Preamble

Much of this book is devoted to technology and its application within specific domains. This chapter will explore the use of unmanned vehicles as conduits of information and the varying purposes to which those conduits can be put.

Student learning objectives

After reading this chapter, students should be able to do the following:

1. Describe the components of communications
2. Define misinformation and disinformation
3. Describe the types of problems that can result from deceptive information in automated systems.

The Ruses of War

The concepts of misinformation and disinformation come from the practices of adversarial competition. In fact, they are only useful in adversarial competition. In collaborative endeavors, misinformation and disinformation can be not only problematic but downright dangerous. Think about a team of medical professionals working together to perform a surgery, or a team of operators working with remote unmanned systems to execute a mission. Any problems with the clarity and common understanding of information could be disastrous. When working with another party
towards a common goal, it is paramount that all parties understand the goal, the steps, and the strategies clearly. Any mistakes in information, whether originating from the sender or by faults in the transmission or misinterpretation by the receiver, causes friction in relationships. That friction slows down the effectiveness and speed of collaboration, because clarification must be sought, sometimes multiple times. A savvy competitor uses such friction to gain an advantage. An aggressive competitor creates and promulgates such friction to undermine and damage abilities to interpret, analyze, and strategize.

In competition, it is sometimes useful to increase the friction rather than decrease it. As the Earl of Chesterfield observed in 1749, “without some dissimulation, no business can be carried on at all.” (Breuer, 2001, p. viii) In warfare, the practice falls under a category known variously as stratagem, deception, diversion, ruse, or camouflage (Whaley, 2007). Disinformation can be considered as “the most important single broad category of ruses … fed into another's information system in order to deceive him” (Whaley, 2007, p. 8). The practice of disinformation has spanned all of history (Breuer, 2001) (Whaley, 2007) and has been observed in the animal kingdom as well (King, 2019). As noted by Breuer (2001), “force and fraud have been the two cardinal principles of warfare since Sun Tzu, the Chinese warlord who conquered huge expanses of Asia, recorded his military theories in 550 BCE: ‘undermine the enemy, bewilder and confuse him, strike at his morale, then his army will fall to you.’” (Breuer, p. 1) As such, it is prudent to understand both effective communication and how that process can be subverted or perverted.

**Understanding Effective Communication**

In order to understand the subversion of communication, it is necessary to understand what communication is and what distinguishes effective communication. There have been many, many, many tomes written on effective communication, but for the purposes of this discussion, we will focus on the complexities
of communicating from person to person through the lenses of effective listening techniques and a model of communicative elements.

The Elements of Communications

There are several different elements of communication that are important to understand. The most common way of referring to these elements is as 'signal' and 'noise'. However, that type of nomenclature obscures the subtleties associated with deception. For the purposes of this discussion, the ‘signal’ is described in four categories while ‘noise’ is treated through two categories.

First, there is information that is both relevant and truthful. An example of this could be a fire alarm that correctly alerts a homeowner to a fire in the home while he is home. It would be less relevant if the homeowner were away and unable to respond to the matter.

Next, there is information that is truthful but irrelevant. For example, if a person interrupted a business meeting to inform everyone present that two people in the grocery store were seen arguing, that would be truthful but highly irrelevant to the business meeting. It is a distraction.

Following that, there is information that is relevant but false or misleading. An example of this could be a lie about a situation or manipulated media that presents a situation differently than what really happened.

Finally, there is information that is irrelevant and false or misleading. An example of this might be casual gossip that spreads an untrue rumor.

Technical problems in the communications channel, such as static or blurred focus, are distinguishable from the previous categories and deserve a separate discussion. While technical problems are neither true nor false, they do impede the effectiveness of communications. Further, they may be caused by either
circumstances (weather, faulty equipment, or user error) or by malicious activity (jamming, sabotages, or computer exploit).

Note that there are 4 components that are undesirable. We can simplify by referring to them as misinformation and disinformation, thusly:

- Misinformation is the general term for information that is one of the following types:
  - Truthful but irrelevant information
  - Irrelevant and false or misleading
  - Technical problems in the communications channel, such as static or blurred focus, are distinguishable from the previous categories and deserve a separate discussion.
- Disinformation is the general term for information that is relevant but false or misleading.

The challenge to the consumer of information is, therefore, threefold:

- Figure out what is truthful information;
- Judge the relevancy of the information; and
- Minimize the occurrence of technical problems.

