Evaluating Deception Theories for Applicability to Cyber Operations

Tim Grant[1] and Simon Henderson[2]
[1]Retired But Active Researcher (R-BAR)
[2]Deception by Design, UK

tim.grant.work@gmail.com
simon@deceptionbydesign.com

Abstract: Deception is essential to and inherent in cyber operations of all kinds. In defensive cyber operations, deception is the third line of defence after authentication and access control. Deception can be supported by intrusion detection systems monitoring for suspicious activity. Honeypots are the most obvious technique for misleading intruders, but delaying execution of commands, giving false excuses, and lying about the results may be more effective in some circumstances. Proactive defences also depend on deception. In offensive cyber operations, the attacker may manipulate someone to gain information. He/she may masquerade as an authorised user to access the target system or escalate privileges, install a rootkit to conceal his/her actions, bypass access control by installing a back door, or exfiltrate collected data within normal traffic. There is a wealth of theories of deception, overwhelmingly based on the physical world. Some theories are generic, others are specific to military operations, but few are specific to cyber deception. Some focus on the entities involved, while others focus on the deception process, which itself may be organisational or psychological. Several authors warn that analogies drawn from the physical environment may be counterintuitive in cyberspace. As Miller, Brickey and Conti (2012) memorably express it: "weapons can be reproduced instantly, 'bullets' travel at near the speed of light, destroyed targets can be brought back from the dead, and a seventeen year old can command an army". This warning also applies to deception theory. The purpose of this paper is to evaluate key theories of deception for applicability to cyber operations in a multi-domain environment. There are five chapters. After the Introduction, Chapter 2 summarises relevant theory and doctrine. Chapter 3 summarises seven key theories of deception. Chapter 4 evaluates them, and outlines an ideal theory. Finally, Chapter 5 draws conclusions and recommends further work.

Keywords: CND, CNE, CNA, Manipulation, Surprise

1. Introduction

1.1 Motivation

Since the end of the Cold War, NATO nations have been accused of losing the art of deception (Economist, 2020). They have depended on the technology and brute force that US leadership has brought with it. Technology has made ruses harder to sustain, with satellites, drones, "every soldier a sensor" (Magnuson, 2007), and machine learning algorithms spotting anomalies too subtle for human analysts. Paradoxically, such technologies also create new opportunities for delivering deception. There is a cultural aspect, too. Open societies that prize the rule of law and transparency may be inherently less good at trickery (Economist, 2020). And a deceiver must now successfully deceive in more ways. It is not enough to generate fake radio traffic, as in Operation Iraqi Freedom in 2003, but there must now also be corresponding fake activity on social media.

In multi-domain operations (MDO), military forces are currently struggling with integrating operations in cyberspace with physical ("kinetic") action and effects on the battlefield, whether this is to influence people (i.e. information operations) or to spy on and attack the adversary's information and communication systems (i.e. offensive cyber operations). The physical entities found on land and in the sea, air, and space have different characteristics to the virtual entities found in cyberspace (Seebeck, 2019) (Grant, 2023). Multiple authors warn about making simplistic analogies from kinetic operations to cyber and information operations (Miller, Brickey & Conti, 2012) (Liles, Dietz, Rogers & Larson, 2012) (Kallberg & Cook, 2017). Their warnings apply equally to thinking on military deception.

Officer training, doctrine for planning and executing operations, and the development of supporting software tools ultimately all depend on an underlying theory of deception. To support MDO, this theory must be compatible with both physical and cyber domains. In the literature, there are many theories of deception. Some are generic, applying equally well to the natural world of plants and animals as to the man-made world. Other theories are military specific. There are a few theories of cyber deception, but these are specific to "pure" cyber warfare, not MDO. With the exception of Henderson (2019), no theories of deception that have been designed explicitly to apply to both physical and cyber domains. Even so, it is worthwhile evaluating leading existing theories to see what is required of an ideal theory of deception in MDO.

1.2 Purpose, Scope, and Structure

The purpose of this paper is to evaluate key theories of deception for applicability to cyber operations in a multi-domain environment. Applicability means that generic and military-specific theories – presumably developed with physical domains in mind – must also be appropriate to cyberspace, to all operational phases (before, during, after an operation), to all deception techniques, and to use in both defensive and offensive cyber operations. Counterdeception is excluded.

The paper is structured into five chapters, followed by references. After the Introduction, Chapter 2 summarises relevant theory and doctrine. Chapter 3 summarises seven key theories of deception. Chapter 4 evaluates them, and outlines an ideal theory. Finally, Chapter 5 draws conclusions and recommends further work.

2. Related Theory

2.1 Strategic Context

The global strategic context is increasingly complex, dynamic, and competitive (MODUK, 2021). Traditional distinctions between war and peace, state and non-state actors, and foreign and domestic are becoming blurred. Relationships span a spectrum from cooperation, competition, confrontation, to warfighting. Potential adversaries challenge international norms, exacerbating societal divisions, leading citizens to cooperate – wittingly or unwittingly – in undermining democracy. The effect is designed to force Western nations to become politically cowed, achieving the adversary's objectives without escalating to warfighting level. As typified by UK doctrine (MODUK, 2021), the Western nations' response is to orchestrate all instruments of national power to achieve national security objectives. Orchestration requires integrating a mix of physical, virtual (i.e. cyber), and cognitive actions that will bring about the desired effects not just on the adversary's armed forces, but also on other relevant actors. Action is integrated across all five operational domains (i.e. land, sea, air, space, and cyberspace). The role of Western defence is to create multiple dilemmas that unhinge an adversary's understanding, decision making, and execution by becoming more dynamic and pre-emptive, information-led, and selectively ambiguous. Deception is the best way to create dilemmas and ambiguity, or to make an adversary absolutely certain but absolutely wrong.

2.2 Physical, Virtual, and Cognitive Dimensions

The US DOD defines cyberspace as "*a global domain within the information environment consisting of the interdependent network of ICT infrastructures and resident data*" (US DOD, 2018, p.GL-4). It includes the Internet, communications networks, computer systems, embedded processors and controllers, and the information residing in and passing through the environment. Cyberspace operations are defined as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (ibid., p.I-1), and may be defensive or offensive in nature. In military doctrine, cyberspace is typically modelled as a set of distinct, yet interrelated layers. We adopt UK military doctrine (MODUK, 2022) because it relates cyberspace (the virtual dimension) to the physical and cognitive dimensions (see Figure 1), as the strategic context requires.

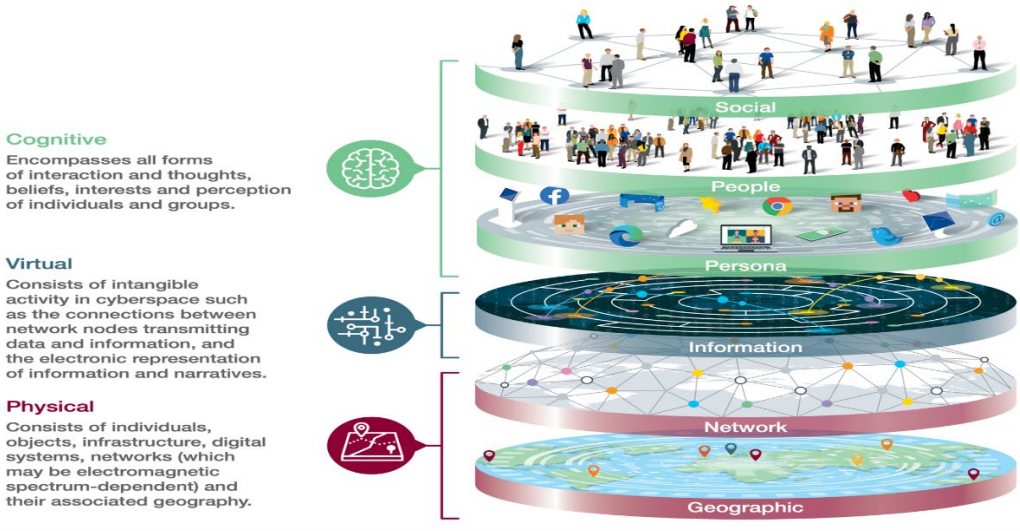

Figure 1: Physical, virtual, and cognitive dimensions of actions and effects (MODUK, 2022, p.7)

Real-world application of this model is complicated by the fact that actors in the operating environment will be a combination of physical, virtual, and cognitive elements. For example, consider a manned weapon system, such as an armoured vehicle, a ship, or an aircraft. It carries a team (*social* layer) of individuals (*people* layer) in a physical platform (*geographical* layer) fitted with information and communication systems (*information* and *network* layers) which the crew can access (*persona* layer). Hence, to be applicable to MDO, the ideal theory of deception must be able to account for all three dimensions and represent entities in all six layers.

