Cyber Threats and Cyber Deception in Hybrid Warfare

William Steingartner[1], **Darko Galinec**[2]

[1]Faculty of Electrical Engineering and Informatics, Technical University of Košice
Letná 9, 042 00 Košice, Slovakia
e-mail: william.steingartner@tuke.sk

[2]Department of Informatics and Computing, Zagreb University of Applied Sciences, Vrbik 8, 10000 Zagreb, Croatia
e-mail: darko.galinec@tvz.hr

Abstract: Paper deals with the design of the model of hybrid threats and cyber deception platform and solution for cyber threat detection. National networks face a broad range of cyber threats. It includes advanced and persistent peril that can evade commercially available detection tools and defeat generic security measures. Cyber attacks are becoming more intense and complex as they reflect an increasing level of sophistication, e. g. by advanced persistent threat (APT) activity. This environment of menace is of a global nature when transcending geographic boundaries and characterized by the emerging development of offensive cyber capabilities that are an inherent part of conflicts. Deception methods and techniques are being successfully employed by attackers to breach networks and remain undetected in the physical and in the virtual worlds. However, in the world of cyber security, deception as a tactic and element of a more robust defensive strategy has been still largely underexploited. The broad concepts of deception within cyber security were introduced decades ago. Still, these were technological solutions focused on providing technical capabilities to distract, mislead or misdirect the attacker. Only recently has the focus shifted on to how to shape the attackers' sense-making of what is happening as they illegitimately explore networks. In this way, Cyber Deception nowadays provides an opportunity to scare, deter, and retaliate against those that violate organizations' systems. In connection with the foregoing authors created and presented the novel model of hybrid threats in hybrid warfare as a combination of multiple conventional and unconventional tools of warfare. Authors investigate the cyber deception platform and industrial model and solution for threat detection using deception-based methods.

Keywords: cyber attack; cyber deception; cyber threats; hybrid threats; hybrid warfare

1 Introduction

The goal of this paper is to construct new Hybrid Threats Model and investigate the cyber deception platform and industrial model and solution for threat detection using deception-based methods.
Our online dependency is going to strongly influence the security of the society. In light of the introduced trends, data integrity, privacy, data security, individual safety and even public safety can be threatened [18]. To summarize, the spread of connected devices and the growing influence of the cyberspace on our life will make it necessary to improve the protection of safety and security [17]. A cyber attack is an act or action initiated in cyberspace to disrupt, deny, degrade or destroy by compromising communication, information and other electronic systems, or the information that is stored, processed or transmitted on these systems. Cyber Defense is the means to achieve and executive defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communications, information or other electronic systems, or the information that is stored, processed or transmitted on these systems [12]. Global security depends on international stability and global prosperity. The fast-paced development and spread of technology and communications have enabled new means of influence and coercion. Adversaries continuously operate below the threshold of armed conflict. Extending one's influence without resorting to physical action is the "new normal". It is possible to provoke and intimidate citizens and organizations without fear of legal or military consequences. The constraints under which the member nations have chosen to operate in cyberspace, which include the adoption of a traditionally high threshold for response to adversarial activity, are well known. This insight may be used to exploit dependencies and vulnerabilities in cyberspace; systems, processes and values [20, 26]. Aims of these actions include to weaken democratic institutions and gain economic, diplomatic and military advantages. Ensuring common defense and security is the ultimate objective to be sustained by its core activities, and that large-scale or irregular armed conflict or hybrid war is an undesirable aspect of international relations. We are living in a world of competition and conflict, in which adversaries are positioning their other elements of power (political/social, diplomatic and economic) in such a way that they have a clear advantage. If the way of positioning ourselves before any existing conflict does not grant us freedom of movement and sometimes information superiority, we may not be able to survive. The tendency to clearly divide areas of expertise such as cyberspace, electronic warfare, signals intelligence etc. [22, 23], and treat them separately may prevent from having a broader view and realizing that being shaped by the adversary's intent. Cyber Deception exploits technical assets such as honeypots and honeytokens to spy on and manipulate the activities of a network attacker [13, 32]. Honeypots are effective precisely because attackers do not know if they are there and where they will be. However, honeypots are also a controversial technique; they essentially bait and capture intruders skirting the fine line between keeping attackers out of a network versus inviting them in [31]. We look at Cyber Deception in a national defense context across the five layers of cyberspace (Figure 1); from the physical through to the persona layers. The current practice should be explored and expand the scope of this rapidly developing new area. Cyber Deception is tipped to be one of the biggest

growing sectors of Cyber Defense and Security in the coming years. There is a fundamental difference between how deception-based mechanisms work in contrast to traditional security controls. Deception-based techniques provide significant advantages over traditional security controls [25, 27]. Cyber deception considers trends and developments in deception technologies, threat hunting, analysis, and sensor capabilities, evolving tactics, techniques and procedures (TTPs) of hostile attackers and explores the contribution that it can make to defeat them as well as additional opportunities for capability enhancements in the near-term [6].

Section 2 deals with basic notions on hybrid threats and Cyber Deception Technology. Section 3 explains Hybrid Threats Model, including convergence between Cyberoperations and Electronic Warfare. Case study on Deception based Defense Platform Design is described in Section 4. Conclusive last section reveals benefits which can be achieved by application of proposed concept. The approach itself is open for enlargement, dynamic adjustments and extensions needed to fulfill business and cybersecurity system needs.

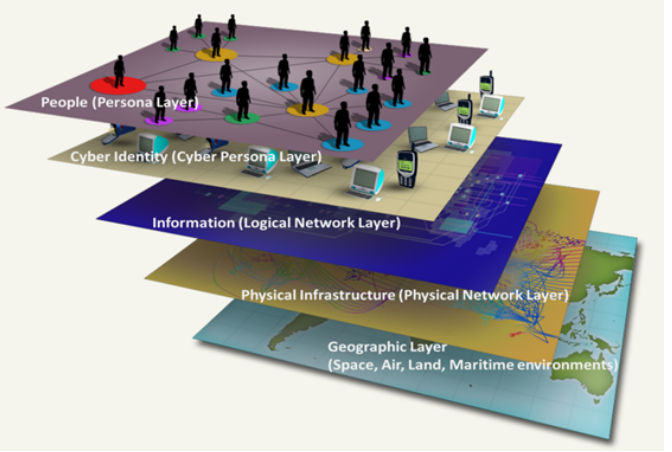

Figure 1
Cyber Environment

2 Basic Notions on Hybrid Threats and Cyber Deception Technology

A cyber attack can be invisible, asymmetric, multi-role, deniable, global/instantaneous and a complete doctrine changer when the attacker has the advantage, which makes it an ideal toolset for big and small actors alike. A wide variety of parties (actors) are active in cyberspace, including own forces, allied forces, neutrals and adversaries. A range of the actors can be classified as threats, actual or potential:

- Nation-states: nation-states are well-resourced actors that are characterized by geopolitical-, economic- and/or military motivations. They are capable of launching enduring and/or sophisticated attacks, often for intelligence and/or sabotage purpose. Nation-states often work through proxies.

