The art of deception revisited (part 1): current insights

Colonel Han Bouwmeester, PhD[*]

He who seeks to deceive will always find someone who will allow himself to be deceived!
- Niccolò Machiavelli, in: *The Prince*

Recently, the international security situation has changed significantly. Mutual trust between states has declined sharply. Policy makers of states and international organisations often no longer know where they stand. In 2016, the *Oxford Dictionary* proclaimed 'post-truth' the word of the year.[1] In 2018, 'fake news' and 'misinformation' were amongst the most commonly used words.[2] Russia's annexation of Crimea in 2014 proved to have been a watershed in the way states interact with each other, but this was not the only event that contributed to great international distrust. Much has also happened in the West since then, not only between states but also within states themselves that has left decision-makers, media and the public at a loss as to where they stand.

Take, for example, Brexit in 2016, the 2016 and 2020 US elections, the Macron leaks in 2017, and politicians who consistently dismissed critical news aimed at them and their administration as 'alternative facts'. People today often feel fooled and do not know what to believe. That puts thinking about deception back on the agenda. In early warfare deception was a tool used by the savvy individual commander on the battlefield, but it is not only reserved for the tactical level. Deception includes activities that can take place at all levels. It is a relatively cheap way of gaining an advantage over an opponent.

Up to World War II the Western world also frequently used deception in conflicts, but soon afterwards it rapidly disappeared. This is a striking fact because nowadays Western people are constantly and unconsciously exposed to deception in their daily lives, coming from a variety of sources broadly ranging from advertising messages to films. Deception even takes place during sports competitions, for example when a simple feint is meant to mislead an opponent during a ball game. Apparently, these forms of deception are considered quite normal, while deception applied during a conflict is considered a very sensitive matter. This observation alone is sufficient reason for delving deeper into the phenomenon of deception. This present research[3] on deception consists of two parts, the first focussing on the art of deception, which is covered in this article, while another article containing the second part zooms in on Russian deception and the annexation of Crimea in 2014. The central research question featuring in this article reads: *What are the Western views on deception and the deception process?*

This article starts with an explanation of deception and the unravelling of the deception process, identifying the different phases and the most important elements of deception warfare per phase. It also shows that deception is by no means always the result of a profound planning process; coincidence may lead to occasional deception. The question whether deception is permissible in all cases is discussed next. The article concludes with explanations why the Western world has become less interested in deception warfare.

The deception definition and process

The article focuses mainly on Western thinking on deception, comprising 18 studies in total (shown in Figure 1), which were consulted for this research, ranging from a 1969 stratagem study to an information disorder report from 2018. All these studies, mainly from American, British and Israeli researchers, are considered to be the most relevant studies published over the past 50 years. This timespan has been chosen for its variety of actions taking place in the security environment, such as conventional actions by armed forces during the Yom Kippur War in 1973, the Falklands War in 1982, and Operation Desert Storm in 1990-1991, but also insurgency and intrastate actions in former Yugoslavia during the 1990s and Somalia in 1992. Later, operations in Iraq, Afghanistan and against Islamic State were added. In addition, this 50-year period also covers the development and use of the Internet for security purposes. A total of 18 studies covering a period of 50 years is not a large yield, especially since only 15 studies deal with deception in the security environment, supplemented by a publication on magic, one on lying and a recent study on disinformation. It does indicate, however, that there was little appetite for deception in the West anymore.

U.S. Soldiers question an unknown person during an exercise. Deception includes activities that can take place at all levels. It is a relatively cheap way of gaining an advantage over an opponent

PHOTO U.S. ARMY, DAVID WIGGINS

*   Colonel Han Bouwmeester, PhD is an Associate Professor of military strategy and land operations at the Netherlands Defence Academy.

1   Katy Steinmetz, 'Oxford's Word of the Year for 2016 is 'Post-Truth'', *TIME*, 15 November 2016. See: https://time.com/4572592/oxford-word-of-the-year-2016-post-truth/.

2   Valerie Strauss, 'Word of the Year: Misinformation. Here's Why', *The Washington Post*, 10 December 2018. See: https://www.washingtonpost.com/education/2018/12/10/word-year-misinformation-heres-why.

3   The research, presented in two articles, is an edited version of Han Bouwmeester's PhD dissertation 'Krym Nash' (Crimea is Ours).

Year	Author & Titel	Kind of publication	Country
1969	Barton Whaley – Stratagem: Deception and Surprise in War	Book	USA
1976	Michael Handel – Perception, Deception and Surprise	Research paper	Israel
1980	Central Intelligence Agency – Deception Maxims: Facts and Folklore	Research paper	USA
1982	Irwin Greenberg – The Role of Deception Theory	Article	USA
	Donald Daniel & Katherine Herbig – Propositions on Military Deception	Book chapter	USA
	Barton Whaley – Towards a General Theory of Deception	Book chapter	USA
1986	Robert Mitchell – A Framework for Discussing Deception	Book chapter	USA
	Myrdene Anderson – Cultural Concatenation of Deceit and Secrecy	Book chapter	USA
1989	Michael Handel – War, Strategy and Intelligence	Book	UK
1999	Peter Lamont & Richard Wiseman – Magic in Theory	Book	UK
2000	Scott Gerwehr & Russell Glenn – The Art of Darkness	Monograph	USA
2002	Abram Shulsky – Elements of Strategic Denial and Deception	Book chapter	USA
	Scott Gerwehr & Russell Glenn – Unweaving the Web	Research paper	USA
2003	John Bowyer Bell – Towards a Theory of Deception	Article	USA
2007	Michael Bennett & Edward Waltz – Counterdeception Principles and Applications	Book	USA
2010	Thomas Carson – Lying and Deception	Book	UK
2012	James Monroe – Deception: Theory and Practice	Thesis	USA
2018	Claire Wardle & Hossein Derakhshan – Information Disorder	Report	EU

