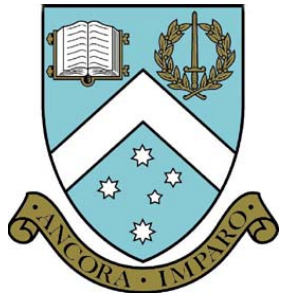


CSE468
Information Conflict

Lecturer: Dr Carlo Kopp, MIEEE, MAIAA, PEng

Lecture 04

The Four Canonical Strategies of Information Conflict

Reference Sources and Bibliography

- There are only two primary sources dealing with the four canonical strategies:

1. Borden, Andrew; What Is Information Warfare? *Air & Space Power Chronicles,* November 1999.
2. Kopp, Carlo; A Fundamental Paradigm of Infowar, *Systems*, February, 2000.

- Supporting definitions can be found in: United States Dept of the Air Force; Cornerstones of Information Warfare; Washington, 1995. 13 p. also at http://www.c4i.org/cornerstones.html

Background to the Four Canonical Strategies

- The four canonical strategies were identified almost concurrently by Col. Andrew Borden, PhD, USAF, and Carlo Kopp, at Monash University CSSE, in 1999.
- Dr Borden published two months before Kopp in *Air Chronicles*, a United States Air Force professional journal. Kopp published in the Australian industry journal *Systems*, formerly *Australian Unix User's Review*.
- Borden's model does not include the 'subversion' strategy as a defined model, and follows the US DoD convention of transparently including it in the 'denial' strategy.
- The subversion strategy was first published by Kopp, and credit for its identification must go to the late Prof C.S. Wallace, foundation Chair of Computer Science at Monash University.

Why a Fundamental Theory/Paradigm?

- Prior to the definition of the Borden-Kopp model for Information Warfare, there was no established mathematical basis to underpin the theory.
- As a result considerable disagreement emerged in the literature and professional debate as to even the basic validity of the idea of information use in survival conflicts.
- With the definition of a mathematically supportable and robust theoretical basis, this area of study can now be explored scientifically and in a systematic fashion.
- Subsequent research has described the relationship between games and information, and the properties of compound strategies.
- Later research by Kopp and Mills also established the role of information conflicts in biological evolution.

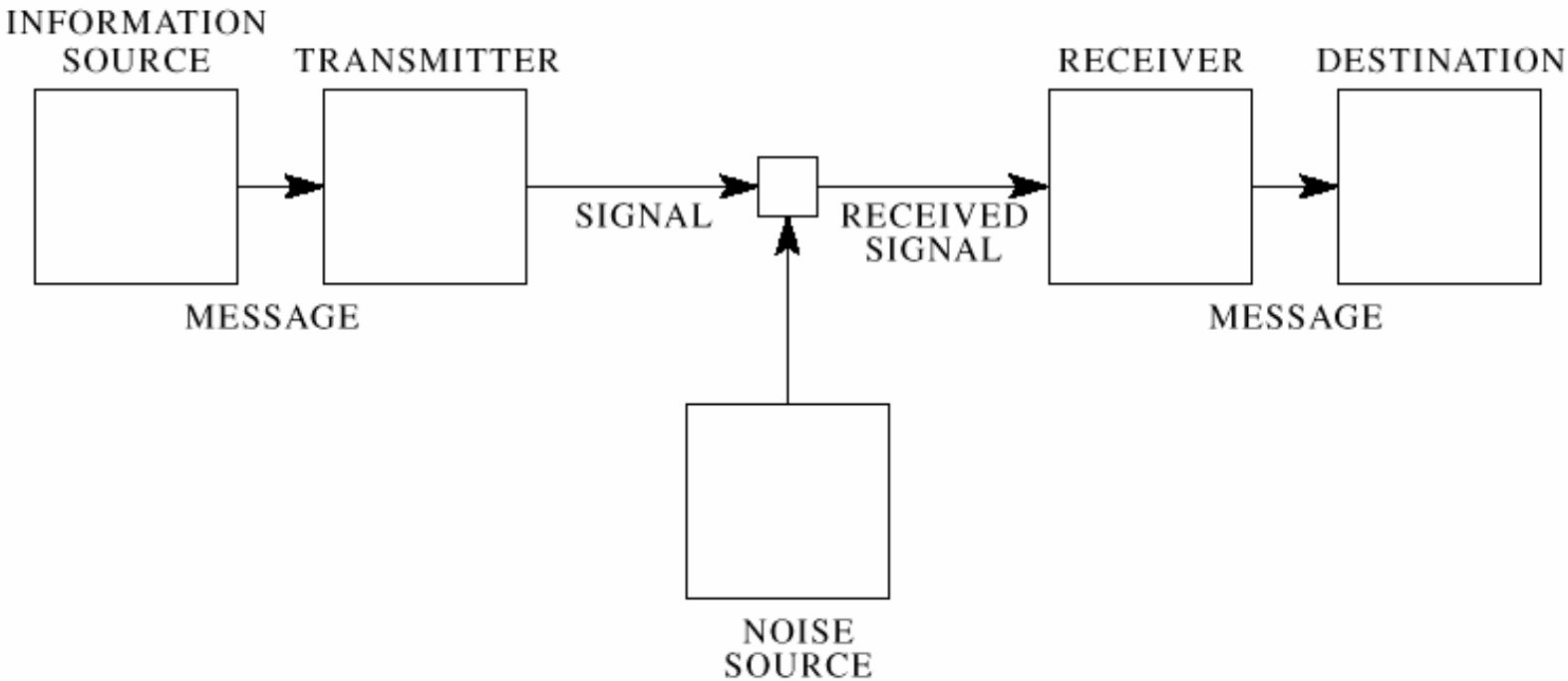
The Starting Point - Shannon's Capacity Model

- To establish a fundamental theoretical model the starting point must be fundamental information theory, which is centred in Shannon's channel capacity theorem:

$$C = W \log_2 (1 + \frac{P}{N}) \quad \text{Theorem 17}$$

- If an attacker intends to manipulate the flow of information to an advantage, the game will revolve around controlling the capacity of the channel, *C*.
- To achieve this, the attacker must manipulate the remaining variables in the equation, bandwidth, *W,* and signal power vs noise power, *P/N.*
- *Three of the four canonical strategies involve direct manipulation of bandwidth, signal power and noise.*