- State-proxies: state-proxies are private organizations and/or institutions that are sponsored and supported by a government to help that government to achieve its geopolitical, economic or military objectives.
- Cyber terrorists: groups of people or individuals who attack or influence networks, systems and information, especially against civilians, to spread terror or in the pursuit of political aims.
- Cyber criminals: criminal groups driven by profits. They are typically looking for personally identifiable information (PII), critical digital resources to hijack for ransom or lucrative ways to conduct their classic criminal business online.
- Hacktivists: individuals who adhere to a specific cause and set up attacks to distribute propaganda or to damage organizations to which they are opposed.
- Insider threats: individuals from within the own organization who misuse privileges and resources accidentally or on purpose (e.g. disgruntled employees).

Overlaps may exist between different categories of threat actors as particular actors may choose to employ other categories as proxies. Extensive reuse of TTPs by different types of threat actors renders the distinguishing of categories by this means a hazardous proposition [14]. This paper aims to construct the novel model of hybrid threats as well as to investigate actions for cybersecurity and cyber defense in conditions of increasing challenge of cyber attacks and the limited capabilities to respond to this threat. Secondly, the aim is to describe the platform and solution for threat detection using deception-based methods putting it into the context of the aforementioned developed model. Deception Technology was one of the most researched hot topics in 2019, only second to Zero Trust. Analysts have also increased their coverage and endorsement of cyber deception as a foundational threat detection solution for organizations of all sizes. Deception has materially changed in its capabilities as well as operational efficiency over the last decade. It is now a far cry from the original honeypot [3].
In comparison with the newest related work in the area related to security operations technologies and services innovations aiming to help security and risk management leaders enhance their strategy [5, 16], our paper originality lays in investigation of the cyber deception platform and industrial model and solution for threat detection using deception based methods, within the Hybrid Threats Model.

2.1 Hybrid Threats

New information technologies have reduced appreciably the distance – physical, temporal, and informational – between the troops and their superiors. Remote engagement of the enemy 'at arm's length' is turning into the principal tactic to achieve the goals of combat action or operation. Adversary targets are now attacked at any point of enemy territory. Differences between strategic, operational, and tactical actions, and between offense and defense are leveling off. High-precision weapons are used on a growing scale. Weapons based on new physical principles and robot-controlled systems are going into service in large quantities [9]. The rapid devel-

opment of information technologies in the late 20^{th} and early 21^{st} centuries, and widespread use of information in society and the leading countries' armed forces have changed significantly nature, methods, and techniques used by state and government political and economic agencies, affected social relationships and the nature, methods, and techniques of military operations, and created new information threats and challenges [10]. Characteristics of hybrid threats are [15]:

- Coordinated and synchronized,
- Deliberately target democratic states' and institutions' systemic vulnerabilities,
- Use a wide range of means,
- Exploit the threshold of detection and attribution as well as the border between war and peace,
- Aim to influence different forms of decision making at the local (regional), state, or institutional level.

Hybrid Warfare is a combination of multiple conventional and unconventional tools of warfare (Figure 2) [15].

Figure 2
Hybrid Warfare

2.2 Cyber Deception Technology

Cyber defense focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with. Security operations technologies and services defend information technology (IT) systems from attack through the identification of threats and exposure to vulnerability, enabling effective response and remediation [21, 28, 29, 30]. The innovations included here aim to help security and risk management leaders enhance their strategy. The

focus of Gartner's Hype Cycle for Security Operations 2020 report's approach to deception is an organization's readiness for deception [5, 16].
The next three paragraphs explain the following terms in connection with cybersecurity: Security leaders, Data points and Maturity.
Security Leaders. It will prove to be an impossible task for any leadership team to be confident that their current security control set allows them to be prepared for every eventuality. More importantly, leadership teams need to try and deliver cyber resilience and keep systems operational. Therefore, being able to detect threats on its own may not be enough. Detection and prevention need to be fused together to deliver operational resilience. The key here is not to spend the security budget entirely on detection but to think about being able to detect attack vectors well before they get anywhere near your networks. This is referenced in the Gartner report as "intelligent business-driven decisions". The challenge for security leaders is how to get to the point whereby they are empowered to make those types of decisions. To make the right decision the correct data points are needed.
Data points. For data points to empower decision making, they need to possess a number of key characteristics. The data points must be contextualized, relevant, timely and have a very low operational overhead to generate and process. Deception technology and security tools can produce these types of data sets in an automated manner, delivering the right data at the right time, thus empowering decision making that is business-centric and intelligent. Most importantly, we do not have to wait to detect the attackers once they are inside our network and impacting our operational processes. Having the ability to deploy deception campaigns beyond our network perimeter (including cloud or a hybrid infrastructure) empowers us to get ahead of our adversaries. Understanding what tactics, techniques and procedures are being used against the organization's TTPs will enable a preventative posture to be adopted by leadership teams. There's a need to collect the correct data sets on attackers that enable to detect them whilst they are trying to breach an organization's network and not after the event.
Maturity. It all sounds like the kind of activity that the very large global organizations would be undertaking because they have the resources that allow them to think about and execute intelligent business-driven security operations. In the Hype Cycle Report, it is made clear that organizations of all security maturity should be examining the value that deception can bring them – allowing them to fuse prevention and detection into a fully strategic security operations model. The next three paragraphs describe Low, Medium and High Maturity organizations levels. For each maturity level, the key strategic benefits of deception technology should be defined.
Low maturity organizations. Those that are defined as not being capable of managing solutions such as Security Information and Event Management technologies (SIEMs) due to a lack of resources. This type of organizations would benefit enormously from deception technology. The Cyber Deception Platform not only scales seamlessly but the scarcity of false positives and high fidelity of alerts powerfully remediates the pain points commonly suffered by such organizations. But it does much more than remediate paint points; it enables powerful new functionalities such as the ability to generate threat intelligence that is specific to such organizations and fully correlated and contextualized. Pivot away from simple detection and into prevention and actionable intelligence.