Figure 1 Overview of the 18 researches used

Combining the insights from the 18 examined deception studies a new deception definition and process can be formulated. Today, deception is an interaction between two or more actors and is based on an information flow constructed by the deceiver in order to lead the target astray. The deception process is comparable to a simple communication process, beginning with a sender intending to share information, thus creating a message, using a medium, and trying to produce an effect on the receiver. A feedback loop completes this communication process.[4] As shown in Figure 2, a deception process actually follows these steps as well and consists of four phases: a planning phase, in which a deceiver decides on how to apply deception, the implementation phase, which focuses on which methods and which channels are to be used, the outcome phase, in which the results become clear by recognizing the effect deception can have on a target, and a feedback phase to determine whether the deception was successful or needs to be adjusted. The deception process takes place in an atmosphere of uncertainty. The four phases and the condition of uncertainty will be explained in the next subsections.

The planning phase
Before a deceiver decides whether to deceive a target and in what way, he will often use a decision-making model. Rational decision-making is frequently propagated, but also criticised. For example, this way of decision-making implies that decision-makers often make deliberate decisions, but the model does not always lead to better outcomes.[5] Another point of criticism is that character traits, such as personality characteristics, personal values and personal experiences, often determine how the decision-maker views the possibilities for solving the problem. These traits are not reflected in a rational model.[6] Nevertheless, the rational

4   Denis McQuail and Sven Windahl, *Communication Models*, Second Edition (Harlow, Essex (UK), Addison Wesley Longman Limited, 1993) 13-17.
5   Jonathan Renshon and Stanley Renshon, 'The Theory and Practice of Foreign Policy Decision Making', in: *Political Psychology* 29 (2008) (4) 512-525.
6   James Robinson, 'The Concept of Crisis in Decision-making', in: Naomi Rosenbaum (ed.), *Readings on the International Political System*, Foundations of Modern Political Science Series (Englewood, NJ (USA), Prentice-Hall, Inc., 1970) 82-83.
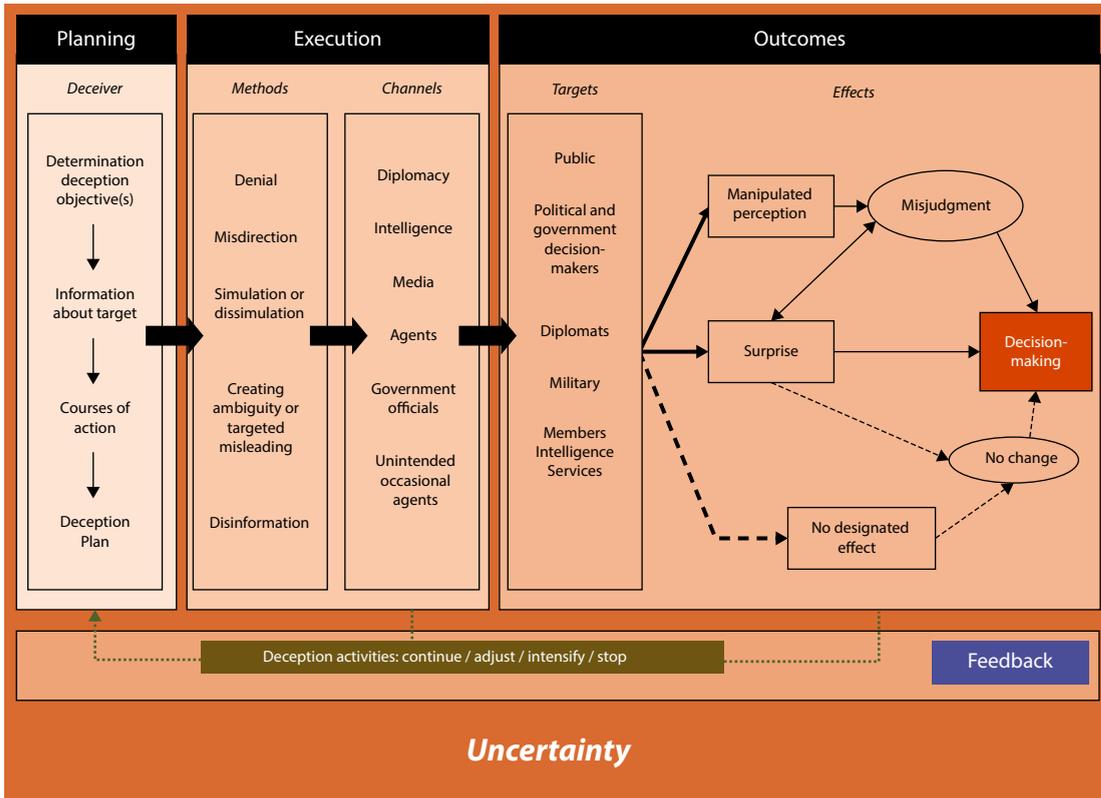
Figure 2 Overview of a deception process

model fits into the Western tradition, especially the military, because the West values reasoned and linear thinking.[7] During this phase the deceiver determines the deception objectives and receives information and intelligence about a potential target, which he needs to formulate possible courses of action. At the end of the planning process, the deceiver decides, and this is how deception comes about. This leads to the next step in the deception process: the execution phase.

