LOOSE LIPS BUILD SHIPS?
Secrecy and Human Capital Management in US NSA and Israel Unit 8200

A THESIS

SUBMITTED TO THE

INTERSCHOOL HONORS PROGRAM IN INTERNATIONAL SECURITY STUDIES

CENTER FOR INTERNATIONAL SECURITY AND COOPERATION

FREEMAN SPOGLI INSTITUTE FOR INTERNATIONAL STUDIES

STANFORD UNIVERSITY

By:

Lisa Catherine Wallace

June 2014

Advisors:

Mariano-Florentino Cuéllar

Colonel Joseph Felter

Abstract

How do intelligence organizations attract and make use of top talent? This paper approaches this question through a comparative case study of the labor ecosystems surrounding both the US' National Security Agency and IDF's signals intelligence branch, Unit 8200. As the cyber realm continues to assume a growing role in modern national security threat environments, intelligence organizations must grow and adapt to accommodate these new objectives. This inevitably involves the question of how to attract and make use of top talent in order to solve difficult and highly technical national security problems. Israel and the United States share similar national security interests, and both possess burgeoning and impressive high-technology clusters. This paper claims that a growing, public network of Unit 8200 and other Intelligence Corps alumni is extant in Israel's high-technology sector. Furthermore, affiliation with Unit 8200 has a positive signaling and social capital value. By contrast, this paper argues that alumni from the NSA do not possess as strong of a signaling or social capital value in the US. This paper argues that the NSA is hindered by the ontology, secrecy, and culture of the organization itself, as well as US public understanding of national security organizations and cyber threats. In Israel, this paper suggests that that Unit 8200's associated signaling and social capital value benefits its alumni, Israel's technology sector, and the unit itself. This paper argues that this phenomenon is unusual, and despite the uniqueness of Israel's national security system, is prescriptive for the United States, where social capital and signaling is not directly leveraged by intelligence organizations as a recruiting tool. This paper argues that increasing the professional signaling and social capital value associated with intelligence organization affiliation is good for the organizations themselves by helping attract and make use of talent.

Dedicated to Clifford Nass.

Acknowledgements

My completion of this project would not have been possible without the help of some truly exceptional friends and mentors. First, I would like to thank my thesis advisors Colonel Joseph Felter and Professor Mariano-Florentino Cuéllar, both of whom devoted an extraordinary amount of time and investment into helping me construct and realize this thesis. Tino, I have been continuously amazed by how much I manage to learn from every session we have. Your advice is always so succinct it sounds rehearsed. Thank you for your patience and steadfast support of my project and of me. Joe, your commitment to undergraduate education and teaching is staggering. I learned so many skills about writing, international relations, and project conceptualization from your mentorship this year, skills that will stay with me long after I graduate. This is only surpassed by what you have taught me about leadership, which will stay with me even longer. Thank you.

I am also incredibly thankful to Dr. Martha Crenshaw and Dr. Coit Blacker, the Co-Directors of the CISAC Honors Program. I have learned more than I can say from their mentorship and teaching of the CISAC Honors class. Both Professor Blacker and Professor Crenshaw are true examples of world-class academics, and it has been a privilege to learn from them this year. Special thanks to our TA Shiri Krebs for encouragement and last-minute assistance with logistical details.

Separate from the official advisors to this project, I would like to thank a number of individuals associated with CISAC who were enormously helpful in the completion of this thesis. I absolutely could not have completed this project without the help of Ryan Mayfield. Ryan's advice, editing, and moral support was absolutely invaluable. Additionally, I am truly grateful for Tim Junio's support, counsel, and friendship over the course of the past year. Thank you to Neil Narang, Patrick Cirenza, and Peter Davis for watching me rehearse my presentation and providing helpful feedback. Thank you very much to Gil-li Vardi and Amir Goldberg for initial discussions of this project and its disciplinary approach. Thank you to Russell Wald for keeping my project and research interests in mind and helping with interview scheduling.

Special thanks to the cyber contingent of the CISAC Honors Program. Mailyn Fidler was invaluable with editing these chapters and extraordinarily generous with her time and support. Connor Gilbert helped significantly in project framing and keen input. I would also like to thank the rest of the CISAC cohort, Yassamin, Claire, Isabella, Lauryn, Elle, Daniel, James, Reed, and Keshav, for their friendship and mentorship. Small Unit Cohesion is a great thing.

Finally, I would like to thank Marc Abramowitz, Yitz Applbaum, and Nimrod Ran for their help securing interviews and opportunities in Israel. I am forever grateful for those experiences and favors.