Figuring out either truthfulness or relevance of communications is not always as easy as it should be. There are charlatans who publish fraudulent data, there are idea thieves who publish plagiarized material, and there are simpletons who publish what they think is good but which suffers from inherent flaws in logic or methodology. Some publishers exert little control over the quality of material. As a result, there is a span of quality in the published literature that ranges from extremely reliable to extremely questionable.[i]

The increasing automation of information collection, interpretation, and fusion makes the challenge even greater:

As dependence on information increases due to the automation
of more and more elements in the surrounding environment, the ability of the warfighter to judge the reliability and accuracy of information content becomes more important. There are two aspects to this challenge:

- Judging relative truth: being able to comprehend the inherent inaccuracies in data that exist due to model uncertainty, source inaccuracies, and so on; and
- Judging continued truth: being able to determine whether the information being considered has been tampered with, replaced, or otherwise interfered with.

The significant technical challenges in both of these aspects range from human interface issues to confidentiality measures. In responding to these challenges, complex information display techniques, such as virtual reality applications, will clearly have some level of payoff. As capabilities for injecting falsehoods into otherwise truthful data continue to be developed, the challenge of determining continued truthfulness will be exponentially greater, particularly in light of the automated fusion capabilities that are being relied on to assist humans in handling the huge amounts of available data in a timely manner.

(Panel on Information in Warfare, 1997, pp. 81-82)

A Simple Model of Communications

For information to be communicated from one entity to another, there is a surprisingly complex set of requirements. Think about communications between a person and a pet, or between two dogs meeting for the first time in the park, or between two people who speak different languages. The goal of communications is to transfer information from one entity to another. Let’s look at what this entails.

First, the entity originating the message must have some way
of encapsulating the information into the message. This can be done with facial expressions, body language, words, music, and even pheromones.

Next, the originator must have some way of transferring the message to the recipient. This can be done by various ways, depending on how the information is encapsulated. One simple way of transferring the message would be to simply place oneself in the visual range of the recipient and make sure that the recipient is looking and paying attention. Another way would be to speak within auditory range of the recipient. Crucially, the actual transmission of a message requires some level of cooperation by the recipient. In other words, the actions of the originator are necessary but not sufficient.

The cooperation of the originator and the recipient are also not sufficient. For communication to occur, the information must be in a form that is understandable by both parties. The pet must understand what the person means by a specific hand gesture or a specific command. Two people talking must have a common language interpretation. Simply speaking the same language is not enough: the dialects and common usage patterns matter as well.

To illustrate this point, consider this anecdote of a person from Australia visiting some American colleagues. Obviously, they shared English as a common language and communication was seemingly problem-free. The Americans, as part of their hospitality, took the Australian to a baseball game. As is customary in the United States, the song “Take Me Out to the Ballgame” was sung with great gusto by the fans in the stadium. The Australian was taking this all-in stride until the song got to the part about “Let me root, root, root for the home team…”, at which point in time a shocked look took over his face. The Americans, noticing this, asked him if he was feeling okay. He then explained how the word “root” was used in Australia, which is as an offensive and vulgar reference to sexual intercourse (O'Shea, 2016). So when the Australian heard an entire stadium of people singing happily about rooting for the home team, he was somewhat taken aback.
The simple model of communications is, therefore, this: an originator forms and encapsulates information into a message medium, which is received and interpreted by a recipient. The effectiveness of the communication is dependent upon the shared knowledge of the originator and the recipient. It is also dependent on several elements that the originator and the recipient may have little to no control over: interference in the environment, in the signal formation, in the signal reception, or in the context. The originator might sneeze while talking, a car backfire might drown out a few words, or the context of the conversation may lead the recipient to misinterpret the intended meaning. In order to reduce the probability of misinterpretation or misunderstanding, active strategies can be adopted, including repeating messages through multiple channels or saying the same thing in many different ways. Crucially, these active measures to reduce misunderstandings are generally dependent upon cooperation between the originator and the recipient.

Effective Listening

There is an entire philosophy about how to reduce misunderstandings in human communication that illustrates this process. The philosophy is called Active Listening (Rogers & Farson, 1957) and it’s actually interesting to consider through the lens of “what can go wrong” in communications. Since the entire point of disinformation and misinformation is to cause problems in communication, it’s worth taking a moment to reflect on how life coaches teach active listening as a way to make things go right.