The execution phase: methods
This phase comprises different methods and channels. Both are now further explained. A method used for deception is denial. It is an attempt to block all information channels through which an opponent could learn some truths, and therefore denial makes it impossible for him to respond in time.[8] A second method is misdirection, which is nothing more than drawing attention to one subject while

distracting it from another. It is the way an audience is misled by an illusionist in what to see and what not to see. Magic has a massive overlap with deception warfare. In most cases, the magician wants to control the spectator's attention. This is called physical misdirection. The counterpart is psychological misdirection. This occurs when the magician aims to shape what the audience thinks is occurring by controlling the spectators' suspicions.[9] It emerged that misdirection determines where and when a target's attention is focused on influencing what the target registers. It may

7   Alex Mintz and Karl De Rouen Jr, *Understanding Foreign Policy Decision Making* (New Cambridge (UK), Cambridge University Press, 2010) 57-58.

8   Abram Shulsky, 'Elements of Strategic Denial and Deception', in: Roy Godson and James Witz (eds.), *Strategic Denial and Deception: The Twentieth-First Century Challenge* (New Brunswick, NJ (USA), Transaction Publishers, 2005) 15-16.

9   Peter Lamont and Richard Wiseman, *Magic in Theory: An Introduction to the Theoretical and Psychological Elements of Conjuring* (Hatfield (UK), University of Heresfordshire Press, 2008) 31-67.

The battle of Gaines' Mill in 1862. The CIA calls capitalising on existing ideas 'Magruder's principle', named after the Confederate general who used this method during the battle of Gaines' Mill

also include sending a clear and unambiguous signal to entice the target to track the deceiver. Military examples of misdirection are feints, demonstrations, decoy, and dummies.

A third method of deception is simulation and dissimulation. Figure 3 explains that deception is the result of a target's misperception, as opposed to his accurate perception. Misperception is a psychological phenomenon that takes place in the 'eye of the beholder'. People are not deceived by others but merely by

themselves. The deceiver only attempts to provoke deception by revealing a fabricated picture of a situation. In order to be deceived a person must both perceive this attempted portrayal and accept it in terms of 'intended' and 'projected'. Misperception can be self-induced in two ways. First, there is a form of self-deception in cases in which one can see through the deception but refuses to do so. This is also called delusion. Second, an illusion occurs when one can neither see nor discover the deception due to one's own shortfalls. Situations in which others cause the misperception are of much greater importance for this chapter. Misperception, induced by others, can be divided into deception that is intended, and misrepresentation that is unintentional.[10]

10　Barton Whaley, 'Toward a General Theory of Deception', in: John Gooch and Amos Perlmutter (eds.), *The Art and Science of Military Deception* (Boston, MA (USA), Artech House, 2013) 178-182.

The next step is that every deception activity consists of only two basic parts, which are simulation, or 'showing', and dissimulation, or 'hiding'. Showing means displaying things that are not actually there to give a certain impression, while hiding assumes that it is better to cover things, so as not to show them openly to the outside world. Showing and hiding can be achieved in different ways and to different degrees, as shown in Figure 4. The effects of showing and hiding can be reinforced by capitalising on existing ideas. There is a human mechanism behind this, because it is generally easier to induce a target to maintain a pre-existing belief than to present notional evidence to change that belief. The Central Intelligence Agency called this premise the 'Magruder's principle', because Major-General John Magruder of the Confederate States Army applied it during the battle of Gaines' Mill in the state of Virginia in 1862.[12] Unionist Major-General George McClellan, commander of the Army of the Potomac, was advised by several of his subordinates to attack the Confederate division of Magruder in the vicinity of Gaines' Mill near the Chickahominy River, but feared an overwhelming Confederate force based on ideas he had before. Magruder used this misinterpretation by ordering frequent, noisy movements of small units and using groups of slaves with drums to pretend large marching columns.[13] Magruder remarked that he and his men merely had to persuade McClellan to continue to believe what he already wanted to believe.[14]
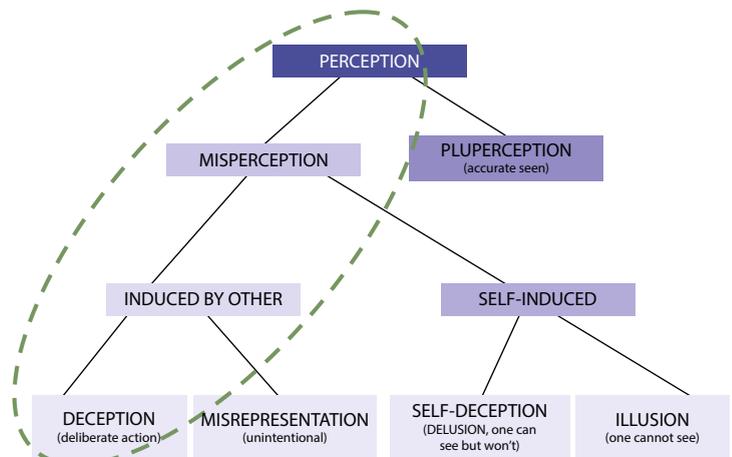
A fourth method of deception is creating ambiguity versus targeted misleading. 'Ambiguity-increasing' or A-type deception, also known as the less elegant version, confuses a target to such an extent that it is unsure as to what to believe. By guaranteeing an impact, A-type deception requires that the deceiver's lies and tricks are plausible enough to the target's comfort so that he cannot ignore them when the deceiver enhances uncertainty by providing extra information. A target may delay decision-making, thereby giving the deceiver wider freedom to arrange resources and take or retain the initiative. By assuring a high level of