Table of Contents

Table of Figures

Chapter 1: Introduction

On October 11, 2012 former Secretary of Defense Leon Panetta delivered the keynote address to the annual meeting of the Business Executives for National Security in New York City. The subject of his address was the growing cyber security threats plaguing the United States Intelligence Community in the 21st century. During his speech he likened the reality of cyber threats to the terrorist threats plaguing the City of New York, promising the audience that just as a 9/11 would never again happen, Americans would also be protected from cyber disasters. Explained Secretary Panetta, “Just as the DoD developed the world’s finest counterterrorism force over the past decade, we need to build and maintain the finest cyber operations. We’re recruiting, we’re training, and we’re retaining the best and brightest in order to stay ahead of other nations.”[1] The cyber age brings with it extraordinary threats to the national security of all nations and presents complex challenges for intelligence organizations in deterring and defending against these threats. Intelligence organizations must grow and adapt to respond to emerging cyber threats, and so too must their human capital approaches to insure they are able to recruit and retain the level of expertise needed to meet these historically unprecedented demands.

Each nation is subject to intelligence environments with unique constraints and limitations. But two significant challenges plague the strategies of all intelligence organizations to maximize the quality of their human capital: the necessity to maintain effective secrecy, and to attract skilled and competent knowledge workers. In the cyber age, the importance of attracting

[1] Panetta, Leon. "Remarks by Secretary Panetta on Cyber Security to the Business Executives for National Security, New York City." Address, Business Executives for National Security from Department of Defense, New York City, October 11, 2012.

the best and brightest into intelligence organizations becomes just as critical to national security as effective cyber technology itself. A recent CSIS report illustrates this, contending that the cyber age represents a human capital crisis for intelligence communities for this reason: "We need to be clear why human capability is so important. Tools and techniques…help greatly, but we will continue to need capable personnel to create such tools…If we have learned nothing else, we now know that those who seek …to do us harm… are every bit as smart as we are."[2] New human capital challenges of intelligence organizations inform to the central question of this thesis: How do differences in secrecy policies and human capital strategies impact on intelligence organization's ability to attract top talent?

To answer this question, this thesis conducts an organizational analysis of the human capital ecosystem surrounding two intelligence organizations with very different approaches to secrecy and human capital: the Israel Defense Forces (IDF) Unit 8200 and the US National Security Agency (NSA). This thesis finds that the NSA and Unit 8200 have two fundamentally different approaches to human capital management and argues that these differences impact on their recruitment and retention of highly skilled members. The NSA prefers to "home grow" labor with technical skillsets, encouraging them to stay for the duration of their careers. Secrecy surrounding employment is practiced and enforced. Their counterpart organization in Israel, on the other hand, has a relatively unenforced policy of secrecy. Identification with secret units like Unit 8200 is technically illegal but rarely carries repercussions in a professional setting. In Israel, there exists a publically observable network of Unit 8200 alumni in the high-technology sector.

[2] Full quote is the following: "Tools and techniques, like automated configuration and patch management, help greatly, but we will continue to need capable personnel to create such tools, and to handle those issues not subject to automated detection and response. If we have learned nothing else, we now know that those who seek to exploit our weaknesses for gain, to do us harm, or even just for mischief, are every bit as smart as we are."
Evans, Karen, and Franklin Reeder. "A Human Capital Crisis in Cybersecurity Technical Proficiency Matters." *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* x (2010): 5.

Unique organizational features of Unit 8200 are observable in this network, and manifest as recognized positive attributes of alumni as knowledge workers in the business world. The efficacy of these features in the business world, combined with the positive signaling power of association with this network, perpetuate and reinforce the existence of the network within the Israeli technology sector.

This thesis argues that secrecy policy remains unenforced because knowledge of Unit 8200's alumni network and the positive signaling power for Unit 8200 alumni is beneficial for Unit 8200 itself. By contrast, this thesis argues that there does not exist a comparable public network of NSA alumni in the United States high-technology sector, and that the NSA's secrecy approach is a contributing factor to this lack of development.

Argument

This thesis argues that intelligence organizations with an observable network, leverageable by members and alumni, can foster positive signaling and network benefits that provide advantages for both the affiliates of the organizations and the organizations themselves by helping to attract top talent. All intelligence organizations must optimize over two constraints: the need to manage secrecy and the need to attract top talent. This project shows that the human capital strategies among different intelligence organizations can have puzzling variance. In the case of Israel's Unit 8200, an unenforced policy of secrecy with regard to its human capital exists. Although official policy mandates that the identities of Unit 8200 members and alumni remain secret, this policy is not actively enforced, posing few repercussions for unit alumni and other members of Israeli society to perpetuate public information about the network. Intelligence alumni and operatives voluntarily make public their association with the unit because there are positive network effects to a reinforced Unit 8200 network. This case demonstrates that Israel

Unit 8200’s unenforced policy of secrecy with regard to its human capital contributes to an observable, public network of its alumni in the Israeli high technology sector, and that this network has positive effects for both its members and the unit itself.

The other case presented in this thesis – the US National Security Agency – describes a much different strategy for human capital management, in which formal secrecy policy broadly correlates with the observed behavior of NSA operatives and alumni. As a result of its different approach to balancing the tradeoff between secrecy and attracting top talent, the NSA does not enjoy a similar public network of alumni in the US high-technology sector and its members do not reap similar networking and signaling benefits in their professional lives outside of the NSA. This thesis argues that strong network effects for intelligence alumni also benefit the intelligence organizations themselves by aiding in the attraction and maintenance of top technical talent. These network effects are fostered when intelligence organizations incorporate loosened policies of secrecy with regard to human capital.

