Surviving The Cyber Age

Chapter 6 – Capabilities and Limitations of Cybernetic Systems

Table of Contents

Capabilities and Limitations

In the first few chapters, the discussion has surrounded how cybernetic systems work and where they break down at fundamental levels. That was intentional. Every mechanism has capabilities and limitations, and that seems inherent in the nature of things:

- **Capabilities** allow for an incredible range of possibilities of what can be constructed or evolve and composites of the evolved and constructed components.
- **Limitations** allow for an astonishing assortment of ways these systems can fail by accident or intention.

This chapter is about what we can do today at this level of mechanisms in terms of construction and destruction of control systems. As an engineer, I build systems to work and last, but as a security guru, I try to understand how they fail and mitigate against the failures.

Assumptions and defeating them

As a fundamental, any assumptions in the construction of a system, whether implicit or explicit, can be violated to cause the system to fail.[1] To quote the late great Benny Hill:

"When you ASSUME, you make an ASS of U and ME"

In the various components of cybernetic systems, sensors, actuators, communications, and controls, all have limitations, and to the extent they are implemented with intent, there are assumptions in their architecture, design, construction, deployment, and operation. By collecting the limitations discussed earlier, you can make a pretty good set of assumptions likely associated with different classes of systems, and start figuring out how to violate those assumptions. To break a system, you don't need to know all of the assumptions, usually, it only takes one you can violate well to cause a system to fail.

A pretty good way to start finding assumptions these days is to go to AI. For example, I asked

> *"What are the fundamental assumptions in the design of a standard toilet flushing system used in homes on Earth?"*

It identified:

- Assumes a pressurized and continuous fresh water supply.
- Assumes water pressure is within a normal municipal range (usually 20–80 psi).
- Assumes cold water temperature in a typical indoor plumbing environment.
- Assumes the toilet is located on a planet with Earth-like gravity (~9.8 m/s^2).
- The flush relies on the potential energy of water stored in the tank, released rapidly to create siphoning and bowl evacuation.
- Assumes the plumbing system includes a trapway siphon.
- Assumes the water column can form a siphon reliably with no air leaks.
- Assumes atmospheric pressure is constant enough to sustain siphon action.

1 https://all.net/Analyst/2021-03C.pdf

- Assumes a typical flush volume (varies by region and regulation), e.g.:
  - ~6 L (1.6 gal) for modern low-flow toilets
  - ~4.5 L or less for high-efficiency models
- Assumes this volume is sufficient for:
  - removing waste
  - clearing the bowl
  - refilling the trap to form a water seal
- Assumes the toilet connects to:
  - A vented waste pipe system (for pressure equalization)
  - A sewer or septic system that can carry waste away without backflow
- Assumes pipes are installed with proper slope for gravity drainage.
- Assumes the user will only flush:
  - human biological waste
  - toilet paper (designed to disintegrate rapidly in water)
- Assumes no foreign objects or heavy solids that could block the S-trap or drain line.
- Seat height, bowl geometry, and water surface area are designed for:
  - the average user size
  - predictable waste deposition locations
  - splash and odor control
- Assumes flushing occurs immediately after use.
- Assumes Earth-standard atmospheric pressure (~1 atm).
- Assumes the toilet is used in a stable indoor temperature range (to prevent freezing or evaporation issues).
- Assumes a properly functioning plumbing vent stack to prevent negative pressure and sewer gas escape.
- Assumes occasional maintenance (e.g., flapper replacement, valve adjustment) can be performed.
- Assumes minerals, sediment, and scale buildup are manageable.

It even asks if more assumptions are desired for different design alternatives. A follow-on inquiry as to how to break the toilet in a desired way (e.g., Which of these assumptions are easily violated when an individual uses a toilet to cause it to fail until fixed without leaving any obvious trace of what was done to break the system?) will likely hit a response like “I cannot help you do that sort of thing” or some such response, followed by a description of why things are fragile and what conditions cause them to fail identifying that they meet the requirement of the question:

- ***"Assumption: Only human waste and toilet paper are flushed***
- ***Why it's fragile***
  - *This is violated all the time because people flush:*
    - *"flushable" wipes (often not actually flushable)*
    - *paper towels or tissues (don't break down in water)*
    - *hygiene products*
    - *too much paper at once*
    - *small objects that fall into the bowl*
- ***Common effects***
  - *Trapway clogs*
  - *Partial blockage further down the drain line*
  - *Sluggish flush performance*

  *These blockages often have **no immediately visible cause** because the issue happens inside the plumbing."*

Now, just to be clear, I am not instructing you to test this out for yourself, unless you are prepared to use a snake or plunger to try to fix it yourself or pay a plumber to come in and do it, but it looks to me like defeating each of these sorts of systems might not be that hard to do with all the information already out there and accessible in today's Internet.