Figure 3 Whaley's typology of misperception[11]

THE STRUCTURE OF DECEPTION	
DECEPTION (distorting reality)	
DISSIMULATION (hiding)	**SIMULATION** (showing)
Masking Concealing one's own or matching another characteristics to eliminate an old pattern or blend it with a background pattern.	**Mimicking** Copying another's characteristics to create an old pattern, or imitating it.
Repacking Adding new or subtracting old characteristics to modify an old pattern by matching another.	**Inventing** Creating new characteristics to produce a new pattern.
Dazzling Obscure old or add alternative characteristics to blur an old pattern, reducing its certainty.	**Decoying** Create alternative characteristics to provide an additional, alternative pattern, and increase its certainty.

Figure 4 Whaley's structure of deception[15]

ambiguity concerning the deceiver's intentions, the target is forced to spread his resources 'to cover all important contingencies', thereby

11 Whaley, 'Toward a General Theory of Deception', 180.
12 Central Intelligence Agency, *Deception Maxims, Facts and Folklore* (Washington, D.C. (USA), CIA, Office of Research and Development, 1980).
13 Stephen Sears, *To the Gates of Richmond: The Peninsula Campaign* (New York, NY (USA), Ticknor & Fields, 1992) 215-216.
14 Bruce Catton, *This Hallowed Ground*, reprint from 1955 (New York, NY (USA): Random House/Vintage Books, 2012) 142.
15 Whaley, 'Toward a General Theory of Deception', 186.

Voting in the Netherlands. Disinformation is a strange phenomenon, because, for instance, politicians have a habit of making unrealistic promises during election campaigns which the electorate were prone to believe

reducing the opposition the deceiver can expect at any time. An example is the way the Russian authorities disseminated different story lines about the downing of flight MH17 in July 2014, such as the notions that the plane had been brought down by a Ukrainian missile or a Ukrainian fighter jet, that it had collided with a CIA satellite or that Russian-unfriendly separatists had mistaken the Malaysian airliner for Putin's presidential plane.[16]

The other version, labelled as 'misleading' or M-type deception, is a form of detailed targeting. M-type deception is designed to reduce the target's uncertainty by showing the attracti-veness of one wrong alternative, which the

target is led to believe. It causes a target to concentrate its resources on a single result, maximizing the deceiver's chances for prevailing in all others.[17] The essence of M-type deception is 'to make the enemy quite certain, very decisive and absolutely wrong'.[18]

A last method of deception is disinformation. Actually, disinformation is a strange phenomenon. For instance, politicians in Western democracies have a habit of making unrealistic promises during election campaigns which the electorate were prone to believe. Organisations and business corporations, on the other hand, have bombarded people worldwide with manipulative advertising campaigns. Likewise, the film industry in Hollywood has a long track record of creating false stories or magnifying certain actions in authentic events in their films in order to boost ratings. These methods of influencing are referred to as 'information pollution'. In addition, the rise of the Internet has brought about fundamental changes in the way information is produced,

16   Fatima Tlis, 'The Kremlin's Many Versions of the MH17 Story', *Polygraphic. Info*, 25 May 2018. See: https://www.polygraph.info/a/kremlins-debunked-mh17-theories/29251216.html.

17   Donald Daniel and Katherine Herbig, *Strategic Military Deception* (New York, NY (USA), Pergamon Press Inc., 1982) 5-7.

18   Barton Whaley, op. cit. in: John Gooch and Amos Perlmutter (eds), *Military Deception and Strategic Surprise* (London (UK), Frank Cass and Company Ltd, 1982) 131.

communicated and disseminated. Today, information is widely accessible and inexpensive. Sophisticated platforms have made it easy for anyone with access to the World Wide Web to create and distribute content. Information consumption has long been a private matter, but social media have made it much more open. The speed with which information is currently disseminated and available has been amplified by mobile phones and other devices, and this tremendous pace makes it much less likely that information will be challenged and verified as it was in the past.[19]

The term 'information disorder' was introduced to cover all damaging information, which includes three types, as shown in Figure 5:
1. *Misinformation.* This is information that is false, but not created with the intention of causing harm. This includes unintentional mistakes, like inaccurate photo captions, dates, statistics, translations, or when satire is taken seriously.
2. *Disinformation*. This is information that is false and deliberately created to harm a social group, an organization or a country. This form of information comprises false context, imposter content, manipulated content and fabricated content. It also includes conspiracy theory and rumours.
3. *Malinformation*. This is information that is based on reality, used to inflict harm on a person, social group, organization or country. Examples are leaks, harassment and hate speeches. People are often targeted because of their beliefs, history or social associations, which considerably affect people in their feelings and emotions.[21]

Today disinformation is considered as a national security problem, because it is primarily a political activity during elections or other democratic processes that varies from nation to nation. Often the intent of disinformation is 'to undermine confidence in legitimate institutions and democratic processes and [to] deepen societal fault lines through entrenching views/beliefs and subverting a society's values'.[22] Within disinformation, too, newer and more visual forms of deception are emerging, such as