Methodology

A central premise of this thesis is that as cyber threats increase, proliferate and evolve, intelligence organizations must grow and adapt to address new threat environments. These adaptations include those relating to human capital and its associated secrecy concerns: a US intelligence official opined that “A critical element of a robust cyber security strategy is having the right people at every level to identify, build and staff the defenses and responses. And that is, by many accounts, the area where we [the US Intelligence Community] are weakest.”[3] It is in the best interests of states to insure they are constructing the best policies and incentives to attract a

[3] Evans, Karen, and Franklin Reeder. "A Human Capital Crisis in Cybersecurity Technical Proficiency Matters." *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* x (2010): 1.

strong and competent technical labor force to defend against cyber threats. This prerogative is made all the more serious in the 21st century, an era in which the gravity and stakes of cyber threats continue to worsen.

In order to understand how human capital strategies work to attract top talent into intelligence organizations, this thesis will conduct a comparative case study of two intelligence organizations with differing approaches to human capital management. Analysis of these cases draws upon organization theory and qualitative social network theory to understand the human capital strategies of each intelligence organization and how the implications of these strategies manifest in their respective human capital ecosystems. The findings these cases seek to inform how different approaches to human capital management can best encourage top technical talent to devote time to national service.

The first case of this study will qualitatively analyze the labor ecosystem surrounding the United States' National Security Agency in the context of the agency's overall human capital strategy and secrecy policy. This case demonstrates an organizational approach to human capital wherein secrecy policy more seriously limits how employees and alumni identify organizational affiliation, job training, and experiences. The second case of this study will qualitatively and quantitatively analyze the labor ecosystem surrounding the Israel Defense Forces' Unit 8200. Unit 8200 is a case that illustrates different approach to human capital strategy from the US NSA, where a secrecy policy puts fewer constraints on public affiliation with and information about the unit. As part of the secondary case, empirical survey evidence will demonstrate a public network of Unit 8200 alumni within Israel's broader high-technology ecosystem its associated effects. This empirical data will inform a qualitative analysis of Unit 8200, its impact in Israel's technology sector, and the role of its human capital strategy.

Significance

This thesis provides qualitative and empirical evidence that different approaches to managing secrecy within intelligence organizations can have a significant impact on these organizations' ability to attract and retain high quality talent. It provides an organizational analysis of the talent ecosystems surrounding two intelligence organizations with differing human capital strategies. Its findings contribute to the body of knowledge surrounding intelligence communities and high-technology industries, which represent primary labor markets with which intelligence organizations must compete for talent in the cyber age. In addition, this study contributes to the field of international security in two broader ways. First, this work combines organization theory and theories of information and networks to improve our understanding of how military organizations and their alumni networks interact. Second, it raises awareness of the impact that network effects of secrecy policy can have on the human capital strategies of intelligence organizations. The threats faced in the cyber age demand that highly technical knowledge workers have incentives to devote time to national service in intelligence organizations. This comparative analysis demonstrates the value of one approach to creating favorable incentive structures to attract the best and brightest.

Road Map

The next chapter of this thesis provides readers with a conceptual framework for understanding the human capital strategy of intelligence organizations through the lens of organization theory. This chapter will detail recent work on networks and social networks, and their role in the function and strategy of organizations, as well as define the labor economic concepts behind signaling theory. Chapter Three builds in a cultural context for Unit 8200 as an intelligence organization, which will inform the phenomenon of Unit 8200's increasing publicity in the high-technology community. This will include a brief historical analysis of Unit 8200, contextualized by an overview of the historic and strategic role of the Israeli military in the development of Israel's economy, and particularly the development of its high-technology cluster. This thesis argues that public shifts of focus on public and private cyber security enterprise is newly topical to the role of signals intelligence alumni in society, giving new power to public Unit 8200 alumni status. At the same time, the cultural phenomenon of Unit 8200 in the modern cyber age is in keeping with Israelis historic strategic culture.

Working from a contemporary context of cyber-security in society, this thesis will then develop a two-part organization theory for the role of Unit 8200 in modern society in chapter four. The first part of this theory will draw upon signaling theory and current understanding about the diffusion of information throughout networks to help shed light on why it is that Unit 8200, and Unit 8200 alumni, have become so public. This theory will argue that there is a positive signaling incentive for members of this network to declare association and perpetuate public knowledge about the unit. In addition this theory will argue that these positive signalers benefit Unit 8200 as well, which accounts for why the policy of secrecy surrounding Unit 8200 appears largely unenforced. The second part of this theory will attempt to distill the organizational facets common to the Unit 8200 alumni network, and how they might function in the Israeli technology community. This theory will be tested against a qualitative social network analysis of Unit 8200 in the Israeli intelligence community. