Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model

Steingartner, William; Galinec, Darko; Kozina, Andrija

Source / Izvornik: **Symmetry, 2021, 13, 1 - 25**

Journal article, Published version
Rad u časopisu, Objavljena verzija rada (izdavačev PDF)

https://doi.org/10.3390/sym13040597

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:249:793730

symmetry

MDPI

Article

Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model

William Steingartner [1,*], Darko Galinec [2] and Andrija Kozina [3]

[1] Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letná 9, 042 00 Košice, Slovakia
[2] Department of Informatics and Computing, Zagreb University of Applied Sciences, Vrbik 8, 10000 Zagreb, Croatia; darko.galinec@tvz.hr
[3] Dr. Franjo Tuđman Croatian Defence Academy, 256b Ilica Street, 10000 Zagreb, Croatia; andrija.kozina@morh.hr
* Correspondence: william.steingartner@tuke.sk

Abstract: This paper aims to explore the cyber-deception-based approach and to design a novel conceptual model of hybrid threats that includes deception methods. Security programs primarily focus on prevention-based strategies aimed at stopping attackers from getting into the network. These programs attempt to use hardened perimeters and endpoint defenses by recognizing and blocking malicious activities to detect and stop attackers before they can get in. Most organizations implement such a strategy by fortifying their networks with defense-in-depth through layered prevention controls. Detection controls are usually placed to augment prevention at the perimeter, and not as consistently deployed for in-network threat detection. This architecture leaves detection gaps that are difficult to fill with existing security controls not specifically designed for that role. Rather than using prevention alone, a strategy that attackers have consistently succeeded against, defenders are adopting a more balanced strategy that includes detection and response. Most organizations deploy an intrusion detection system (IDS) or next-generation firewall that picks up known attacks or attempts to pattern match for identification. Other detection tools use monitoring, traffic, or behavioral analysis. These reactive defenses are designed to detect once they are attacked yet often fail. They also have some limitations because they are not designed to catch credential harvesting or attacks based on what appears as authorized access. They are also often seen as complex and prone to false positives, adding to analyst alert fatigue. The security industry has focused recent innovation on finding more accurate ways to recognize malicious activity with technologies such as user and entity behavioral analytics (UEBA), big data, artificial intelligence (AI), and deception.

Keywords: cyber attack; cyber deception; cyber threats; hybrid threats model; resilience

Citation: Steingartner, W.; Galinec, D.; Kozina, A. Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. *Symmetry* **2021**, *13*, 597. https://doi.org/10.3390/sym13040597

Academic Editors: Kuo-Hui Yeh, Chunhua Su and Shi-Cho Cha

Received: 16 March 2021
Accepted: 1 April 2021
Published: 3 April 2021

1. Introduction

The goal of this paper is to construct a novel Hybrid Threats Model and investigate the cyber deception approach for threat detection using deception-based methods.

As companies adjust their business models and explore digitization opportunities, new risks arise, and companies can become more vulnerable to cybersecurity threats. Procedures need to be reviewed and updated to mitigate any potential vulnerabilities. As a result, an emerging focus on security architecture has arisen to help organizations create a roadmap to mitigate cybersecurity risks. Security architecture is the design of artifacts that describe how security controls are positioned and how they relate to the overall system architecture. In this exercise, organizations define technology standards to prevent development teams from using rogue technologies that may include vulnerabilities. Additionally, monitoring outdated technologies is also important so as not to run into unintended breakdowns. Using security architecture, organizations can view their impact on the business and prioritize their replacement. Another important aspect of mitigating

the cybersecurity risk is creating reference architecture models that integrate regulatory and company policy requirements. Infrastructure diagrams including security items such as firewalls should be designed providing guidelines for their implementations. It is also imperative to track vulnerabilities of each IT asset using online libraries that list all possible weaknesses [1].

Technology is an indispensable and integral part of today's business in helping to drive growth and improve operations. It is now commonplace to think of corporate strategies and digital strategies in the same way. The current COVID-19 crisis has made this viewpoint more urgent than ever as executive leadership moves beyond just seeing technology as a cost-saving vehicle. In a 2020 McKinsey study, more than half of executives say they are investing in technology for competitive advantage or refocusing their entire business around digital technologies. These mindset shifts regarding digital technology are even more apparent at companies with declining revenues as they acknowledge they were behind their peers in the use of digital technology. COVID-19 pushed companies over the technology tipping point and transformed business forever. Organizations must now build a flexible digital organization that can withstand disruption, with an architecture resilient-by-design, embedded in technologies and processes [2]. An efficient, high-performing, and adaptable information technology (IT) ecosystem becomes a real business asset [1].

Deception should not be viewed as a"rip and replacement" of existing security controls; it complements and enhances them. The decision to add deception should be based on a need for early and simplified threat detection, closing in-network detection gaps, and strengthening security programs across multiple environments and threat vectors, and a need for the ability to do things that other security solutions cannot do. Additionally, deception provides visibility into exposed attack paths, attacker activity, and captured threat intelligence. This, paired with forensic recording, enhances and elevates a security team's ability to prevent an attack and to respond decisively when under attack. Adding a new capability to a security stack can come with complexity as security teams work to incorporate the solution into their operations. This is generally not the case with a deception platform. Such platforms integrate with existing systems in a way that requires minimal effort to deploy, operate, and manage.

Security technologies must continually evolve to match transformations across digital business landscapes. Product managers must address new security risks and threats posed by new infrastructures, business-enabling technologies, and evolved security programs [3]. "It's true that when distributed deception technology first emerged, honeypots were the most analogous solution to describe the way that deception worked, in that a honeypot also tries to trick attackers into an engagement. However, deception has come a long way since the early heyday of honeypots, and its more lightweight, far more valuable descendant is proving extremely versatile when it comes to use cases. Unlike honeypots that are typically used to trap attackers to study their late-stage attack behaviors, endpoint deceptions are false data elements meant to be encountered early in the attack lifecycle. At first interaction with any false data, a high-fidelity notification is triggered, showing exactly what has been attempted and where. In fact, next-generation deception technology has emerged as the most effective and earliest way to detect and stop attacker movement inside the environment. With all the overblown promises on the market, coupled with the extreme and immediate need for strong cybersecurity, organizations can have a hard time figuring out whether any particular security product or service is really going to be effective at catching attackers before they reach critical data. Gartner notes that deception technology not only 'does well in proof of concept (POC)' and 'perform(s) well during the sales cycle;' it also 'proved to be a worthy technology to add to security programs.' By understanding the truths about deception technology—and clearing up the misconceptions—organizations can start implementing a new security approach that is easily deployed, proactive, and effective" [4].

Advanced deception platforms will not disrupt other network functions. They operate out of the band and have the flexibility to white-list devices to avoid conflicts. They also

do not require the installation of endpoint agents. A deception platform's high-fidelity alerts become a true forces multiplier when applied to endpoint detection and response (EDR), network traffic analysis (NTA), and security information and event management (SIEM) [5] solutions for better and more accurate detection. Native platform integration with existing security infrastructure provide seamless sharing of attack information and facilitate automation. Benefits include automated blocking, isolation, threat hunting, and repeatable playbooks that accelerate incident response. Some solutions also provide integrations with threat orchestration tools for streamlined operation [6].

Cyber deception exploits technical assets such as honeypots and honeytokens to spy on and manipulate the activities of a network attacker [7,8]. 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 [9].

Deception-based techniques provide significant advantages over traditional security controls [10,11]. Cyber deception considers trends and developments in deception technologies, threat hunting, analysis, and sensor capabilities, evolving tactics, and 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 [12].

Section 2 deals with basic notions of Cyber Deception Technology. Section 3 explains the Hybrid Threats Model, including Resilience as the first line of defense, New Generation War with Cyberwarfare, Cyber Resilience and Further Development of Cyber Deception. Section 4 elaborates and depicts Military Education for Cybersecurity. Case study on Cyber Deception is described in Section 5 with The Attack Cycle, Deception Goals and Types of Deception Technology along with Advanced Deception for an Active Defense. The conclusive last section reveals benefits that can be achieved by the application of the proposed approach. The approach itself is open for enlargement, dynamic adjustments, and extensions needed to fulfill business and cybersecurity system needs.

2. Basic Notions on Cyber Deception

As the founder of the Honeynet Project, Lance Spitzner Director, SANS Institute has always been fascinated by the world of deception. Deception brings tremendous advantages to the cyber defender, from simplified threat detection and hunting to cyber intelligence gathering and dynamic defenses. Early attempts at deception technologies, including honeynets, were hampered by complexity. However, since those early days, deception has rapidly evolved in efficacy, scalability, and ease of use. His history with honeynets started when their solution was built in 1998, which eventually led to the Honeynet Project. In many ways, this is when cyber deception was born. A lot has changed over the last 23 years. Commercial deception has increased its overall efficacy and has dramatically decreased the time it takes to create and manage a deception network from weeks down to what a single systems admin can do during their lunch break [6].

"Increased compute power, artificial intelligence, and tools on the Dark Web are equipping cyber attackers with the resources to launch more sophisticated and destructive attacks. Reactive defenses are no longer enough to stop attackers from infiltrating even the best security architectures. Environmental dynamics are also changing and disrupting resiliency with the rapid adoption of cloud infrastructure and the proliferation of IoT devices. The concept of a perimeter as we have known it is disappearing and the battle against cybercrime has moved inside the network. With this shift, organizations need to rethink their security strategies as well as the tools they have traditionally come to rely on" [13]. Prevention-only defense is no longer enough, and organizations are seeking new tools and programs for early detection, faster response, and gaining a better understanding of their adversaries. Cyber deception is serving to meet these needs driven by its simplicity, ease of use, and ability to complement security solutions already in place. The solution

uniquely carries the benefit of not only being able to disrupt and derail attacks but also, in its power to shift the asymmetry in the direction of the defenders [6].