INFORMATION DISORDER

FALSENESS   INTENT TO HARM

Misinformation   Disinformation   Malinformation

False connection   *False content*   *Leaks*
Misleading content   *Imposter content*   *Harassment*
                       Manipulated content *Hate speech*
                       Fabricated content

Figure 5 Information disorder venn diagram by Wardle and Derakhshan[20]

imagefare, the use of images to influence public perception about a conflict,[23] and *deep fakes,* the manipulation of human images by synthetic media.[24]

Conspiracy theories are a special form of disinformation. Conspirators often have an unpleasant experience within society. For them, belief in a conspiracy is often very therapeutic; it offers an explanation as to why they are so unlucky. Many humans are uncomfortable with unpredictability and coincidence. If something happens, there must be a reason. A conspiracy theory, therefore, is an attempt to explain a certain event by referring to secret machinations of powerful groups of people who manage to

19 Claire Wardle and Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making,* Second Revised Edition (Strasbourg (FRA), Council of Europe, 2018) 10-12.
20 Wardle and Derakhshan, Information Disorder, 5.
21 Ibidem, 20-21.
22 Rachael Lim, *Disinformation as a Global Problem – Regional Perspectives* (Riga (LTV), NATO Strategic Communications Centre of Excellence, 2020) 6.
23 Sterre van Hout, 'Verdediging tegen Imagefare: Het Gebruik van Beeldvorming als Wapen', in: *Militaire Spectator* 189 (2020) (9) 432-434.
24 Nina Schick, *Deep Fakes: The Coming Infocalypse* (New York, NY (USA), Twelve/ Hachette Book Group, 2020) 24-50.

conceal their role in the event.[25] There is always a coalition or a group of multiple actors involved for a single individual cannot cause a conspiracy.[26] Conspirators tend to distrust established institutions, such as the government, the media or other social institutions, and also people in general, even family, friends, neighbours and colleagues. Conspirators often make use of stereotyping. This conformation to prejudice makes people believe the conspiracy stories. Insecurity, caused by the lack of proper knowledge about the situation, is particularly conducive to this. A perception of unethical behaviour by authorities and the use of hidden agendas can arouse suspicion, creating ambiguous situations. People no longer know what to think, who to trust and often come to negative conclusions about others. In this way people create their own versions of the truth, which form the basis of a conspiracy theory.[27] It is also often difficult to debunk a conspiracy theory; conspirators do not believe in the hard evidence presented by authorities.[28] Moreover, a new generation of conspiracy theories has emerged in recent years. The persuasive power of these conspiracy theories lies in the repetition of the message. The pseudo-scientific evidence on which first generation conspiracy theories still rested has now been replaced by social evidence. If one person constantly says, 'a lot of people are saying', many followers are convinced that this is the absolute truth.[29]

The execution phase: channels
Another important element in the execution phase of deception are the channels through which signals can be distributed. As shown in Figure 2 there are many channels, such as *intelligence, diplomatic* and *news channels*. They allow a deceiver to reach his target audience in a variety of ways. Many of these channels may remain relatively hidden to the public at large. Some experts think that deception and propaganda are the same, but there is a difference. Deception aims to induce a target to do something that is in the deceiver's interest, while propaganda attempts to affect a target's beliefs more generally and is directed at the populace at large rather than at the nation's leadership. Furthermore, there are *agents-of-influence*: persons who are able to get close to important government officials in order to influence their views and actions concerning major issues. Usually, a target is unaware of the loyalty of the agent-of-influence; ideally, from the deceiver's point of view, a target considers the agent the best of friends, who has the target's best interests at heart, whereas the agent is loyal to the target's opponent. Agents-of-influence also include operators of security services, who often use local trade as a cover to recruit and train local citizens for possible subversive activities. Not only can specially designated agents be deployed, but a state can also temporarily task *government officials,* representing their department at official meetings, assemblies or conferences abroad, to spread inaccurate information. The category *others* contains travellers, businessmen or relief workers, temporarily recruited to work for an intelligence service.[30]

A CIA report on deception maxims warns of the Jones' lemma, which implies that deception becomes more difficult as the number of channels of information available to the target increases. However, within limits, the larger the number of controlled channels, the more likely it is that deception is believed.[31] The phrase 'Jones' lemma' comes from Professor Reginald Jones, who was a key figure in British scientific intelligence during World War II. At that time, Jones focused on the detection of forgeries. He stated that the success of detecting was much greater when different channels of investigation were used at the same time. Jones' conclusion

25 David Aaronovitch, *Voodoo Histories: The Role of the Conspiracy Theory in Shaping Modern History,* Originally printed in 2009 by Jonathan Cape (New York, NY (USA), Penguin Books, 2010) 5-49.

26 Jan-Willem van Prooijen, *The Psychology of Conspiracy Theories* (London (UK), Routledge, Taylor&Francis Group, 2018) 6.

27 Michael Wood and Karen Douglas, 'Conspiracy Theory Psychology: Individual Differences, Worldviews, and States of Mind', in: Joseph Uscinski (ed.), *Conspiracy Theories & the People Who Believed Them* (New York, NY (USA), Oxford University Press, 2019) 246-248.

28 Van Prooijen, *The Psychology of Conspiracy Theories*, 6.

29 Russell Muirhead and Nancy Rosenblum, *A Lot of People Are Saying: The New Conspiracism and the Assault on Democracy* (Princeton, NJ (USA), Princeton University Press, 2019) 3.

30 Shulsky, 'Elements of Strategic Denial and Deception', 19-26.

31 CIA, *Deception Maxims*, 21-22.

was that it was better to use several independent means of detection, instead of putting the same total effort into the development of only one.[32] The CIA used an analogy of Jones' principle in its deception research.

The outcome phase

The last phase of the deception process is focused on the outcome. It starts with a target of deception in a conflict, which can be the general public, politicians and decision-making authorities of a nation, diplomats, the military, or members of intelligence services. In general, when a target believes the deception, two effects may occur: the target may be surprised or gain a manipulated perception. Surprise can paralyze a target to such an extent that he is not able to think straight and decide, which can lead to the inability to arrive at a correct perception. In other words, when a target is surprised there is a chance that he or she will come to an incorrect decision or none at all, which facilitates the possibility of a manipulated perception. Manipulated perception, like misperceptions, may cause misjudgements, which, in turn, may lead on the one hand to surprise, as the target misunderstands a situation leading to the unexpected. On the other, misjudgement can also affect the quality of the decision-making of a target. It is also possible that deception does not work. In that case there are unintentional effects and it will not have a major impact on decision making. It means there is no change in the situation and the status quo will be maintained.

The feedback phase

Although it is sometimes hard for a deceiver to measure the levels of success of deception, it is necessary for the deceiver to get feedback from the target to indicate what the effect of the deception was and to determine the degree of success.[33] The deceiver's response to the feedback could be to *maintain*, *stop*, or *intensify* the deception. If a target ignores the deceiver's signals, the deceiver is in the difficult position of having to blindly decide what option to take. This is a situation in which the deceiver lacks insights into what the target may be responding to.[34] As soon as the deceiver decides to continue

When a target believes the deception two effects may occur: the target may be surprised or gain a manipulated perception

the deception, he needs to know which methods and channels were successful, and which of them need to improve. All factors must be considered, even if the created illusion is effective, changes need to be made, because the deception effect, even if it is successful, is never everlasting.[35] It is not only the deceiver who can learn from his deception experience, but also the target. Both deceiver and target evaluate their actions and will correspondingly try to improve their performance. However, there is a risk for the deceiver that when his target discovers ongoing deception activities, or parts of them, he will use the feedback channel for counter-deception.[36]

The condition of uncertainty

A fundamental aspect in deception warfare is uncertainty. The deceiver may be uncertain about the results of the deception, while a target is uncertain about what happens in a

32 Reginald Jones, 'The Theory of Practical Joking – Its Relevance to Physics', in: *Bulletin of the Institute of Physics*, (June 1967), 7.

33 Daniel and Herbig, 'Propositions on Military Deception', 8.

34 Myrdene Anderson, 'Cultural Concatenation of Deceit and Secrecy', in: Robert Mitchell and Nicolas Thompson (eds), *Deception, Perspectives on Human and Nonhuman Deceit* (Albany, NY (USA), State University of New York, 1986) 326-328.

35 John Bowyer Bell, 'Toward a Theory of Deception', in: *International Journal of Intelligence and Counterintelligence* 16 (2003) (2) 253.

36 Daniel and Herbig, *Strategic Military Deception*, 8.

Uncertainty is a fundamental aspect in deception warfare. It makes a target unsure about what his opponent will do

situation.[37] People involved in deception, especially potential targets, make decisions under conditions of uncertainty, in other words they operate without full knowledge and lack the necessary information. A target, suffering from uncertainty, does not know what his possible opponent will do, whether, 'if', 'when', 'where' and 'how' he will strike or deceive.[38] In other words: deception is not possible when a target exactly knows the desired goals, preferences, judgments and abilities of its suspected deceiver.

Occasional deception

Deception need not always rest on a deliberate plan. Coincidence and opportunism can also play a role in deception. Accidental circumstances and a well-developed sense for deviousness may lead to deception on the scene. This was demonstrated on many occasions before, during and after World War II, as is exemplified by the

name-giving of the famous Special Air Service (SAS). In January 1941 Colonel Dudley Wrangel Clarke, a flamboyant military genius with a great sense of humour and a unique talent for devising tricks, had set up a non-existing unit of paratroopers in the Middle East under the name of 'First Special Air Service Brigade'. This phantom unit's purpose was to make Axis-troops believe that the British had organised a large airborne force in the region. Clarke spared no expense; pictures of men dressed as paratroopers pretending to be recovering from jump injuries in Egypt were distributed, and documents were falsified and shared. When Clarke heard that Major David Stirling was transforming his mess of irregulars who conducted raids in the desert into a special para-trained unit, he saw the opportunity to increase his deception effect. Clarke suggested to name Stirling's rabble the 'L Detachment, Special Air Service Brigade', as if his fictive brigade consisted of many detachments. Stirling immediately agreed, and the detachment became the founding unit of the later 22 SAS Regiment.[39]

Legitimacy of deception

After this detailed explanation of the deception process and deception by occasion, the question whether deception may be applied indiscriminately also arises. To answer this question, reference is often made to the difference between perfidy and ruses of war. A detailed denunciation of perfidy can be found in Additional Protocol I to the Geneva Conventions, as Article 37(1) stipulates, 'it is prohibited to kill, injure or capture an adversary by resorting to perfidy', while defining perfidy as any 'acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence'.[40] Perfidy constitutes a breach of the laws of war, and is considered a war crime. In total 174 states have ratified this Additional Protocol I, which shows that a vast majority of states are bound by treaty-based perfidy prohibition.[41] Examples of perfidy are faking surrender to lure an enemy

37 Michael Bennett and Edward Waltz, *Counterdeception, Principles and Applications for National Security* (Boston, MA (USA), Artech House, 2007) 35.

38 Richard Betts, *Surprise Attack: Lessons for Defense Planning* (Washington, D.C. (USA), Brookings Institution, 1982) 4.

39 Ben Macintyre, *SAS: Rogue Heroes* (London (UK), Penguin Random House UK, 2017) 24-25.

40 *Protocol Additional I to the Geneva Conventions* of 12 August 1949, adopted in 1977, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I).

41 Mike Madden, 'Of Wolves and Sheep: A Purposeful Analysis of Perfidy Prohibitions in International Humanitarian Law', in: *Journal of Conflict and Security Law* 17 (2012) (3) 442.

Some soldiers of the 'L Detachment, Special Air Service Brigade' in North Africa during the Second World War. Accidental circumstances and a well-developed sense for deviousness may lead to deception on the scene, as was the case with the SAS

into an ambush, an infantry group wearing civilian clothes pretending to be local population, or feigning the protected status of internationally recognised organisations, such as the Red Cross and the United Nations or of neutral or other states not involved in the conflict, by the abuse of symbols, signs, or emblems.

Three decades before the ratification of this Additional Protocol I, a US military tribunal found *SS-Obersturmbannführer* (Lieutenant Colonel) Otto Skorzeny not guilty of violating the laws of war in force at the time. During the battle of the Bulge in December 1944, Skorzeny ordered his men to wear American GI uniforms

as part of Operation Greif to create confusion behind Allied lines. In its verdict the tribunal emphasised the difference between using enemy uniforms for espionage versus combat. Immediately following the verdict, the United Nations War Crimes Commission reacted in shock stating that no hard-and-fast conclusion could be drawn from the acquittal of all the accused in the Skorzeny case as where the legitimate use of enemy uniforms as a stratagem was concerned.[42] With the current Additional

42 Maximilian Koessler, 'International Law on the Use of Enemy Uniforms As a Stratagem and the Acquittal in the Skorzeny Case', in: *Missouri Law Review* 24 (1959) (1) 16-17.

Protocol I, Article 37 in force, the rules have been amended. This protocol prohibits the use of enemy flags, military emblems, insignia or uniforms while engaging in combat or while shielding, favouring, protecting or impeding military operations.[43] The Statute of the International Criminal Court in The Hague adds that the improper use of enemy uniforms in armed conflict is a war crime when it causes fatal casualties or serious physical injury.[44]

On the other hand, ruses of war are not prohibited. Such trickery includes acts intended to mislead an opponent or to incite him to act rashly, but do not violate any rule of inter-national law applicable in armed conflicts. Neither are they perfidious because they do not inspire confidence in an opponent as regards the protection under that law. Examples of such stratagems are the use of camouflage, lures, feints and non-factual information.[45]

Less interest in deception

History is full of examples of deception, stratagems and cunning plans during conflicts, but the Western world has lost its interest in deception. Many officers in NATO's armed forces do not have a profound understanding of what deception means and why it should be an integral part of a military plan as they, almost unanimously, embrace the Western physical way of warfare. There are four main causes for the waning recognition of deception in Western military thinking.

43   Additional Protocol I, Article 39 (2).
44   International Criminal Court Statue, Article 8 (2) b (vii).
45   Gary Solis, *The Law of Armed Conflict: The Humanitarian Law in War* (Cambridge (UK), Cambridge University Press, 2016) 420-435.

U.S. Marines fire the M1A1 Abrams tank. Western armed forces still have a strong 'destroy and defeat' mentality, a factor in the West's loss of interest in deception
PHOTO U.S. MARINE CORPS, MARCIN PLATEK

First, deception has not been taught at Western military academies for decades as a mere reflection of the nature of operations the Western armed forces were involved in. During the Cold War, the armed forces of most NATO countries were focused on physical operations to stop the armoured echelons of the Warsaw Pact, to prevent their fighter and bomber support, and to ensure unrestricted use of the Transatlantic sea lines of communication. After the collapse of the Warsaw Pact in the first half of the 1990s, most Western countries became involved in peace and stabilisation operations, e.g. in the Balkans, Iraq and Afghanistan. One of the main idiosyncrasies of these operations is the concept of transparency.[46] By and large, the consensus opinion in the 1990s and later was that deception plans were neither considered serious business nor an important part of military strategy anymore.[47] So, soldiers in Western nations gradually became less and less familiar with deception operations.

Second, most Western democracies and their armed forces seem to uphold the medieval code of chivalry when waging wars, as if they were fighting like knights on horseback. Currently military officers are still considered the custodians of the chivalric code of honour in wartime.[48] Western military officers represent state systems in which freedom, human rights and ethical standards are principal values, and they do not want to lose this moral high ground. Deception warfare has acquired a dubious, even devious, ring to it and is often judged to be ungentlemanly. Decent people should not be engaged in what is sometimes seen as an 'indecent activity'.[49]

Third, Western institutions dealing with security and acting in the information environment, like armed forces, are often involved in an asymmetric battle in which they do not want to be caught spinning and distributing manipulated information. A government does not lie to its people in a Western democracy; that is a fundamental principle. Moreover, Western media and governments keep hammering on the need for balanced reporting of events and thus avoid accusations of spin and deliberate framing

at all costs.[50] This attitude should prove its durability, even in this cyber era.

Fourth, Western armed forces still have a strong 'destroy and defeat' mentality. The desired style of warfare in the Western world is firmly rooted in cumulative destruction, and it hardly leaves any latitude for indirect methods like deception. A spectrum of warfare can be created with the mentioned cumulative destruction and systemic disruption at both ends. Cumulative destruction, which includes a strategy of annihilation and attrition, seeks to destroy the opponent's capacity for war leading to a decisive defeat of the opponent's military force. Successful application of the cumulative destruction approach depends on force superiority.[51] This style of warfare has two main warfighting functions: manoeuvre and fires.[52] Systemic disruption yields victory through engaging the opponent's weaknesses, which impairs the opponent in such a way that he is left incapable of reacting straight and successfully. This approach is not dependent on absolute force superiority alone. An inferior force could achieve a strategic victory over a superior force, provided it focuses on systemic disruption involving ways of exploiting the opponent's flaws, even the societal ones.[53] The main warfighting functions are deception (although momentarily not recognized as a warfighting function), information and intelligence.

However, warfare does not merely belong just to one end of this spectrum. All warfare can be projected as existing somewhere in this spec-

46   Royal Netherlands Army, *Doctrine Publication 3.2 Land Operations* (Amersfoort (NLD), Land Warfare Centre, 2014) 7-3 & 7-4.

47   Martijn Kitzen, 'Western Military Culture and Counter-Insurgency: An Ambiguous Reality', in: *Scientia Militaria, South African Journal of Military Studies* 40 (2012) (1) 1-8.

48   Paul Ducheine, *Je Hoeft geen Zwaard of Schild te Dragen om Ridder te Zijn, Mythen over Digitale Oorlogsvoering en Recht*, Inaugural Speech Nr. 559 (Amsterdam (NLD), University of Amsterdam, 2016) 6.

49   John Gooch and Amos Perlmutter, *Military Deception and Strategic Surprise* (London (UK), Frank Cass and Company Ltd, 1982) 1.

50   David Betz, *Carnage and Connectivity: Landmarks in the Decline of Conventional Military Power* (Oxford (UK), Oxford University Press, 2015) 117-130.

51   James Monroe, *Deception: Theory and Practice*, Thesis (Monterey, CA (USA), Naval Postgraduate School, 2012) 25-26

52   Sean McFate, *Goliath: Why the West Isn't Winning, and What We Must Do About It* (London (UK), Penguin Random House, 2019) 236-237.

53   Monroe, *Deception*, 26-27.

	Cumulative Destruction	**Systemic Disruption**
Target	Strength against strength.	Strength against weakness.
End State	Incapacitation through attrition of resources (strategy of annihilation).	Incapacitation through strategic paralysis.
Focus of Effort	Tactical level, with objects in terms of enemy and terrain.	Operational level, with objectives in terms of shattering the opponent.
Outcome	Predictable, based on 'overall superiority'.	Unpredictable, based on ability to perceive and affect the opponent's weaknesses.
Orientation	Interior focus on processes to achieve maximum efficiency of tasks.	External focus to identify enemy weakness and limitation.
Force Design	Systems and formations designed for all-around capabilities – infrequent, revolutionary changes to capabilities.	Systems and formations designed for specific enemyforces – frequent, evolutionary changes to capabilities.
Main warfighting functions	• Movement and manoeuvre • Fires	• Deception • Information and Intelligence

Figure 6 Overview of Cumulative Destruction and Systemic Disruption[55]

trum. Yet, the degree to which a commander's solution for an operation tends either to cumulative destruction or to systemic disruption affects the degree in which deception is used in that operation.[54] Figure 6 shows differences between the two ends of the spectrum.

Concluding remarks

This article, the first in a diptych about modern deception in conflicts, answers the question: What are the Western views on deception and the deception process? Deception is an activity that causes surprise or manipulates the perception of a target, leading the target astray. In most cases, this state of the target affects its decision-making, ultimately creating a situation that is beneficial to the deceiver.

The deception process comprises four phases: phase 1 is the planning phase, in which the

deceiver determines the ultimate deception goal. In preparation, the deceiver will gather information about the target and weigh possible courses of action. Phase 2 deals with the methods and channels, while phase 3 is focused on the outcomes. The aim of deception is twofold: creating surprise and/or manipulated perceptions. And an atmosphere of uncertainty is necessary to evoke deception. Phase 4 comprises feedback. The deceiver may decide to adjust or stop the deception activities, or he might decide to continue or intensify the deception when it is successful. Not all deception is the result of a well-considered plan; there are also cases of occasional deception in which coincidence and opportunism play a role. Deception does not always turn out to be fully applicable. Cases of perfidy, such as the misuse of Red Cross symbols, are classified as war crimes. Ruses of war, on the other hand, are permitted. In addition, it has been noted that deception has hardly been addressed in the West in recent decades. With this knowledge of deception in mind, the second article in this diptych will focus on Russian deception and the annexation of Crimea in 2014. ■

54   Ibidem, 28-29.
55   Ibidem, 27. The bottom row in the table was created by the author to accentuate the different warfighting functions.