There are major differences between the physical domains and cyberspace (Seebeck, 2019). Land, sea, air, and space are natural domains containing physical entities located in a continuous, three-dimensional space. A physical entity can be in only one location at a time. When they move, physical entities have inertia and are subject to gravity. For this reason, operations, actions, and effects in physical domains are termed kinetic. By contrast, cyberspace is a man-made domain containing inertia-less, virtual entities that can move close to the speed of light through a discrete, multi-dimensional space. Being man-made, cyber terrain can be created, changed, or dissolved at will by whoever owns it. Cyber systems are socio-technical systems.

Several authors warn about the dangers of making naïve analogies from the physical world to the virtual world of cyberspace, cyber action, and cyber effects. Miller, Brickey & Conti (2012) memorably express this as: "weapons can be reproduced instantly, 'bullets' travel at near the speed of light, destroyed targets can be brought back from the dead, and a seventeen year old can command an army". Liles, Dietz, Rogers & Larson (2012) analyse the differences in terms of the traditional nine principles of war to characterising possible cyber warfare attacks, techniques, and scenarios. Kallberg & Cook (2017) state that strategic theories specifically for cyber operations have not yet been established. Using traditional military strategy and operational concepts in the cyber world can mislead, resulting in spurious assessments and unfavourable outcomes. They identify four tenets of the cyber world that present profound challenges, as follows:

- *A lack of object permanence*. In cyberspace, one can create, change, move, duplicate, and delete objects at machine speed, undermining the principle of manoeuvre.
- *Limited or absent measures of effectiveness*. An attacker in cyberspace has limited ability to verify, assess, and act based on information gleaned from a previous attack and its aftermath.
- *Conflicts are executed at computational speed*. Cyber conflict will execute far too quickly for involvement by leadership at any level. Execution risks becoming a chain of reactions to events.
- *Anonymity makes the parties to the conflict unknown*. The lack of proper identification in cyberspace undermines the ability to engage and increases the risk of friendly fire. Anonymous attacks could trigger counter-attacks on assumed adversaries, guilty or not, possibly leading to uncontrolled escalation.

2.3 Deception

We define deception as "deliberate measures to induce erroneous sensemaking and subsequent behaviour with a target audience, to achieve and exploit an advantage" (Henderson, 2024). This definition is generic and accounts for non-human deception, including cyber deception. It is value neutral, embracing both malevolent and benevolent applications. Key aspects are:

- Deception is intentional, creating an advantage for the deceiver;
- Deception induces errors in the target's sensemaking and decision making;
- Deception requires action, aiming to change the target's behaviour by manipulating the target's core psychological processes of attention, perception, sensemaking, decision making, expectations, and emotions. These processes occur in the social layer within the cognitive dimension.

According to Clark and Mitchell (2019) – a modern textbook on deception informed by military practice – all deception has four essential components:

- A desired *objective*;
- A *target*, i.e. a person or group of people who are to be deceived;
- A *story* has to be presented, giving a false picture of reality; and
- One or more *channels* through which the story is transmitted to the target.

Clark and Mitchell (2019) fail to identify an obvious, fifth component: the *deceiver*, usually a person or group of people desiring the objective, who create the story and transmit it through the channels to deceive the target. The deceiver and target interact with one another through the operating environment, which may also contain

other actors (e.g. allies or neutrals). The cognitive aspect is represented in Clark and Mitchell as the deceiver's and target's Observe-Orient-Decide-Act (OODA) loops (Boyd, 1996).

In cyber operations, the deceiver and/or target can be virtual entities, as when malware exploits a vulnerability in an application to gain entry into a computer system (Rowe & Rrushi, 2016). In information operations, cyberspace is used as a channel for transmitting deceptive messages. While the target may be human, the deceiver can be a virtual entity, as when disinformation is disseminated by bots. Whether or not virtual entities should be accorded social or cognitive faculties is a philosophical issue.

2.4 Military Doctrine on Deception

Military deception doctrine distils centuries of practical experience into formalised strategies for manipulating the thinking and behaviour of adversaries. The study of military deception doctrine reveals national perspectives on deception theory and its exploitation in planning and execution. While deception doctrine dates back to Sun Tzu (c500 B.C.E./2000), formalised doctrine began to emerge in the 1980s. The role of cyber deception in supporting cyberwarfare and MDO has been recognised only recently (Henderson, 2024).

For this paper, we studied contemporary U.S. single-service (U.S. Army, 2023) (U.S. Marine Corp, 2024), U.S. joint (U.S. Joint Chiefs of Staff, 2012), NATO (NATO, 2020)**,** and Canadian (Chief of the Defence Staff, 1998) doctrine. We found that doctrine focuses largely on organisational structures, staff processes, and information management procedures. It provides little guidance on some of the most challenging parts of deceptive practice, such as course of action generation, or how best to 'sell' a deception plan to senior staff for approval. While deception doctrine has evolved to recognise cyber deception, it is generally not well suited to offensive action. Areas where physical-world doctrine falls short for cyber deception include:

- The notion of the adversary or target is different in cyberspace.
- The Target Audience in cyber deception is different to physical audiences.
- Doctrine does not fully recognise or accommodate the unique deceptive capabilities in cyberspace.
- Planning for deception in cyberspace involves different considerations than those in physical domains.
- The sources of risk in cyber deception operations are different.
- Execution, monitoring, and feedback are different in cyberspace.
- Staffing for physical versus cyber deception planning and execution are different (Leenen, Aschman, Grobler & van Heerden, 2018).
- Legal and ethical concerns do not map cleanly onto cyber deception, especially acts of cyber perfidy.

3. Key Theories of Deception

There is a wealth of theories of deception. Over 20 years, the second author has established an Endnote database of over 7000 references to all forms of deception. Of these, at least 21 are bibliographies. For this paper, the second author compiled a long-list of 31 theories. Space limits us to summarising a shortlist of seven theories: three generic, three military-specific, and one cyber-specific.

3.1 Generic Theories

3.1.1 Bell & Whaley (1982) and Whaley (2008)

Bell & Whaley (1982) and Whaley (2008) describe a general model of deception founded upon the activities of *hiding the real* (dissimulation) and *showing the false* (simulation). Their theory articulates three strategies that are used to enable these activities, thereby implying that deception incorporates six fundamental strategies in total. Dissimulation is enabled through *Masking* (putting something between the target and the object, or making the object resemble and blend into its background), *Repackaging* (wrapping the object in other signifier cues), and *Dazzling* (breaking up the object's pattern of cues). Simulation is enabled through *Mimicking* (making the object resemble something else by adopting its cues), *Inventing* (creating an alternative object from scratch), and *Decoying* (creating a competing target object with a greater source of conspicuity). Bell and Whaley suggest that effective deception incorporates five features: an *Objective* (clearly defined goals that deception aims to achieve), the *Target* (the individual or group whose perceptions the deception aims to manipulate), a *Plan* (a well-structured plan that outlines how the deception will be executed), the *Means* (resources and methods used to implement the deception, such as fake equipment, false radio traffic, etc.), and *Feedback* (mechanisms to assess the effectiveness of deception and adjust plan execution accordingly). While Bell and Whaley's deception theory is entirely generic, it has, nonetheless, been influential in shaping modern military doctrine and has been used to train military deception practitioners and intelligence officers. The theory has also been used extensively

within cyber deception theory (e.g., Yuill, Denning & Feer, 2006), although its applicability in cyber has also been questioned by some authors (e.g., Porter, 2016).

3.1.2 Reid (2016)

Reed (2016) proposes a Holistic Model of Deception that has been synthesised from analysing the deception literature from different domains. The model has been validated by deception subject matter experts. It incorporates a representation of the deceiver, his/her intent, deception strategies and tactics, interpretation by the target, and the target's decision making. The model supports a tailored approach to deception detection that considers the context and cultural background of deceiver and target. The model supports risk assessment and management strategies as a foundation for countering deception, to anticipate and mitigate potential deception threats posed by individuals and groups. The model has utility for anticipating, understanding, and countering deception in both physical and cyber worlds.

3.1.3 Henderson (2019)

Henderson (2019) presents a generic framework for analysing, representing, planning, and executing deception. The theory is derived from a body of research analysing cases of deception from across a wide variety of domains. He proposes a framework based upon six psychological building blocks of deception (known as the *Six Block Model*, or 6BM), comprising attention, perception, sensemaking, expectations, emotion, and behaviour. These processes are manipulated to achieve behaviour change in the target, to the benefit of the deceiver. He then identifies strategies that are used for manipulating each of these blocks, presenting these as a *Gambit Table*. His frameworks provide a basis for conducting target audience analysis for deception, determining measures of deception effectiveness, managing counterdeception, and conducting deception analytics to deconstruct and understand a given case of deception. The theory and associated frameworks are generic and derived from or applicable to any specific domain. The frameworks have been taught to and used by organisations engaged in physical and cyber deception.

