion criteria:** we include studies that are related to deception and describe some type of model or process. Although the focus of this paper is cyber security, we decided to include studies in the military scope because they contribute to grasp similarities and differences between them. Abstracts, editorials, posters, keynote, papers not written in English and duplicated studies were excluded. Duplicated studies are identified in two stages. For those easily identified by the title, we flag it as duplicated and consider only one of the copies. For those identified as repeated, i.e. configuring an extension of a previous study, we consider to merge them and count them as one. The remaining papers are checked using inclusion criteria by reading abstract and conclusions of the papers. Snowballing was then applied to extend our search with other papers, technical reports and books about the subject.

As a result, a total of 10 articles were kept as the basis for this study. These articles were then fully read and analyzed according to the survey protocol.

IV. Main Findings

A. Model Types

Deception planning models are classified into three main scopes: general models, military models and cyber defense models. They are very interrelated since deception is a matter of misperception and not a particular concern of one other domain. Military deception models are specializations of general deception models, as deception models for cyber spaces inherit many characteristics from military deception models. Among 10 deception planning models, two are general models [35], [7], four are devoted to military purposes [36], [37], [38], [39] and other four are related to cyber security [33], [40], [6], [41].

B. Model Features

To assist answering the RQs, we identified multiple characteristics in the analyzed studies, which we translated into features, as presented in Table I. A feature in the context of deception planning models represent an activity or a deception property. Features are classified into explicit or implicit. While explicit features are clearly stated as part of the model, implicit feature are those which authors recommend to be performed during planning activities. For example, performing risk assessment is an explicit activity identified in [39], [40], [7], [41]. In [35], [33] deception techniques are assigned as an implicit feature since they are not part of the model. However, they were mentioned or suggested by the author. We discuss each feature as follows:

TABLE I: Comparison of deception process models

Refer.	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
	K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
[35]	●	○	●	○	⊙	○	○	○	○	●
	○	○	○	○	○	○	○	-	○	○
[36]	○	○	○	○	●	○	○	○	○	●
	○	○	○	○	○	○	○	○	●	○
[37]	●	○	●	○	●	⊙	⊙	○	○	○
	○	○	○	○	○	⊙	○	-	⊙	○
[7]	●	○	●	○	○	○	○	○	○	●
	○	○	○	○	○	○	○	-	●	○
[38]	●	○	●	○	●	○	○	○	○	○
	○	○	○	○	○	●	○	○	○	○
[39]	●	○	⊙	○	●	●	●	○	○	●
	●	●	●	●	○	●	●	○	●	○
[33]	●	○	⊙	○	●	⊙	⊙	○	○	●
	●	●	●	○	○	●	●	○	○	○
[40]	●	○	●	○	●	○	●	○	●	●
	○	●	○	○	○	○	●	○	●	○
[6]	●	○	○	○	●	○	○	○	●	○
	○	○	○	○	○	○	○	○	○	○
[41]	●	●	●	●	●	●	●	●	●	○
	⊙	●	●	●	●	●	●	●	●	⊙

●-Explicitly considered, ⊙-Implicitly considered, ○-Not evidenced
A. Goals/Objectives setting, B. Conflicts&Contributions, C. Deception technique, D. Threat model integration, E. Deception stories, F. Deception metrics, G. Deception risks, H. Variability model, I. Bias exploitation, J. Deploy&Execution, K. Termination plan, L. Overall defensive integration, M. Timing, N. Responsibilities/Roles, O. Multiple operationalizations, P. Target identification, Q. Response for problems, R. Software development life cycle integration S. Specify the feedback channels T. Tool support

(A) Goals/Objectives setting: these aim at justifying a deception operation and take the required approvals to implement it. Although subtle differences[2], both terms, goal and objective, have been used interchangeable. Depending on the dimension and coverage of the deception operation, top management approval is required. It represents a common situation in military field since deception may involve a detailed resource planning. With exception of [41] that applies a goal-oriented approach to determine the rational of each deception tactic, other studies do not specify how to describe goals and objectives. Notably, [37] provide a set of evaluation criteria for deception objectives.