Medium-Maturity Organizations. Defined as organizations that may already have SIEM and Endpoint Detection and Response as an emerging technology that addresses the need for continuous monitoring and response to advanced threats (EDR) type technologies. The cost in terms of time and resources can make leveraging such technology to deliver preventive security very difficult. EDR is also up against a number of different techniques that can circumvent it, such as process hollowing. To mitigate these pain points, deception technologies can provide a different means of detecting the attackers, by forcing the attackers to be right all of the time instead of those that are defending the network. There is a possibility to turn the probability of detecting an attacker in an organization's favor by forcing him into impossible choices. The solution that allows to pivot away from detection into prevention by allowing an organization to deploy campaigns that enable it to map and correlate attackers well before they get anywhere near the organization's network is needed. Fusing together detection and prevention into a single platform allows us to develop a defense-in-depth strategy that is coherent and forward-thinking.
High-maturity organizations. According to the report, may want to use deception technology in a number of different situations, such as in operational environments Supervisory Control and Data Acquisition (SCADA), Operational Technology (OT), where traditional security toolsets are not a viable option. In addition to this, the report states that deception technology can generate local threat intelligence. Mature security organizations use deception technology to actively collect data points on different types of threat vectors and actors that are looking to target them. Rather than wait for attackers to get inside the network, organizations have to map adversary behavior to draw out not only TTPs but also the strategic objectives of the threat actors. Understanding both data sets allows an organization to understand if currently deployed security controls would be effective against attackers with these particular strategic objectives in mind. With the cyber deception platform, multiple campaigns can be created and automated, allowing an organization to create intelligence-led deception campaigns that allow an organization to gather the intelligence they need to empower themselves and to make "intelligent business-driven decisions" [16].
The question is not if the organizations are mature enough for deception, but: if they want to make "intelligent business-driven decisions". If the answer is yes, then they have to leverage the power of cyber deception to empower the organization. Intelligence-led decisions will not only create a more cohesive security strategy, but it will drive down risk and the costs associated with those risks if they were ever to materialize [9].

3 Hybrid Threats Model

This Section, first of all, deals with Convergence between Cyberoperations and Electronic Warfare, given in Section 3.1. Then, in Section 3.2, New Generation War concept is explained. Section 3.3 explains such a terms as Identified Knowledge, Identified Risk and Unidentified Risk as qualitative approach to threats and risk identification and classification. In the last Section (3.4), some directions on further development of cyber deception are elaborated.

3.1 Convergence between Cyberoperations and Electronic Warfare

Communications and Information Systems (CIS) and weapon systems must face an increasing number of cyber-attacks using the Electro-Magnetic Spectrum (EMS) as a component of the kill chain. Moreover, a combination of cyber activities and Electronic Warfare (EW) are proliferating and tend to lessen systems' resilience to an unacceptable level. Therefore, cyber defensive operations have to integrate EMS comprehension and dominance as a key factor. Exploring similarities and differences between cyber and EW is yet necessary to strengthen detection and remediation of offensive Cyber Electro-Magnetic Activities (CEMA), and contribute to developing defensive CEMA schemes.
Cyberspace defensive operations can benefit from EW techniques when the electromagnetic spectrum is used as a vehicle for a cyber-attack. For example, active electronic scanned array (AESA) radars (which allow thousands of radio beams to transmit at once) and software-defined radios (which transform how a radio wave is transmitted) can rely on computer systems to manage their exposure to spectrum operations. The software can help shape how these radars and radios transmit, potentially making it difficult for an adversary to either detect jam or attack their transmissions. Changes to the software can easily transform a radar or radio from a receiver to a transmitter. Having small, adjustable arrays allows AESA radars, in particular, to focus small beams of radio energy on potential targets.
Electronic warfare is part of Electro-Magnetic Spectrum Operation. Spectrum Management Operations (SMO) mission is to manage the administrative, engineering and operation of the electromagnetic spectrum. Electronic warfare can also be defined in missions (such as support measures or countermeasures), which contain several objectives of actions.
We can define the following activities that would be part of cyber operations:

- offensive cyber operations (OCO);
- defensive cyber operations (DCO) (including active defense);
- cyber intelligence, surveillance and reconnaissance (cyber ISR); and
- cyber operational preparation of the environment (cyber OPE).

The convergence between cyber and EW is defined as the synchronization and coordination of offensive, defensive, inform and enabling activities, across the electromagnetic environment and cyberspace – CEMA (Cyber and Electro-Magnetic Activities).
Cyberspace can be described with the following properties:

– Bilateral Human and network engagement,
– Hyperconnectivity and networking,
– No geographical boundaries,
– Not owned or controlled by governments, but by commercial entities.

3.2 New Generation War

Cyber threats are multi-faceted and rapidly evolving. A military commander needs a cyber decision support system tailored to the mission to react quickly and assign tasks to subordinate units. Impact assessment and risk management are essential parts to evaluate the cyber situation and to offer remediation as part of a mitigation plan [7].
Exploring similarities and differences between cyber operations and Electronic Warfare we can notice that Electronic Warfare and Cyberspace are interdependent because as Electromagnetic spectrum is used as a medium for Cyberspace in a similar manner. Cyberspace can have an impact on Electromagnetic systems which are vital for military operations. The main challenges of conflicts where cyber-attacks are involved, affect all military domains. Digitalization provides opportunities but also new risks for cyber-attacks. With respect to the strategic and tactical planning, the biggest problem lies in attribution, i.e. finding out who carried out a cyber-attack. Attribution is vital when it comes to actions of retaliation against another nation-state and possibly engagement in a cyberwar. A malicious attack can easily be spoofed therefore disguise its actual origin, making it nearly impossible to trace back to the original source. This reality fosters covert cyber operations and becomes vital for cybercrime and cyberwar. In order to avoid international misinterpretations and retaliation against possibly innocent countries, it is necessary to develop an international system of order for the cyber world. The probability of starting a cyber war based on a misunderstanding and, or pre-emptive retaliation based on missing information, against an innocent actor, is high in the current unregulated cyber world that is directly connected to our future IoT (Internet of things) and our military IoBT (Internet of battle things) [7, 33].

