Assignment: Questions for Reading Texts – Robots

I. Systems Theory: The "Swarm" vs. The Individual

Q: Does intelligence require individual autonomy, or is "intelligence" purely a result of collective behavior? If a system works intelligently but the parts are «dumb», can we call the machine intelligent?

According to the text, intelligence does not come from each robot individually. The individual nanobots are not intelligent, but the collective behavior of the swarm is. The system exhibits intelligent behavior even if the parts are "dumb". Therefore, we can still call the machine intelligent because the intelligence emerges from the network, not the individual robots.

Q: If we move toward systems we can explain but not predict, does this change the definition of "programming"? Are we still "engineers" if we cannot predict the precise outcome of our creations?

As systems become more complex, we may only be able to explain their behavior after it happens, rather than predict it beforehand. This means programming is no longer about controlling each step but guiding the system. The role of engineers changes, but we are still engineers because we design the rules, the network, and the conditions under which the system learns. Even if we cannot predict every outcome, we still create and influence the system's behavior.

Q: How does this challenge the idea of efficiency? Is a highly efficient system inherently fragile?

The text shows that a system can be very efficient but still fail if something small goes wrong, such as running out of parts. This means too much efficiency can make a system fragile because it lacks flexibility or backup. Therefore, a highly efficient system can be fragile since it works well only when everything is perfect.

II. Philosophy of Technology: “Teaching” vs. “Programming”

Q: The text suggests this is a “difference between programming and teaching”. Is this distinction real, or is “teaching” just a different user interface for programming? Does this change the relationship between the human operator and the machine?

According to the text, “teaching” a machine is different from traditional programming. Instead of writing code, we guide the robot physically, and it learns the movement. In practice, teaching is just another way of giving the machine instructions, but it feels more natural. This changes the human-machine relationship, as the human becomes more of a trainer than a programmer.

Q: According to this definition, can a user be proficient in Technique (using the tool) without understanding the Technology (the knowledge behind it)? Is this separation dangerous?

Yes, a user can be skilled in Technique (using a tool) without fully understanding the Technology behind it. Many people use machines without knowing how they work. However, this separation can be dangerous because users might depend on systems they do not fully understand and may not know what to do if something goes wrong.

III. Cultural Perspectives: Fear vs. Partnership

Q: Why does the author suggest that Europeans view automation as a threat to the “paradigm of work”, whereas the Japanese tradition views robots as “human companions” derived from folk culture?

The text explains that Europeans tend to see robots as unnatural and dangerous, influenced by stories like *Frankenstein*, where machines become uncontrollable. This causes Europeans to fear robots replacing human labor, which is highly valued in their culture. In contrast, Japanese tradition, which draws from myths and folk culture, sees humanoid figures as friendly helpers. As a result, the Japanese view robots more as companions than threats.

Q: Do modern developments in AI support Hoffmann’s 19th-century view that humans are irreplaceable, or are we moving toward the “Android” reality where machines are indistinguishable from humans?

Modern AI is advancing, but the text suggests that some human qualities—like emotions, creativity, and true understanding—are still irreplaceable. This supports Hoffmann’s idea that humans cannot be fully replaced by machines. However, we are also moving closer to the "android" reality, where machines can imitate human behavior more closely than before. Thus, we are somewhere in between: machines are improving, but they are still not fully human.

IV. The Cybersecurity Context

Q: In cybersecurity, we rely on predicting attacker behavior. If modern threats (like AI-driven botnets) operate on "swarm intelligence" that cannot be predicted, only explained post-mortem, how does that change how we build defense strategies?

The text explains that we can observe intelligent behavior but cannot always predict it. In cybersecurity, this means we cannot rely solely on predicting attacks from AI-driven botnets using swarm intelligence. Defense strategies must focus on flexible and adaptive systems that can react quickly, rather than trying to predict every action in advance.

Q: This describes a system with low resilience. How does this parallel "brittle" security software that works in a test lab but fails when encountering "noisy" real-world network traffic?

Just like robots fail when the environment changes, security software that works well in controlled tests may fail in real-world, unpredictable networks. This illustrates that systems with low resilience are brittle. Cybersecurity tools must be tested in real-world conditions to ensure they are strong and reliable.

Q: How might an organization's "culture" regarding automation affect their willingness to adopt SOAR (Security Orchestration, Automation, and Response)? Does the "Frankenstein" fear stop companies from letting AI handle their security automatically?

According to the text, culture plays a big role in how we perceive machines—as either partners or threats. In organizations that fear automation (influenced by the "Frankenstein" effect), companies may hesitate to let AI manage security automatically. In contrast, organizations that view machines as partners are more willing to adopt tools like SOAR. Cultural trust is therefore crucial for successfully using AI in security.