General Education Reflection

Anish Nag

Throughout my engineering education at Iowa State University, I initially viewed my general education courses as required checkboxes, necessary prerequisites separate from my "real" engineering coursework. However, as I've progressed through my cybersecurity engineering program and gained professional experience through multiple internships, I've come to realize that my general education courses fundamentally shaped how I approach engineering problems. In particular, International Studies 235 and Introduction to Psychology have profoundly influenced my ability to think beyond purely technical solutions and consider the broader implications of engineering decisions in our world.

My International Studies 235 course challenged me to think about engineering problems within a global context rather than in isolation. The course examined how globalization, international trade, and cross-cultural communication shape our modern world. At first, I struggled to see the connection between topics like global supply chains and international policy with my work in cybersecurity. However, as we discussed case studies of how different cultures approach privacy, data protection, and government surveillance, I began to understand that technical solutions cannot exist in a vacuum. What I learned fundamentally changed how I evaluate engineering solutions. I now ask not just "does this work technically?" but also "how will this solution be perceived and implemented across different cultural contexts?"

This shift in thinking became especially relevant during my internships at John Deere, where I worked on security systems for agricultural technology that would be deployed globally. International Studies taught me that a security solution designed with only American privacy expectations in mind might face serious adoption challenges or regulatory issues in Europe, where GDPR imposes stricter data protection requirements, or in developing nations where infrastructure limitations demand different approaches. The course helped me recognize that engineering innovation isn't just about creating the most advanced technical solution. It's about creating solutions that work within the complex realities of our globalized economy and diverse cultural values. When assessing cybersecurity risks or designing security protocols now, I consider questions that would never have occurred to me before this class: How do different regulatory environments impact this solution? What are the geopolitical implications of this technology? How might cultural differences in trust and privacy affect user adoption?

Introduction to Psychology complemented this global perspective by teaching me about the human dimensions of engineering that technical courses often overlook. The course covered cognitive biases, decision-making processes, human motivation, and how people actually interact with technology versus how engineers assume they will. One particularly eye-opening topic was the concept of cognitive load and how humans process information. This fundamentally changed how I think about user interface design and security systems. The best encryption algorithm or firewall configuration is worthless if it's so complex that users circumvent

it or make mistakes that compromise security. Psychology taught me that human behavior, not just technical specifications, must be central to engineering problem solving.

This psychological insight proved invaluable when I worked on third-party risk management at John Deere. I realized that security isn't just a technical challenge. It's a human challenge. People make decisions based on convenience, habit, and perceived effort, often in ways that contradict rational security practices. Understanding concepts like the "availability heuristic" where people judge risk based on how easily they can recall examples helped me design security training and policies that account for how people actually think and behave, not just how we wish they would. Rather than simply implementing technically sound security controls, I learned to consider: Will users understand this? Will they comply with it? How can we design systems that align with natural human behavior rather than fighting against it?

Both courses taught me to see engineering problems as multidimensional challenges requiring consideration of economic, global, and societal contexts. From an economic perspective, International Studies illuminated how engineering solutions must account for varying economic conditions across markets. A cybersecurity solution requiring expensive hardware might be technically superior, but it's not a viable global solution if most of your user base cannot afford it. Psychology reinforced this by showing how economic stress affects decision-making and risk assessment. People in economically constrained situations might prioritize immediate functionality over long-term security, which engineers must account for in their designs.

From a global perspective, International Studies made me acutely aware that engineering solutions deployed internationally must navigate different legal systems, infrastructure capabilities, and cultural expectations. What constitutes acceptable data collection in one country might be illegal in another. The course taught me to approach problems with cultural humility, recognizing that Western engineering assumptions don't necessarily translate universally. Psychology added another layer by revealing how cultural backgrounds shape the way people interpret and interact with technology. User experience isn't universal. It's culturally informed.

From a societal perspective, both courses emphasized that engineering decisions have ripple effects beyond their immediate technical function. International Studies highlighted how technology can either bridge or widen global inequalities, while Psychology demonstrated how design choices can either empower or manipulate users. When I work on cybersecurity solutions now, I think about questions like: Does this solution protect vulnerable populations or does it create new barriers for them? How might this technology be misused by authoritarian regimes? What are the broader societal implications of collecting and storing this data? These aren't engineering questions in the traditional sense, but they're essential questions that responsible engineers must grapple with.

My general education courses taught me that being a professional engineer means more than technical competence. It requires understanding the human, cultural, economic, and global contexts in which our solutions will operate. International Studies gave me the framework to

think about engineering problems in a global, interconnected world where solutions must account for diverse regulations, cultures, and economic realities. Psychology taught me to center human behavior and decision-making in my engineering approach, recognizing that the best technical solution is worthless if it doesn't align with how people actually think and behave.

Together, these courses transformed me from an engineer focused solely on technical optimization to a professional who considers the full spectrum of implications in problem solving and innovation. They taught me to ask not just "what's the most technically elegant solution?" but "what's the most responsible solution that accounts for how humans behave, how cultures differ, and how global systems interact?" This broader perspective doesn't make engineering easier. If anything, it makes it more complex. But it makes me a better engineer capable of creating solutions that actually work in the messy, complicated reality of our diverse, globalized world. As I move forward in my cybersecurity career, the lessons from these general education courses will remain just as important as my technical training, ensuring that I approach engineering challenges with the breadth and depth they require.