3.3 Identified Knowledge, Identified Risk and Unidentified Risk as qualitative approach to threats and risk identification and classification

Although unknown unknowns may be unidentifiable, they might be presumed likely in some component of the system. A likely event cannot be thought to be unknown unknown because it is already identified, but its consequence may fall into the category of unknown unknowns. The occurrence of an event like a natural disaster may be forecasted easily, but its impact is not easy to predict or estimate because of knock-on effects. Despite that project risk management acts as “forward-looking radar” it is not possible to identify all risks in advance, in part for the following reasons [11]:

- Some risks are inherently unknowable.
- Some risks are time-dependent.
- Some risks are progress-dependent.
- Some risks are response-dependent.

A typical classification of risks is based on the level of knowledge about a risk event’s occurrence (either known or unknown) and the level of knowledge about its

Table 1
Schematic Structure of Modified Risk Categorization

Identification \ Certainty	Certain (Known)	Uncertain (Unknown)
Identified (Known)	Known known (identified knowledge)	Known unknown (identified risk)
Unidentified (Unknown)	Unknown known (untapped knowledge)	Unknown unknown (unidentified risk)

impact (either known or unknown). This leads to four possibilities:

- Known–knowns (knowledge),
- Unknown–knowns (impact is unknown but existence is known, i.e., untapped knowledge)
- Known–unknowns (risks) and
- Unknown–unknowns (unfathomable uncertainty) [4].

The proposed model modifies and extends these categories to incorporate insights and explain how to use the model to identify hidden uncertainties and shows how recent catastrophes can be mapped to the model. Table 1 [11] shows a schematic structure of the risk categorization. In this table, the model categorizes events by "identification" and "certainty".

In this matrix, if the nature of an event is certain, it is more like a fact or knowledge. It could be what we already know, i.e., known known, or what we don't know yet, i.e., unknown known. If the nature of an event is uncertain, the occurrence can be uncertain, i.e., the probability of occurrence is less than 1, and the impact can be uncertain as well. For example, a hurricane has two basic uncertainties. One is a track, represented by the chance of landfall, and the other one is intensity, represented by wind speed or hurricane category. If either one of occurrence or impact is uncertain, that event is considered to be uncertain. Often, people know the identity of an uncertain event, which means known unknown. Sometimes, people even don't know what that is, which means "unknown unknown". Most natural disasters are uncertain events, but people already know what they are.
Once identified, an unknown unknown is converted to a known unknown and moved to the quadrant at the right top in this matrix. Converting unknown unknowns to known unknowns means reducing the number of unidentified uncertainties even though we don't know how many of them are still remaining unidentified. The more unknown unknowns are identified, the less chance a project will have to be affected by a surprise [8, 11].

3.4 Further Development of Cyber Deception

Following the establishment of UK National Cyber Deception Laboratory (NCDL) as a non-profit entity will bring together a unique range of internationally renowned practitioners and researchers in the field of Cyber Deception across government,

academia and industry. By building on this existing foundation NCDL aims to create an environment that catalyzes imaginative and innovative cyber deception research. Cranfield University, in partnership with the UK Defense Cyber School, will support the establishment of the NCDL which will facilitate, encourage and promote a world-class portfolio of research activity, and provide advice across the full spectrum of cyber deception operations. In particular, NCDL will conduct research aimed at exploring concepts within each of the following themes:

- Cyber Deception in the context of national defense and security,
- Denying attackers the freedom to operate within organizations' networks,
- Cyber Deception as an effective means of manoeuvre in cyberspace,
- Communicating intent to aggressively defend,
- Deterring Cyber attacks,
- Shaping the behavior of cyber attackers,
- The layered approach to defensive cyber operations,
- Developing the means to exploit cyberspace to the best advantage,
- Moving Cyber Defense on to the front foot.

4 Case Study

One reason for the bump of deception technologies is the typically low signal-to-noise ratio of traditional enterprise security systems, which disposed tons of data and not nearly enough meaningful, actionable priorities. Attivo's platform is designed to do the aforementioned while touching on important use cases for detection, verification, vulnerability management and analysis, controls and automation, and anti-malware. The method is to see and recognize critical behavioral signals among gobs of noise. The expectation is that network-based deception technologies will continue to rise in terms of relevance as a key adjunct to broad-based layered security, certainly in key verticals, and perhaps extending over the longer term to mainstream use.

4.1 Deception-based Defense Platform Design

Sometimes is heard that defensive security technologies need to adapt and play some offense, too. Offensive security includes capabilities and orientation to see and process intelligence and target opportunity data in the manner of an attacker. Target analysis is the focus of penetration testing, vulnerability management and attack simulators – each an area of intensified product and service innovation in recent years. Attack surface area has been broadly elevated to blatant conceptual risk, and technologies such as micro-perimeters can reduce and obfuscate application target profiles to very low levels. Network and endpoint targets are getting an upgrade as well, with deception technologies converting attacker data for active defense use

cases. Lack of dedication to improving contextual intelligence and work prioritization has come to the surface in the dialogue between customers and vendors. Vendors can look over customers' shoulders and see a range of underutilized commercial so-called 'solutions' – perhaps even their own. Deception technologies have evolved from honeypots and honeynets and are now mainstream in spots, such as a sandbox capability to overcome malware's resistance to emulation [2].