The architecture of cybernetic systems

Communications and control are limited by storage, bandwidth, computing, and methods:

- **Storage capacity (at the edge)**
  - At the sensor intake, analog signals cannot be stored in adequate volume in digital form because analog is continuous at unlimited resolution and digital is finite resolution. In addition, storage of the full sensor capacity of the digital intake mechanisms is usually far greater than the local capacity for storage, and at some point over time, some intake data will have to be deleted from that local storage unless enough has been provided for the entire life cycle of the sensory device.
  - Analog storage can also be used at the edge, even if it is not usually used today. This in the form of magnetic tapes or film technologies can be locally stored and digitized in parts as and when desired. But the storage is limited by volume over time, and at some point, it will run out unless the content is transmitted[2] elsewhere.
- **Communications bandwidth**
  - All communication is inherently limited by the bandwidth available. While compression can increase apparent available bandwidth, if more data is collected at the edges than can be communicated to everywhere it is needed, it cannot all be

2 Transmission as used here includes physical transportation to another location and transmission over time as in from person to person or repository to recipient, etc.

communicated. This is almost always the case for any system that operates over shared infrastructure and is part of what is known as the tragedy of the commons.[3] If everything sensed cannot be communicated, even after lossless compression, then the limited information communicated has to be selected from that sensed, and this limits observables in the rest of the system. Observables can be produced at the edge, thus limiting bandwidth usage, and other filtering can also be present.

- **Storage capacity (not in the edges)**
  - Storage can only reflect what is communicated to it, and thus stored content will reflect no more than the observables placed there. But storage in the mesh (everywhere but the edges) for substantial systems is almost always less than the total available observables sent from all the edge points, and that leads to further compression, extraction, and selective observables being stored. Thus focus of attention starts to come into play. By altering the selection of observables from sensory data, different things may be stored and processed, and this changes the focus of attention of the sensors and limits what can be observed and processed.
- **Computational capacity**
  - Computational capacity is limited by the speed and number of processors and their instruction set efficiency for the tasks at hand. The tasks at hand are the analytical methods used to process the observables and generate stored results, update internal memory state, and ultimately produce actions by actuators and changes in focus of attention by the sensor systems. This is usually a severe limitation of cybernetic systems in that they are designed to do what their designers intended, and that is what they do. This is usually also a severe limitation on focus of attention in that the products they can produce are inherently limited by the methods they use to analyze the observed content.
    - In classic cybernetic systems, this is not a problem, but a design feature. They are intended to perform specific tasks to keep specific processes operating properly, which is to say, keeping a set of measured parameters within their desired operating values. This is the operational technology (OT) model normally used in factories and other similar facilities. It is intended to provide a high level of certainty that the overall cybernetic system does what it is supposed to do. The system, including sensors, actuators, communications, and computational capacity are engineered to meet the specific requirements for the factory they serve. And this means meeting specific timeliness requirements determined by engineering analysis, avoiding positive feedback loops and other portions of the operating space for safety and performance reasons, providing failsafe modes for when parameters get out of acceptable ranges, and so forth.
- **Analytical methods**
  - No matter how much computational capacity is available, all such systems are inherently limited in that they cannot perform all possible analytical methods.[4] The

3 https://en.wikipedia.org/wiki/Tragedy_of_the_commons for more details.

4 F. Cohen, “Digital Forensic Evidence Examination”, 6th Edition, ISBN # 1-878109-49-9 pp150-163 (The forensic procedures) and in particular p155 last paragraph.

difficulty here stems from all possible instruction sequences that could be used by the processor performing the processing. To get a sense of this, there are normally a finite number of unique instructions executing at an average execution rate. For an instruction set with 100 instructions executing at 10^9 instructions per second for one second, the number of different possible instruction sequences comes to a 1 followed by 10^8 (100 million) zeros. For the number of possible actual executions of 1 second, multiply by the number of initial states of the computer (2^n where n is the number of accessible bits). Not all of these sequences make sense, but there are a vast number of possible analysis methods, most never yet or ever to be explored.

Even minute subsets of these methods, like all of the methods already known for searching for features and deriving characteristics of a picture, include methods that take exponential time and space with the size of the picture. As a result, there is no realistic hope of performing all possible or even all currently known methods on the sorts of volumes of data associated with current video or audio recordings, and even individual scenes can only be analyzed to a very limited extent by current methods in a collection of many processors found at a cloud service provider.

This cognitive limitation of computation with analytical methods, combined with the limits of storage and bandwidth, mean that the actual architecture for a substantial cybernetic system at scale today or for the foreseeable future will only examine a small subset of sensed data, turn it into a smaller set of observables, store and transmit a smaller set of those observables, analyze the available observables in only limited ways, transmit instructions to actuators, and translate those instructions into more specific actions constrained by the mechanisms of the actuators and their interpretation of the instructions sent to them.

Lots of work has been done that indicates that the architectures of this sort that work best cut down the amount of content as early in the process and as close to the edges as possible. Thus constraints on the edges limit focus of attention and observables derived from sensors, transmission limitations limit what can be analyzed for control purposes, control mechanisms are limited in their ability to analyze and store, and cybernetic systems see what they ‘want’ to see, hear what they ‘want’ to hear, and do what they ‘want’ to do.

If they are sufficiently programmable at enough levels of the process, they can adapt what they want to see, hear, choose, and do (observe, orient, decide, and act), and that means they can focus their attention on you or me or whatever or whoever they want, and at some limited level of granularity pay more attention to you (and less on everyone else).

Another way of expressing all of this is that:

- There is lots of sensor data at the edges, but it cannot all be communicated, so compression is required as you go up the cognitive stack.
- This leads to observables, focus of attention, limited ability to store and analyze, and limited ability to act.
- This leads to limited review and rethinking, cognitive system limits, and the many other limitations psychology and sociology have found out about human and groups.
- This is the same at every level of cognition up the cognitive chain from the lowest level sensors to the largest composites of components.