To practice active listening, six skills are emphasized. These skills are used to enable a “listener to thoroughly absorb, understand, respond, and retain what is being said.” (Center for Creative Leadership, 2019) Each of the skills identifies some element of communication that can improve the effectiveness of
communication but also identify targets for a disinformation campaign. These six skills are:

- **Paying attention**
- **Withholding judgment**
- **Reflecting**
- **Clarifying**
- **Summarizing**
- **Sharing** (Center for Creative Leadership, 2019)

Paying attention is exactly what it sounds like: actually listening to what a speaker is saying. But it is also paying attention to what the speaker is conveying through other aspects: tone of voice, volume, pauses, emphasis, word choices, body language, and other elements of the conversation.

Withholding judgment is meant to imply keeping an open mind but a more sophisticated interpretation of this skill is developing an understanding of what the person speaking is actually trying to communicate, taking into account that person’s culture, language skill, opinions, and purpose. By integrating the spoken message into an appreciation of where the person is coming from, a listener develops a better platform for productive conversation.

Reflecting is the process of repeating what you think you have heard in other words, with the purpose being to confirm that you have received the correct message. If your paraphrase of what you think you have heard is rejected, then you know that there has been some breakdown in the communication effort.

Clarifying the message is done through asking questions, either to ensure you have interpreted the context of the conversation correctly or to request amplifying information. By asking questions, you give the speaker a chance to expand a topic to contextualize it better or to explain something that may be slightly ambiguous. Using reflection and clarification iteratively can be a powerful method for getting the speaker to be more descriptive and precise.

Similarly, summarizing the message briefly back to the speaker
can test your comprehension of the conversation, particularly the sensitive elements. Once you have established that your understanding is correct, then you have the ability to share some of your own thoughts and insights.

The purpose of describing the processes associated with active listening is to underscore how very complex the act of communication is. Communication consists not just of the information contained in the transmitted message; it also includes all the noise and extraneous information in the communication channel, including the brains of the communicators.

**Deception As A Strategy**

When one has perfect knowledge, one can choose the timing of actions and go fast or slow as appropriate to the situation and to the goals of action. Perfect knowledge of any situation is the product of communication: collecting, analyzing, and interpreting messages that are both deliberately and inadvertently sent by an adversary. In the real world, achieving perfect knowledge is both desired and impossible: there is too much information, variation and change, and deception.

Deception is used to deny perfect knowledge, to seed confusion into intelligence, and to mislead adversaries, which ultimately slows them down, from an effectiveness perspective. Effective deception can result from hiding information, changing information, and seeding information. Some examples of the use of deception include the following:

- In the early 1960s, the Walt Disney Productions company used a series of companies to buy the land around Orlando that became the site for Disney World. These companies were created specifically for the purpose of shielding the true identity of the purchaser in order to keep land prices from rising, which surely would have happened if people had known the truth about who was buying the land and for what purpose. In fact, when the news broke, “land prices skyrocketed in Orlando, where in some cases the land went up to $80,000 an
In 1944, as the planning for the Allied invasion of Normandy was increasing in intensity, an actor playing the part of Field Marshall Montgomery was taken to alternative locations in order to deceive the Germans as to where the invasion would take place. This was only one of the many deceptions associated with Operation Overlord, but an effective one as it distracted the Axis powers with information that “Montgomery” had been observed in Gibraltar and North Africa, leading them to speculate that the invasion would be in the Mediterranean region. (Breuer, 2001, pp. 198–202) (Whaley, 2007, p. 376) (Howard, 1995, p. 125)

During the Cold War, agents of the Soviet Union used the tactic of injecting false news reports into media. One example of this type of activity was included in a 1981 US Department of State advisory:

“In 1980, Pierre-Charles Pathe, a French Journalist, was convicted for acting as a Soviet agent of influence since 1959. His articles – all subtly pushing the Soviet line on a wide range of international issues – were published in a number of important newspapers and journals, sometimes under the pseudonym of Charles Morand. The journalist also published a private newsletter which was regularly sent to many newspapers, members of parliament, and a number of foreign embassies. The Soviets used Pathe over a number of years to try to influence the attitudes of the prominent subscribers to his newsletter and to exploit his broad personal contacts.” (U.S. Department of State, 1981)

Deception is a technique that can be reasonably low cost as well as effective. Deception includes many ruses, such as camouflage, diversions, and disinformation (Whaley, 2007, p. 7). Barton Whaley, a scholar of deception and military successes over the century, noted in his seminal book *Stratagem: Deception and Surprise in War* (2007):
The most important single broad category of ruses includes all false information fed into another's information system in order to deceive him. The standard technical term is “disinformation”. It is conventionally meant to cover only the verbal or written forms of information, leaving “camouflage” and “diversion” to cover the nonverbal or visual forms. (pp. 8-9)