3.2 Military-Specific Theories

3.2.1 Maxim et al (1980)

Maxim, Walsh, Daniel, Herbig, & Whaley (1980) present a set of key deception principles and strategies derived from historical military and intelligence deception operations. They assert that successful deception exploits a target's preconceptions by reinforcing existing beliefs rather than introducing new, contradictory information. Deception works by exploiting limitations in human information processing, such as susceptibility to conditioning and desensitisation to false alarms. Deception can induce the target to experience surprise regarding location, timing, strength, or intent. The believability of deception can be enhanced by increasing the number of deceptive channels or layers employed. Sequencing deception activities can deepen the target's belief in a false narrative. Maintaining feedback loops to assess the deception's effectiveness is critical to operational adaptation. The authors highlight the importance of subtlety when designing deceptive activities, care in creating leaks, and the necessity to manage potential unintended consequences. Maxim et al.'s theory of deception is often used to underpin cyber deception theory (e.g., Cross, Raymond, & Conti, 2014).

3.2.2 Monroe (2012)

Monroe's (2012) theory explains how deception involves manipulating an adversary's perception of reality to achieve operational goals. His theory is built upon the manipulation of cognitive biases and decision-making processes, personal and cultural schemata, and exploitation of communications channels to deceive a target. Monroe outlines key types of deception, including *active deception* (displays, feints, demonstration, disinformation) and *passive deception* (cover, camouflage, denial). Deception is viewed as a communication process, in which false indicators are fed through targeted channels to mislead opponents about real intentions. Monroe also uses Boyd's (1996) expanded OODA loop as a basis for representing how deception impacts an adversary's decision making. Monroe suggests that the success of deception depends on exploiting existing perceptions, maintaining security, conditioning, and ensuring coordination across operations. Coordination relies upon timing, flexibility, and controlling the information flow to the adversary. Monroe's theory of deception is cited widely in cyber deception theory (e.g., Guerra, 2023).

3.2.3 Clark & Mitchell (2018)

Clarke and Mitchell (2018) suggest that false beliefs are induced through manipulation of the target's perceptions, reinforcing pre-existing beliefs, creating plausible alternative narratives, and exploiting cognitive

biases. Their theory incorporates concealment, simulation, and disinformation, and emphasises the necessity for counterdeception strategies based on rigorous analysis of one's own vulnerabilities. Clarke and Mitchell highlight the symbiotic relationship between deception and counterdeception, where both sides attempt to outmanoeuvre and gain advantage over each other through information-based and psychological strategies. Clark & Mitchell's theory discusses the use of cyber as a channel for delivering deception, the nature of deception in cyberspace, web-based deception, false news and social media, online mimicry, and deception on the dark web.

3.3 Cyber-Specific Theory

Rowe and Rrushi (2016) is a book offering "a set of interrelated ideas about using deception as a framework for attack and defense of computer systems and networks, and mostly defense". The book covers the psychology of deception, its professional use, deception methods for defence and offence, deception techniques, the measurement, planning, and software engineering of cyberspace deception, decoy input/output devices, application to the electrical power industry, and law and ethics. The theory underlying Rowe and Rrushi (2016) is a taxonomy drawn from linguistic case theory. The same taxonomy is applied to defence and to offence, but the suitability and effectiveness of the linguistic cases differ. For example, the top three cases in defence are deceptive external preconditions (e.g. giving a false excuse for why you cannot do what the intruder wants), deceptive results (e.g. saying a file was downloaded when it was not), and deceptive content (e.g. planting disinformation in files for an intruder to find). By contrast, the top three cases for offence are deception of the agent (e.g. when an intruder falsifies his identity), an accompaniment (e.g. concealing malicious code within innocuous software), and frequency (e.g. swamping system resources).

One limitation of Rowe and Rrushi's (2016) theory is that it assumes that the target is a computer system or network. This excludes human users (and, in particular, system administrators defending the target system), their cognitive world, and any physical devices that the computer system may control or exchange information with. Moreover, since their theory is based on linguistic case theory, it assumes that interaction between deceiver and target occurs by means of communication. In short, it is restricted to the virtual dimension.

