Security Clearances: Barriers to Entry and Defense Innovation

Paul Bracken
Yale University

January 21, 2021

This paper analyzes security clearances in a nontraditional way. Namely, that clearances are a significant barrier to innovation in defense technology and strategy. To show how clearances impede innovation in the defense industry I use a simple theory that is taught in every business school in the country.

The paper concludes that the cost of security clearances as a barrier to innovation will increase as advanced network technologies like AI and cloud computing are adopted, and as small and medium sized companies become an increasingly important locus of defense innovation.

The Role of Security Clearances

Security clearances have two roles. One is to protect critical information from falling in to the hands of foreign enemies. But clearances have another use as well. Companies and government agencies use them as a competitive weapon to restrict access to programs in order to protect a monopoly on technologies, to hide embarrassing failures and wrong doing, and to increase the value of a program by restricting competition. Clearances are used as deterrents to entry, to limit competition, and to block substitute products that meet mission needs.

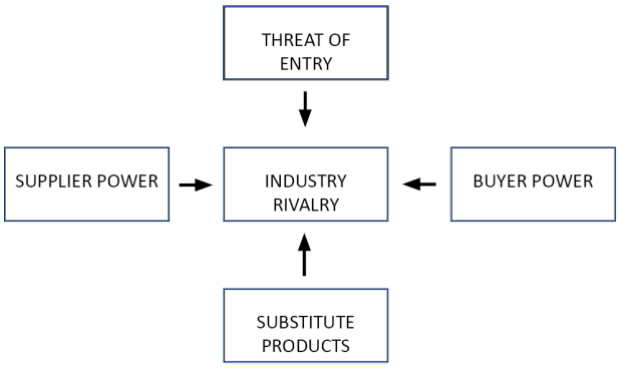
There are two things going on in the classification process. One is a valid effort to prevent information or technology from falling into the hands of those who would harm the United States. The other is as part of a competitive strategy in the marketplace and for bureaucratic infighting in the government.

Security Clearances in Defense Competition

In the defense and intelligence marketplace clearances are a key competitive weapon. Special access clearances are a particularly high value weapon. This is readily seen using some simple theory. This theory, called the Five Forces Model, is taught in every business school in

the United States and is the most widely used framework in the management consulting industry. What I had never realized before applying the theory to the subject at hand is just how negative the impact of clearances is on quashing innovation.

The Five Forces Model shown below describes the intensity of competition for any industry. Here, think of industry as made up of distinct markets, e.g. drones, cyber, military aircraft, AI, cloud computing, or data analytics.



THE FIVE FORCES MODEL OF INDUSTRY RIVALRY

The factor in the center of the figure, *industry rivalry*, is the degree of competition. This could range qualitatively from low to medium to high. Or, it could be measured quantitatively, as profit, EBITDA, or ROI. The theory asserts that the degree of competition is shaped by four factors.

Supplier power measures the ability of companies to restrict supply in order to drive up prices or to maximize some other benefit. Supplier power suppresses innovation because a supplier with power has little reason to innovate, given they are in a controlling position. Or the supplier may choose to reinforce their power by withholding information. The intelligence community may have collection programs whose existence is limited to a small group of people. In the 1998 Kosovo War a senior NATO commander was told of a collection program he did not know existed only after the war started. Had he known of it beforehand he would have changed his campaign plan considerably. The innovation that didn't happen in this case was in strategy, not in technology.

Threat of entry describes the chance that a new player will enter a market. If a new entrant does come in, it obviously increases competition, and thereby lowers profits for those already in the market. A good example is Amazon Web Services (AWS) entering the CIA cloud computing competition in 2013 and beating out IBM. The largest barrier to entry AWS faced was getting people who had the necessary clearances to know enough to bid on this contract. High barriers to entry keep potential rivals from bidding on a contract because they can't easily assemble the necessary skills and information to offer a competitive proposal. For intelligence this is especially critical because it keeps rivals (like AWS) away from a particular market. More, it reduces a government agency's ability to evaluate a proposal because they cannot freely speak with innovators who do not have the appropriate clearances. This, obviously, reduces innovation.

The AWS win over IBM in 2013 is an interesting case because it required the significant backing of a large new player, Amazon, to win the contract. It is doubtful that a small or medium sized company could have displaced IBM. Even with truly superior cloud technology a medium or small firm would have found it difficult to enter the market. Amazon with its deep pockets could do this. Most challengers could not.