4.1.1 Example 1

Product. Attivo characterizes the market opportunity for its ThreatMatrix platform as one of continuous threat management, geared to early and high-efficacy detection, verification, and response to advanced external and internal threats. Deploys out of band using a switch trunk port; components emphasize a lightweight yet comprehensive presence, authentic and dynamic behavioral deception, early and accurate detection capabilities, and scalability. Competes roughly equally, we would say, on the basis of deception realism, detection accuracy and comprehensive capabilities. By its nature, post-breach deception technology has to be able to detect and inform on attacks that were able to overcome other defenses. ThreatMatrix for detection and tracking is designed and indicates that customers derive strong value from their ability to follow, in a safe environment, attack steps and lifecycles, including lateral movement, privilege escalation, polymorphic obfuscation, and time-triggered strategies. The ThreatMatrix platform includes BOTsink engagement servers and decoys, ThreatStrike endpoint deception suite, ThreatPath for attack path vulnerability assessment, and Central Manager for larger deployments and threat intelligence. An approach to deception is designed to facilitate simulation of user networks, endpoints, data center and cloud environments, industrial control systems, IoT and point-of-sale environments. Out-of-the-box integrations with major perimeter, endpoint and SIEM vendors facilitate automated blocking and quarantine of attacks based on ThreatMatrix detection and analysis. An additional console (ThreatOps, in development) will add bidirectional controls to bring Attivo's detection and verification capabilities to a wider security operations footprint, including attack intelligence sharing, playbook enhancements, attack scoring and threat hunting. BOTsink appliances and cloud instances are available in two sizes, depending on the number of virtual local area networks (VLANs) supported. ThreatStrike deception objects may include credentials, browser cookies, ransomware bait with attacker engagement and file detainment, and email phishing (ribbon bar) icons for users to submit suspicious messages for analysis. The suite includes an endpoint device. ThreatPath calculates potential vulnerabilities associated with misconfigurations and misused credentials and is priced by an endpoint, and complements adversary tracker, which indicates attacker movement and associated timelines. Management reports good trajectories for average deal size and renewals; service terms are typically twelve months, but occasionally run to multiyear.
Technology. Deception and other simulation technologies meet a growing need for advanced behavioral-driven detection and analysis to improve, if not change, traditional network security, and not merely perimeter-based weaknesses. Deception is but one example of simulation technique applied to cybersecurity challenges; security vendors leveraging simulation for a range of use cases may be on the cusp

of breaking into wider view. Deception technology platforms have evolved from honeypots and honeynets to encompass a cross-section of techniques, including detection through simulation (i.e., deception), sandboxing, attack verification, attacker surveillance through engagement, automation, forensic analysis, and increasingly wider assimilation with production environments. BOTsink engagement (deception) server hosts the company's core Multi-Correlation Detection Engine (MCDE), which includes a network sandbox. Management contends that the design approach for MCDE provides for not only high-fidelity attack verification and drill-down inspection, but also vital integration with incident response activities, including forensics, compliance (e.g., chain of custody) and automation. The company indicates that some customers are also using MCDE to ingest artifacts from other sensors and detection systems. MCDE analytic output (including IOC, PCAP, STIX, CSV formats) can be viewed through Threat Intelligence Dashboard or SIEM consoles and used by prevention, isolation, or remediation workflow systems. Components of a comprehensive deception setup include an engagement server and a diverse set of decoy lures (typically virtual machines) running over real OS instances, including network services, endpoints, credentials, data and file shares, servers, cloud environments and applications. Realism in decoy targets is critical and includes attributes such as golden images of customized environments, currency and logical proximity to actual targets, and protection with similar fortifications. Recently introduced Camouflage is a branded framework for authenticity through dynamic behavioral deception, and it underscores the company's targeted edge in terms of breadth and depth for the platform's lures. Camouflage updates in field trials include automated self-learning for disparate environments, and continuous post engagement bait freshening (i.e., decoy respins) to avoid attacker fingerprinting and evasion [2].

4.1.2 Example 2

Innovation in threat detection. Detection using deception-based methods provides the innovation required to non-disruptively evolve to an Active Defense security posture. By placing a detection net over endpoints or by deploying a fabric of decoy-based detection throughout the network stack, companies can achieve efficient detection for every threat vector, early in the life-cycle of an attack. Deception uses a mix of high-interaction decoys, lures, and misdirections to deceive attackers into revealing themselves, quickly alerting on and identifying the lateral movement of threats that have evaded other security controls (Figure 3) [2].
These solutions are proactively uncovering and responding to external, internal, and third-party threat actors. Organizations of all security maturity levels are aggressively adopting these technologies to mitigate risks related to employee credential theft, data exfiltration, ransomware, crypto-mining, and attacks that try to disrupt services or impact public safety. The accuracy and ease of use of this detection method have been a significant driver in its adoption and wide-spread deployment [2].

Solution. The ThreatDefend® Detection and Response Platform uses endpoint lures, misdirections, and high-interaction deception decoys that provide early visibility into in-network threats, efficient continuous threat management, and acceler-

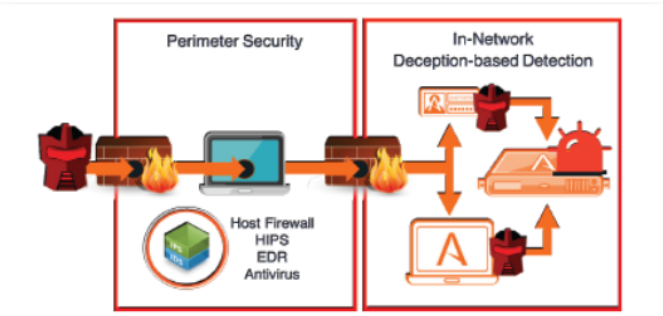

Figure 3
Deception-based Methods for Innovation and Evolvement to Active Defense

ated incident response.
The ThreatDefend platform, recognized as the industry's most comprehensive in-network detection solution provides a detection fabric for cloud, network, endpoint, application, data/database, and Active Directory decoys and is highly effective in detecting threats from virtually all vectors such as APTs, stolen credentials, Man-in-the-Middle, Active Directory, ransomware, port knocking and more. These deceptions can deploy within all types of networks, including endpoints, user networks, server, data center, ROBO, cloud, and specialty environments such as IoT, SCADA, POS, SWIFT, infrastructure, and telecommunications (Figure 4).
The ThreatDefend Deception Platform creates an active defense against cyber threats. It includes the BOTsink® deception servers for decoys, the Informer dashboard for displaying gathered threat intelligence, as well as the ThreatOps® incident response orchestration playbooks; and the Endpoint Detection Net suite, composed of the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, and ADSecure for Active Directory defense. The ThreatDirect deception forwarders support remote and segmented networks, while the Central Manager (ACM) for BOTsink and the Endpoint Detection Manager for EDN deployments add enterprise-wide deception fabric management.