For millennia, deception has been used to effectively confuse and outmaneuver opponents in warfare, sports, and gambling. Now, deception is being applied to the cyber realm to create uncertainty in the attackers' mind, to trick them into making mistakes that reveal their presence, and to make the overall attack economics unfavorable. With deception technology, security teams do not need to wait and react to an attack. Instead, they can deploy bait, lures, and decoys designed to derail attacks early and throughout the attack life-cycle. Attackers typically harvest credentials, conduct reconnaissance, and move laterally to complete their attack. With a deception fabric, organizations create a virtual minefield consisting of credential bait and decoys that mirror the production environment's operating systems, applications, and data. As soon as an attacker interacts with a deceptive asset, the security team receives a high-fidelity, engagement-based alert with the information required to not only stop the threat's actors but also understand them. Unlike other detection tools, a high-interaction deception environment provides defenders with the option to safely study their opponent while gathering adversary intelligence. By gaining insight into the attacker's tools, methods, and intent, the defender is armed with deeper knowledge for strengthening overall defense strategies, leveling the playing field with their opponent [6].

Attackers have remained undetected in networks for much too long after the initial compromise. Dwell time ranges from 79 days to over 200 days, depending on the region and source of the report. These numbers reinforce that an attacker is afforded far too much time in an enterprise while remaining undetected. Conversely, even when defenders successfully disrupt and remediate attacks, too often, little useful information is gathered about the adversary. This lack of information makes verifying the removal of the attacker's foothold and preventing a successful return extremely challenging. Unlike attackers, who gain knowledge about the environment each time they attack, defenders do not acquire additional insight, putting them at a distinct disadvantage. As in physical attacks, understanding potential adversaries is critical to countering their next move [6].

2.1. Hybrid Threats

"Hybrid warfare can be seen as 'a concept of operations, or perhaps, an operational concept, rather than a strategy or a theory of warfare.' We also adopt the term 'hybrid adversary' for an actor applying the hybrid warfare concept and 'hybrid threats' as potential actors and trends that exist in the security environment before the hybrid warfare concept is applied (which is more an act). Hybrid warfare can be more easily characterized than defined as a centrally designed and controlled use of various covert and overt tactics, enacted by the military and/or nonmilitary means, ranging from intelligence and cyber operations through economic pressure to the use of conventional forces. By employing hybrid tactics, the attacker seeks to undermine and destabilize an opponent by applying both coercive and subversive methods" [14].

"Hybrid threats can be characterized as a mixture of coercive and subversive activity, conventional and unconventional methods (i.e., diplomatic, military, economic, technological, information) which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of open organized hostilities. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalize (even with propaganda [15]), recruit and direct proxy actors can be vehicles for hybrid threats" [16].

2.2. Cyber Attacks and New Cyber Threats

Heading attackers off at the pass begins with quality threat defense. This could be a layered solution approach or leading threat intelligence spread across the security environment. Seven types of cyber-attacks exist, shown mapped to the layers of information

systems' Open Systems Interconnection Model (OSI-Model) created by the International Organization for Standardization (ISO), as shown in Figure 1 [17].

The characteristic of the OSI-model is that it standardizes the communication functions of a communication and information system regardless of the underlying technology and internal structure. The model aims at achieving the interoperability of miscellaneous communication systems through standard communication protocols. Furthermore, the role of security protocols is irreplaceable [18,19].

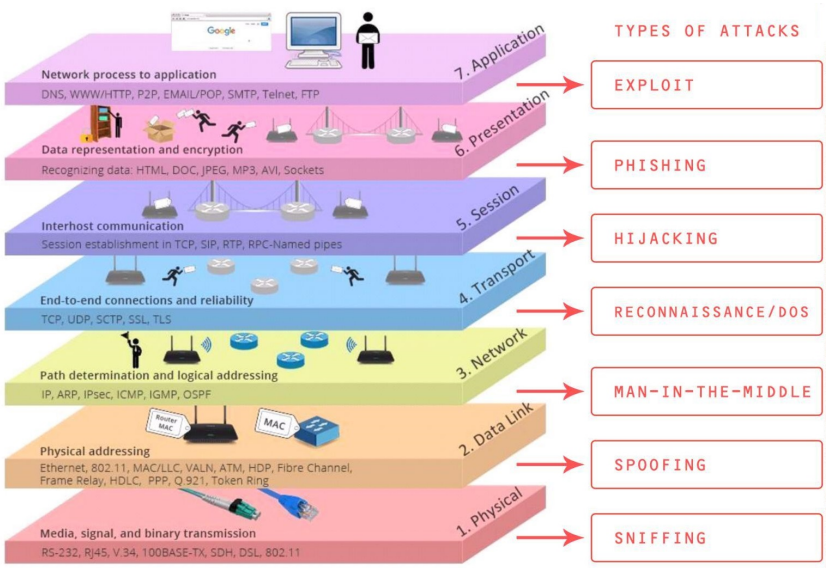

Figure 1. Information Systems' Open Systems Interconnection Model (OSI-Model) layers and types of attack mapping.

"Advanced cyber threats are already here, 2020 has been an outlier in countless categories, including cyber threat trends. The year has taught us many things the hard way, including the importance of preparing for known threats. Yet, as we all adjusted to the new realities of the pandemic, the world kept turning. Technology continued to advance. Markets continued to grow. Cyber threats continued to evolve. Today importance of preparing for known threats exists. In the span of a few weeks, the economy, education systems, and lifestyles are altered by a scenario that experts had long been warning about. Cyber threats are increasing in both scope and frequency.

"Much of that evolution is related, at least somewhat, to the pandemic. From ransomware operators refining and polishing their business models, to the rapid adoption of cloud as organizations seek to gain operational efficiencies, threat actors are evolving and attack surfaces are expanding. In a time of change and adaptation, upcoming cybersecurity challenges, and guidance on how to prepare for them are to be explored." [20]

The report [20] covers eight key cyber threat trends anticipated for 2021:

1. Next-Generation Extortion and Evolution in Malware Business Models
2. Supply Chain Attacks via Cloud-Hosted Development Environments
3. AI, Evasion, and Theft
4. Parcel and Shipping as Critical Infrastructure
5. Mandated Contact Tracing Apps May Open Doors for Large-Scale Cyber Attacks
6. Cybercriminals Will Likely Capitalize on Rapid U.S. Telehealth Adoption
7. Fifth Generation Network (5G) to Expand the Attack Surface for Industrial Internet of Things (IoT)
8. 5G to Increase Security Pressure on Mobile Hotspots.

2.3. Cyber Deception Approach

Deception is based on planned, deliberate, and controlled actions to conceal the networks, create uncertainty and confusion in the adversary's mind, delay and manipulate their efforts to establish situational awareness, and influence and misdirect perceptions and decision processes [21], thereby causing them to take or not take actions that are beneficial to the defender's security posture. Active defense goes one step further in applying the learnings from attacks to confidently respond to the immediate incident, mitigate risks from a returning adversary, and build pre-emptive defenses. Cyberwarfare is "the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes." Deception in information security gives public and private sector organizations the same defensive advantages the military gains from deception in actual warfare: causing an adversary to make mistakes, wasting the opponent's time and resources as they pursue false targets, and giving the defense valuable intelligence on their adversary and the data they need to confidently stop an attack.

3. Hybrid Threats Model

This Section first deals with resilience as the first line of defense, given in Section 3.1. Then, in Section 3.2, New Generation War with Cyberwarfare is explained and the novel Hybrid Threats Model is presented. Section 3.3 explains Cyber Resilience. In the last Section 3.4, some directions on the further development of the cyber deception approach are elaborated.

3.1. Resilience: the First Line of Defense

Modern societies are highly complex with integrated and interdependent sectors and vital services. This makes them vulnerable to a major disruption in the case of a terrorist or hybrid attack on critical infrastructure (Figure 2) [22].

Figure 2. Interdependent societal sectors and vital services vulnerable to a major disruption in the case of a hybrid attack.

Hybrid threats (particularly recent cyber attacks) continue to target the civil population and critical infrastructures, owned largely by the private sector. These developments have had a profound effect, bringing into sharp focus the need to boost resilience through civil preparedness. Today, Allies are pursuing a step-by-step approach to this end—an effort that complements NATO's military modernization and its overall deterrence and defense posture [22].

3.1.1. Baseline Requirements

In 2016, at the Warsaw Summit, Allied leaders committed to enhancing resilience by striving to achieve seven baseline requirements for civil preparedness [22]:

1. assured continuity of government and critical government services
2. resilient energy supplies

3. ability to deal effectively with the uncontrolled movement of people
4. resilient food and water resources
5. ability to deal with mass casualties
6. resilient civil communications systems
7. resilient civil transportation systems.

"This commitment is based on the recognition that the strategic environment has changed, and that the resilience of civil structures, resources and services is the first line of defense for today's modern societies. More resilient countries—where the whole of government, as well as the public and private sectors, are involved in civil preparedness planning—have fewer vulnerabilities that can otherwise be used as leverage or be targeted by adversaries. Resilience is therefore an important aspect of deterrence by denial: persuading an adversary not to attack by convincing it that an attack will not achieve its intended objectives. Resilient societies also have a greater propensity to bounce back after crises: they tend to recover more rapidly and can return to pre-crisis functional levels with greater ease than less resilient societies" [22]. The recovery process is usually connected with an increase in optimism among economic parties, and a belief that the situation is going back to normal, i.e., a growth trend. People should again trust each other and the system. Trust and boundaries seem to be irreplaceable in building and sustaining socio-economic growth in the pandemic world [23]. As researchers Tokarčíková et al. reported, improvement of appropriate professional skills of further generations [24] and acting in a social responsible way [25] can generate positive consequences increasing achievement of sustainability goals and building resilient societies. This makes continuity of government and essential services to the population more durable. Similarly, it enhances the ability of the civil sector to support a NATO military operation, including the capacity to rapidly reinforce an Ally.