One way to deal with the barrier to entry problem is for a "broker" who does understand the government's needs, and who also has the clearances to speak with outside suppliers, i.e. new innovators. Defense private equity (PE) and VC firms have partners who are retired from various agencies and the military services. The PE firm tracks the world of technology. The goal is to spot opportunities in order to link private business outsiders with government insiders. It's a valuable service, which threatens long standing suppliers to the government. The PE's strategy is to spruce up small companies by linking them with new opportunities inside the government, markets which they never could discover on their own because they lack the knowledge and special access clearances.

Valuation of small and medium size enterprises by PE firms is contained in an investment banking "book" which details the assets of the company. The balance sheet, audited financials, physical assets, and the company's intangible assets are in it. This book has an appendix listing the number of employees with TS/SCI clearances and special

compartmented clearances. The more of these the better. It's a measure of a firm's intellectual property (IP) and it has significant positive impact on valuation. Companies without a large set of clearances are at a disadvantage, both in raising investor capital and in the potential for bidding on new business which requires them.

Buyer power deals with the ability to dictate terms to suppliers. Here, the ultimate buyer is a single entity, like the Pentagon, or a three letter agency. In theory, then, buyer power is high because these are what are called monopsonies, a single buyer.

In practice however, buyer power is limited because government is not a smart buyer. It is hemmed in by complex federal regulations. Those inside the government find it difficult to even speak with outside companies if they aren't adequately cleared. This has the effect of shielding existing firms from new competition. The AWS win over IBM was a major surprise to most industry observers since IBM was so thoroughly entrenched in the Federal acquisition system. Nonetheless, AWS had a more innovative approach and won the CIA contract. This win catapulted Amazon's cloud business into leadership in the global cloud computing market.

Substitute products are alternative ways to meet a need or requirement. Uber, for example, is an alternative to automobile ownership. Streaming video substitutes for cable TV. Defense examples include drones as a substitute for manned aircraft. Cyber can neutralize a target instead of a missile strike. Lasers can kill a satellite. Today, substitution is especially important for innovation because there are so many new possibilities arising from all of the new technologies.

But to analyze these substitution possibilities one first needs to know enough about the different technologies. The current security clearance system is built on a need to know basis, for an era when technologies operated in independent vertical silos. This is no longer the case with networked technologies, or with many different (substitute) ways to meet a requirement.

Conclusions

Two conclusions come out of this discussion. First, clearances have multiple roles and this needs to be understood. They are used for business and bureaucratic competitive

advantage as well as to protect national security. Here, clearances have a serious negative effect on innovation. This includes strategy as well as technology innovation.

Second, these impediments to innovation will become a much bigger problem in the future than they are now. There are two reasons for this. First, the defense and intelligence system of the United States is becoming more interconnected. Networks are the name of the game. To plug into these networks one needs to know about the interfaces that link the different subsystems. These are highly classified, but even more, are moving toward greater complexity for cybersecurity reasons. Cyber is the most highly classified area in defense today, like nuclear weapon secrets in the 1950s. This trend will provide a strong boost to supplier power, and it will make deterrents to entry greater.

Another reason clearances and innovation will become more important in the future is that the locus of defense innovation has shifted to a considerable degree to small and medium size enterprises. These are the small firms in Silicon Valley, northern Virginia, Austin, around Route. 128 in Boston, and elsewhere. They tend to be highly specialized and technical. And they have a quite narrow ability to discover defense needs because they don't have a breadth of knowledge or clearances to work outside of their restricted domain.

The larger defense companies can leverage their informational advantage, especially clearances, to squeeze these firms. The big firm says to the small one "Look, we don't care how great your new technology is. We've cornered the clearances and access to NSA -- and you haven't. Cut your price -- or you're out of the contract." Especially in a networked technology world, the small firm needs the larger one as it's the only gateway to large projects.

For a long time I've urged DoD to do a study which asks a simple question: do large defense companies -- the lead systems integrators -- take too much? Are they crushing innovation in the lower tier suppliers? Today I would modify the question slightly to include the new big technology companies entering defense, and the PE and VC firms too. But the thrust of my question is the same. I've never found any interest by DoD in this most fundamental question of innovation: Who gets what?

A final point is worth making. The definition of "innovation" is usually misconstrued to mean something that is new and better. But this isn't a good definition. Innovation requires two

things: something new and better, and someone willing to pay for it. It needs a buyer. The use of clearances to shape and protect a market, deter entry, or to control information for bureaucratic power reasons, is rarely considered in national innovation policy. This has to change if the United States is to leverage its immense technological potential into real military advantage.