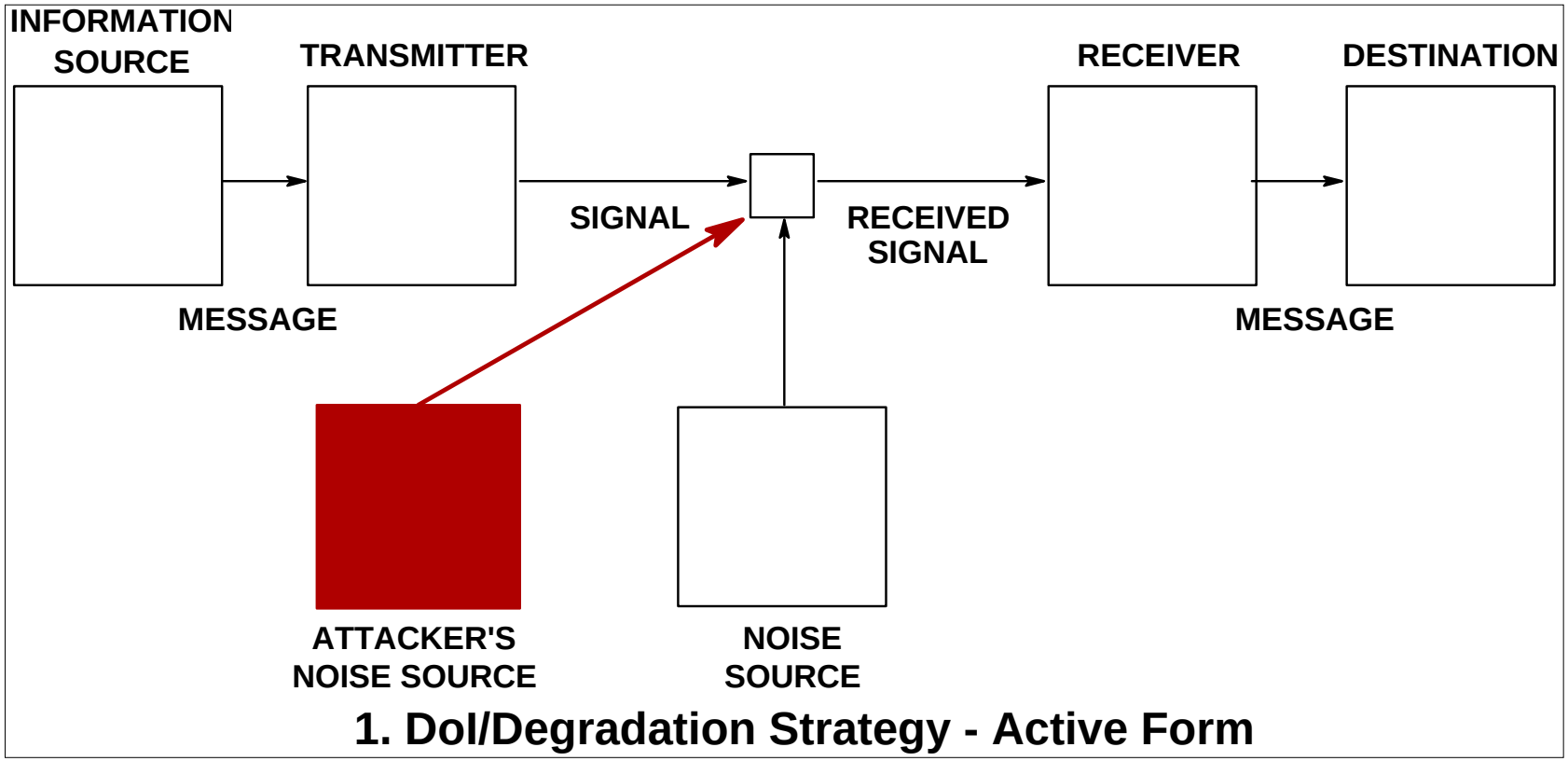
Shannon's Model



The Degradation Strategy [Denial]

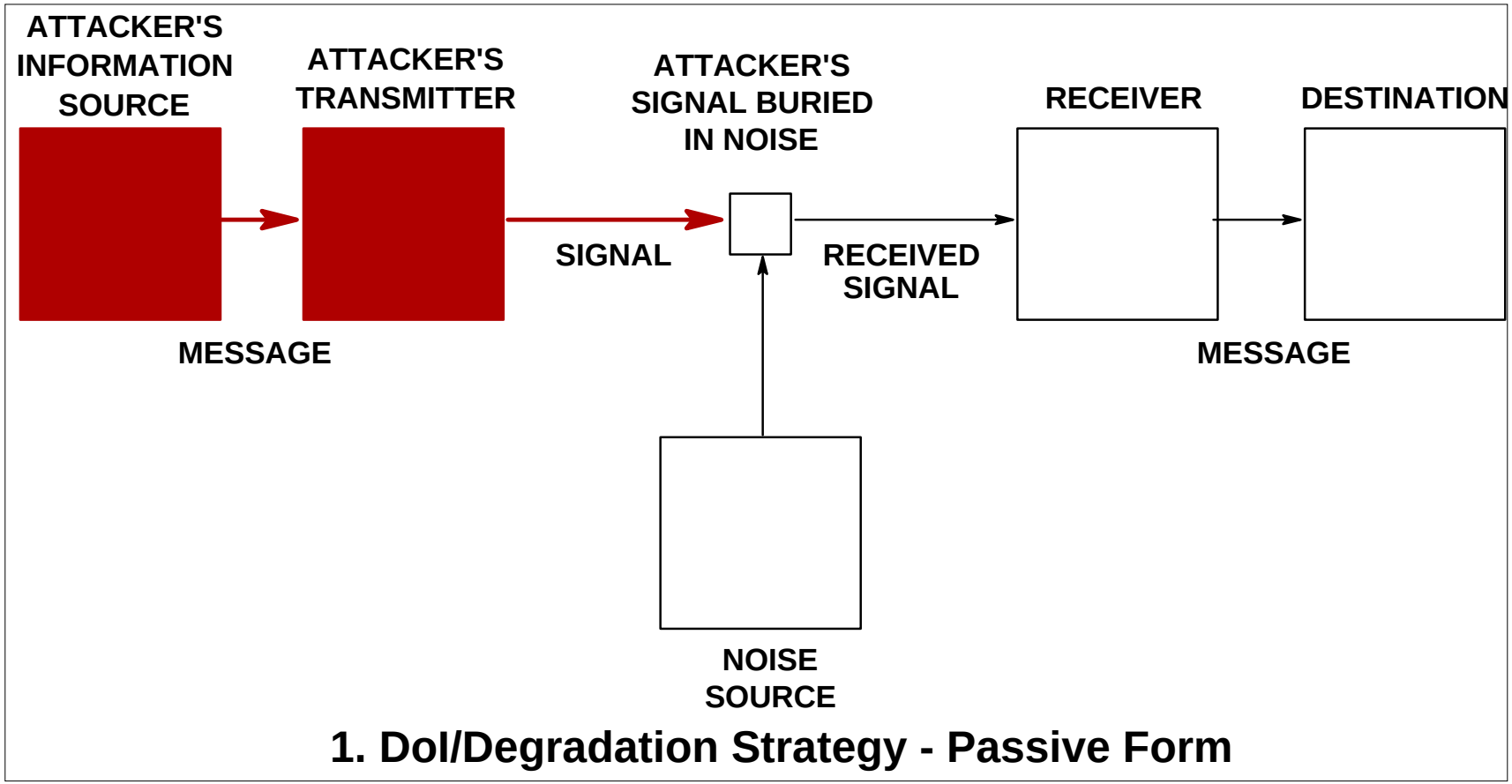
- The degradation strategy involves manipulation of the P/N term in Shannon's equation.
- The flow of information between the source and destination is impaired or even stopped by burying the signal in noise and driving $C \rightarrow 0$.
- There are two forms of this strategy, the first being the 'camouflage/stealth' or 'passive' form, the second being the 'jamming' or 'active' form.
- The first form involves forcing $P \rightarrow 0$ to force $C \rightarrow 0$. In effect the signal is made so faint it cannot be distinguished from the noise floor of the receiver.
- The second form involves the injection of an interfering signal into the channel, to make N>>P and thus force $C \rightarrow 0$. In effect the interfering signal drowns out the real signal flowing across the channel.

Degradation Strategy – Active Form



1. DoI/Degradation Strategy - Active Form

Degradation Strategy –Passive Form

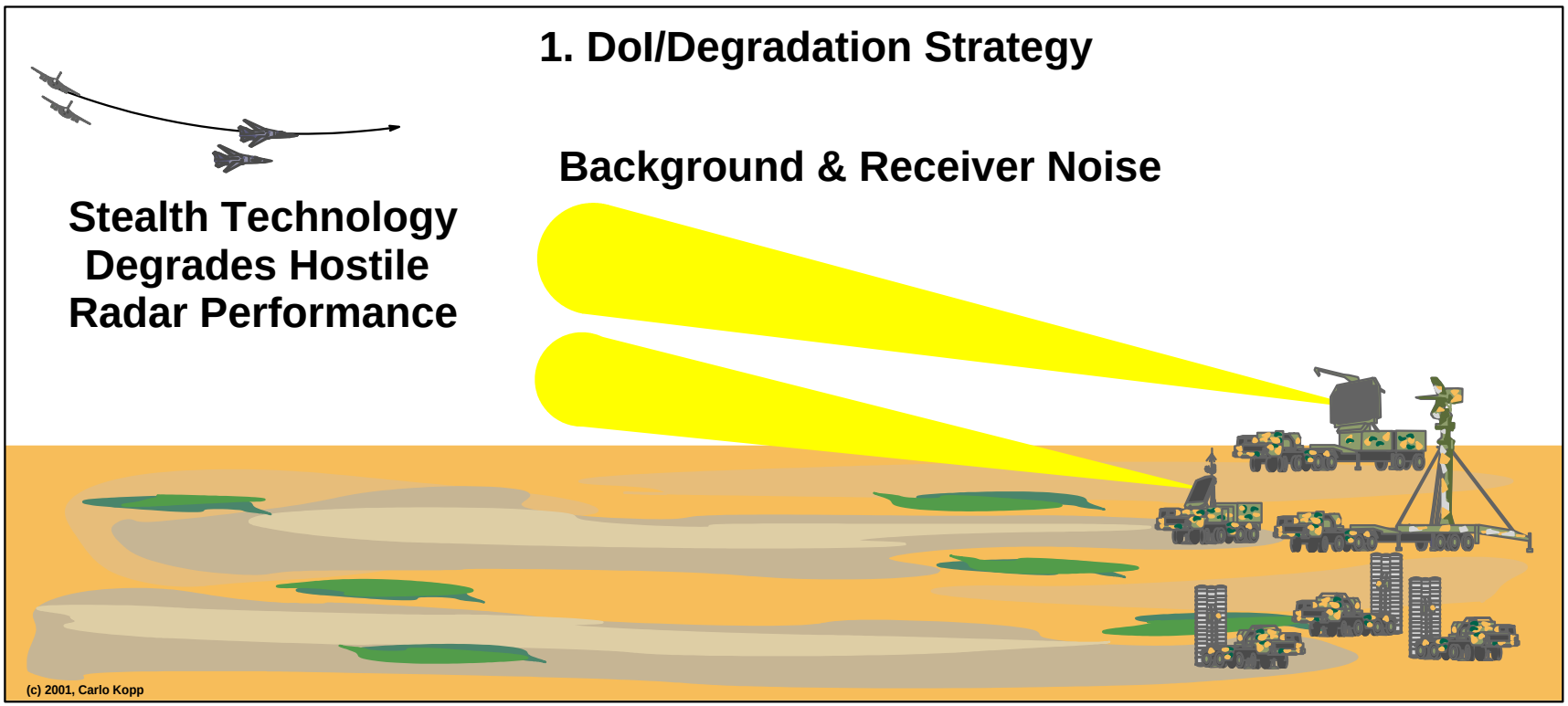


1. DoI/Degradation Strategy - Passive Form

Passive vs Active Forms of Degradation

- There is an important distinction between the active and passive forms of the degradation strategy.
- In the *passive form* of this attack, the victim will most likely be unaware of the attack, since the signal is submerged in noise and cannot be detected. This form is therefore ‘covert’ in the sense that no information is conveyed to the victim.
- In the *active form* of this attack, the signal which jams or interferes with the messages carried by the channel will be detected by the victim. Therefore this form is ‘overt’ in the sense that information is conveyed to the victim, telling the victim that an attack on the channel is taking place.
- Both forms are widely used in biological survival contests and in social conflicts.