Such resilience is of benefit across the spectrum of threats, from countering or responding to a terrorist attack to potential collective defense scenarios. Consequently, enhancing resilience through civil preparedness plays an important *rôle* in strengthening the Alliance's deterrence and defense posture [22].

3.1.2. Ensuring Coherence of Effort

With the changing security environment, defense planning efforts have been reinforced, including in the area of civil preparedness. Seven baseline requirements (Section 3.1.1) include a systematic approach to improving these capabilities. Regular assessments are an essential aspect, helping to identify and measure areas of progress and challenges.

"Civil preparedness is the subject of more active engagement with capitals and civil ministries in a collaborative effort to assess and advise on improvements. Assessments allow the testing of assumptions about the availability of resources, the levels of preparedness and protection of civil resources and infrastructure, including those that support the military. They help ensure coherence between efforts on resilience through civil preparedness with those on the military side. Over the longer term, they aim to promote greater civil-military cooperation in member states.

"Building on the seven baseline requirements, the commitment by Allies and the detailed planning guidance, regular assessments have provided a greater understanding of areas of progress, as well as remaining challenges" [22].

3.2. Hybrid Warfare

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 [26].

3.2.1. Active Defense vs. Cyberwarfare

The Active Cyber Defense Certainty Act (ACDC) bill submitted in 2017 proposed making changes, but to date has not been approved, and even if legalized in the US,

would still be subject to international laws that predominantly prohibit this type of activity. Law and ethics aside, attribution is typically not easy, and most organizations simply do not have the skills or tools to do this successfully. Hacking back also presents a high risk that could result in unintended consequences. This may stem from attacking the innocent or bringing on heightened attacker retaliation, which organizations may find themselves ill-prepared for. Threat deception is a much better option than retaliation. Instead, organizations can use the rich forensic, threat, and adversary intelligence gathered in a deception environment to take pre-emptive measures to fortify their defenses. By better understanding the attacker, an organization can confuse, slow down, and stop an attacker while gathering information on how they are attacking and what they may be targeting. In addition to threat and adversary intelligence, the use of decoy document beaconing functionality provides counterintelligence on what an attacker is seeking and geo-location of where the document is accessed, inside and outside the network. This capability can be invaluable in understanding what and whether something is stolen and for protecting research, intellectual property, or case files.

"Two major variables affect the utility of cyber technologies in war: the timing and operational complexity of cyber operations. Timing refers to questions of when and how long to engage in cyber operations to maximize effects. Operational complexity describes how hard it is to pull off the entire operation. Operational complexity includes various aspects such as the number of targets (one system vs. hundreds of systems to be hit at the same time), the defense level of the targets (multiple open attack surfaces vs. air-gapped systems), the availability of resources (intelligence and malware stockpile) as well as the size and internal organization and coordination of attacker teams" [27].

3.2.2. Hybrid Threats Model Components

Cyberspace is the fifth domain of operations, alongside the domains of land, sea, air, and space: the successful implementation of EU missions and operations is increasingly dependent on uninterrupted access to secure cyberspace and thus requires robust and resilient cyber operational capabilities [28]. Within the non-hierarchical Hybrid Threats Model, military and nonmilitary activities using conventional and unconventional tools and tactics are combined. Interactions between some individual layers of the model by the means of cybersecurity and cyber defense are being achieved in cyberspace as the common denominator of particular components of the model, enabling multiple threats to be realized through system's (state's) vulnerabilities [29].

To cope with the challenges, which today are manifested as unknown unknowns, systems tend to enable personnel and develop new processes, organization, and technology. Technologies are being developed that, unlike traditional approaches [30,31], can protect systems from serious threats by learning what is "normal" for the organization and its people, thereby spotting emerging anomalies. Unlike the traditional rules and signature-based approach, this technology can spot threats that could harm the organization and network that the traditional approaches would be unable to detect [32]. It can deal with uncertainty and delivers adaptive protection for organizations from both insider threats and advanced cyber-attacks [33]. A new-generation war will be dominated by information and psychological warfare that will seek to achieve superiority and weapons control and depress the opponent's armed forces personnel and population morally and psychologically. In the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory. Asymmetric actions, too, will be used extensively to level off the enemy's superiority in the armed struggle by a combination of political, economic, information, technological, and ecological campaigns in the form of indirect actions and nonmilitary measures (see Figure 3), refined and improved from [29].

Figure 3. Hybrid Threats Model.

Within the non-hierarchical Hybrid Threats Model, military and nonmilitary activities using conventional and unconventional tools and tactics are combined. Interactions between some individual layers of the model by means of cybersecurity and cyber defense are being achieved in cyberspace as the common denominator of particular components of the model, enabling multiple threats to be realized through systems' (states') vulnerabilities [29].

"These nonmilitary actions will help lessen and remove military hazards and threats by the opponents entering into peace treaties and taking other amicable steps. nonmilitary measures serve to reduce the possibility for the aggressor to engage in hostile activities against other countries, give it an unflattering image in public opinion, make sensational denunciations of its aggressive plans, and so on. Beyond a shadow of a doubt, the aggressive side will be first to use nonmilitary actions and measures as it plans to attack its victim in a new-generation war. With powerful information technologies at its disposal, the aggressor will make an effort to involve all public institutions in the country it intends to attack, pri-

marily the mass media and religious organizations, cultural institutions, non-governmental organizations, public movements financed from abroad, and scholars engaged in research on foreign grants. All these institutions and individuals may be involved in a distributed attack and strike damaging point blows at the country's social system with the purported aims of promoting democracy and respect for human rights" [34,35].

3.3. Cyber Resilience

Whether penetration testing is driven by compliance or as part of standard security resiliency testing, it is a vital component of an organization's defenses, especially in today's era of high-profile breaches [36]. In 2017, there was an unrelenting stream of headline news highlighting over 2000 successful security breaches. Attacks that led to massive amounts of compromised personal information, IP theft, financial loss, ransomware attacks, and even attacks on energy and medical organizations, which put human safety at risk. With the growing sophistication and frequency of attacks, organizations, now more than ever, need to evaluate the effectiveness of their defenses to quickly identify and close gaps that attackers can exploit. A Red Team penetration test against a Blue Team defense plays an instrumental role in identifying weaknesses in both security infrastructure and security processes. A Red Team's "real" attack on defenses will discover ways an attacker can to get into the network based on vulnerabilities or inefficiencies. Once in the network, the Red Team attacker gathers intelligence through reconnaissance activities to assess the location of assets, which credentials to harvest, and likely attack paths. Next, the team will test in-network defenses and whether the internal controls are sufficient to prevent them from accessing sensitive or critical data or from causing damage to critical infrastructure. All too often, organizations will fail their penetration tests, which can put them at compliance risk and, more concerning, at risk of a breach. Repeatedly, the root of these failures often lies in the inability to detect attacker lateral movement or credentials that are exposed to theft. The Role of Deception in Penetration Testing Organizations use deception technology to change the asymmetry against attackers. It can also be a valuable resource for tipping the odds in favor of a Blue Team over a Red Team. Deception is designed for visibility and early detection of in-network threats that have successfully bypassed perimeter and antivirus defenses. Human resources will be considered as one of the main assets in cybersecurity that will play crucial roles. To develop a human resource, the recruitment process for the competencies needed must encompass skills to develop, prevent, detect and respond in a timely manner to attacks. Cyber Resilience can be realized by strengthening all cyber defense, cybersecurity, and cyber sovereignty [37].

"In cyber deception, decoys and lures offer similar benefits in their use of camouflage to keep corporate networks and their information safe. This creates an advantage that other security tools cannot do. By hiding in plain sight, attackers can be tricked and derailed, causing adversaries to make mistakes and turning the tables on those that try to infiltrate systems. Cyber deception defense tactics protect a network by convincing a cybercriminal that they are accessing the actual network, when in fact they are wandering aimlessly through a virtual 'hall of mirrors'. This starts by providing the in-network attacker with attractive targets that replicate the look, feel, and behavior of the actual network. This is done through the use of decoy networks, which are based on the same operating systems, applications, and identities of the production systems. Placing attractive 'breadcrumbs' based on credentials and mapped drives will also proactively and quickly lure the attacker into the deception environment. So too is populating the decoy with recent, seemingly valuable, content that the attacker would expect to find. Being attractive is important, but it must also be balanced with authenticity. As such, decoy networks should not be too obvious or easy to infiltrate or attackers will promptly identify them as fakes and avoid them. A well-designed decoy network will not only reduce risk by detecting threats early but will also benefit the defender with the intelligence they could not gather elsewhere. This can be used to reduce response time down from hours to minutes and can provide a competitive advantage by using this information to fortify defenses. Whether the

motivation is in the fidelity of the detection or in the desire to gather adversary intelligence and forensics, deception is providing a unique offering and one that the adversary is not often expecting or prepared for. There are clear benefits to adding a synthetic deception environment to an organization's network. As soon as a would-be predator interacts with the decoy, they immediately reveal their presence and their activities can then be monitored and recorded. This is a unique advantage to defenders that can only be achieved within a deceptive environment. The actions taken by the attacker within the decoy system are immediately gathered and analyzed to reveal indicators of compromise and their tactics, techniques, and procedures, as well as highlighting what they might be looking to access. Such intelligence empowers IT security teams to not only deal with the present danger but also to eradicate and defend against future threats. There is also the benefit that the cybercriminal will be wasting time and resources trying to infiltrate further and further into a system that will ultimately offer up no reward. When the attacker eventually realizes they are in a fake network, they will either have to start their infiltration all over again or, not wanting to deal with the complexity a deception network adds, will move on and look for other, easier targets. For maximum adversary intelligence, it is useful for the attacker to believe for as long as possible that they are in the actual production network. This requires a deception environment that looks and behaves like the real thing and includes a safe 'sandboxed' environment so that the actions can be studied without risk to their organization. Typically, an attacker has the benefit of gathering intelligence with every attack. With deception's ability to engage the adversary, the playing field is leveled and the defender can now gain critical information to proactively fight back. The use of cyber deception has grown rapidly based on its ability to trick predators and accurately detect their presence" [38].

