**How can we describe cyber security engineering in terms of complex systems analysis? What is good about this approach? What is not? What is the end goal of cyber security engineering? Consider this. If you all do your jobs perfectly, you will have no more jobs. So then, what is the best approach?**

Cyber security engineering can be described in terms of complex systems analysis by examining the related elements that exist within both. Cyber security engineering can be described like a mix of information technology, systems engineering, electrical engineering, computer engineering, and computer science. This is evident when you break down everything that comprises the functions of cyber security engineering which include taking a large variety of existing infrastructure, understanding how they work at a relatively low level, a comprehensive understanding of security fundamentals, knowledge of programming languages – particularly their capabilities and limitations, and the ability to put all of these concepts together to identify potential vulnerabilities, threats, and exploitable vectors.

The systems that cyber security engineers work on can be explained as complex systems in that there are an immeasurable number of components that make up the system, each with their own conceptual and quantitative frameworks. When examining complex systems, you will most often be discussing natural systems such as ant hills or the climate. However, we live in the age of information and the study of complex systems is not only relevant, but also extremely important to study.

When we analyze cyber security systems at a high level, the components can be broken down into groups and those groups are broken into a smaller subset of groups, and so on until you have a very granular look at individual pieces of a much larger system, yet they all work together to make the total system operate as intended. Consider the fact that these individual pieces each have their own set of unique security flaws, each have their own level of relative importance to the enterprise, and they all perform different functions that cyber security engineers need to consider when securing the system. The good thing about this approach is that a scientific framework for how to study complex systems is already established so you already have somewhat of a framework to start with.

Given that cyber systems can be very complex, there isn't much of a reason to suggest that this approach is bad in any way. However, just like everything else, it isn't perfect. Sometimes looking at the system from a high level – and by extension, less complex – makes reacting to failures much quicker, it requires a lot less expertise to fix issues that will inevitably present themselves, among other inefficiencies. Increased complexity generally requires increased resources so depending on the system, so the benefits expected from higher complexity – which is not exempt from the law of diminishing returns – need to be compared with the available resources in order to find the right balance for the stakeholders.

The end goal of cyber security engineering is to be able to analyze a system (cyber systems in particular), identify the risks and vulnerabilities that each component brings to the larger system, and work to mitigate the risks you've identified. This requires a wide range of knowledge related to the tools, services, hardware, software, corporate policies, security fundamentals, etc. of the system you are working with to effectively prevent or mitigate attacks and failures. Any and all cyber systems are systems of systems, which is the relation to systems engineering. But unlike systems engineers, cyber security engineers need to be able to identify nuances in sometimes extremely complex systems that often present more challenges than systems engineers typically have to contend with. This is the reason a big reason why cyber security engineering is a separate field in the first place.

If you do all your jobs perfectly, you will have no more jobs. Before explaining the best approach after considering the previous statement, I will define my interpretation of that statement. In a cyber system, if you do all of your jobs perfectly, then that means you have accurately – and permanently – identified and not only mitigated but eliminated all vulnerabilities and risks. This is undoubtedly impossible with today's technology, but let's assume that it could be a reality. Assuming we have some kind of AI using super ML technology that can identify vulnerabilities before they can be exploited and fix them automatically, then what work can we do? Well, there you go – you have no more jobs. Jobs being eliminated by 'robots' is a bittersweet thought to consider, but it's just as unrealistic as it sounds. At least for now, anyway!

**Ok, now I want you to consider how to apply your modeling approach for the first answer to the second question: How does cyber security play a role in Transportation Systems Design?**

Cyber security plays a major role in transportation systems design – especially since transportation systems are implementing technology at an incredibly high rate. Think about it, Tesla vehicles are massive, super powerful computers on wheels. Teslas are an excellent example of a cyber system. They have wireless connectivity for software updates. That's right, they have… well, software updates. Just like any existing software, Tesla's software definitely has vulnerabilities and the wireless connectivity doesn't help the security of the overall system either.

Let's zoom out a little and look at other transportation systems. Metro trains rely on technology too, right? What about airlines? They have lots of technology and they obviously rely on wireless communications as well. There are countless other examples of complex transportation systems and there will be more and more as time goes on as we continue to increase our reliance on technology, and by extension, on security and big data to make our infinitely high expectations a reality.

When I talked about complex systems and compared them to cyber security engineering, I mentioned that cyber systems can be broken down into extremely granular components, they all have their own vulnerabilities and risks to consider. I also talked about the importance of each component to the larger system they're a part of. When we talk about transportation systems design, it's clear that security is extremely important because it involves human lives. So the real challenge is going to be finding the right balance between the resources that are available to be put forth and the consequences of a system failure or compromise, which could both result in loss of human life.

So how do we approach this problem with intelligent transportation system design? Granted I have limited knowledge as a student in a bachelor's degree program, I would argue that cyber security engineers would need to prioritize the security of the transportation systems and if they can't nearly guarantee security, then they need to keep the design as safe as possible. If that means including less technology then that's what needs to happen. Cyber security engineers are *engineers first*, and therefore have a supreme responsibility of keeping people safe. No matter the desire to make everything interconnected and automated, if it involves the transportation of large groups of people (or even one person for that matter) then the security and safe functionality of that system are paramount over everything else.

In sum, when we discuss transportation systems design, especially as it becomes more involved with artificial intelligence, it's imperative that cyber security engineers are involved in considering the vulnerabilities in the components that the systems are made of. Cyber security engineers can essentially serve as systems engineers that specialize in cyber systems and therefore have a unique ability to consider the ever-changing cyber threats that will surely present themselves at some point.

One day cars will be driven without the assistance of human beings and the concept of humans at the wheel will be similar to the way my generation-Z views home phones. One day trains will be controlled remotely and probably fully automated. Yes, these systems are in need of extreme security measures and will need to be evaluated as complex systems broken down into very granular pieces so that the engineers can attempt to prevent any vulnerabilities that, in the event of an exploit, could result in loss of human life. So yes, complex transportation systems are very much reliant on cyber security for its future to continue.

# References

Nicolis, G., & Rouvas-Nicolis, C. (2007). Complex systems. *Scholarpedia*, *2*(11), 1473. https://doi.org/10.4249/scholarpedia.1473

*What are complex systems?* (2016, December 16). Waterloo Institute for Complexity & Innovation. https://uwaterloo.ca/complexity-innovation/about/what-are-complex-systems