Example - Degradation



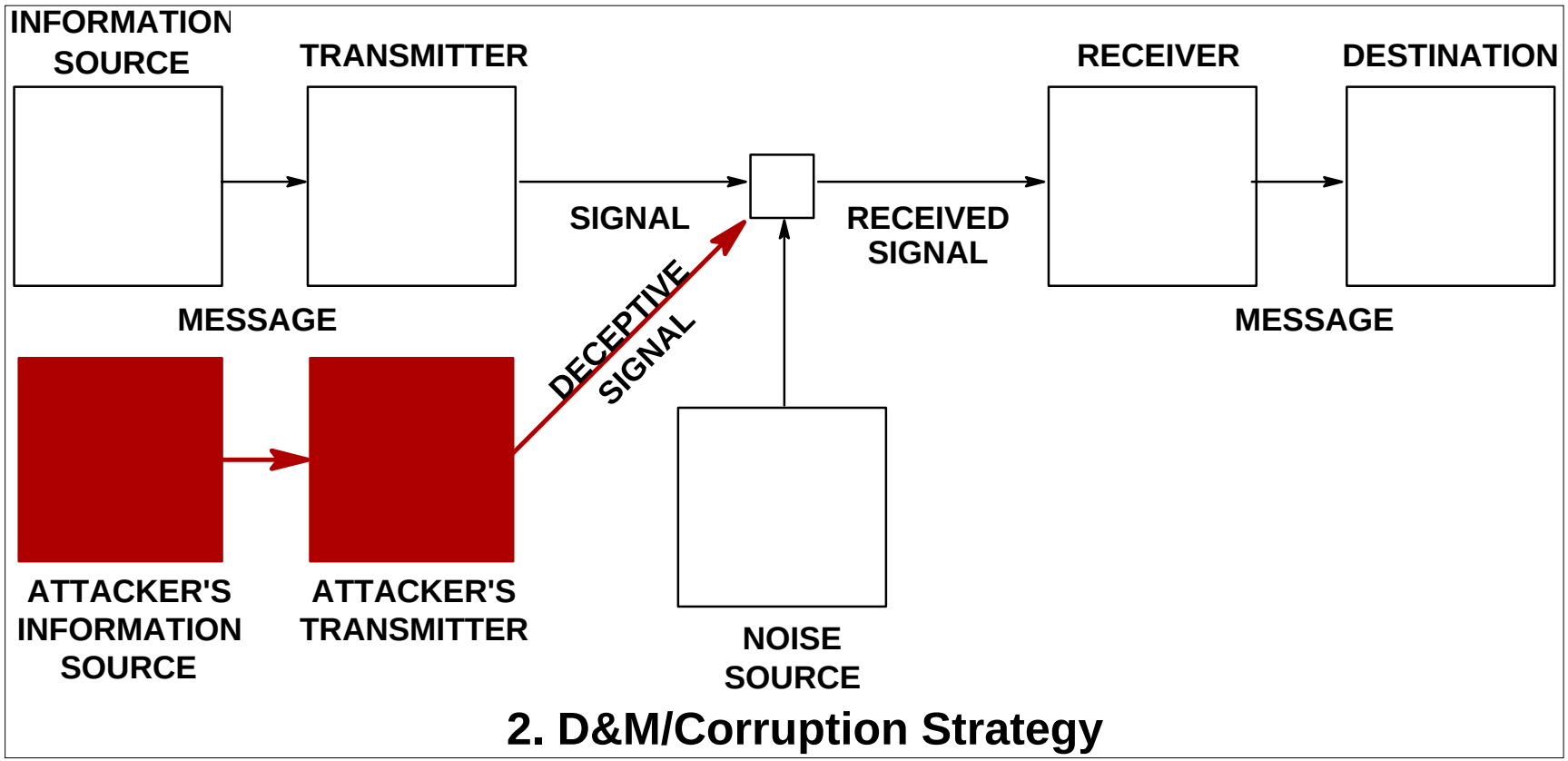
Examples - Degradation

- Passive form – biological or military camouflage patterns.
- Passive form – military stealth to hide from radar.
- Passive form - encryption and concealment to prevent unwanted parties from reading or finding what they ought not to.
- Active form – barrage jamming of wireless radio broadcasts or communications links.
- Active form – the use of smoke screens to hide troops from enemy gunfire.
- Active form – biological examples such as squid squirting ink at predators to hide themselves.

The Corruption Strategy [Mimicry]

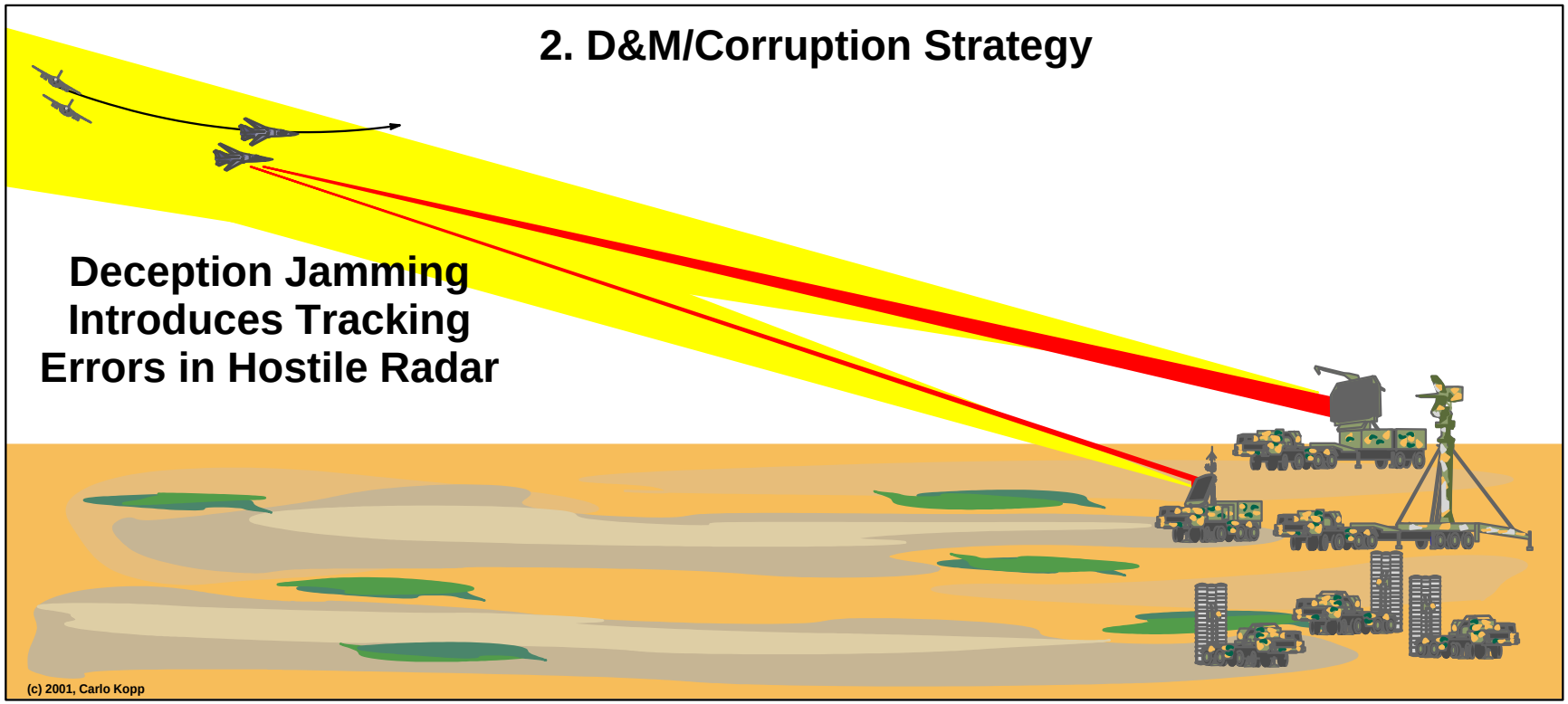
- The corruption strategy involves the substitution of a valid message in the channel with a deceptive message, created to mimic the appearance of a real message.
- In terms of the Shannon equation, P_{actual} is replaced with P_{mimic}, while the *W* and *N* terms remain unimpaired.
- The victim receiver cannot then distinguish the deception from a real message, and accepts corrupted information as the intended information.
- Success requires that the deceptive message emulates the real message well enough to deceive the victim.
- Corruption is inherently ‘covert’ since it fails in the event of detection by the victim receiver.
- Corruption is used almost as frequently as degradation in both biological and social conflicts.

Corruption Strategy



2. D&M/Corruption Strategy

Example - Corruption



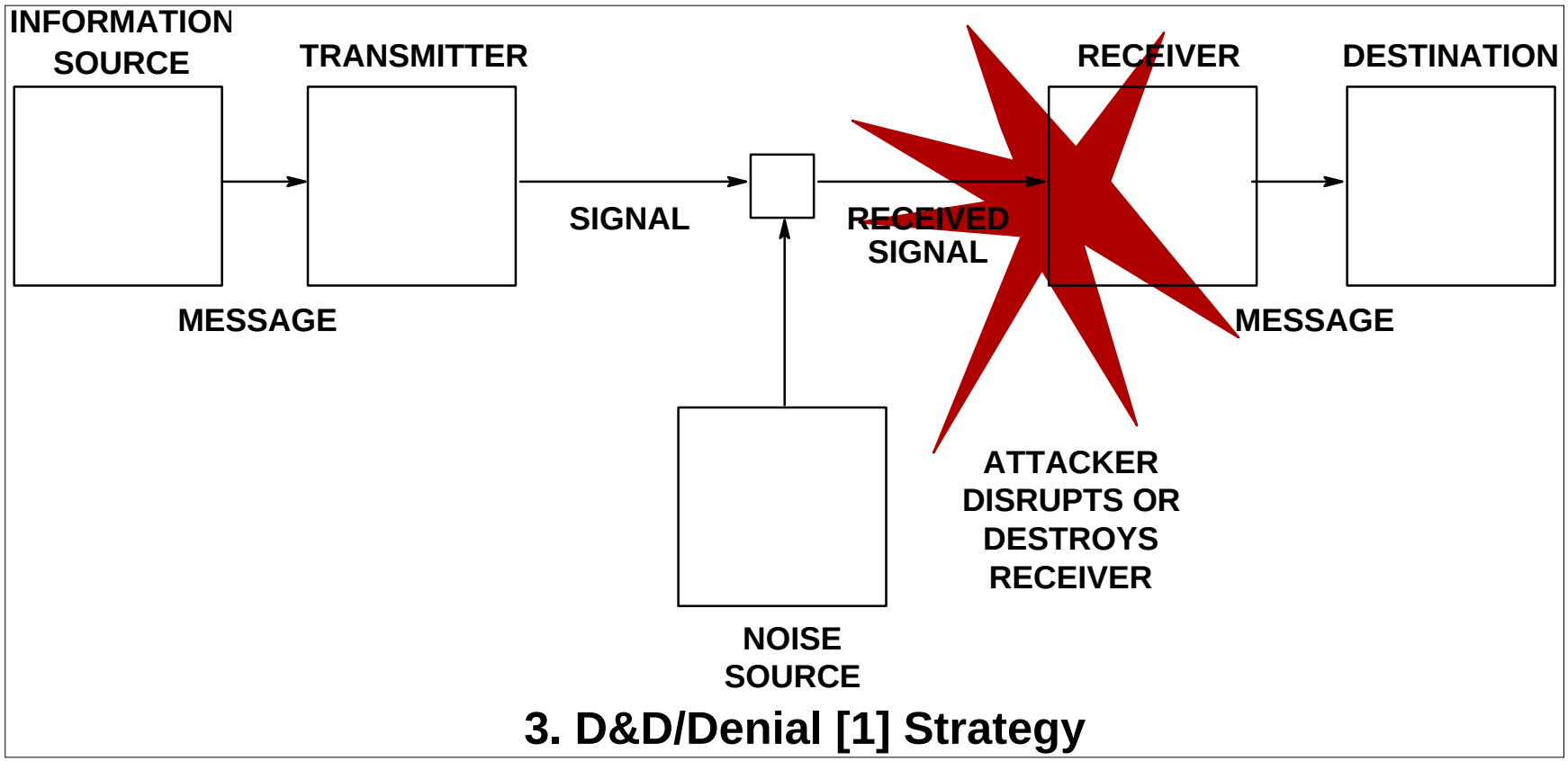
Examples - Corruption

- Biological examples of organisms which mimic the appearance of harmful, predatory or toxic species to deceive predators.
- Biological predators which mimic the appearance of prey organisms to attract lesser predators and eat them.
- Deception jamming techniques used against radars, producing errors in angle/range measurements, or producing false (non-existent) targets.
- The use of deceptive propaganda radio broadcasts, or deceptive radio transmissions emulating real messages.
- Deceptive advertising in the commercial and political domains.
- Identity theft, phishing, phracking, hacker use of stolen usercodes, spammer email address substitution.

Denial Strategy [via Destruction]

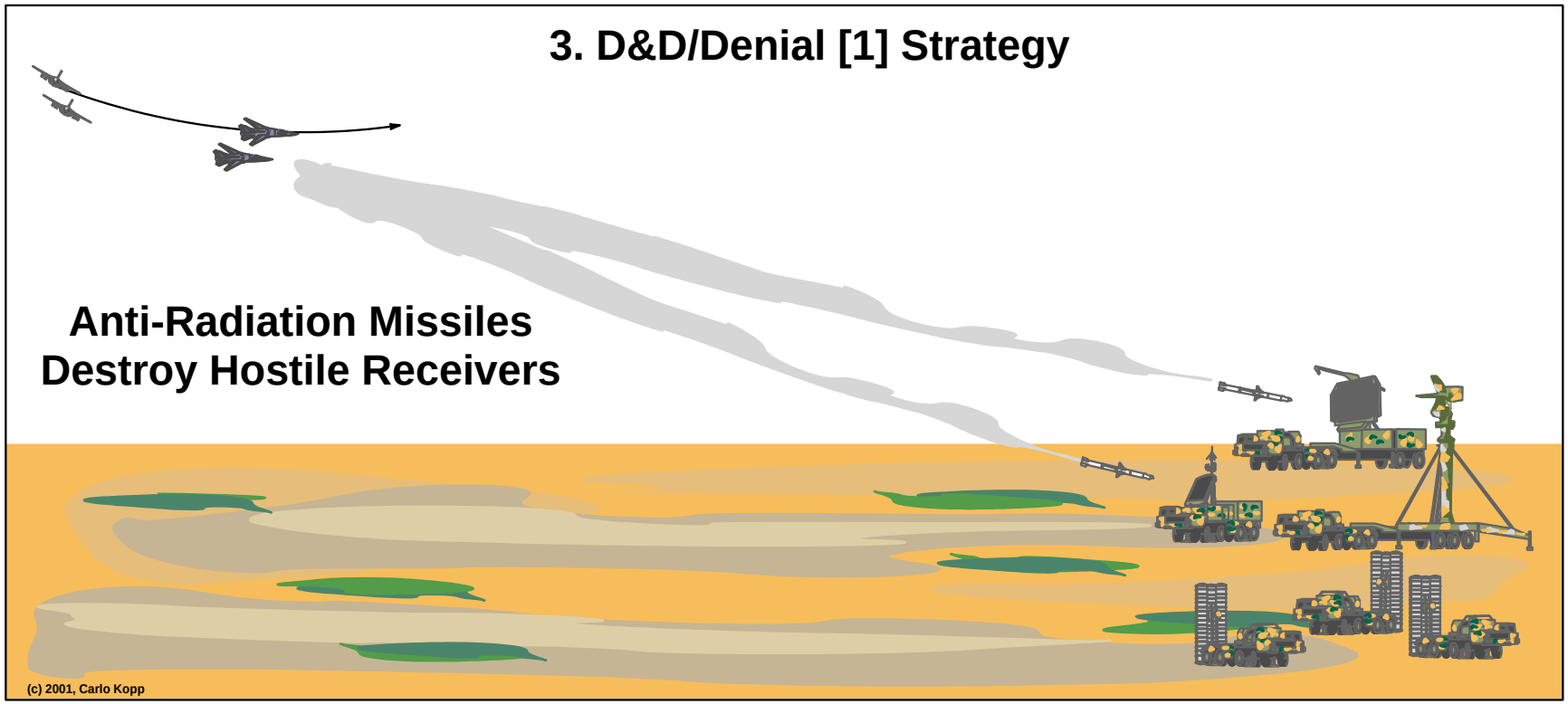
- The degradation and corruption strategies both focus on the *P* and *N* terms in the Shannon equation.
- The denial strategy manipulates the *W* term, by effecting an attack on the transmission link or receiver to *deny* the reception of any messages, by removing the means of providing bandwidth *W*.
- This means that $W \rightarrow 0$ or $W = 0$ if the attack is effective.
- The denial strategy is inherently 'overt' in that the victim will know of the attack very quickly, as the channel or receiver is being attacked.
- A denial attack may be temporary or persistent in effect, depending on how the channel or receiver is attacked.
- Numerous biological and social examples exist.