By projecting decoys that appear and operate like production assets on the network and at the endpoint, the organization obfuscates the attack surface, making it increasingly difficult for an attacker to distinguish what is real and what is fake, inevitably causing them to make a mistake during early reconnaissance. Deception credentials and ransomware bait placed on endpoints will serve to direct an attacker attempting to harvest credentials or access shared drives to a deception engagement server where attempted credential use or access immediately raises an engagement-based alert. By injecting deception into the network, the attack surface becomes exponentially more complex for an attacker to penetrate. This can be used to the Blue Team's advantage to prove network resiliency for network reconnaissance, credential theft, man-in-the-middle, and Active Directory Attacks. Additionally, advanced deception platforms will offer built-in attack analysis that can be used to substantiate attacks, create documentation containing the full TTPs of the attackers and Indicators of Compromise (IOC), and provide forensic reports to help attribute of the attack [39].

3.4. Further Development of Cyber Deception

The establishment of the 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 [12]:

1. Cyber Deception in the context of national defense and security
2. Denying attackers the freedom to operate within organizations' networks
3. Cyber Deception as an effective means of manoeuvre in cyberspace
4. Communicating intent to aggressively defend
5. Deterring Cyber attacks

6. Shaping the behavior of cyber attackers
7. The layered approach to defensive cyber operations
8. Developing the means to exploit cyberspace to the best advantage
9. Moving Cyber Defense on to the front foot.

4. Military Education for Cybersecurity

Nowadays, there are more and more cases of cybersecurity threats. Most threats are still covered by cybercrime, but there are more and more cyber attacks on critical infrastructure information systems. Therefore, modern military education should be directed towards properly defined learning outcomes that support cyber culture and security and develop the competencies of active military personnel in this field. Thus, it enables military personnel to be trained and prepared for cyber threats. The interactivity, flexibility and practicality offered by information and communication technologies enable the active participation of all participants in the learning process. In addition, competitive aspects in cybersecurity education promote understanding and development of analysis skills. Kozina [40] points out that military education is changing all over the world and is growing into places of development, change, scientific research, and quality teaching in a wide range of necessary skills that every officer must acquire. Many theorists when talking about military education think only of military training that develops skills, habits and abilities; therefore, the focus is on the practical part. In contrast, in the academic community, there has always been a tendency for knowledge to prevail over skills and abilities.

The military organization is, in itself, strictly structured. The ability to function and the great reliability of the military system rests on a hierarchy in which the creation of will takes place from top to bottom. The most prominent elements are command, obedience, and reporting. The authors of [41] note that the rapid growth and diversity of technical and technological knowledge is increasing. Predictions warn that military knowledge is becoming obsolete even faster, so military education should be prepared for activities and technologies that do not yet exist. The rapid development of science and technological progress lead to the necessary need to link military training with academic knowledge. This is why the purpose of military education is changing, and it is becoming a synergy of academic and military knowledge, skills, and abilities. Military education for cybersecurity must provide an answer to what activities must be carried out to protect all users of modern electronic services in the armed forces, both in commands and in units, covering all cyber threats as a whole.

From the research conducted by the US military related to Professional Military Education (PME), the following conclusions about professional military education emerge:

- professional military education must be ready to anticipate current and future challenges and adapt to them;
- there is a growing need for additional common and specific topics that should be addressed in military schools;
- experiences from lessons learned must be used in professional military education; it must not only meet current requirements but also must be flexible;
- officers must prepare for joint military operations, and this education must be part of the curriculum;
- some officers lack the key competencies needed to perform tasks effectively, so professional military education must be tailored to military needs;
- military education must train officers to make decisions independently and take responsibility for their implementation;
- the school curriculum of military education must be subject to change to be able to respond to future challenges;
- military education must improve teaching practice and adopt more demanding standards of modern teaching methods [42].

Kozina [40] states that military education, as well as education worldwide, is affected by many changes. The changes are primarily related to maintaining the common policies

of the supranational NATO and EU alliances. All adjustments have been made in such a way as to achieve a balanced education in military schools that are in the European Union or NATO members.

To make military education recognizable for the needs of anti-cyber threats, it is necessary to take into account how education is defined in NATO's: "(...) systematic implementation of teaching individuals that will improve their knowledge and skills and develop competencies." It is a developmental activity that enables individuals to make a reasonable response to an unpredictable situation [43]. It is clear from the above definition that in NATO, education is associated only with the individual. Military education is a systematic implementation of designed and organized training of military personnel, which will improve their knowledge and skills, abilities, independence, and responsibility and develop their competencies for making the right decisions in different situations.

Figure 4, adapted from [44], presents a model of military education in the armed forces; we can see that it consists of four domains: operational, professional, institutional and self-development.

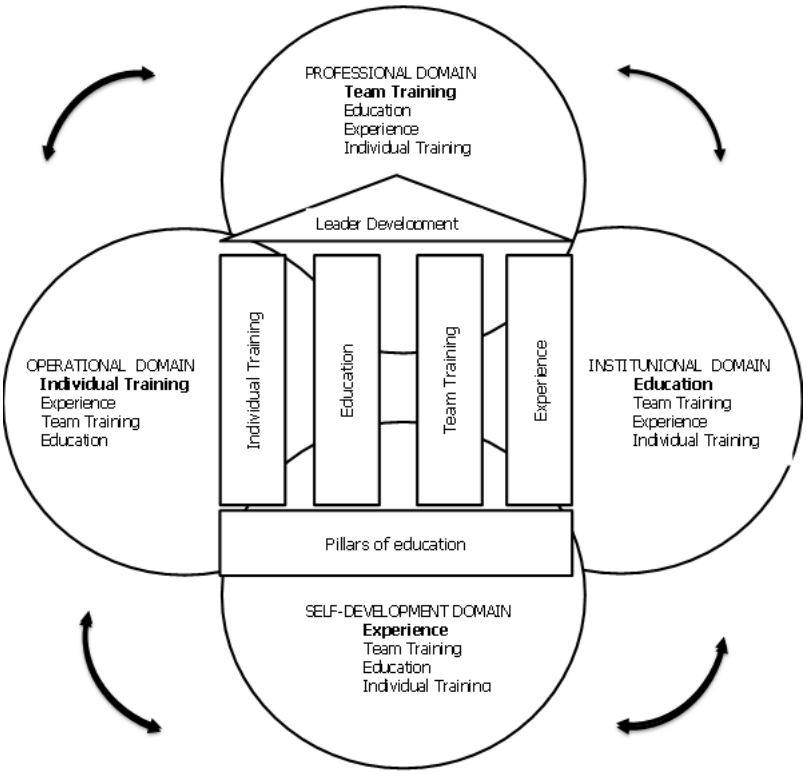

Figure 4. Military education model.

Military education for anti-cyber threats consists of four basic pillars (foundations): individual training, education, team training, and experience that supports these domains.

In the institutional domain (formal schooling), education comes first and is complemented by team training, experience gained and various forms of education and individual training provided. Formal knowledge is acquired in military educational institutions, supplemented by experience, expertise, and team and individual training. In this domain, knowledge is gained about the key concepts of cybersecurity and the principle of their operation, how to analyze hardware, software, network components and their relationships to achieve system security.

The professional domain is implemented through team training, military knowledge, and skills that are necessary for the work and professional development of each officer and are developed and supplemented by acquired education and experience so far, as well as individual training actions and procedures. In the professional domain, knowledge and

skills are developed in the use of the necessary steps for the development of a cybersecurity management system. The officers learn to distinguish the roles and responsibilities of each individual that are related to cybersecurity.

In the operational domain, the first priority is individual training with members of the armed forces who are trained to perform dedicated tasks (safe operation of information systems at different levels of command), which is complemented by experience gained in team training and education. In the operational domain of military education, skills and abilities to respond to any threat promptly are developed, using best practices that facilitate the implementation of recovery from a possible threat.

The self-developmental domain as the highest level of education. In this domain, active military personnel independently establish control over the learning process, as well as responsibility for learning outcomes. In the self-developmental domain, the most important is the will (intrinsic motivation) for learning and learning experience. Everything is based on acquired experience, team training, expertise, education, and ultimately, individual training. In this domain, employees independently study various security models (some of them are presented in [45]) that provide solutions for networking and addressing security challenges. They compare the quality of different security models that can be used with minimal modifications.

Likewise, education for civilian structures can also be identified with four domains and four basic pillars as mentioned above. There is no difference in the education for military experts and civilian experts because the threat is identical. The only thing is that education for anti-cyber threats in civilian life is not unified in one institution, rather, knowledge is acquired in different institutions.

When developing military education for the needs of cybersecurity, the basic concept of military education, which is guided by the following criteria, must not be neglected:

a. There must be a sequence of training that enables the individual to perform a higher level of responsibility and ensures the acquisition of an optimal level of knowledge for a specific higher duty.
b. There must be cooperation with the university community to synergistically use the knowledge developed by the latest research and implementation practice.
c. There must be a guarantee of the quality achieved through the evaluation of educational programs and institutions, internal evaluation, and external audits.
d. Diploma mobility and transferability of ECTS (European Credit Transfer and Accumulation System) credits earned in different educational institutions, even in different countries, must be ensured. Prerequisites for mobility include the development of procedures for the recognition of higher education qualifications following the requirements of the Bologna Process.

Every school, including the military, is constantly looking for successful and easily measurable ways of training (methods and procedures). Military schools must be efficient and satisfy the needs of all participants, including the principal, students, teachers, and other participants in military education. The authors of[46] point out "(. . .) that the purpose of any organization, public or private, is to produce a quality product or to perform a quality service." Military education is under the care of the state and officers and non-commissioned officers are educated at the expense of the budget. "One of the major challenges is to link civilian and military training—joint training of civilian and military personnel based on a comprehensive approach" [47].

In military education for cybersecurity, two basic types can be identified: general education and special education. General military education encompasses all the necessary knowledge and skills necessary for all military personnel dealing with cybersecurity, knowledge related to mass media and information technology, and text analysis and processing skills [48]. Specialist education is the narrow education needed only by military personnel working on special sophisticated systems or in specific conditions. Participants in all forms of military education should acquire military knowledge, skills, independence, and responsibility—in one word, competence—that will help them in their work and

further professional development. Fountain [49] states that they are as follows: cooperation and joint action to achieve a common goal, collaborative way of working, ability to analyze phenomena and their consequences, recognizing prejudices, stereotypes and egocentric attitudes, critical reflection on available information, ability to understand other people's attitudes, ways life and beliefs, taking responsibility for one's actions, etc.

The current system of education in military schools provides officers and non-commissioned officers (NCOs) with the necessary level of knowledge, abilities, skills, and responsibilities depending on the level of training. Based on the acquired knowledge, officers perform their tasks in various duties in the armed forces. Military education for cybersecurity is greatly affected by the reduction of the armed forces, as well as the introduction of modern systems that are increasingly complex, all of which require greater competence of officers who must make quality decisions in a shorter time.

5. Case Study

"Security investments are typically made in preventing an attack and ex-filtration. This leaves a giant blind spot for organizations as attackers that bypass the perimeter can then move laterally and steal credentials as they quietly establish a foothold, gain privileges, and recon the network in search of their targets. Deception closes the in-network detection gap by placing attractive endpoint lures, data deceptions, and traps throughout the network. Organizations will immediately gain the visibility needed to derail these attacks and remediate compromised devices" [50].

In this section, we describe cyber deception approach to cyber threats in more detail.

5.1. The Attack Cycle

Attackers have proven they can evade the perimeter to establish a beachhead inside a network from which they can laterally move while remaining undetected, often for months to years. Traditional security controls are simply not designed to stop the in-network tactics that attackers use to elude detection while traversing the network. Cyber Deception Platform should be equipped to prevent, detect, and reveal these tactics while denying attackers visibility and access to sensitive or critical data to exploit. The first system an attacker compromises from outside is just a beachhead, usually accomplished using social engineering (such as phishing emails) or exploiting externally vulnerable services (Figure 5).

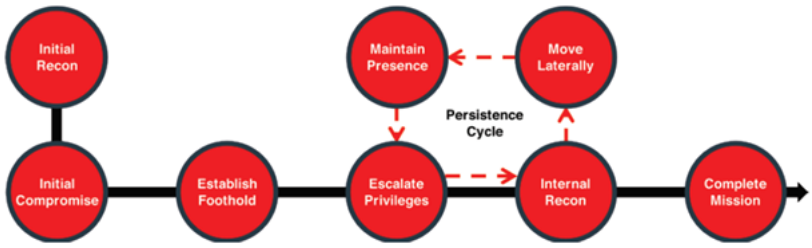

Figure 5. The attack cycle.

Once attackers compromise a host inside the network and establish a foothold, they must ensure that they can always return to continue their attacks. They install back doors and remote access tools to establish persistence mechanisms, using covert communications channels to remain hidden. They must then break out from this initially compromised system to move around. In the next stage of the attack, they conduct discovery activities to identify subsequent targets. They search the local system for data and credentials they can steal to progress their attacks. They also query Active Directory (AD) from a domain-joined system and extract sensitive information, such as domain administrator accounts, domain controller addresses, service principal names, or Kerberos tickets. They can use this data to find targets, compromise systems, and elevate privileges. Many recent attacks involved

attackers compromising Active Directory for lateral movement. Once they identify their next targets, they fingerprint the systems for any open ports or services to exploit or use the data they gathered from AD to compromise them. They then move laterally to the target and install their persistence mechanisms. Next, they look for sensitive or critical data to either use to further their attacks or exploit for gain. They repeat this cycle of discovery, credential theft, privilege escalation, lateral movement, and data collection until they complete their mission. These steps can occur in any order and often do.

5.2. Deception Goals

According to security professionals, attackers are most concerned about intrusion detection system (IDS) and deception technology at 56% and 55%, respectively. IDS stops known attacks, while deception detects those that evade security controls. User and entity behavioral analytics (UEBA), big data, AI, and other forms of network traffic analysis rely on signatures, database lookup, or pattern matching to identify threats. This requires time for the systems to learn and become effective and will also require ongoing tuning. Throughout this process, security teams often experience excessive false positives that create alert fatigue. The "noise" created by these solutions has limited deployments and be a barrier to usage.

"Deception works very differently from typical analytics-based anomaly detection systems such as SIEM, UEBA etc. These probabilistic approaches create massive data stores—logging virtually every action—and require frequent tweaking of analytical models and rulesets to reduce false positives. Gaining value from these systems virtually demands a large, sophisticated security team, and an even larger budget. Because modern deception technology reduces anomalies to a binary choice—either a bad actor has interacted with a deceptive element or not, threat detection is a simple, automated deterministic approach. The system operates unseen, with no effect on legitimate users, but creates an environment that is hostile to attackers. No wonder that shops with limited staff have come to quickly appreciate the combination of peace of mind and high efficiency delivered by deception platforms. Deception is not a last-ditch effort or the last thing to layer on an already complex stack. The technology is solid, well-tested by large and established firms, and offers such value that it should be considered an essential component of any well-architected security strategy" [51].

Deployment goals center on better detection of attackers with the benefits of improved visibility and faster response. Primary goals typically include detection for (Figure 6):

- Lateral Movement Across Attack Vectors:
  - Network reconnaissance, stolen credentials
- Reconnaissance:
  - Enumeration, device exploitation of IoT, app servers, etc.
  - Application vulnerability (for example, SQL injection)
  - Default or simple passwords, brute force attacks
  - Misconfigured systems, network share reconnaissance
- Advanced Attack Techniques:
  - Man-in-the-Middle, Active Directory recon, kerberoasting
  - Group policy preferences, network traffic capture
  - Malware, WMI exploitation, hard-coded credentials
  - Open ports and services reconnaissance.

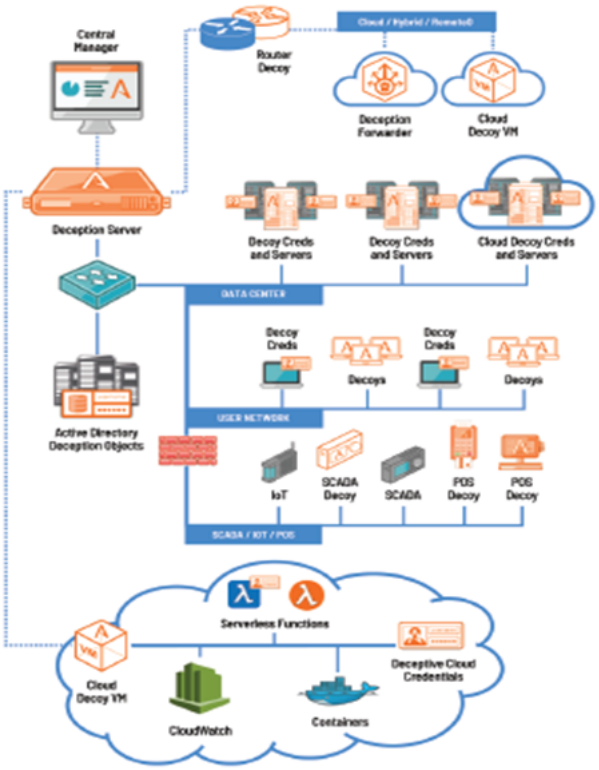

Figure 6. Typical Deception Deployment.

5.3. Types of Deception Technology

Today, there are several approaches to threat deception—network, endpoint, application, and data. Deception technology is available as a full deception fabric or platform, as features within a broader platform, and as independent solutions. When choosing a solution, factors such as attack surface coverage, scalability, and efficacy against multiple attack vectors are considered.

5.3.1. Network Deception

High-interaction decoys that appear identical to production assets are deployed throughout the network and are designed to detect attackers during reconnaissance and lateral movement attempts. The concept is to hide in plain sight by creating a camouflaged environment where the attacker is tricked into believing that what is fake is real. For optimal detection and attack surface coverage, deception decoys should be able to mimic and seamlessly blend in with the production asset.