Detection and attack path visibility. The platform provides unparalleled visibility into threats inside the network and attacker lateral movements and tactics. The platform detects advanced threats propagating throughout the network by laying strategic decoys and lures to deceive, detect, and defend against attacks as they scan network clients, servers, and services to target and seek to harvest credentials.
Lures and decoys work together to attract and detect attackers in real-time, raising evidence-based alerts while actively engaging with them so that the platform can safely analyze their lateral movement and actions. For attacker believability, the decoy systems mirror-match production assets by running real operating systems, full services, and applications, along with the ability to customize the environment by importing the organization's golden images and applications. As a result, the platform creates environment designed to redirect attackers away from company assets. Machine learning prepares and deploys the decoys, keeping the network and endpoint deceptions fresh and making ongoing maintenance easy.

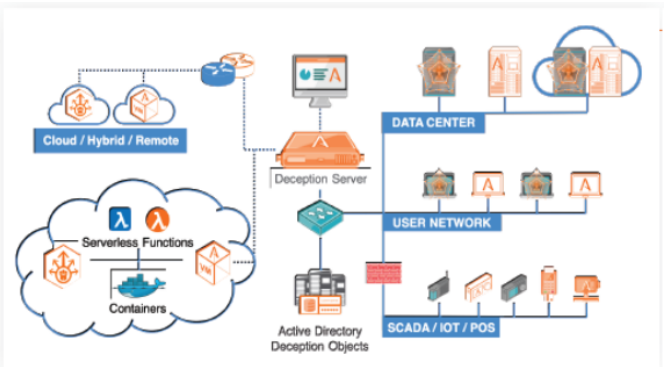

Figure 4
The ThreatDefend Platform

To increase decoy authenticity and for visibility into attempts to compromise systems or recon Active Directory, the solution creates AD decoys both as fake AD controllers and at the endpoints to modify unauthorized AD queries. By inserting deception into areas that attackers target for reconnaissance, the deployment appears as part of the production environment in multiple layers. The ADSecure solution looks out for unauthorized AD queries, alerts on the activity, and alters the response to return fake AD objects that lead to decoys for engagement. The solution disrupts network discovery attempts by detecting and alerting on ping sweeps and port scans. Additionally, it redirects any port scans that touch a closed port on a host to an open port on a decoy, making host fingerprinting difficult and misinforming the attacker as to the actual ports and services accessible on a host. This capability does not interfere with any production services while providing early detection of attacker lateral movement. The solution can natively isolate any inbound or outbound traffic on a host to connect only with the decoy environment. Endpoint deceptions and hidden mapped shares provide easy and highly effective redirection of attacks seeking to harvest credentials or execute a ransomware attack. Additionally, the endpoint defenses can hide local files, folders, removable drives. For remote workers, the ThreatDefend platform protects both the VPN infrastructure and credentials for VPN, cloud PaaS, IaaS, and SaaS. The solution can deploy decoys within the VPN network segment to identify network discovery and AD reconnaissance activities that indicate lateral movement. It seeds fake VPN credentials at remote endpoints that alert on remote theft and reuse and integrates with cloud services to monitor for unauthorized use. With the rapid migration to the cloud, the detection fabric needs to scale seamlessly anywhere the enterprise network sits. The ThreatDefend platform offers extensive support for AWS, Azure, Google, and Oracle cloud environments inclusive of decoys and lures for containers, storage buckets, and other native cloud technologies. The ThreatDefend platform capabilities include support for serverless functions, access keys, reconnaissance, credential harvesting, and verifying the efficacy of security controls, along with CloudWatch/SIEM monitoring for finding attempted use of deception credentials. The ThreatPath solution reduces the attack surface and proactively increases se-

curity by identifying misconfigurations and credential exposures that create attack paths for attackers to use for lateral movement. A topographical visualization and attack path associations provide a straight-forward view of how attacks can reach their target. When paired with the BOTsink server's threat intelligence and attack time-lapsed replay, defenders achieve unprecedented levels of threat visibility and the information required to build a pre-emptive defense against its adversaries [2].
Active defense and accelerated incident response. In addition to the early detection of attackers inside the network, the ThreatDefend platform's actionable alerts, automated analysis, and native integrations for incident handling work collectively to dramatically improve a responder's time-to-remediation. When an attacker engages with a decoy system, credential, application, data, or Active Directory object, the ThreatDefend platform records, and alerts on the activity while simultaneously responding to the attacker. The Informer dashboard consolidates the data and assembles forensics, correlates events, and raises evidence-based alerts on malicious activity. Alerts only occur on confirmed attacker interactions with the decoys or engage within the Endpoint Detection Net, and, unlike other detection methods, does not depend on signatures or behavioral analysis to detect an attack. The attack analysis substantiates alerts the security teams can use to automate the blocking of an attacker, to isolate an infected system, and to hunt for other compromises so that a company can completely eradicate the threat from the network. Minimizing false positives and creating high fidelity alerts save valuable hours for security teams in both investigation and response time. The Informer dashboard presents a comprehensive view of the incident and forensic information gathered during an attack. Forensic reports include identifying infected systems and command and control (C&C) addresses and available as exported IOC, PCAP, and STIX file formats to allow easy information sharing and attack recording. By correlating all relevant information and forensics from an event into a single interface, the Informer dashboard gives analysts and incident response teams a streamlined view of an attack to effectively contain and remediate the incident. This accelerates intelligence-driven response, enhances network visibility, and creates a predictive defense to improve their security posture. The solution enables offensive counterintelligence functions designed to disrupt the attacker's ability to collect accurate information. It also provides defensive counterintelligence functions as it diverts attacks from production assets, and collective counterintelligence information on attacker TTPs and IOCs, giving insight into attacker objectives. Additionally, DecoyDocs delivers data loss tracking, allowing organizations to track stolen documents inside or outside the network, and the ADSecure solution gives insight into attacker goals based on the high-priority AD objects they are targeting. Organizations can also use the ThreatOps functions of the BOTsink server to automate incident handling and create repeatable incident response playbooks. Organizations can fully customize this threat orchestration function to match their environment and policies so that security teams can make faster and better-informed incident response choices [2].

Conclusions

The future of warfare will be in a digitalized multi-domain environment, which needs new doctrines [24, 35] for the conduct of operations. To ensure the readiness of the capacities needed for this new environment, research in all relevant domain-specific cyber capabilities is needed. Each military domain has its own requirements for cyber as different sensors are used, different procedures and different tactics for automated responses are needed. The Cyber research requirements for the military cyber domain are often underestimated, as the research requirements are twofold. First, the military cyber domain needs to develop its own protection and attack capabilities, which are often not available on the market. Second, the military cyber domain needs to develop protection techniques, sensors and procedures to protect the military cyber infrastructure of all other military domains. Moreover, the military cyber domain needs to be prepared for attacks on the national cyber infrastructure, including infrastructure for civilian use, in case, commercial cyber protection measures are not working. This range of military cyber responsibilities is often underestimated. But the main result of the cyber threat assessment showed clearly, that the existing cyber defense strategies, need improvement to counteract the existing cyber threats [7].

New technologies are expected to increase the speed of conflict dramatically. The military strategy is confronted with the pervasive connectivity of sensors and various sources of information. The internet of the battle things (IoBT) will bring radical changes to the digitalization of the battlefield [34]. Solutions are yet to be tested on how this abundance of information is going to be leveraged, by new technologies like the use of big data (e.g. [19]). This fast transformation will also affect the commander's decisions and the way information is processed. In this context, the existence of a Global Information Grid (GIG) is evident. It comprises a group of networks to connect ground, maritime, air, space and cyberspace assets, able to communicate in a joint operation. The joint network must ensure a "secure register" to identify whether an asset is trustful or not. One of the main challenges affecting the "internet of the battle things" is that devices can be lost, reverse engineered and brought back to the battlefield by an opponent. To avoid losing our tactical advantage, a "secure register" is needed. Other features - to maintain the confidentiality, integrity and availability of the information handled by military communication and information systems – are interoperable secure sensors connected to the GIG, intelligent devices fed with AI algorithms to identify an exchange of meaningful information, the availability of secure clouds to store information and AI-supported multi-domain operations to achieve tactical and strategic effectiveness. In this realm, quantum computing [36] will be a crucial factor further increasing battlefield complexity. A holistic approach to new scenarios opens the operational environment to non-military aspects highlighting the need to implement information exchange practices with civilian actors. Moreover, apparently unrelated events in other sectors e.g. economy or energy may have consequences for military missions. These features, influence the design of future Command and Control (C2) systems and need to be considered when new processes, regulations and strategies, for military forces are developed to take full advantage of the digitization of military technology [7].

Organizations are applying deception and detection techniques to the global fight for information dominance, where they need an advantage against the adversary. Well-architected deceptive environment can be used in a tactical manner, to aid awareness, identification, and provide the necessary fidelity around alerts and adversarial movements. We can use deception to monitor the awareness of our attacker, and measure or assess the effectiveness and integrity of our response options [3].
Finally, Cyber Deception Platform and Industrial Solution are presented: Threat-Defend® Platform scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory, and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response [1]. The novel constructed model of hybrid threats as well as the results of investigation of actions for cybersecurity and cyber defense in conditions of increasing challenge of cyber attacks and the limited capabilities to respond to this threat is presented.
Some future research should be conducted within NCDL (as mentioned in Section 3.4) where researchers, suppliers and customers will be brought together to address problems, explore opportunities and advance capabilities in a space not previously explored, in order to support collective understanding in the space of cyber deception to aid the development of capabilities and strategies as well as in the provision of advice and guidance on cyber deception in proactive defense more broadly [6].
We described the design and performance of industrial model – cyber deception platform and solution for threat detection using deception-based methods, introducing a novel approach to cybersecurity and cyber defense putting it into the context of the Hybrid Threats Model within Hybrid Warfare.
The ways (processes) and means (resources) of cyber deception pre-emptive approach can impair the effects of cyber-attacks through getting information about adversaries' behavior into an organization and consequently achieving the enhancement of the level of resilience by reducing "unknown unknowns" (unidentified risk: unidentified/uncertain), transferring them to identified risk (identified/uncertain) and "known knowns" (identified knowledge: identified/certain) sequentially.

Acknowledgement

This work was supported by the Project KEGA 011TUKE-4/2020: "A development of the new semantic technologies in educating of young IT experts".

References

[1] Attivo Networks: Attivo Networks Named as a Sample Vendor in Gartner Hype Cycle for Security Operations 2020, Press Release, Attivo Networks, Fremont, CA, 2020.

[2] Attivo Networks: Threatdefend Platform Solution Overview, Attivo Networks, Fremont, CA, 2020.

[3] BrightTALK: Deception Technology in APAC – Looking Forward to 2020, `https://www.brighttalk.com/webcast/17319/387403/`

deception-technology-in-apac-looking-forward-to-2020, Accessed: Aug 24th, 2020.

[4] D. Cleden: Managing Project Uncertainty (Advances in Project Management, 1st Edition), Gower, 2009.

[5] Counter Craft: Am I Ready for Cyber Deception? Gartner Hype Cycle for Security Operations, https://www.countercraft.eu/blog/post/am-i-ready-for-deception-technology/, Accesed: Aug 24th, 2020.

[6] Cranfield University: Cyber Deception, The National Cyber Deception Symposium, UK MoD's Defence Academy and Defence Cyber School, Nov 6th, 2019, Shrivenham, Swindon, UK, https://www.cranfield.ac.uk/events/symposia/cyber-d, Accesed: Aug 24th, 2020.

[7] European Defence Agency (EDA): Strategic Research Agenda On Cyberdefence, EDA, Brussels, Belgium, 2020.

[8] D. Galinec, Lj. Luić: Design of Conceptual Model for Raising Awareness of Digital Threats, *WSEAS Transactions on Environment and Development*, Vol. 16, Art. #50, World Scientific and Engineering Academy and Society – WSEAS, Athens, Greece, pp. 493–504, 2020.

[9] V. V. Gerasimov: Tsennost' nauki v predvideniyi [Prevision is what Science is Valued For], *Voyenno-promyshlenniy kur'yer*, # 8(476), Feb 27–Mar 5 2013.

[10] Y. Y. Gorbachov: Kibervoyna uzhe idyot [A Cyber-War is Already on], Nezavisimoye voyennoye *obozreniye*, # 13, Apr 12^{th}-18^{th}, 2013.

[11] S. D. Kim: Characterizing unknown unknowns. Paper presented at PMI® Global Congress 2012–North America, Vancouver, British Columbia, Canada. Newtown Square, PA: Project Management Institute, 2012.

[12] NATO: Report on Cyber Defence Taxonomy and Definitions AC/322-N(2014)0072, May 2014.

[13] NATO Communications and Information Agency (NCIA) and AFCEA TechNet International: NITEC '16 - The NCI Agency Industry Conference and AFCEA TechNet International, June, 7th – 9th 2020, Tallinn, Estonia, 2016, https://docplayer.net/55237431-Ncia-business-opportunities-cyber-security.html, Accesed: Aug 24th, 2020.

[14] The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE): Commanders' Handbook A. Dalmjin, V. Banse, L. Lumiste, J. Teixeira, A. Balci (Eds.) 2020 © NATO CCDCOE Publications, Tallinn, Estonia, 2020.

[15] NATO Special Operations Headquarters – NSHQ: Countering Hybrid Threats Seminar, Croatian Military Academy "Dr. Franjo Tuđman", Croatian Armed Forces, Ministry of Defence, Zagreb, 3^{rd}–5^{th} Sep, 2019.

[16] P. Shoard: Hype Cycle for Security Operations 2020 report, Published: 23rd Jun 2020, ID: G00467096, Gartner, Inc., 2020.

[17] Á. Török, Z. Szalay, B. Sághi, Development of a Novel Automotive Cybersecurity, Integrity Level, Framework, *Acta Polytechnica Hungarica*, 17(1):141–159, 2020.

[18] National Research Council, Engaging Privacy and Information Technology in a Digital Age, J. Waldo, H. S. Lin, L. I. Millett (eds.), The National Academies Press, Washington, DC, 2007.

[19] M. Tang, M. Alazab and Y. Luo, Big Data for Cybersecurity: Vulnerability Disclosure Trends and Dependencies, *IEEE Transactions on Big Data*, 5(3):317–329, 2019.

[20] W. Wu, R. Kang, Z. Li, Risk assessment method for cybersecurity of cyber-physical systems based on inter-dependency of vulnerabilities, In *2015 IEEE International Conference on Industrial Engineering and Engineering Management* (IEEM), pp. 1618–1622, 2015.

[21] J. Akram, L. Ping, How to build a vulnerability benchmark to overcome cyber security attacks, *IET Information Security*, 14(1):60–71, 2020.

[22] J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity, *Journal of Computer and System Sciences*, 80(5):973–993, 2014.

[23] Z. Haig, Electronic warfare in cyberspace, *Security and Defence Quarterly*, 7(2):22–35, 2015.

[24] A. Colarik A, L. Janczewski, Establishing Cyber Warfare Doctrine, In: Lemieux F. (eds) *Current and Emerging Trends in Cyber Operations*. Palgrave Macmillan's Studies in Cybercrime and Cybersecurity. Palgrave Macmillan, London, 2015.

[25] M.H. Almeshekah, E.H. Spafford, Planning and Integrating Deception into Computer Security Defenses, In: *NSPW '14: Proceedings of the 2014 New Security Paradigms Workshop*, Victoria, British Columbia, Canada, ACM, New York, NY, USA, Sep 2014.

[26] S. Achleitner, T. La Porta, P. McDaniel, S. Sugrim, S.V. Krishnamurthy, R. Chadha, Cyber Deception: Virtual Networks to Defend Insider Reconnaissance. In *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats* (MIST '16). Association for Computing Machinery, New York, NY, USA, pp. 57–68, 2016.

[27] N. Virvilis, B. Vanautgaerden, O. S. Serrano, Changing the game: The art of deceiving sophisticated attackers, In *2014 6th International Conference On Cyber Conflict* (CyCon 2014), Tallinn, 2014, pp. 87–97, 2014.

[28] S. Szymoniak, How to be on time with security protocol?, *Societal Challenges in the Smart Society*, ETHICOMP Book Series, Universidad de La Rioja, pp. 225-237, 2020.

[29] O. Siedlecka-Lamch, S. Szymoniak, M. Kurkowski, I. El Fray, Towards Most Efficient Method for Untimed Security Protocols Verification, In *Proceedings of the 24th Pacific Asia Conference on Information Systems: Information Systems (IS) for the Future*, PACIS 2020, Dubai, Jun 20–24, 2020.

[30] O.S. Yeremenko, M.O. Yevdokymenko, Ohlyad teoretychnykh rishen' shchodo vidmovostiykoyi marshrutyzatsiyi v telekomunikatsiynykh merezhakh [Review of theoretical solutions for fault-tolerant routing in telecommunication networks], *Problemy telekomunkatsiyi* [*Problems of telecommunications*], Kharkiv National University of Radio Electronics, 22(1):25–42, 2018.

[31] B. Scottberg, W. Yurcik, D. Doss, Internet Honeypots: Protection or Entrapment?, In: *Proceedings of the IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology*, Raleigh, NC, USA, Aug 2002, pp. 387–391.

[32] N. Kambow, L. K. Passi, Honeypots: The Need of Network Security, International Journal of Computer Science and Information Technologies (IJCSIT), 5(5):6098–6101, 2014.

[33] A. Kott, A. Swami, B.J. West, The Internet of Battle Things, *Computer* 49(12):70–75, Dec 2016.

[34] F. Popescu, From the IoT to the IoBT. The Path to Superior Situational Understanding, Land Forces Academy Review, Vol. XXIV, No 4(96), 2019.

[35] D. Ormrod, B. Turnbull, The cyber conceptual framework for developing military doctrine, *Defence Studies*, 16(3):270–298, 2016.

[36] J. Kollár, V. Florko, Solution of Selected Problems using IBM QX, *Science & military*, Vol. 1, Armed Forces Academy of General M.R. Štefánik, Liptovský Mikuláš, pp. 5–10, 2019.