Denial Strategy [via Destruction]



3. D&D/Denial [1] Strategy

Example – Denial [via Destruction]



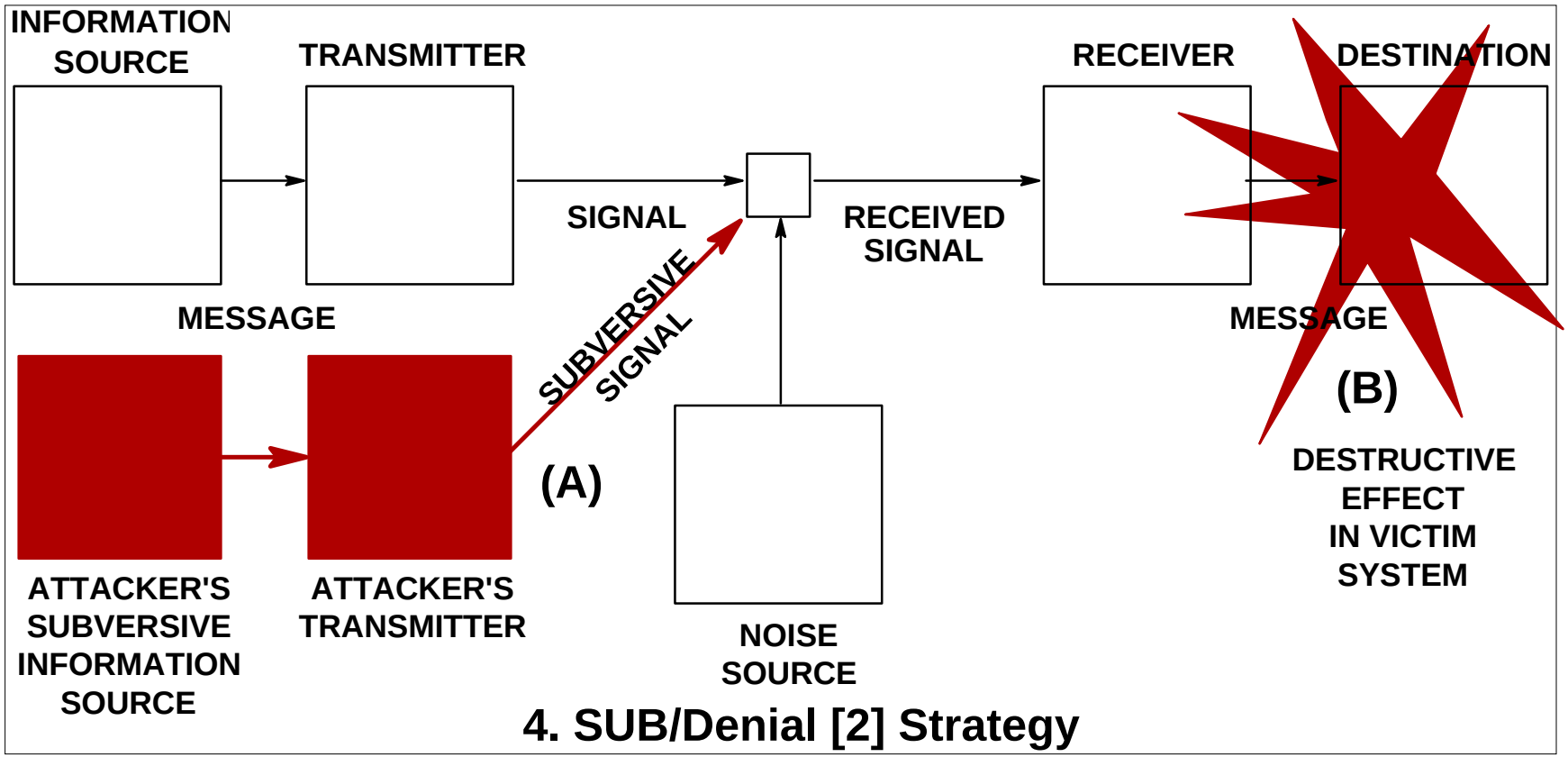
Examples – Denial [via Destruction]

- Organisms which spray noxious fluids on predators, thereby blinding and numbing the predator's visual and olfactory senses, temporarily or permanently.
- Very high power radio frequency weapons which can permanently or temporarily impair the function of victim receivers by overloading input circuits.
- Destroying the receiver system by direct attack, for instance by fire, bombing or other such means.
- In the IT domain, any temporary or permanent ‘denial of service’ attack, such as ‘ping of death’, induced packet storms, cutting data or power cables, or using electromagnetic weapons.

Denial Strategy [via Subversion]

- Denial via subversion differs from the first three strategies in that it does not involve an attack on the message, its contents or the channel/receiver.
- Subversive attacks involve the insertion of information which triggers a self destructive process in the victim system or organism.
- At the most basic level this is the diversion of the thread of execution within a Turing machine, which maps on to the functional behaviour of the victim system. It amounts to surreptitiously flipping one or more specific bits on the tape, to alter the behaviour of the machine.
- The attack may impair or destroy the victim system.
- Numerous biological, social and technological examples exist.

Denial Strategy [via Subversion]