(B) Conflicts&Contributions: these can be made explicit during the deception planning phase to assist in the potential risk analysis, evaluate alternative options, and prioritize operations. Conflicts may emerge from multiple origins, such as other operations (objectives, timing, etc.), divergent stakeholders objectives, integrated security mechanisms, and the environment. Contributions assist in determining priorities within operationalization options [42]. In the analyzed studies, [41] provide a mean to express conflicts in deception models, and [6] provide implicit evidence in their planning model.

(C) Deception technique: several techniques may be necessary during the execution of a deception operation. [7] suggest that deception occurs in the context of two orthogonal techniques: simulation and dissimulation. The authors propose a taxonomy of deceptive techniques compounded by mimicking (imitating something/someone's identity), inventing (making up information), decoying (distracting the attention from the transaction), masking (concealing relevant information about the item), repackaging (making a relevant object appears to be something else), and dazzling (increasing uncertainty to cause confusion). These taxonomy is shared with the works [40] and [41]. The latter leverages deception techniques as first class entities in goal-oriented models, so that engineers can express multiple techniques in different deception tactics. [38] suggest additional techniques (camouflage/concealment/ cover, demonstration/feint/diversion, display/decoy/ dummy, mimicry/spoofing, dazzling/ sensory saturation, Disinformation/ruse, conditioning). The description of these techniques can be consulted in the referenced study ([38]).

(D) Threat model integration: a deception operation requires identifying how a target can exploit a system, or at least pressure points where deception can employed to enhance the overall security. Thus, a threat model helps, as it identifies potential threats that can prevent an actor from achieving her goals [43]. We could not identify any model that integrates a threat model in the planning phase, except in [41] that consider a threat model as part of the process of designing deception tactics.

[2] In general, a goal is achieved by accomplishing one or many objectives

(E) Deception stories: representing a scenario that outlines the actions that will be portrayed to cause the target to adopt the desired perception and take the intended target action. Describing the scenarios of deception is crucial to create successful deception operations. [40] offers guidance on which components of a system can describe a deception story. These components are divided into system functions and states, such as system decisions, software and services, internal data, and public data, vulnerabilities, and performance. [41] suggests the model deception stories using collaborative diagrams as a sequence of actions and constraints representing the target interaction with system components. Other studies consider explicitly or implicitly the development of deception stories without any guidance or support to create them.

(F) Deception metrics: defined to determine whether a deception operation has succeeded or not. [39] provide guidance on how to create metrics associated with the activities needed to portray the deception story. It proposes a set of qualitative and quantitative assessments based upon the aggregation of discrete, observable, and quantifiable indicators. In particular, the model suggests metrics for effectiveness, efficiency, and adaptability. The latter describes the ability of the deception plan to respond to changing demands. [41] consider the definition of deception metric explicitly in the planning model, but do not provide any guidance of which kind of metric could be applied in different phases of the deception operation.

(G) Deception risks: every deception operation implies risks that need to be identified in advance. Risks can be mitigated or accepted as part of the operation. [39] highlights the need of assessing risks of deception failure, risks of exposuring the means of deception (techniques), or risks located on feedback channels, and risk to third parties. [33], [40], [41] present risk assessment as part of the planning process model.

(H) Variability model: a variability model describes a set of possible deception operations that can be applied in a certain situation. When dealing with multiple stories and operations, there is a need to specify how these stories constraint each other and how they can be activated. [41] propose the modeling of variability model representing by feature models.

(I) Bias exploitation: deception operations can be designed to exploit a particular bias (e.g., cognitive or cultural), which can be explicitly described during the planning. Bias exploitation can be assigned in multiple levels of the deception. For example, an entire deception operation can be assigned to a single bias exploitation or a particular story can exploit a particular bias, while another story can be assigned to other. Despite of the importance of the systematic bias exploitation in deception operations, very few models exploit explicitly which bias will be exploited during the operation [40], [41]. Bias exploitation are assigned in distinct phases of the planning. [40] assign bias exploitation as one step in their planning process. [41] assign bias exploitation in cover stories, which allows to exploit different biases in multiple deception tactics.

(J) Deploy&Execution: the deploy activity involves the deployment of the deception operation, and execution refers to the activation of a deception operation, monitoring and counteractions. The core planning process presented in Figure 1 represents an example of this situation. Most of the planning models present some extension to activities to be performed during execution [35], [37], [39], [33], [40]. [35] presents a two states model, which the activities planned (decision) is enacted into a runtime enviroment (perception). Other authors incorporate activities into deception execution phase to be monitored and constantly verified against the plan.