He made this assessment of the importance of disinformation from his painstaking analysis of the effects of surprise in warfare over history. A key analytical finding from his scholarship:

Of the 61 cases of strategic military surprise that occurred between 1914 and 1968, no more than 4 can be exclusively or even mainly attributed to the initiator’s passive security. More or less specific warning signals almost inevitably filter through the security screen and reach the intended victim. Moreover, these warning signals usually increase in frequency and specificity as the attacker’s preparations unfold, drawing more and more indiscreet persons into the planning and making ever more visible the necessary adjustments in mobilizations, deployment, logistics, and perhaps diplomacy. ... There is only one type of activity still available that will multiply [the commander’s] chances of gaining surprise. That is stratagem. (Whaley, 2007, pp. 1-2)

In this quotation, the word stratagem in its classic meaning, which is as a reference to strategic deception.

The world that he studied is not the world of today. The growth and integration of information technologies is a dramatic change that has affected all aspects of life. Further, the types and representations of information has increased exponentially, to the point where it makes less sense to separate non-verbal and visual information from written or spoken information. The growth of augmented and virtual reality (AR and VR) applications, the widespread adoption of artificial intelligence implementations, and the integration of video, photography, data, and sound has changed the environment of deception activities. As such, the discussion in this chapter includes manipulation of non-verbal and visual information in the definition of deception.
Implications for Unmanned Systems

Unmanned systems rely on information technology. As noted in Chapter 1 of this book:

The separation of human labor, cognition, and equipment into disparate pieces means that a concomitant need for collaborative technologies becomes important. The most obvious collaborative technologies are communications – exchanging data, commands, and responses. Other types of collaborative technologies that need to be considered are those that prevent adverse interactions between system components, environmental sensing and reaction technologies, and control guidance technologies. All of these enable the remote operation of an unmanned system.

In other words, communication between the various components are a critical part of unmanned system operations. It is therefore necessary for operators to plan for identifying and mitigating deception. A solid information security regime provides a platform to build upon. Having the people, processes, and technologies in place that protect the integrity of data in storage as well as in transactions is a critical first step.

That first step is, obviously, only a first step. It provides a way of adjudicating information already in the system and that being shared with trusted edge systems. The next steps need to address the deception challenges that come from external data of all types: sensor collected data, aggregated data from a data market, and deliberately introduced deceptive data. Problems to consider include the following:

- Sensors that correctly work as engineered but which are triggered to misread a sensed situation because the target environment has been manipulated. For example, an unmanned car could be tricked into “reading” a road marking because the marking had been augmented with material designed to trick the car’s sensor.
- Aggregated data from a data market that is used to create highly detailed virtual reality depictions of a target.
environment, in which the data has been seeded with deliberately misleading information, such as multiple altitude power lines in a place where none exist. UAS operations would use that deceptive information to avoid flying in the vicinity of the powerlines, which could reduce the effectiveness of their mission operations.

- Deliberately introduced deceptive data could come from an insider or from a modified infrastructure component. For example, an AI application that quickly processes data inputs to a system could follow a set of rules that leads it to an incorrect decision. That incorrect decision then becomes deceptive data: relevant but misleading or untruthful.

Any approach to addressing the problem of deceptive data will be unique to the operations and mission of the unmanned systems, so a one-size-fits-all solution is not possible. As with every engineering problem, the solution lies in understanding what the threats are, what the potential impacts might be, and what countermeasures can effectively be used.

**Sensing and Interpreting Challenges**

Because there is no one-size-fits-all solution to the challenge of deceptive data, it is helpful to review some examples of historical events.

**“Hidden” Information Embeds**

In 2018, researchers experimented with overlaying what they called “adversarial examples” on actual stop signs to see if autonomous vehicle detection systems could be fooled. The overlays used did not change a human’s ability to identify the sign as a stop sign: the overlays were smaller than many of the graffiti stickers commonly seen on stop signs in cities. The researchers were able to make the
sensors miss the stop sign. Further, they were able to make the sensor detect things that were not present:

... we create perturbed physical objects that are either ignored or mislabeled by object detection models. We implement a Disappearance Attack, in which we cause a Stop sign to “disappear” according to the detector—either by covering the sign with an adversarial Stop sign poster, or by adding adversarial stickers onto the sign. In a video recorded in a controlled lab environment, the state-of-the-art YOLO v2 detector failed to recognize these adversarial Stop signs in over 85% of the video frames. In an outdoor experiment, YOLO was fooled by the poster and sticker attacks in 72.5% and 63.5% of the video frames respectively. We also use Faster R-CNN, a different object detection model, to demonstrate the transferability of our adversarial perturbations. The created poster perturbation is able to fool Faster R-CNN in 85.9% of the video frames in a controlled lab environment, and 40.2% of the video frames in an outdoor environment. Finally, we present preliminary results with a new Creation Attack, wherein innocuous physical stickers fool a model into detecting nonexistent objects. (Eykholt, et al., 2018)

One can easily understand the potential impact of an unmanned system missing or inventing information: the problems could cascade to the entire system as well as cause harm to external elements, such as people or property.