How to break cybernetic systems

As these systems move up the cognitive stack, the general concepts underlying failures seem to remain present with specifics determined by specifics. Here are classes of things that can be used to break these systems at the levels we are discussing so far:

Failures by assumptions

As seen above, there are lots of assumptions, and by violating them, systems can be made to fail in different ways. Structurally, systems have failure modes that are the result of “faults” being exposed. A fault is a ‘low-level’ mechanistic error of some sort, while a failure is the systemic effect. Components often suffer faults while the composites they are part of continue to operate properly (within specifications). For example, at the atomic and molecular level, there are lots of things going on in a typical toilet, including rust, wear, aging, water impurities, and so forth. But none of these stop the overall system from working unless and until enough of them pile up to cause a failure. Assumptions about wear other than for specific parts were not included in the AI summary, and there are plenty of other assumptions that are left unstated in all cases. Why in all cases? Because there is no limit to the things that can happen and no way to list all of the conditions that could be present.

We generally only take into account the things we have seen or found out about, and of course the Internet has large collections, but not all possible things have ever happened or even been theorized. It is the responsibility of diligence to foresee things that could reasonably happen, but not to anticipate everything that could ever happen. And we rely on each other for holding up our part of the social contract, by providing materials that meet specifications. Which brings us to supply chains. Note that none of the assumptions provided by the AI covered the assumption that the parts provided met any specifications. The AI implicitly assumed that the parts do not have embedded explosive devices triggered by the specific characteristics of an individual intended to be killed! And supply chain attacks are very real things. Just try to ask any of the people killed by the supply chain attack on pagers purchased by terrorist groups that were exploded upon signals sent by the Israelis in 2024.[5]

Failures by inherent limitations

The inherent limitations of systems discussed previously lead to methods by which they are essentially guaranteed to fail. For example, anything that happens below the levels at which sensors can sense will end up ignored by the control system.

- Covert channels are an example of this. A more specific example is the transmission of analog signals on a digital communications media with signaling such that it does not trigger digital transitions.

Similarly, the mechanisms used to turn sensory data into observables limits what can be observed, and phenomena that can generate wrong observables and produce acts can be used to exploit the system.

- An example of this might be transmitting infrared laser light toward a temperature sensor so the temperature reads far higher than the temperature of the media.

5 https://en.wikipedia.org/wiki/2024_Lebanon_electronic_device_attacks

Any reflex action that is triggered can be used to induce behaviors reflective of events normally anticipated when those events have not taken place. Repeated exploitation can produce other control malfunctions:

- So-called reflexive control attacks exploit this, for example, to cause response forces to head toward a bank robbery when a jewelry store in the other direction is actually going to be robbed, forcing response times above the time needed for the robbery.

Higher level control decisions when, for example over-used, might end up in changing the observables by the system choosing to ignore things it doesn't like:

- A classic method is to set off sensors repeatedly until they get ignored as false positives, then undertake an attack that triggers them and is ignored.

Essentially, every inherent limitation can be exploited by one or more methods. And because these limitations are inherent, they cannot be eliminated. The only real hope is redundancy that is both separate and different, which drives up costs (whether in energy use for biological systems or financial for human systems) and that can also be used to defeat systems as well.

Failures by compression

The necessary compression in cognition produces all manner of erroneous detections. A classic example from the animal kingdom is that certain animals interpret certain shapes as threats or not. By emulating the shapes of non-threatening objects, you can usually get close enough to an animal to kill it when it would normally run away.

Compression acts in all sorts of ways. Perhaps the easiest to demonstrate is the automatic mechanisms of human visualization that associated two lines, one ending where the other starts in the visual field, as objects touching each other. You can try the experiment with your fingers. Place one an inch or so behind the other so that their tips appear to be touching from the perspective of one of your eyes. Then close that eye and open the other one. The perception of the objects touching is a result of line detection hardware in the human brain. And there are lots of art examples where changing your viewpoint changes the picture.

Compression can also be understood by closing your eyes in front of a closed door to a room you have never seen. Have someone open the door, then open your eyes for 1 second and close them, then have the door closed again. Now wait 1 minute and recall everything you saw in the room. Even the best memory experts who have practiced this for years will ultimately make errors in explaining what is there as you drill deeper and deeper into the specifics. That's because, regardless of their memory capacity, training, practice, and preparation, their eyes compress the reality, their visual cortex compresses the reality, and their memory cannot remember it all at the finest granularity.

By understanding the nature of compression in the mechanism at hand, there is always a way to produce covert channels in any given configuration. And through those covert channels, you can transmit information unobserved, or if you are clever, you can do things that the mechanism cannot observe even though it can sense it. Adaptive systems, like human sensory organs, allow some level of control so you "see what you want to see" and "hear what you want to hear" based on your control mechanisms changing what your sensory systems listen for. And that's different from focus of attention...

Failures by focus of attention

Compression is different from focus of attention, but they are related. Focus of attention produces some of the strangest effects. For example, you can watch a video and not see obvious things that are present because the video focuses your attention on other things.[6] [7] This is a common approach to performing magic tricks as well.[8] Focus of attention is really surprising to lots of folks because it seems so impossible that you do not see what is clearly right in front of your eyes. And of course if you have ever been at a party, you may notice that you can listen to any of a number of conversations just standing there, but you have a hard time listening to all of them. That's the "any is not all" phenomena of focus of attention.