(K) Termination plan: referring to activities to determine how a deception operation ends, to perform the clean-up process, the scope of information that can be disclosed, and if it can be reused in the future. Few planning models offers termination procedures. [39] provide guidance to develop a termination plan that includes the reason the operation ends, contingencies for unforeseen events, control of exposure of the existence elements, etc. [33] considers the development of a termination plan, however, there is no guidance about how to produce it.

(L) Overall defensive integration: deception operations can be explicitly integrated with other security operations to enhance overall security. For example, honeywords consider the use of fake accounts in a legitimate file containing real user accounts. [40] advocate that a successful deception operations needs to be integrated with the real operation. In their model, they propose the integration of deception in real components of the system, but do not provide any support to analyze such integration. [41] integrates deception design into the software development life cycle, to produce integrated models between deception and security requirements. [33] provides security integration via an activity during the deception planning.

(M) Timing: time-constraints in a deception story help sequencing multiple concurrent or overlapping events, or defining a decision flow to describe the interdependency of events. Timing is also related to synchronization of distinct deception operations. [41] suggest to express timing using behavior models, which allows to determine specific time constraints of interactions. [39], [33] offer event-schedule mechanisms to control the beginning and finalization of a deception operation.

(N) Responsibilities/Roles: these define explicit roles and responsibilities to conduct the deception operation. Two studies allow defining responsibilities/roles. In [39], responsibilities are defined in multiple levels, from strategic to operational. [41] allow to express agents and roles based on the adopted goal-oriented language to model deception.

(O) Multiple operationalizations: these define implementation strategies to ensure the goals of the deception operation. The description of multiple operationalizations assist in the identification of contributions and conflicts. Two distinct operationalizations can be analyzed against a goal to determine which one contributes or conflicts more with other operationalizations or oher goals in a system. Goal-oriented models allow modeling such kind of feature [41].

(P) Target identification: this refers to understand how hackers think to reveal and exploit vulnerabilities. This relates to the feature "threat model integration", even though it is concerned with identifying attackers' *modus operandi*, not threats. In [33], [38] target identification considers the identification of how a target works to reveal her vulnerabilities to deception. [39] performs target identification during the staff deception estimation. [41] integrates a threat model in the development of deception tactics, which allows to describe target actions.

(Q) Response for problems: there are a number of problems that can cause a deception operation to fail. Examples include the deception story isn't received, the target discovers the deception, the story is not interpreted as intended, or the intended action isn't taken. Explicit responses for these problems consider alternative paths, including the termination of the operation. Recovery for problems occurring during deception operation can be planed in advance [40], [41] or it can be part of the risk analysis [39].

(R) Software development life cycle integration: integrating deception specification and planning is typically formalized as part of security requirements engineering, where engineers specify security requirements and controls necessary for a particular application. Of course, this feature is exclusive of models applied to cyber space. [41] connects architectural model with deception strategies to compound a repertory of deception that can be realized by multiple components in the system. Other models applied to cyber war are agnostic of any software development cycle [33], [40], [6].

(S) Specify feedback channels: these are channels used to monitor the actions taken by a target. Feedback channels provide information to compute metrics and evaluate deception operations. In [36], [7], [39], [40], [41] feedback channels are part of the planning process, but offers few insights to select appropriate feedback channels.

(T) Tool support: assisting engineers in the task of specifying and design deception plans. We could not identify any native tool to support deception planning. However, [41] shows how to use goal-oriented requirements modeling languages to specify deception operations (called strategies in their work), which existing tool support can be used (e.g. Open ME[3], and KAOS[4]).

V. Discussion

A significant portion of the surveyed models presents a very basic set of features [35], [36], [38], [6], which means they are general models, described at a high abstraction level. These models present only the basic structure of the deception planing operations. Figure 2 illustrates the feature distribution in the analyzed deception planning processes. We analyze each research question as follows:

RQ1: we extracted a set of 20 features from the surveyed works, which provided a baseline and scope for comparison between the models. A predominant amount of models ([35], [36], [37], [7], [38]) still remains with few explicit features ($<= 4$), which means they are compounded by high-level activities and general properties. As a result, they can be used in a wide range of deception planning, but it provides little guidance on how to specify and design deception-based defense. [40], [41] deem the integration of deception in security computer defenses.