In another set of experiments, researchers developed a set of eyeglass frames that fooled a facial recognition system. The choice of glasses frames was to minimize the perturbation components while using something that was easy to modify and widely available:

One advantage of facial accessories is that they can be easily implemented. In particular, we use a commodity inkjet printer (Epson XP-830) to print the front plane of the eyeglass frames on glossy paper, which we then affix to actual eyeglass frames when physically realizing attacks. Moreover, facial accessories, such as eyeglasses, help make attacks plausibly deniable, as it is natural for people to wear them. (Sharif, Bhagavatula, Bauer, & Reiter, 2016)
The results were impressive. In all but one experiment, the device worked perfectly. In the one in which it didn't, the device worked 91% of the time. They were able to successfully show that their “eyeglass frames enabled subjects to both dodge recognition and to impersonate others.” (Sharif, Bhagavatula, Bauer, & Reiter, 2016)

These two examples represent a rich and growing field of research. As the rush towards full automation for unmanned systems continues, this type of work is both useful for improving the sensing systems and for identifying the types of threats that need to be considered during operations.

Distinguishing Signals in Noisy Environments

In 2013, a group of students conducted an experiment on a 213-foot ship to see if they could successfully change the course of the yacht without the crew noticing. From the top deck of the yacht, they:

broadcasted a faint ensemble of civil GPS signals from their spoofing device a blue box about the size of a briefcase toward the ship's two GPS antennas. The team's counterfeit signals slowly overpowered the authentic GPS signals until they ultimately obtained control of the ship's navigation system.

Unlike GPS signal blocking or jamming, spoofing triggers no alarms on the ship's navigation equipment. To the ship's GPS devices, the team's false signals were indistinguishable from authentic signals, allowing the spoofing attack to happen covertly.

Once control of the ship's navigation system was gained, the team's strategy was to coerce the ship onto a new course using subtle maneuvers that positioned the yacht a few degrees off its original course. Once a location discrepancy was reported by the ship's navigation system, the crew initiated a course correction. In reality, each course correction was setting the ship slightly off its course line. Inside the yacht's command room, an electronic chart showed its progress along a fixed line, but in its wake there was a pronounced curve showing that the ship had turned.
“The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line,” Humphreys said. After several such maneuvers, the yacht had been tricked into a parallel track hundreds of meters from its intended one the team had successfully spoofed the ship. (Animation by Erik Zumalt, 2013)

This type of attack is not just in the lab. Around the world, there have been increasing reports of navigation problems of varying sorts, all related to the electronic navigation aids in use to make navigation possible through storms, night, and disputed waters. The misuse of the technology has led to some very interesting situations:

Automatic Identification Systems (AIS) are causing problems for mariners transiting waters where there are high concentrations of fishing vessels, particularly in the East China Sea. ... Local fisherman discovered that by putting AIS transponders on their fishing nets, large ships would change course for the nets, thinking they were vessels. ... If we are to see more unmanned ships in the future, this needs to be rectified. What would an unmanned ship approaching a literal “sea” of AIS targets do without a professional mariner in charge to properly assess the situation? Ships would be changing course to avoid fishing nets, only to be “faced” with a whole new set of AIS targets on the new course. Shipowners may find their unmanned vessels turning circles in order to avoid what the automated equipment deems to be dangerous, but may only be crab pots or fishing buoys. (Kovary, 2018)

Conclusions
These two examples underscore the challenge of sensing and interpreting, particularly in noisy environments where competing interests collide.

References


King, B. J. (2019, September). Deception in the Animal Kingdom: Homo Sapiens is not the only species that lies. Scientific American.


[i] For an excellent overview of how to approach understanding the believability of published information, see The University of Groningen’s “Information literacy – Media Studies: Evaluation criteria: relevance and reliability”, found online at https://libguides.rug.nl/c.php?g=560673&p=3857909