4. Evaluation

4.1 By Dimensions

Deception aims to change the target's behaviour by inducing errors in the target's sensemaking. Thus, all theories of deception must focus on the target's psychological processes, which are entities in the Cognitive dimension. Bell & Whalley (1982) model deception as six strategies for manipulating the target's sensemaking by hiding real objects and/or showing false ones. These objects must be in the Physical or Virtual dimension for the deceiver to be able to manipulate them. All the theories in our shortlist, bar one, refer to the six strategies. The exception is Maxim et al (1980), which predates Bell & Whalley. As shown in Table 1, the theories' ontology all include the Cognitive dimension, and most also include Physical. The Virtual dimension is added by later authors or by applying the theory in practice.

Table 1: Ontology and dimensions of each key theory

Theory	Ontology (key concepts)	Dimension(s) derived from ontology
Bell & Whalley	6 manipulation strategies; 5 features (objective, target, plan, means, feedback).	Cognitive & Physical (target; means; entities hidden/shown). Applied to Virtual by Yuill et al (2006) but questioned by Porter (2016).
Reid	Deceiver; strategies & tactics; manipulate target's interpretation & decision making.	Cognitive & Physical. Has utility to Virtual.
Henderson	6 psychological building blocks; manipulation strategies; target's behavioural change.	Cognitive. Used in Physical & Virtual.
Maxim et al	Exploits target's preconceptions; induce surprise; feedback loops to maintain effectiveness.	Cognitive & Physical. Applied to Virtual by Cross et al (2014)
Monroe	Active & passive deception; manipulate target's perception; viewed as communication process.	Cognitive & Physical. Widely applied to Virtual, e.g. Guerra (2023)
Clark & Mitchell	Manipulate target's perception; reinforce beliefs; exploit biases; create narrative; cyber as channel.	Cognitive, Physical & Virtual
Rose & Rrushi	Linguistic case theory; mostly defensive; assumes target is computer system.	Cognitive, Physical (IT hardware) & Virtual (software, data, communications).

4.2 By Tenets

Evaluating the seven key theories in the light of Kallberg and Cook's (2017) tenets results not only in findings on deception theory, but also on the tenets themselves. These findings are as follows:

- *Object permanence*. The lack of object permanence which Kallberg and Cook (2017) regard as cyberspace-specific can be extended to physical objects by employing deception. This is shown by Bell and Whalley's (1982) strategies for *hiding the real* and *showing the false*. To the target the object may appear to lack permanence, but the deceiver knows that in reality it is permanent.
- *Limited measure of effectiveness*. Discussion of measures of effectiveness for deception differs significantly across the seven theories reviewed. In Bell and Whaley (1982) and Whaley (2008), effectiveness is often implicit, being inferred from the target's behaviour and decision-making. Maxim et al. (1980) regard surprise as a measure of effectiveness, but this is unreliable because the target may never realise that they have been fooled. Reid (2016) does not discuss measures. Henderson (2019) provides guidance on measuring the six stages of the deceptive process that leads to the target's change in behaviour. Rowe and Rrushi (2016) identify a comprehensive set of technical measures for detecting deception in networks.
- *Execution at computational speed*. All authors comparing physical and virtual dimensions mention the speed of execution in the virtual world. Recall Miller et al's (2012) "'bullets' travel at near the speed of light". Deception enables various strategies for manipulating the target's perception of time. Temporal manipulations can include simulating near-instant actions and object transformations. This is easier to achieve in the virtual dimension than in the physical dimension. For example, deploying a decoy tank in the physical dimension requires significantly more time and effort than copying and pasting a virtual tank object. However, many theories fail to mention temporality as an attack vector.
- *Anonymity*. Deception has been used for millennia in the physical dimension to achieve anonymity, in the form of mimicry, impersonation, false-flagging, and the simulation of false identities. Examples range from the Trojan Horse to the "little green men" in Crimea in 2014. However, the effort required for virtual anonymity is usually less than in the physical dimension, and AI can further enhance the effectiveness of false identities.

4.3 In the Light of Experience

The second author has 20 years of experience delivering deception training, supporting operations, and evaluating practice. He assesses that most deception theories possess only incomplete, fragmented, and limited relevance to real-world deception operations. Few deception theories appear to have been stress-tested in operations or refined iteratively under practitioners' leadership. Many are specific to one application domain. Translation to military deception in MDO would likely involve substantial effort.

Many theories are not based on scientific knowledge of the psychology of deception (Stech, Heckman, Hilliard & Ballo, 2011). They rarely incorporate classic deception components, well-established terminology, or recognised sources of authority. Such oversights are particularly apparent in cyber deception theory, which tends to focus on technologies and software architectures. Psychologically based theories often rely on outmoded models. Newer theories more accurately explain how deceptive processes work. Other theories quote examples of military deception that are trite, hackneyed, and, in some cases, wrong (e.g. citing cases for which no historical evidence exists). Case studies may describe the execution of deceptive action, but leave out the preceding processes of planning, resourcing, internal 'selling' of the plan, explanation to operatives, and rehearsal. They also often fail to draw out the key lessons learned.

4.4 An Ideal Theory

For applicability to cyber operations in MDO, an ideal theory of deception should:

- Be based on contemporary models of the human psychology of deception and counterdeception.
- Be informed by case studies in the physical, virtual, and cognitive dimensions, including failure.
- Represent objects, actions, and effects in all five warfighting domains.
- View operations as information-led (US Army, 2023), with deceiver and target being physical or virtual.
- Express concepts in language common to physical, virtual, and cognitive dimensions.
- Cover offensive and defensive action at strategic, operational, and tactical levels over the spectrum of cooperation, competition, confrontation, to warfighting.

- Model the interactions between deceiver and target, including collateral effects on allies and neutrals, and between deception and counterdeception.
- Model deception design in organisations, including intelligence, planning, approval, execution, and after-action assessment, harmonising military and cyber cultures (Leenen et al, 2018).
- Account for unique forms of deception that are only feasible in cyberspace (Henderson, 2024).
- Consider the legal and ethical issues of deception, including cyber perfidy.

5. Conclusions and Further Work

This paper has evaluated some key theories of deception for applicability to cyber actions and effects in multi-domain operations. From the strategic context, we conclude that the ideal theory of deception must be applicable to the physical, virtual (i.e. cyber), and cognitive dimensions of the world. Drawing on Clark and Mitchell (2019), we observe that deception involves an interaction through the operating environment between the deceiver and his/her target, possibly involving other actors. The cognitive aspect is represented by an OODA loop (Boyd, 1996) within each actor.

Next, the paper identifies differences between the physical and virtual dimensions, with several authors warning that traditional military thinking may be misleading in cyber operations. We identified at least 31 theories of deception in the literature, with a selected set of three generic theories, three military-specific theories, and one cyber-specific theory being evaluated in this paper. After discussing them, the paper offers some reflections in the light of practical experience and outlines what an ideal theory could look like.

There are two key contributions of this paper. Firstly, we show that an ideal theory of deception must combine physical, virtual, and cognitive dimensions. Secondly, we find that none of the key theories we evaluated satisfied this ideal, and thus none are able to account fully for deceptive operations in MDOs. Key limitations of the paper are that counterdeception was excluded and that the number of theories evaluated was space-limited.

Much further work remains to be done. Most obviously, more theories of deception and counterdeception must be considered. To support integrated cyber-kinetic operations, theories must be combined or extended to cover all three dimensions. Moreover, military deception doctrine must be extended to cover offensive cyber and integrated cyber-kinetic operations. In addition, doctrine should also provide guidance on the hard parts of deception practice, such as on developing deceptive courses of action, on incorporating risk management for deception operations, and on how to communicate deception plans internally to obtain the commander's sign-off. In the scientific realm, research is needed into adapting the cognitive aspects of deception to autonomous and/or artificially intelligent weapon systems and to Command and Control. Theory must also be developed on the interaction between deceiver and target to support red-teaming and the measurement of effectiveness.

References

Bell, J. B., & Whaley, B. (1982). Cheating: Deception in War & Magic, Games & Sports, Sex & Religion, Business & Con Games, Politics & Espionage, Art & Science. St Martin's Press.

Boyd, J.R. (1996). The Essence of Winning and Losing. Unpublished lecture notes, Maxwell Air Force Base, Alabama, USA.

Chief of the Defence Staff. (1998). Land Force Information Operation - Deception. (B-GL-354-003/FP-001). Chief of the Defence Staff, Canada.

Clark, R.M. & Mitchell, W.L. (2019). Deception: Counterdeception and counterintelligence. CQ Press, Thousand Oaks, CA, USA.

Cross, T., Raymond, D., & Conti, G. (2015). Deception for the Cyber Defender: To Err is Human; to Deceive, Divine. In Proceedings, SchmooCon 2015, https://shmoo.gitbook.io/2015-shmoocon-proceedings/bring_it_on/02_deception_for_the_cyber_defender (accessed 21 February 2025).

Economist. (2020). Democracies need to re-learn the art of deception, December 16th.