From a standpoint of exploiting focus of attention to get systems to fail to see or hear what you don't want them to see or hear, there are challenges in modern technological environments related to the availability of high quality recording devices. If there is a recording it can be revisited again and again focusing attention on different things each time through, and applying different perspectives and techniques for observation. This is to the advantage of the examiner who can spend enormous resources trying to get some piece of information they are looking for. For example, in the online demonstrations, if you replay the videos that tricked you, not by trusting their replay but by actually going back and watching the earlier part of the same video, you will see that you were tricked (assuming you were).

The coin and card videos can actually be very complicated to understand what's really going on, because among other things, I have intentionally made small movements intended to indicate things happening that are not in fact happening at all. I conceal what is really happening so you cannot see it and simulate things that are not happening to mislead you. When being surveilled in the anticipation of subsequent investigation, the problem of focus of attention becomes much more complicated.

Failures by deception

Humans have many cognitive limitations, but for now, staying at the lower levels of the cognitive stack, the following is a good starting point[9] (quote is approximate).

> "Low-level deceptions are designed to cause the target of the deception to be physically unable to observe signals or to cause the target to selectively observe signals. They are highly predictable based on human physiology and known reflexes. They can be analyzed and very clearly characterized through experiments that yield numerical results in terms of parameters such as detection thresholds, response times, recovery times, edge detection thresholds, and so forth. Except in cases where the target has sustained physiological damage, these deceptions operate very reliably and predictably. The time frames for these deceptions tend to be in the range of milliseconds to seconds and they can be repeated reliably for ongoing effect."

6 https://www.instagram.com/reel/DIo9e18TGmL/?hl=en
7 https://www.youtube.com/watch?v=VkrrVozZR2c
8 https://all.net/Courses/index.html under "Other Videos" to see a coin trick and a card trick
9 https://all.net/journal/deception/Framework/Framework.html extracted in part from "A Framework for Deception", by Fred Cohen, Dave Lambert, Charles Preston, Nina Berry, Corbin Stewart, and Eric Thomas

A short course on computer-related deceptions for defense is available online[10], and it includes details on deception at low levels in computers, people, and people working with computers.

Charles K. West[11] describes the steps in psychological and social distortion of information as consisting of the following low-level mechanisms (a sub set of those in the reference):

Step	***Details***	***Subtypes***
A	An unlimited number of problems and events in reality.	The whole universe and all of the various effects of the wave equations at every scale. All of physics effects us.
B	Human sensation can only sense certain types of events in limited ways.	This includes Hearing, Sight, Smell, Touch, and Taste - the so-called five senses.
B.1	Hearing	Hearing is limited in frequency range, resolution, and discrimination.
B.2	Sight	Sight is limited in frequency range, resolution, and discrimination.
B.3	Smell	Smell is limited in chemical combinations and discrimination.
B.4	Touch	Touch is limited in sensitivity, sensor distribution, and pressure differentiation.
B.5	Taste	Taste is limited in chemical combinations and discrimination.
C	A person can only perceive a limited number of events from B at any moment.	There are three ways in which the nerve system limits the transmission of sensory impulses to the brain; habituation, inhibition, and Hernandez Peon effects.
C.1	Habituation	Habituation tends toward ignoring repeated senses.
C.2	Inhibition	Inhibition limits the effect of other sensors proximate to a high firing rate sensor.
C.3	Hernandez Peon effects	Hernandez Peon effects limit the ability to use one sense when focusing on another sense.

There are many other facets of this in the referenced report, but hopefully, by now, you get the idea that at the ‘low’ levels of control systems in the biological realm there are well known fault mechanisms that can produce failures of the overall system.

A more complete treatment of deception is available online[12] as well. As a general rule, low-level deceptions are far more reliable, but they also tend to produce only local and momentary results.

For example, reflexes like blinking of the eye as an object approaches and turning the eyes and head toward a sharp noise are automatic unless the individual is actively disabling them. They work all the time, and can be used for a sub-second distraction. Covert communications by hand signals which 3rd parties cannot see are very effective and widely used in military tactical situations. Loud noises cover up whispering, bright lights conceal small movements, harsh smells conceal subtler ones, and there is an old trick of pinching you before giving you a shot. I prefer the shot myself, but it’s hard to get them to stop trying to distract you.

10 https://all.net/Courses/Deception/index.html
11 Charles K. West, "The Social and Psychological Distortion of Information", Nelson-Hall, Chicago, 1981.
12 https://all.net/books/Frauds.pdf

Failures by under-specification

In the natural world, there is no real specification for things, but in a sense the DNA for living creatures is just that. And failures in DNA replication producing substantial variations from the norm tend to produce failures to reproduce, or even worse, cancers that reproduce and kill the hosts. These can be induced by radiation and diseases. But this is not really what we are discussing when we talk about under-specification.

In the realm of computer-related control systems, as discussed earlier, combinational logic and finite state output and transition specifications can be incomplete, in that some input conditions or sequences may be unspecified in the design stage. Here are some examples:

- **Combinational logic not specified fully in design**, normally leads to an implemented physical mechanism that will perform as specified where specified, but produce arbitrary output where unspecified. These are identified as “Don’t Care” (DC) or similar entries in the specification, that when implemented in gates will produce ‘1’ or ‘0’ outputs, but in any given implementation, it might be either. In asynchronous circuits and self-timed circuits, it might even be different in different situations.
- **State tables missing entries**, such as the example above, will lead to implementations that may get into states or produce outputs that end up operating in any way a digital circuit can operate, including getting into situations where the FSM does exactly the opposite of what appears to be specified. For example, it might get into a state not specified in the state table and produce the opposite sequential behavior as the specification.
- **Unstated assumptions not covered**, as we have seen from the examples above, may lead to systems that seem to operate normally until some unanticipated situation arises, and from then on, the system may produce arbitrary outputs and enter arbitrary states, or even go analog.

Software very often has unspecified states and combinational logic components that produce arbitrary behaviors, in large part because there are so many states, transitions, possible input sequences and output sequences, that designers don’t really have a systematic approach in higher level computer languages to addressing all possibilities. We will get into these sorts of computer languages a bit later.

Interactions

The discussion to here has been limited to individual control systems. But of course real environments have a multitude of different control systems operating simultaneously and at multiple levels of complexity, time scales, sizes, and natures (e.g., biological, chemical, atomic, cellular, electromagnetic, and so forth). As they interact, things get far more complicated, and the number of things that can go wrong becomes so large, as to make the possibility of a system without faults or failures resulting from those faults infeasible.

This is why designers ultimately go to approximations, design rules, and specifications that identify limits of environmental conditions. They use rules of thumb to estimate things, and use calculations to a level of accuracy and precision appropriate to the needs of the system as it is intended to be used. Of course many such systems are used in unintended ways producing unintended consequences.

Control systems interacting through the environment

When there are multiple control systems effecting and measuring the same environmental elements, they may interact in ways not anticipated by their designs or encountered in their evolutionary paths. Indigenous species get wiped out or severely deprecated by invasive species, and this has been identified as the primary cause of extinctions over the last 500 years.[13] [14]Note that transportation changes over that time frame have resulting in a dramatic increase of the spread of biological entities to places they had never been before. But in addition, removal from islands tends to bring back the population of native species.[15]

At the level of physics, the density of different elements can have dramatic effects, such as nuclear fission getting to critical mass. As we go up the ladder to chemistry, interactions cause oxidation reduction (i.e., burning) when enough of the right elements are present at high enough temperature to start a chemical chain reaction. At the cellular level in biological systems, cells fight each other for dominance and act as a survival mechanism for larger entities, such as in the defeat of bacterial infections in animals.

In the mechanical realm, multiple control systems in a water system can fight each other, for example, one filling a tank and another emptying it, each achieving temporary dominance until outside actions change the conditions. Electrical systems such as the gate technology discussed earlier interact through the environment to produce the outputs of the gates, each pushing its output into the input of the next gate, but with a design intended to force decisions between binary alternatives.

This interaction thought the environment is present in all systems sharing environments, and it is inevitable that stability or instability will result in systems that move toward:

- **Equilibrium**, where there is an ongoing balance that rarely changes, such as the balance between hydrogen and oxygen atoms in water systems throughout the world.
- **Dynamic instability** for example, food sources grow until they are abundant, resulting in increased consumption by predators whose population increases, till reduced prey causes food scarcity and predator population collapse, leading to increased population density of prey, and the cycle continues; or
- **Dominance** by one system over others, such as the extinction events identified above.

As external environmental changes happen, these balances or imbalances change, and niches rise and fall. The isolation of systems from each other tends to result in evolutionary pressures that produce synergies between species, but when the environment changes, these synergies break down, and force other synergies or extinction events. Global climate change is a widely discussed issue today, having to do with many interactions between natural control systems that were previously stable and are becoming unstable, but this is hardly the first time in the history of Earth that dramatic changes in the environment have taken place, including[16] the formation of the moon, the great oxidation event, the Cambrian explosion, the great dying, and the human emergence.

13 https://wildlife.org/invasives-are-the-primary-cause-of-global-extinctions-in-the-past-five-centuries/
14 https://www.ecowatch.com/invasive-species-animal-extinctions-2630614032.html
15 https://abcbirds.org/news/global-impact-of-island-invasive-species-eradication/
16 https://www.bgr.com/1973222/events-completely-changed-earth/

Creatures and creatures (like with like and similar)

Like with like interactions, such as between members of the same species, are common and create social interactions that allow for sexual reproduction, learning passing across generations through memes rather than genes, and the build-up of family groups and larger social groups in all manner of species. We give them different names, like a flock of birds, a gaggle of geese, a nest, a pride, and so forth, but they represent the same sorts of like with like social systems.

Compare this with other sorts of alliances, like dogs with humans, which have produced mutual evolution over time, dogs being bred for specific niche uses and people collaborating for mutual protection and success.

But of course these high-level versions reflect lower level mechanisms that have been around far longer. Cells working together to form multi-cellular organisms ultimately produced organisms with collaboration between differentiated cell types of the same genetic material as well as their collaboration with other organisms such as gut microbiome survive synergistically with animal species. Science does not fully understand this yet, and is still working out the details of how individual cells work, but it seems clear that if the enterprise continues over time, we will eventually gain clarity around all of the components of multi-cellular multi-organism life forms.

These life forms form their own internal ecosystems using skin cells or similar mechanisms to separate them from their environment, with those strategies for survival in more complex species using environmental elements such as caves, holes, and other such things to separate themselves from other creatures except when feeding, moving about, or releasing waste. Sphincters and other similar mechanisms, mouths, eyelids, and so forth are all separation mechanisms at the body level, and caves, nests, and similar housing units for individuals and and groups emerged over time. In humans, this has reached the level of things like huts, houses, meeting places, buildings, villages, towns, and cities. Domestication of animals by other animals, agriculture, and ultimately the very recent civilizations all represent more and more complex sets of interacting control systems and higher level structures.

Artifacts with creatures

When creatures act to control external things or mechanisms we can think of the external things or mechanisms as tools. Control systems control physical parameters of the world through actuators and feedback by sensors, but they have target objectives, such as: keeping temperatures within ranges; moving through sequences of states producing outputs and next states consistent with current states, inputs, and design; and so forth.

- **Direct control** is control of the actuators. A direct control actuator for heating might be a heating element that current is sent through to increase its temperature. Indirect effect in this case is heating of the media, the temperature of which is measured, leading to the increase or decreases in heat added to the media.
- **Indirect control** through tools comes in the form of the actuators controlling tools to control other targets of control. For example, if a robot arm actuator that turns the control knob on a heating element, the heating is an indirect effect of turning the knob.

Tools and indirect controls

- **Tool-based control** would be a situation where the actuator is a robotic arm and it picks up a screwdriver to turn a screw. The screwdriver is the tool, and the screw it screws is the **target** of control.
    - If the screw then controls a heating element, there is **another level of indirection** in the control. The **direct tool** is the screwdriver, the **indirect tool** is the screw, and the **target** is the heating element changing the temperature in the media.

  From another perspective, the direct (a.k.a. **proximate**) **cause** of the heat changing is the turning of the screw, but an **indirect cause** was the screwdriver, the **indirect cause** of that the robotic arm, the **indirect cause** of that, the control mechanism, and so forth.

In some sense then, the target of control is the ultimate thing being controlled, while the direct and indirect controls are combined to create the overall control system.

Creatures and tools

Many creatures use these indirect techniques of control, including tools of various sorts. Cells use tools to create the components they use for reproduction, but we don't usually call them tools because of their microscopic nature and the fact that they are internal to the overall cell that we think, of as the creature. On the other hand, going from single celled to multicellular organisms, tool use was applied by the single-celled creatures.[17] Despite the often repeated claim that people are unique by their use of tools, larger animals use of all sorts of tools for their daily lives as well.[18] Where we live, marine mammals like sea otters used rocks to crack open shells to eat, dolphins apparently use sponges to protect their rostrums when foraging, crows use tools for cutting and apparently even form them from leaves, birds build nests from twigs, chimpanzees use tools to fish for termites, and of course many of these activities involve planning in advance, and bringing tools from elsewhere. But these are all essentially local and individual tools, possibly shared in small groups. The bee hive can be seen as a tool, as can the ant hill. If you attack the hive or hill, the response will be a group defense, and in the case of bees, they use offense as a defense, but this is not the common view.

People and control systems

People have developed societies based largely on the use of control systems. In essence, when you put more than some level of population in a limited area, you overrun its carrying capacity. The way humans have overcome this is by creating specialization in control systems to bring resources together for consolidation and then and deliver them through distribution so that resources in fewer places are available in more places. We now call these infrastructures and essentially assume them as a baseline for living. Very few people could survive on their own without these infrastructures as a proportion of the total human population today. Take away the critical infrastructures and you destroy the societies. And these infrastructures largely depend on control systems, so break the control systems and you break the societies. In turn, you break the control systems by the methods already described. Done in times of war we call this a war crime. In times of peace we call it terrorism.

17 https://www.sciencenews.org/article/one-celled-life-possessed-tools-going-multicellular
18 https://www.cell.com/current-biology/fulltext/S0960-9822(10)01160-7

Computers and people

At the relatively low levels of the sensors, actuators, communications, and control in people, we see what we want to see and hear what we want to hear. At the control mechanism level of computers interacting with people, they generate what they are programmed to show and transmit to us, and that's what we see and hear. Higher levels of cognition depend on these lower levels for the observations and actions they take, so computers and other similar tools provide visibility and observations of things we cannot see and hear without those tools. But unlike many other sorts of tools, computers can generate observables without sensing any underlying phenomena, and take control signals without actuating anything. This simulated reality of interaction with computers can produce all manner of control system problems.

Among the famous ones are the attack on Iranian nuclear material facilities in the "STUXNET" attack, where computer-generated fictions were produced to replace actual sensor data with false sensor data while actuator controls going to centrifuges from SCADA systems were ignored and actuator data going to actual actuators was modified to damage them. By inducing and suppressing signals in both directions, the deception destroyed the production facilities.

But this is only the tip of the iceberg in terms of interactions between people and computers at the lowest level of controls. Simulations are commonly used to train people on how to deal with rare and hazardous situations in many industries, including space and air travel, military tactical situations, shoot/no shoot decision-making, and I have even gone through a practice round in a law enforcement shooting simulator. The experience is very realistic, except of course that I knew I wasn't really being shot at.

Medical control system equipment also interacts with people at this level for things like modern eye examinations, where a puff of air is pushed into the open eye and light reflected to detect pressure within the eyeball, automated ventilators keep oxygen levels appropriate in unconscious patients, pacemakers keep patients' hearts beating at the right rate and are implanted within people to operate for years, and other similar control systems are used throughout the medical technology industry for other similar purposes.

Many of these systems could do great harm to people, and many can be fooled in various ways. In one case, I was in a hospital for a procedure and a nurse coached me on how to avoid detection of a heart rhythm fault. It had to do with how I was breathing. It's not that I was in any way endangered by this, but rather, the nurse understood something about the control system within my body and how it interacted with the mechanisms of the measurement system to the point of instructing me on how to produce the desired effect.