RQ2: Analyzing the feature tool support, it is clear that deception planning and specification still demands additional effort to offer guidance and tools to assist engineers in the task of creating deception-based defense in multiple granularity.

RQ3: Some deception planning models have considered the execution and termination phases in the cycle of deception (RQ3), but there is no integration between the phases. Artifacts generated by planning phase are lost in the process. Again, initiatives like [40], [41] to integrate deception into computer security can promote a better integration between planning and development phases.

Based on the RQs and our gap analysis, we suggest three main areas of research related to deception planning:

1. Tool support: the development of tools requires strong methodologies to plan and integrate deception into security operations. Being deception a psychological matter, it is necessary to assist engineers with models that facilitate the work of choosing the best bias exploitation for a certain situation and which technique best fit the operation when integrated with traditional security mechanisms.

2. Trade-off analysis: as the amount of deception tactics and operations augment, it is crucial having mechanisms to assist in trade-off analysis.

3. Risk assessment: finally, we point for one of the most important aspect when specifying and design a deception operation: the risk assessment. A comprehensive risk analysis of deception operations aligned with security operations augment the chances of deception succeed. In this sense, risk assessment support is paramount to leverage deception-based mechanisms as a reliable approach to enhance security.

Threats to Validity. To conduct this survey, we scrutinize different sources with different objectives (from military to cyber space), which naturally raise distinct terms to conceptualize a deception process. Despite of our constant effort to align those term in a common language, one threat to internal validity consists of some conceptual misinterpretation we might have done. This can lead to a gap in the feature