Grant, T.J. (2023). Using C2 Problem Space to Integrate Cyber and Kinetic Operations. In Proceedings, 28th International Command & Control Research & Technology Symposium (ICCRTS 2023), paper 27.

Guerra, L.M.D.F.C. (2023). Proactive Cybersecurity Tailoring Through Deception Techniques. BSc Thesis, Instituto Superior De Engenharia De Lisboa (Lisbon Higher Institute of Engineering).

Henderson, S. (2019). The Artifice System Handbook. National Cyber Deception Laboratory and Artifice Ltd, UK.

Henderson, S. (2024). Deception in cyberwarfare. In Stevens, T. & Devanny, J. (eds). (2024). Research Handbook on Cyberwarfare, Edward Elgar Publishing, Cheltenham, UK, chapter 14, 223-246.

Kallberg, J. & Cook, T.S. (2017). The unfitness of traditional military thinking in cyber. IEEEAccess, 5, 8126-8130.

Leenen, L., Aschman, M.J., Grobler, M.M. & van Heerden, A. (2018). Facing the cultural gap in operationalising cyber within a military context. In Proceedings, 18th International Conference on Cyber Warfare & Security (ICCWS 2018), 387-394.

Liles, S., Dietz, J.E., Rogers, M. & Larson, D. (2012). Applying traditional military principles to cyber warfare. In Proceedings, 4th International Conference on Cyber Conflict (CyCon 2012), 169-180.

Magnuson, S. (2007). Army wants to make 'every soldier a sensor', National Defense Magazine, May 1st. https://www.nationaldefensemagazine.org/articles/2007/5/1/2007may-army-wants-to-make-every-soldier-a-sensor (accessed 6 February 2025).

Maxim, D.L., Walsh, M.E., Daniel, D.C., Herbig, K.L., & Whaley, B.S. (1980). Deception Maxims: Fact And Folklore. Everest Consulting Associates Inc. / Mathtech Inc.

Miller, M., Brickey, J. & Conti, G. (2012). Why your intuition about cyber warfare is probably wrong. Small Wars Journal, November 29th (8).

MODUK. (2021). The Orchestration of Military Strategic Effects. Development, Concepts & Doctrine Centre, MoD Abbeywood South, UK, January.

MODUK. (2022). Cyber Primer. 3rd edition, Development, Concepts & Doctrine Centre, MoD Shrivenham, UK, October.

Monroe, J.D. (2012). Deception: Theory and Practice. Master's thesis, Naval Postgraduate School. Monterey: Naval Postgraduate School Institutional Archive.

NATO. (2020). Allied Joint Doctrine for Operations Security and Deception. Allied Joint Publication 3.10.2: NATO Standardization Office.

Porter, C. (2016). Toward Practical Cyber Counter Deception. SIPA, February 9th, The Cyber Issue, Winter 2016. https://jia.sipa.columbia.edu/news/toward-practical-cyber-counter-deception (accessed 21 February 2025).

Reid, I. D. (2016). A Holistic, Risk, and Futures-Based Approach to Deception: Technological Convergence and Emerging Patterns of Conflict. PhD Thesis, University of Lincoln.

Rowe, N.C. & Rrushi, J. (2016). Introduction to Cyber Deception. Springer International Publishing, Switzerland.

Seebeck, L. (2019). Why the Fifth Domain is Different. The Strategist, Australian Strategic Policy Institute, September 5th.

Stech, F., Heckman, K., Hilliard, P. & Ballo, J.R. (2011). Scientometrics of Deception, Counter-deception, and Deception Detection in Cyber-space. PsychNology Journal, 9 (2), 79-122.

Tzu, S. (c500 B.C.E./2000). The Art of War (L. Giles, Trans.). Allandale Online Publishing.

U.S. Army. (2023). Information. U.S. Army ADP 3-13, Washington, DC: Headquarters Department of the Army.

U.S. DOD. (2018). Cyberspace Operations. U.S. DOD Joint Publication 3-12, June 8th.

U.S. Marine Corp. (2024). Deception. MCTP 3-32F, Quantico, VA: United States Marine Corps.

U.S. Joint Chiefs of Staff. (2012). Military Deception. Joint Publication 3-13.4.

Whaley, B. (2008). Toward a general theory of deception. Journal of Strategic Studies, 5 (1), 178-192.

Yuill, J., Denning, D., & Feer, F. (2006). Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques. Journal of Information Warfare, 5 (3), 26-40.