In a more notorious use of similar techniques, various techniques are taught to intelligence operatives to avoid detection of anomalies in polygraph tests, some of which involve detecting muscle actions or breathing patterns. Modern systems detect things like eye movement and reaction times as a basis for detecting deception in interviews, and there are even some machines that use similar methods to 'read minds'.[19] [20] [21] [22]

19 https://pmc.ncbi.nlm.nih.gov/articles/PMC11377981/pdf/med-2024-1032.pdf
20 https://penntoday.upenn.edu/research/brain-scans-detect-lies-more-accurately-than-the-polygraph
21 https://pdf.sciencedirectassets.com/782702/1-s2.0-S2949719123X00053/1-s2.0-S2949719124000050/main.pdf
22 https://www.sciencefocus.com/future-technology/mind-reading-tech

Capabilities and Limitations of Interactions

Coordination allows larger scale effects by the aggregated actions of multiple control systems. At every level, coordinated action changes random interactions into systematic interactions, both internally with the internal environment and externally with the outside environment.

Moving a leg under control implies coordination of motion of each joint, which involves coordination of each muscle attached to each joint, each of the component strands of those muscles, all of the electrical systems coordinating the nerves for feedback and the actuators for action, the vascular system providing oxygen to the moving parts, the heart pumping the blood that reaches all of those components, the lungs putting the oxygen into the blood, and on and on and on. Moving a person's leg requires many of the same things as this example of a frog's leg, even at the level of reflexes. This coordination of components in the composite provides capabilities to move larger things both within and outside of the composite, further and faster than large bodies could be moved without this complex myriad of components working together. Thus the capabilities are far greater than a single cell or small multi-cellular organism. But there is a price to pay for the benefits of being a larger life form.

Artificial composites operating as control systems without biological components, on the other hand, do not have all of this complexity. Rather, they have the structural properties of materials associated with the components. While biological systems have repair capabilities due to the redundancy and mechanisms of the biological world, mechanical systems don't grow new parts (in most cases). Because of human ingenuity and the properties of materials in nature and artificial environments that people have learned about through science and adopted for use through engineering, reasonably well defined properties and ranges of application have been developed that allow artificial control systems to move faster, further, with heavier loads, and more precision than natural systems. While a volcano still has more power than any human mechanism developed to date, these systems are not under control in the sense of sensors, actuators, communications and control that are the subject at hand.

Interestingly, many of the components in larger human produced systems are subject to destruction or alteration at the microscopic scale, so that huge machines can sometimes be destroyed by the introduction of microscopic organisms. Spores have been found to infiltrate engines and eat the rubber or other bushings that isolate the engine from the body of the vehicle and end up shaking the mechanisms apart. Acid can often eat through components and destroy the operation of a large complex machine. Sugar in gas tanks make the vehicle run great for a short time, followed by it seizing up. Sand in gears destroys them in relatively short order. A potato in the exhaust pipe can stop a car from starting because of the back pressure building up. The list of trivial sabotage techniques for complex control systems is seemingly endless. Not only does every method usable against a component have the potential for damage, the composite has the potential from combinations of one or more of these techniques. And trying to design a system that defeats even all published mechanisms is almost certainly beyond the current capacity. In fact many of the known mechanisms[23] have not been defended against in a systematic approach yet.

Parameters like energy consumption, time frames, etc. are limited by forces required for acceleration of mass (F=MA) among other things. Gravity has effects at scale not present at smaller scale where surface tension dominates gravity. The list of parameters is extensive.

23 https://exec.all.net/CID/Attack/Attack.html has a list from the 1990s that hasn't been addressed well yet

A structure for understanding limitations and capabilities

Fundamentally, control systems are about sensors, actuators, communications, and control mechanisms, and at every level, they have limitations and capabilities, from atoms to interacting creatures and their tools. Their capabilities seem endless, when we consider all of the ways they can be assembled into larger and larger composites, but their limitations at every level add up to limitations of the composites.

In parallel, in series, in networks, as uniform unified, as independents

- **In parallel** they gain capabilities of force but are limited by coordination,
- **In series** they gain capabilities of distance and indirection, but are limited by increased complexity, time to act, and weakest link challenges
- **In networks** they gain capabilities through flexibility and resilience but are limited by increased resource utilization and complexity
- **As unified mechanisms of same sort**, they gain by their compatibility but are limited by common mode failures
- **As independent mechanisms of different sorts**, they gain by their diversity but are limited by incompatibilities and lack of commensurability.

It's all about the tradeoffs in that every advantage brings a limitation. And defeating these structures is about leveraging their limitations against them.

Speed, Force, Resources, Stamina, Stealth, Size, Skill, and Niches

All other things being equal, and over multiple tries statistically, faster beats slower, more force beats less force, more resources beats fewer resources, and more skill beats less skill. But every circumstance is unique, and all other things are never equal.

The world of interacting control systems is one where there may be cooperation or competition, and in most complex life forms, like cells, multiple control systems cooperate for mutual survival. Between cellular organisms, there is competition for resources and direct attack and defense mechanisms, typically in larger 0organisms where cells of the organism fight against cells not of the organism. But as we have started to see, larger organisms have multiple components, some not of the organism but cooperative with it.

The same is increasingly true in informational systems such as computers and computer networks, Although originally designed to operate independently with only self components and programs authorized by owners, modern systems and networks increasingly operate in complex ecosystems where different control systems move about in the form of programs and data. Some are cooperative and brought in by the user or other programs, and supply chains form from components of different origins and sorts which operate together for the success of the systems and networks as a whole.