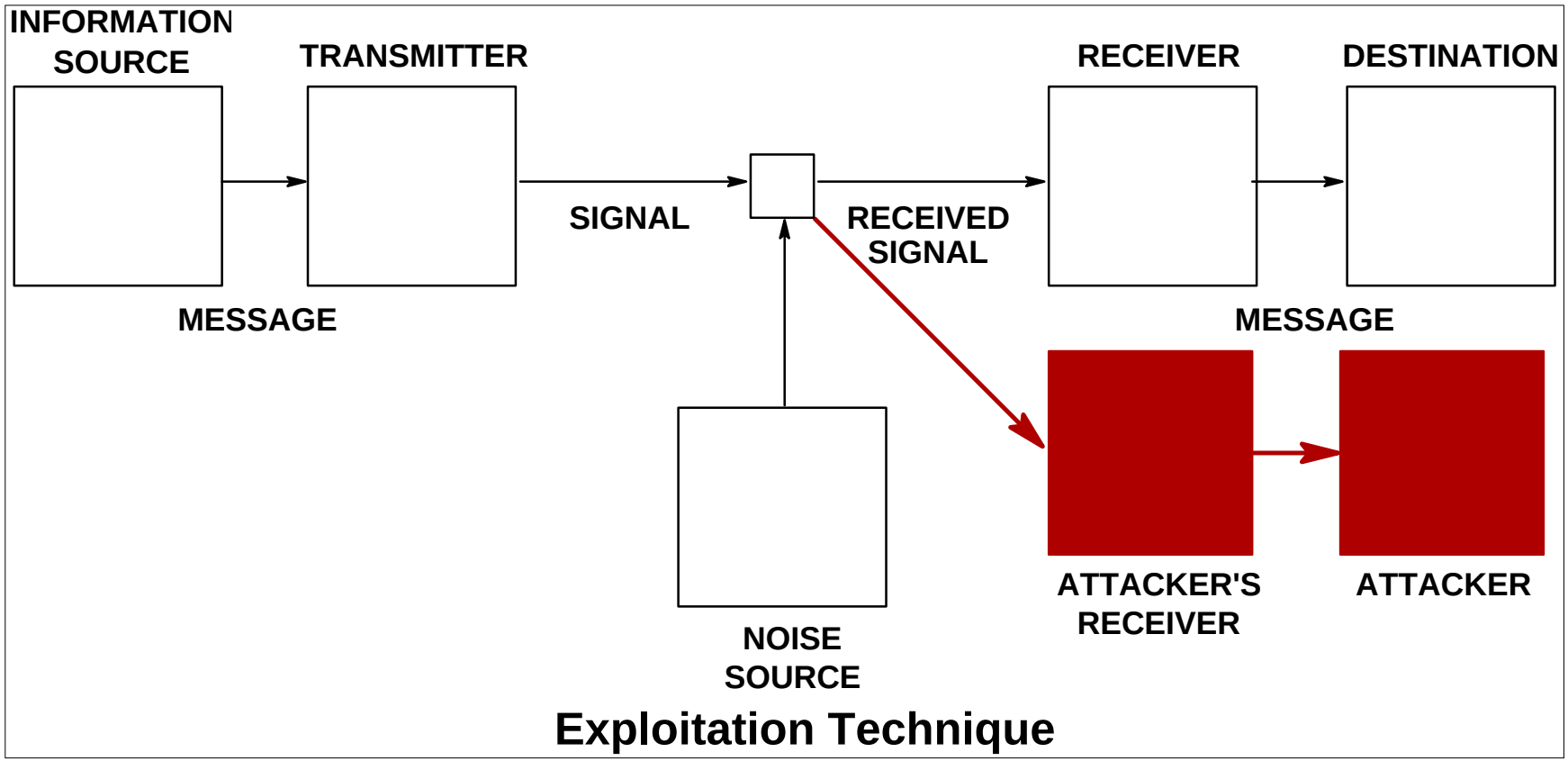
Examples - Denial Strategy [via Subversion]

- Parasites which emit chemicals which alter the internal functions of the victim organism to favour the parasite, such as the production of favourable nutrients or weakening of immune defences.
- The use of deceptive radio or optical signals which trigger the premature initiation of weapon fuses, such as proximity fuses on guided missiles or artillery shells.
- Logic bombs, viruses, worms and other destructive programs which use system resources to damage the system itself.
- Most examples of subversion rely on the attacker's use of corruption to penetrate the victim's defences and create conditions to effect the subversive attack.

Why Exploitation is Not a Canonical Strategy

- The US DoD definitions of the four strategies of information attack include ‘exploitation’, which is effectively the eavesdropping of victim messages.
- As eavesdropping is a wholly passive activity which does not involve a direct attack on the victim channel, receiver or system, thus impairing or altering the function of the victim, it cannot be a canonical strategy defining a mode or type of attack on a system.
- For completeness, exploitation is defined and illustrated.

Exploitation



Proving the Four Canonical Strategies

- Early critics argued that IW did not exist and had no scientifically provable basis (none of them were scientists).
- ***Proof****: If IW does not exist as an artifact of evolution in nature, then no examples of its use should exist. As examples exist in abundance, then this hypothesis is clearly false.*
- Do other possible canonical strategies exist?
- There are only three variables in the Shannon equation, each accounting for one of the first three strategies. In a Turing machine, information can be used to alter the program but not the nature of the machine.
- *Hence, there are no obvious candidates for further canonical strategies*.

Properties of the Four Canonical Strategies

- **Orthogonality**: A canonical strategy cannot be formed by combining any number of the remaining canonical strategies. **Proof**: each strategy attacks the victim system in different ways.
- **Indivisibility:** Canonical strategies cannot be further divided or decomposed. **Proof**: Each of the canonical strategies represents the simplest way to effect their respective modes of attack.
- **Concurrency:** A victim system can be subjected to any number of concurrent attacks. **Proof**: For *like* attacks, the effects on the victim system are additive; for dissimilar attacks, the effects on the victim system are *orthogonal*.

Nomenclature

US Department of Defense Nomenclature (1995)	Monash University Nomenclature (1999)
Degradation	Denial of Information (DoI)
Corruption	Deception and Mimicry (D&M)
Denial	Disruption & Destruction (D&D)
Denial	Subversion (SUB)
Exploitation	N/A

Key Points

- The four canonical strategies define all modes of attack involving information in terms of basic manipulation of fundamental models – the Shannon channel model and the Turing machine.
- All attacks on information processing or transmission systems comprise either a canonical strategy or some combination of canonical strategies.
- The canonical strategies are ubiquitous in the biological and social domains.
- The four canonical strategies provide a mathematically robust and provable model for conflicts involving the use of information.

Tutorial

- Q&A
- Discussion of examples
- Mills' Paradox - discussion

Mills' Paradox

- First identified in 2002 by Mills.
- How do we distinguish a Denial via subversion attack from a Corruption attack?
- How do we distinguish a destructive Denial via subversion attack from a Denial via destruction attack?
- How do be distinguish a Degradation attack from a mimicking Corruption attack?
- How do we distinguish an intensive active Degradation attack from a soft kill Denial via destruction attack?
- *Note that Degradation attacks can always be easily distinguished from Denial via subversion attacks, and Corruption attacks can easily be distinguished from Denial via destruction attacks.*

Mills' Paradox