[3] http://istar.rwth-aachen.de/tiki-index.php?page=OpenOME

[4] http://www.objectiver.com/index.php?id=25

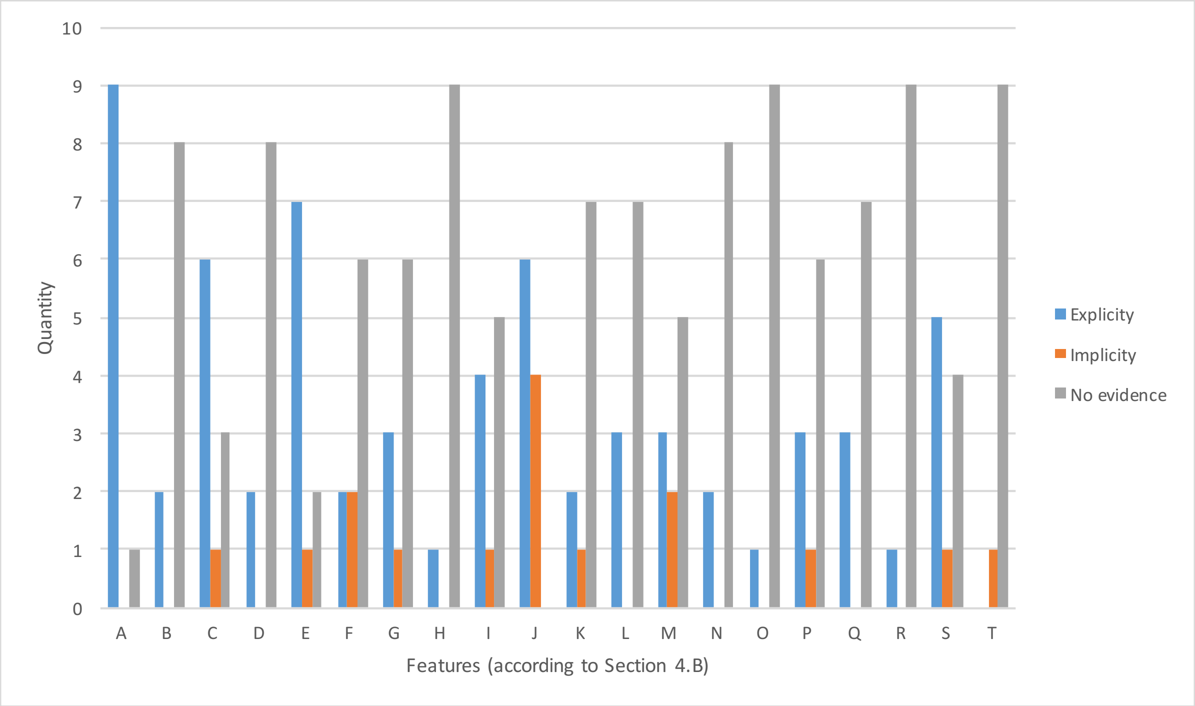

Fig. 2: Feature distribution in deception processes

list or mistakes in the classification. A form of mitigate this threat should consider pair discussion about the concepts. An external threat concerns the possibility of not having considered some planning model in the military scope, mainly because military documents use to be confidential.

VI. Conclusions

Deception may enhance the overall security by applying techniques to induce adversaries to erroneous inferences and consequent actions, or inactions, in favor of defense. Deception planning is a critical phase since every deception involves risks that need to be assessed and mitigated to successfully accomplish the operation goals. This survey highlights important deception process features that should be considered when designing a deception plan, and outlines potential directions for future research. It is important to note that other features can be considered, and grouped into multiple dimensions as deception planning processes evolve and integrate to other methodologies and tools.

Acknowledgments

We are grateful to CAPES foundation and NOVA LINCS Research Laboratory (Ref. UID/CEC/04516/2013) for their support in the development of this work.

References

[1] J. Masip, E. Garrido, and C. Herrero, “Defining deception,” *Anales de Psicología/Annals of Psychology*, vol. 20, no. 1, pp. 147–172, 2004.

[2] C. Stoll and J. W. Connolly, “The cuckoo’s egg: Tracking a spy through the maze of computer espionage,” *Physics Today*, vol. 43, p. 75, 1990.

[3] B. Cheswick, “An evening with berferd in which a cracker is lured, endured, and studied,” in *Proc. Winter USENIX Conference, San Francisco*, 1992, pp. 20–24.

[4] F. Cohen *et al.*, “The deception toolkit,” *Risks Digest*, vol. 19, 1998.

[5] J. D. Monroe, “Deception: Theory and Practice,” 2012.

[6] K. E. Heckman, F. J. Stech, R. K. Thomas, B. Schmoker, and A. W. Tsow, *Cyber Denial, Deception and Counter Deception*. Springer, 2015.

[7] J. B. Bell and B. Whaley, *Cheating and deception*. Transaction Publishers, 1991.

[8] D. L. Smith, *Why We Lie: The Evolutionary Roots of Deception and the Unconscious Mind*. Taylor & Francis, 2005.

[9] R. Wassermann, M. F. Gulen, C. Sala, S. G. Perin, Y. Lou, J. Rybniker, J. L. Schmid-Burgk, T. Schmidt, V. Hornung, S. T. Cole, and Others, “Mycobacterium tuberculosis Differentially Activates cGAS-and Inflammasome-Dependent Intracellular Immune Responses through ESX-1,” *Cell host & microbe*, vol. 17, no. 6, pp. 799–810, 2015.

[10] F. Cohen, “A Framework for Deception,” *National Security Issues in Science, Law, and Technology*, p. 123, 2007.

[11] D. C. Daniel and K. L. Herbig, *Strategic military deception*. Pergamon, 1982.

[12] M. Hilbert, “Toward a synthesis of cognitive biases: How noisy information processing can bias human decision making.” *Psychological bulletin*, vol. 138, no. 2, p. 211, 2012.

[13] J. Thompson, R. Hopf-Wichel, and R. E. Geiselman, “The cognitive bases of intelligence analysis.” DTIC Document, Tech. Rep., 1984.

[14] M. G. Haselton, D. Nettle, and P. W. Andrews, “The evolution of cognitive bias,” *The handbook of evolutionary psychology*, pp. 724–746, 2005.

[15] D. M. Buss, *The handbook of evolutionary psychology*. John Wiley & Sons, 2005.

[16] J. Baron, “Thinking and deciding 4th ed,” 2008.

[17] M. H. Almeshekah, “Using deception to enhance security: A taxonomy, model, and novel uses,” Ph.D. dissertation, Purdue University, 2015.

[18] R. J. Heuer, *Psychology of intelligence analysis*. CIA Center for the Study of Intelligence, 1999.

[19] L. Spitzner, *Honeypots: tracking hackers*. Addison-Wesley Reading, 2003, vol. 1.

[20] L. Spitzner, “The honeynet project: Trapping the hackers,” *IEEE Security & Privacy*, vol. 99, no. 2, pp. 15–23, 2003.

[21] M. T. Qassrawi and H. Zhang, “Client honeypots: Approaches and challenges,” in *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*. IEEE, 2010, pp. 19–25.

[22] M. Wählisch, A. Vorbach, C. Keil, J. Schönfelder, T. C. Schmidt, and J. H. Schiller, "Design, implementation, and operation of a mobile honeypot," *arXiv preprint arXiv:1301.7257*, 2013.

[23] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Hostage: a mobile honeypot for collaborative defense," in *Proceedings of the 7th International Conference on Security of Information and Networks*. ACM, 2014, p. 330.

[24] C. C. Ho and C. Y. Ting, "A conceptual framework for smart mobile honeypots," *Available in:<goo.gl/UutvCT> Acessed in Mar, 2016.*

[25] L. Spitzner, "Honeytokens: The other honeypot," 2003.

[26] A. Juels and R. L. Rivest, "Honeywords: Making password-cracking detectable," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 145–160.

[27] M. H. Almeshekah, C. N. Gutierrez, M. J. Atallah, and E. H. Spafford, "Ersatzpasswords: Ending password cracking and detecting password leakage," in *Proceedings of the 31st Annual Computer Security Applications Conference*. ACM, 2015, pp. 311–320.

[28] J. Yuill, M. Zappe, D. Denning, and F. Feer, "Honeyfiles: deceptive files for intrusion detection," in *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC*. IEEE, 2004, pp. 116–122.

[29] B. M. Bowen, S. Hershkop, A. D. Keromytis, and S. J. Stolfo, *Baiting inside attackers using decoy documents*. Springer, 2009.

[30] M. Bercovitch, M. Renford, L. Hasson, A. Shabtai, L. Rokach, and Y. Elovici, "HoneyGen: An automated honeytokens generator," in *Intelligence and Security Informatics (ISI), 2011 IEEE International Conference on*. IEEE, 2011, pp. 131–136.

[31] K. Padayachee, "Aspectising honeytokens to contain the insider threat," *IET Information Security*, vol. 9, no. 4, pp. 240–247, 2014.

[32] J. White, "Creating personally identifiable honeytokens," in *Innovations and Advances in Computer Sciences and Engineering*. Springer, 2010, pp. 227–232.

[33] J. J. Yuill, "Defensive Computer-security Deception Operations: Processes, Principles and Techniques," Ph.D. dissertation, 2006.

[34] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Information and software technology*, vol. 51, no. 1, pp. 7–15, 2009.

[35] B. Whaley, "Toward a general theory of deception," *The Journal of Strategic Studies*, vol. 5, no. 1, pp. 178–192, 1982.

[36] D. C. Daniel and K. L. Herbig, "Propositions on military deception," *The Journal of Strategic Studies*, vol. 5, no. 1, pp. 155–177, 1982.

[37] U. Army, "Field manual 90-2, battlefield deception," 1988.

[38] S. Gerwehr and R. W. Glenn, *The art of darkness: deception and urban operations*. Rand Corporation, 2000, vol. 1132.

[39] "Joint publication 3-13.4 - military deception," Tech. Rep., 2006.

[40] M. H. Almeshekah and E. H. Spafford, "Planning and integrating deception into computer security defenses." ACM, 2014, pp. 127–138.

[41] C. De Faveri, A. Moreira, and V. Amaral, "Goal-driven deception tactics design," in *Software Reliability Engineering (ISSRE), 2016 IEEE 27th International Symposium on*. IEEE, 2016, pp. 264–275.

[42] A. Van Lamsweerde, "Requirements engineering: from system goals to uml models to software specifications," 2009.

[43] A. Van Lamsweerde, "Elaborating security requirements by construction of intentional anti-models," in *Proceedings of the 26th International Conference on Software Engineering*. IEEE Computer Society, 2004, pp. 148–157.