Authenticity: Believability is critical. For full deception authenticity, the decoys should run the same operating systems and services as production assets so that highly skilled attackers cannot discern which assets are decoys and which are real. They should match the other networking characteristics of production devices to be credible to the threat actor. The highest level of authenticity can be achieved if decoys run the same "golden image" that is used in production.

Lateral movement. A dynamic, high-interaction deception environment enables decoys to communicate with each other to capture an attacker's lateral movement and techniques as they believe they are advancing their attack.

5.3.2. Endpoint Deception

In addition to endpoint decoys, genuine-looking and attractive deceptive credentials and lures are placed on existing systems and servers. The solution also provides capabilities to monitor available services on production endpoints, and redirects attempted access into

a deception environment. Plus, exposed credential mapping provides for visibility into lateral attack paths.

- *Credentials.* Comprehensive endpoint deceptions cover a wide variety of application and memory credential lures, browser credentials, history, and items such as identity and access management (IAM) access accounts, access keys and tokens, S3 buckets, serverless functions, and Domain Name Service (DNS) entries for cloud environments. Customization of these credentials as well as timestamping keeps them attractive. For authenticity, credentials should be able to validate within AD. Additional AD deceptions can hide high-value objects such as administrator or service accounts and present decoy credentials in their place without altering the production AD environment.
- *Deployment.* Agentless deployment models are generally preferred, as they require less overhead to operate and maintain. Integration with existing endpoint management systems can also provide deployment and management flexibility.
- *Deflection.* Endpoint scan deflection and obfuscation of Active Directory information deflects attacker activities to decoys for engagement and reduces the risk of lateral movement Attack Path Visibility. Exposed, orphaned, or misused credentials stored at the endpoints for attack surface risk reduction ar identified. This also identifies misconfigurations that attackers can leverage to move between systems.

5.3.3. Application Deception

Application deceptions allow an organization to publish internal decoy applications, such as a SWIFT terminal, a web application with a supporting database backend, or network directory services [52]. Application deception provides additional targets for an attacker to pursue in the deception environment. It is especially useful for learning what attackers are pursuing within the network as well as for identifying external and internal threat actors using valid credentials.

5.3.4. Data Deception

Database, network, and endpoint data deceptions can be placed strategically, giving attackers the promise of personally identifiable information (PII), intellectual property, AD privileged accounts, or other valuable data. They can also redirect network-enabled malware or ransomware attacks from production systems to the deception environment. Data deceptions can include decoy file servers and services, fake credentials, decoy documents, server message block (SMB) shared drives, and network shared folders. Adding deceptive files, databases, or decoy document beaconing functionality provides additional insight into what an attacker is seeking to steal and the geolocation of where files are accessed.

5.4. Deception and the Attack Cycle

Deception is an extremely effective detection mechanism throughout various stages of an attack, providing visibility into actions that most organizations cannot easily detect. Traditionally, most security investments have focused either on preventing the attacker from successfully getting in (firewalls, antivirus, intrusion prevention systems, and similar technologies), or detecting attackers who try to leave with any data of value (data loss prevention). However, attackers spend the most time inside the network in the persistence cycle of privilege escalation, internal reconnaissance, lateral movement, and maintaining a presence [53]. Deception excels at providing internal visibility to such activities while denying accurate intelligence to the threat actor through misinformation and misdirection.

5.5. Advanced Deception for an Active Defense

An active defense strategy involves direct defensive actions taken to destroy, nullify, or reduce the effectiveness of cyber threats against an organization's assets [54]. These defensive activities increase attacker resource expenditures while reducing those of the defender. With deception, the attacker focuses on targets with no corporate production

value, while the defenders gather information on the attacker's tools, techniques, and methods. Deception puts the burden on the attacker to discern real from fake. Network decoys, endpoint breadcrumbs, deceptive applications, and decoy data disrupt the attacker's advantage of stealth by detecting them early in the attack cycle. When attackers attempt to use deceptive credentials or engage with a network decoy, they spend precious time and resources interacting with an asset that does not advance their attack. Conversely, the defender gains valuable threat and adversary intelligence. With deception, the attacker cannot gain an accurate picture of the network. Network decoys appear as regular systems and respond to discovery scans, causing uncertainty and polluting the attacker's information with inaccurate data. Endpoints deflect port and service scans to decoys for engagement, making it appear to attackers that they are engaging with a production system instead of a decoy. This misinformation alters attackers' understanding of the network, slows them down, and causes them to make mistakes. Introducing deception adds uncertainty to the environment that attackers must now factor into their activities. Attackers that suspect or are aware of deception in the environment must now question their discovery scans and whether the system they are targeting is a valid production asset or a decoy that alerts on malicious activities. The attackers can no longer trust their tools or target a system with confidence, increasing their costs as they slow their activities in an attempt to validate information, avoid the decoy systems, and identify real targets. The known deployment of deception can be a strong deterrent. As attack processes become more complex, there is a higher likelihood that attackers must repeatedly restart their attacks, and the economics are no longer favorable. Collectively, these challenges motivate attackers to seek easier targets.

5.5.1. The Defender's Edge

A critical advantage of deception-based defenses is that they give defenders an edge, a home-field advantage. They can actively feed their adversaries deceptive information that affects the observe and orient phases of a decision-making cycle called the OODA loop [6,55,56]. The OODA loop (Observe, Orient, Decide, and Act) is a cyclic process model proposed by Colonel John Boyd, USAF, from their observations of air combat in the Vietnam War [10]. He found that fighter pilots continuously cycled through four phases while engaged with the enemy: observe what is happening, orient to the situation, decide on a course of action, and then act on it. Pilots who cycled through this process faster than their opponent usually won the engagement. To gain the advantage, one must either find a way to cycle through their OODA loop faster or slow the adversary's loop by adding friction. Deception inserts significant friction through misdirection and misinformation in the observe and orient phases of the adversary's OODA loop. The defender gains an edge over the adversary by slowing the attacker's process, giving themselves more time to decide and act, and providing a clearer understanding of how the adversary is moving and reacting to the deception. Attackers make decisions based on faulty or inaccurate information that clouds their situational awareness and disrupts their OODA loops. With deception, defenders manipulate the adversary's OODA loop, disrupt the attack cycle, and gain a significant advantage.

5.5.2. Deception for Accelerating Incident Response

Deception provides support in identifying the extent of a breach and the efficacy of existing security controls. Knowing that an attacker has bypassed the perimeter is a useful first step, but gaining visibility into what other systems may be affected, lateral movement paths, and what methods attackers used to bypass defenses provides benefit beyond the immediate alert. In addition to providing actionable alerts backed by forensics, high-interaction decoys gather information for the defender for post-incident analysis. Any data about the methods or tools attackers leveraged to bypass security on a network decoy aids the analyst in identifying how a security control failed and to mitigate the risk of a returning adversary. The captured data also provide IOCs for the analyst to use in finding other potential victims the attacker may have compromised. For example, during an attack,

the attacker drops an unknown binary onto a decoy that contacts a previously unknown C2 server through an encrypted channel to download a malicious payload. This set of actions provides the security team with information that can be used during and after the incident response process. The security team can add the C2 Internet IP address to the firewall and external DNS blocks to increase defenses. This prevents malware from communicating out and discovers other potential C2 servers' IP addresses through malware connection attempts. Additionally, through native integrations and APIs, response actions can be automated. This often starts by augmenting detection with known threat intelligence, which can include malware identification and domain reputation information. Examples of solutions that integrate with deception platforms include McAfee DXL, ThreatConnect, ReversingLabs, VirusTotal, and Webroot. In addition to expediting attack analysis and correlation, integrations are available for automated incident response actions such as blocking, isolation, and threat hunting. Advanced deception solutions will offer native integrations with most major firewalls, NAC, SIEM, endpoint, and orchestration offerings. Some go as far as automating with ticketing systems to expedite remediation. In particular, the deflection function and Active Directory obfuscation combined with an EDR solution essentially locks down the endpoint, preventing the attacker from moving laterally while remaining undetected. Companies such as Attivo Networks have expanded beyond simple automation and also offer extensive native integrations and incident response playbooks. These accelerate response, either automatically based on policy or with user intervention. For example, data can be sent to a range of tools to automate forensics, reporting, incident response, isolation at the endpoint, or blocking on the network, and it can handle it in any combination. Incident response analysts can identify other potential victims by searching the SIEM for systems that had communicated with the C2 IP address or by matching the SHA1 hash of the malicious payload to find infected endpoints. Responders can then expand the scope of their remediation efforts to include these systems. The security team can subsequently check if they have found and remediated all potential victims. The information captured by the deception platform is added intelligence for defenders to use and share as needed to elevate the security posture across multiple organizations.

5.5.3. Deception for Identification and Prevention

Other useful deception functionality includes being able to identify and prevent attacks. A deception platform is designed to learn the network so that deceptions can be automatically prepared and deployed. Within this process, the tool gathers information on exposed or orphaned credentials as well as misconfigurations. It will also pick up network changes and show when devices come on and off the network. This visibility is extremely effective for reducing the attack surface and is not typically achievable with other security tools. Either in the form of tables or topographical maps, defenders can visualize the paths an attacker would take and shut them down before the attacker can exploit them. In some cases, the deception platform can also automate the remediation in addition to passing the information to ticketing systems. With deception's ability to hide priority AD objects at the endpoint and present deception in their place, the technology diverts attackers away from critical assets, countering attacks that target AD from gaining accurate information. Additionally, the ability to deflect port and service scans at every endpoint reduces the likelihood that the attacker can move from the initially infected system without touching a decoy. Not only does this prevent attackers from expanding their foothold into the production environment, but it also allows for detection earlier in the attack cycle.

5.5.4. Advanced Deceptions and Detection

Security teams can leverage deception for advanced deployments and cases (Figure 7). Using a full-featured deception platform, they can create an entire deceptive Active Directory or LDAP server with associated decoys as part of the environment. They can also choose to deploy deception routers, switches, and VOIP telecom deception, or application and data deceptions specific to their organization, such as a deceptive SWIFT terminal

for a bank, or a deceptive gift card web portal with a fake database backend server. If the security team operates a device network, such as IoT cameras or multifunction printers, they can deploy deception assets that match those as well. Security teams can also create decoy documents that beacon home when ex-filtrated, providing information on what attackers are targeting and where the data are accessed.

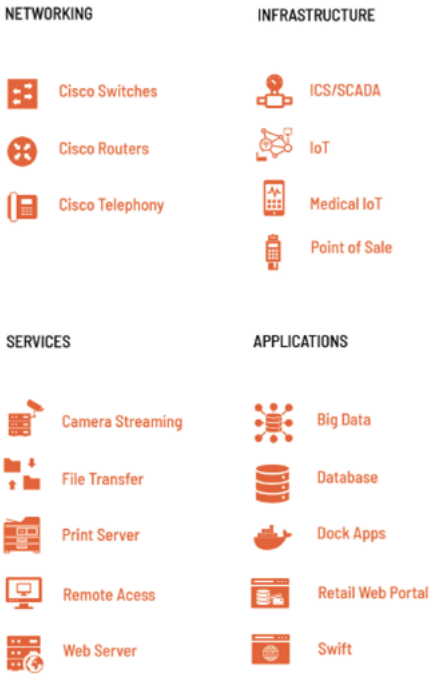

Figure 7. Comprehensive deployment.

6. Conclusions

The future of warfare will be in a digitalized multi-domain environment, which needs new doctrines [57,58] 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 cyber requirements as different sensors are used and 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 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 cyberinfrastructure of all other military domains. Moreover, the military cyber domain needs to be prepared for attacks on the national cyberinfrastructure, including infrastructure for civilian use, in case, commercial cyber protection measures are not working. This range of military cyber responsibilities is often underestimated. However, the main result of the cyber threat assessment showed clearly that the existing cyber defense strategies need improvement to counteract the existing cyber threats [26].

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 [33,59], our paper's originality lays in the investigation of the cyberattack cycle and deception technology model for threat detection using deception-based methods, within the Hybrid Threats Model.

"As many organizations look to test their network resiliency, penetration tests are playing an increasingly integral role in understanding a network's vulnerabilities through the simulation of a real attack. Deception provides early and efficient warning of attacks, whether they be from malicious internal or external threat actors or a Red Team penetration

tester. The outcome of these tests illustrates how deception can be used to validate network resiliency, demonstrates the power of in-network deception-based threat detection, and exhibits how attack information gathered can be used to accelerate incident response and strengthen network defenses. These tests are also an impactful way to show the instant value of deception and how easy it is to deploy and operationalize" [39].

Organizations need to consider and prepare for the impact of potentially disruptive events such as natural disasters, cyber-attacks, pandemics, global warming, and political unrest. Business resiliency is an organization's ability to withstand failure so it can deal with potential threats and survive and thrive. Being business-resilient means having the ability to scale quickly and adjust operations to meet new market changes. In the immediate term, organizations need to understand how to ensure the business continues. When turmoil occurs, organizations need to know the following:

- Which systems can be powered down and which systems are critical to maintaining?
- What can be scaled back or done without?
- Which parts of the business are going to be strained or at risk of failing? To strengthen business resilience, an organization needs to focus on critical applications and accelerate cloud migration to support the digitization of the business [1].

In this paper, we made an introduction to deception technology and an overview of detection to creating an active defense. We showed how deception fits within overall security architecture and designed the conceptual Hybrid Threats Model and military education for cybersecurity indispensable to achieve as well as the role it plays in detecting, identifying, and responding to threats. Besides the basics of the cyberattacks cycle and deception technology, we emphasize that deception should be used strategically to stop advanced attackers.

In future research, NCDL researchers, suppliers, and customers will be brought together to address problems, explore opportunities and advance capabilities in a space not previously explored, 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 [12].

Author Contributions: Conceptualization, W.S. and D.G.; methodology, D.G.; software, W.S.; validation, W.S., A.K., and D.G.; formal analysis, D.G.; investigation, W.S.; resources, A.K.; data curation, D.G.; writing—original draft preparation, W.S.; writing—review and editing, W.S.; visualization, A.K.; supervision, A.K.; project administration, W.S.; funding acquisition, W.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Project KEGA 011TUKE4/2020: 'A development of the new semantic technologies in educating of young IT experts.'

Conflicts of Interest: The authors declare no conflict of interest. The funder had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

ACDC	The Active Cyber Defense Certainty Act
AD	Active Directory
AI	artificial intelligence
API	Application programming interface
DNS	Domain Name Service
ECTS	European Credit Transfer and Accumulation System
EDR	endpoint detection and response
EU	European Union
IAM	identity and access management
IDS	intrusion detection system

IOC	Indicators of Compromise
IT	information technology
NAC	Network Access Control
NATO	The North Atlantic Treaty Organization
NCDL	National Cyber Deception Laboratory
NCO	non-commissioned officer
NTA	network traffic analysis
OODA	Observe, Orient, Decide, and Act
PII	personally identifiable information
PME	Professional Military Education
SMB	server message block
SIEM	security information and event management
TTPs	tactics, techniques and procedures
UEBA	user and entity behavioral analytics
UK	United Kingdom
US	United States

References

1. MEGA International. *Business Resilience, How Strategic Planning and Enterprise Architecture Help Companies Successfully Rebound from a Crisis*; White paper; MEGA International: Raynham MA, USA, 2021.
2. How COVID-19 Has Pushed Companies over the Technology Tipping Point—And Transformed Business Forever. 2020. Available online: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-COVID-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever (accessed on 22 March 2021).
3. Contu, R.; Driver, M.; Kim, E.; Wheeler, J.A.; Smith, N.; Pingree, L.; Rakheja, S. Emerging Technologies and Trends Impact Radar: Security. G00724138. 2020. Available online: https://www.gartner.com/en/documents/3991219/emerging-technologies-and-trends-impact-radar-security (accessed on 22 March 2021).
4. Pingree, L.; Smith, N.; Kim, E.; Wheeler, J.A.; Contu, R.; Ahlm, E.; Driver, M. Emerging Technologies and Trends Impact Radar: Security. G00450798. 2019. Available online: https://www.gartner.com/en/documents/3975191/emerging-technologies-and-trends-impact-radar-security (accessed on 22 March 2021).
5. What Is XDR? Available online: https://www.paloaltonetworks.com/cyberpedia/what-is-xdr (accessed on 22 March 2021).
6. Crandall, C.; Salazar, J. *Deception Based Threat Deception: Shifting Power to the Defenders*; Attivo Networks, Inc.: Fremont, CA, USA, 2019.
7. NATO Communications and Information Agency (NCIA) and AFCEA TechNet. In Proceedings of the International: NITEC '16 - The NCI Agency Industry Conference and AFCEA TechNet International, Tallinn, Estonia, 7–9 June 2020. Available online: https://docplayer.net/55237431-Ncia-business-opportunities-cyber-security.html (accessed on 24 August 2020).
8. Kambow, N.; Passi, L.K. Honeypots: The Need of Network Security. *Int. J. Comput. Sci. Inf. Technol. (IJCSIT)* **2014**, *5*, 6098–6101.
9. Scottberg, B.; Yurcik, W.; Doss, D. 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, 6–8 June 2002; pp. 387–391.
10. Almeshekah, M.H.; Spafford, E.H. Planning and Integrating Deception into Computer Security Defenses. In Proceedings of the 2014 New Security Paradigms Workshop, Victoria, BC, Canada, 15–18 September 2014; NSPW '14; Association for Computing Machinery: New York, NY, USA, 2014; pp. 127–138, doi:10.1145/2683467.2683482.
11. Virvilis, N.; Vanautgaerden, B.; Serrano, O.S. Changing the game: The art of deceiving sophisticated attackers. In Proceedings of the 2014 6th International Conference On Cyber Conflict (CyCon 2014), Tallinn, Estonia, 3–6 June 2014; pp. 87–97.
12. Cranfield University. The National Cyber Deception Symposium, hosted by the UK MoD's Defence Academy and Defence Cyber School, Nov 6th, 2019, Shrivenham, Swindon, UK. Available online: https://www.cranfield.ac.uk/events/symposia/cyber-d (accessed on 24 August 2020).
13. Crandall, C. The Evolution Of Cybersecurity. 2019. Available online: https://www.healthcareinfosecurity.com/whitepapers/deception-based-threat-detection-shifting-power-to-defenders-w-5780?highlight=true (accessed on 22 March 2021).
14. European External Action Service (EEAS): Food-for-thought Paper "Countering Hybrid Threats". 2015. Available online: http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf (accessed on 25 February 2021).
15. Cenková, R. The content and the form in public relations. Managerial Trends in the Development of Enterprises in Globalization Era. In Proceedings of the 7th International Scientific Conference on Managerial Trends in the Development of Enterprises in Globalization Era (ICoM), Nitra, Slovakia, 1–2 June 2017; Košičiarová, I., Kádeková, Z., Eds.; Slovak University of Agriculture: Nitra, Slovakia, 2017; pp. 544–551.
16. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE): EU Policy on Fighting Hybrid Threats. Available online: https://ccdcoe.org/incyder-articles/eu-policy-on-fighting-hybrid-threats (accessed on 25 February 2021).
17. The Cyber Security Hub™: Information Technology and Services, London, UK, 2021.

18. Siedlecka-Lamch, O.; Szymoniak, S.; Kurkowski, M.; Fray, I.E. 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, UAE, 22–24 June 2020.
19. Szymoniak, S. How to be on time with security protocol? In *Societal Challenges in the Smart Society*; ETHICOMP Book Series; Universidad de La Rioja: La Rioja, Spain, 2020, pp. 225–237.
20. Booz, A. 8 Cyber Threat Trends to Watch Out for in 2021. McLean, VA, USA, 2021. Available online: https://www.boozallen.com (accessed on 25 February 2021).
21. Yang, S.; Wu, C.; Zhang, Y.; Wang, W.; Xie, W. Attack-Defense Utility Quantification Furthermore, Security Risk Assessment. In Proceedings of the 2019 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, UK, 19–23 August 2019; pp. 1456–1461, doi:10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00263.
22. Roepke, W.; Thankey, H. Resilience: The First Line of Defence. 2019. Available online: https://www.nato.int/docu/review/2019/Also-in-2019/resilience-the-first-line-of-defence/EN/index.htm (accessed on 28 February 2021).
23. Kossecki, P.; Wachowicz, J. Economic Crisis, Trust and Socio-Economic Aspects of Sustainable Development. *Probl. Ekorozwoju Probl. Sustain. Dev.* **2013**, *8*, 65–71.
24. Tokarčíková, E.; Malichová, E.; Kucharčíková, A.; Ďurišová, M. Importance of Technical and Business Skills for Future IT Professionals. *Amfiteatru Econ.* **2020**, *22*, 567, doi:10.24818/EA/2020/54/567.
25. Tokarčíková, E.; Ďurišová, M.; Bartošová, V. Corporate social responsibility of public administration employees. In Proceedings of the 25th International Business Information Management Association Conference—Innovation Vision 2020: From Regional Development Sustainability to Global Economic Growth, IBIMA 2015, Amsterdam, The Netherlands, 7–8 May 2015; pp. 1437–1445.
26. European Defence Agency (EDA). *Strategic Research Agenda On Cyberdefence*; EDA: Brussels, Belgium, 2020.
27. Schulze, M. Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. In Proceedings of the 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade, Tallinn, Estonia, 26–29 May 2020; pp. 183–197, doi:10.23919/CyCon49761.2020.9131733.
28. Attivo Networks. *Threatdefend Platform Solution Overview*; Attivo Networks: Fremont, CA, USA, 2020.
29. Galinec, D.; Steingartner, W.; Zebić, V. Cyber Rapid Response Team: An Option within Hybrid Threats. In Proceedings of the 2019 IEEE 15th International Scientific Conference on Informatics, Poprad, Slovakia, 20–22 November 2019; pp. 43–50, doi:10.1109/Informatics47936.2019.9119292.
30. Tang, M.; Alazab, M.; Luo, Y. Big Data for Cybersecurity: Vulnerability Disclosure Trends and Dependencies. *IEEE Trans. Big Data* **2019**, *5*, 317–329.
31. Galinec, D.; Luić, L. Digital Security Perspectives and Engagement for Resilience in Information-Communication Environment. In Proceedings of the 2019 3rd European Conference on Electrical Engineering and Computer Science (EECS), Athens, Greece, 28–30 December 2019; pp. 106–112, doi:10.1109/EECS49779.2019.00032.
32. Galinec, D. Resilience Is Key. *Per Concordiam* **2018**, *9*, 14–21.
33. Counter Craft: Am I Ready for Cyber Deception? Gartner Hype Cycle for Security Operations. Available online: https://www.countercraftsec.com/blog/post/am-i-ready-for-deception-technology (accessed on 24 August 2020).
34. Attivo Networks. *Attivo Networks Named as a Sample Vendor in Gartner Hype Cycle for Security Operations 2020*; Attivo Networks, Inc.: Fremont, CA, USA, 2020.
35. Chekinov, S.; Bogdanov, S. The Nature and Content of a New-Generation War. *Mil. Thought* **2013**, *22*, *12–23*.
36. Case Study: A View of Deception Technology in Security Testing. 2020. Available online: https://www.bankinfosecurity.com/whitepapers/case-study-view-deception-technology-in-security-testing-w-5785 (accessed on 22 March 2021).
37. Permana, A. Indonesia's Cyber Defense Strategy in mitigating the Risk of Cyber Warfare Threats. *Syntax Idea* **2021**, *3*, 1–11, doi:10.36418/syntax-idea.v3i1.860.
38. Crandall, C. How Security Teams are Turning to Decoy Networks. 2019. Available online: https://attivonetworks.com/how-security-teams-are-turning-to-decoy-networks (accessed on 22 March 2021).
39. Attivo Networks. *The Role of Deception Technology in Security Penetration Testing*; Attivo Networks, Inc.: Fremont, CA, USA, 2018.
40. Kozina, A. Hrvatsko vojno učilište—Ustroj i uloga. *Anali za Povijest Odgoja* **2013**, *12*, 129–141.
41. Purković, D.; Bezjak, J. Kontekstualni pristup učenju i poučavanju u nastavi temeljnog tehničkog odgoja i obrazovanja. *Školski Vjesnik* **2015**, *64*, 131–152.
42. Committee on Armed Services Subcommittee on Oversight & Investigations. *Another Crossroads? Professional Military Education Two Decades After The Goldwaternichols Act and The Skelton Panel, U. S.*; House of Representatives: Washington, DC, USA, 2010.
43. North Atlantic Military Committee. *Military Decision On Mc 0458/3 NATO Education, Training, Exercises Furthermore, Evaluation (ETEE) Policy*; North Atlantic Military Committee: Brussels, Belgium, 2014.
44. Headquarters Department of the Army. *Army Leader Development Program, Department of the Army Pamphlet 350-5*; Headquarters Department of the Army: Washington, DC, USA, 2013.

45. Pevnev, V.; Tsuranov, M.; Zemlianko, H.; Amelina, O. Conceptual Model of Information Security. In *Integrated Computer Technologies in Mechanical Engineering—2020. ICTM 2020. Lecture Notes in Networks and Systems*; Springer: Cham, Switzerland, 2021; Volume 188, pp. 158–168, doi:10.1007/978-3-030-66717-7_14.
46. Glasser, W. *Kvalitetna Škola: Škola bez Prisile*; Educa: Zagreb, Croatia, 1994.
47. Kozina, A. Interkulturalne kompetencije vojnih nastavnika. *Andragoški Glas.* **2013**, *17*, 37–48.
48. Kapitzke, C. Cyber Pedagogy as Critical Social Practice in a Teacher Education Program. *Teach. Educ.* **2000**, *11*, 211–229, doi:10.1080/713698968.
49. Fountain, S. *Education for Development—A Teacher's Resource for Global Learning*; Hodder & Stoughton: London, UK, 1999.
50. Waitt, T. No Nonsense Cyber Threat Detection Made Simple with Deception. 2019. Available online: https://americansecuritytoday.com/no-nonsense-cyber-threat-detection-made-simple-with-deception (accessed on 22 March 2021).
51. Lance, W. Debunking the Myths of Deception Technology. 2020. Available online: https://www.networkcomputing.com/network-security/debunking-myths-deception-technology (accessed on 22 March 2021).
52. Kvet, M.; Kršák, E.; Matiaško, K. Locating and accessing large datasets using Flower Index Approach. *Concurr. Comput. Pract. Exp.* **2019**, *32*, e5209, doi:10.1002/cpe.5209.
53. Mandiant. Red Team Operations (RTO): Test Your Ability to Protect Your Most Critical Assets from a Real-World Targeted Attack. 2019. Available online: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/pf/ms/ds-red-team-operations.pdf (accessed on 28 March 2021).
54. Johansson, F.; Falkman, G. A testbed based on survivability for comparing threat evaluation algorithms. In *Intelligent Sensing, Situation Management, Impact Assessment, and Cyber-Sensing*; Mott, S., Buford, J., Jakobson, G., Eds.; International Society for Optics and Photonics, SPIE: Bellingham WA, USA, 2009; Volume 7352, pp. 119–129, doi:10.1117/12.816819.
55. Galinec, D.; Macanga, D. Observe, Orient, Decide and Act Cycle and Pattern-Based Strategy: Characteristics and Complementation. In Proceedings of the Central European Conference on Information and Intelligent Systems – CECIIS, 23rd International Conference, Varaždin, Croatia, 7–9 October 2012; Faculty of Organization and Informatics: Varaždin, Croatia, 2012; pp. 371–378.
56. Galinec, D.; Steingartner, W. A Look at Observe, Orient, Decide and Act Feedback Loop, Pattern-Based Strategy and Network Enabled Capability for Organizations Adapting to Change. *Acta Electrotech. Et Inform.* **2013**, *13*, 39–49.
57. Colarik, A.; Janczewski, L. Establishing Cyber Warfare Doctrine. In *Current and Emerging Trends in Cyber Operations*; Palgrave Macmillan: London, UK, 2015; pp. 37–50.
58. Ormrod, D.; Turnbull, B. The cyber conceptual framework for developing military doctrine. *Def. Stud.* **2016**, *16*, 270–298.
59. Shoard, P. *Hype Cycle for Security Operations*; ID: G00467096; Gartner, Inc.: Stamford, KT, USA, 2020. Available online: https://www.gartner.com/en/documents/3986721/hype-cycle-for-security-operations-2020 (accessed on 22 March 2021).