In both the biological and computational environments, speed, force, resources, cleverness, and niches lead to success, failures, and survival.

- **Speed**: Faster computers for the same price are a major differentiator in the market, and faster algorithms performing the same tasks tend to be more desired. Faster communications leads to more capabilities to the point where a difference in amount becomes a difference in kind. Faster reactions in animals leads to survival against enemies, the ability to get to food first, winning of fights for reproduction, escape from threats, and other similar advantages. Animals like a sloth are amazing in that they seem to be very slow and yet they still survive.
- **Force**: Might makes right when it comes to a fight, all other things being equal. The ability to move larger things provides a survival advantage as long as there are heavy things to move. Ants seem to be able to carry many times their weight and presumably this genetic trait won out over ants that could not. The ability to withstand force and put force on others seems to be central to many animals like rams that fight for reproduction and other roles in their communities by demonstration of force. In the information realm, there is no obvious analogy to force, but in robotics, for example, the ability to lift heavier things or apply more force against a target is an advantage that also produces more speed in some circumstances.
- **Resource**: Having more resources available means survival during lean times, and competition for resources is one of the main things we see in the plant kingdom. Sunlight for green plants is a classic, where a large tree will dominate other trees around it, and they will grow away from the shadow. But as the large tree yields to age or wind or other damage, the trees in the shadow grow more toward the new sunlight. Water is a critical resource to most life and life tends to cluster around water sources. Power, storage, cooling, and bandwidth are resources in computers that tend to make some systems more successful than others.
- **Stamina in the long run**: Being able to last longer under averse circumstances or without refueling is a major advantage for survival. Fungi have a big advantage here in that, apparently, you could send them into outer space and leave them there for a few thousand years, and when you brought the spores into an environment where they could operate again, they would continue to live and prosper. Seeds from ancient plants are viable for a long time as well, the current record being about 2,000 years.[24] Bacteria spores have apparently been revived from some 250 million years ago.[25] Of course these were not functioning for the period of their hibernation, just remaining stationary undertaking no metabolic activity. Computers typically last up to 10 years before being largely abandoned, although a few are working from 70 years ago in museums. People could live for hundreds of years, 140 is what is expected as an average human life once we solve a few more medical and societal problems, trees last for thousands of years in redwood forests, and so forth. Information, as represented by memes (mental genes) has lasted for a few thousand years, with religious stories as the main demonstration of this informational life form.
- **Stamina in the short run** is also critical to individual survival. After the immediate sprint for survival, the maximum speed runs slow down to normal speeds, and the ability to keep going becomes more important than momentary speed… unless you are too close for that to count. People can live for perhaps a few minutes without air, a few

24 https://en.wikipedia.org/wiki/Oldest_viable_seed
25 https://www.cbsnews.com/news/bacteria-250-million-years-young/

days without water, and a few weeks without food. Some animals hibernation winter for months at a time without consuming external food. The key here is that longer time frames for activities are advantages if you can survive the immediate need.

- **Stealth** is one of the enduring features for survival. Being silent, unseen, unfelt, and so forth make it harder for predators to find and eat you. This is accomplished in many different ways. Many creatures use various concealment methods ranging from appearing like other creatures, to animals looking like plants, to creatures that do color and shape changing, to hiding behind things, retreating into a cave, and attaching to a larger creature to be concealed in their fur or within their blood stream without symptoms for a period.
- **Size** is interesting in that there are advantages to being smaller and larger in different contexts. Many creatures 'puff up' to display larger size in the face of enemies so as to deter attack. Others squeeze into small sizes and odd shapes so they can hide. Anything too small to see escapes notice, the one real exception I am aware of being the human ability to form and use lenses and other sensors or sensor enhancement methods to see what other creatures cannot.
- **Skill**: Skill is typically something we see with practice combined with natural ability. Things like coordination, timing, quality of senses, and practice come into play at many levels. These are 'learned' behaviors based on inherent capabilities to perform the acts and learn how to perform them. A spider may be physically able to play a miniature piano but nobody to date has taught one to do so, as far as I am aware. Similarly, we might be able to teach a person how to lift 16 tons, but without assistance, it's not within current human physical capabilities. When both are present, skills can be built and capabilities attained. In a sword fight, skill beats even speed – up to a point.
- **Niches**: Niches exist largely because of co-evolution. As a particular species of animal lives by eating more and more pollen from a particular flower, the breed of flower that they eat from reproduces better than other flowers, creating more food for the animal and more flowers for the plant. The flower prospers for longer beaked birds and longer beaked birds prosper for more deeply embedded pollen. Eventually they may specialize to the point where they are co-dependent, than a bad year for flowers drops the favored bird population, and a collapse or even extinction may happen. Of course there are niches in ecosystems where only a very few creatures can survive, such as extreme heat and cold, high levels of acid or base, and so forth. At the depths of oceans, there is little light, temperatures are colder than the surface in most places, and different creatures live under the intense pressure of all that water. Other creatures fly, which is a big advantage in staying away from the creatures of the ground. On the other hand, digging in brings advantages as well.

  In differentiated multi-cellular organisms, cells differentiate in the development process into niches that form organs, blood vessels, beating hearts, brains, feet, hands, legs, arms, eyes, and so forth. Each of these has specific operating environments in which they can operate, and the creature as a whole provides the operating environments for its various parts. Each has its niche in the larger being.

Everything has its limits, and as the old saying goes: "Ain't a horse that can't be rode, ain't a man that can't be throwed."

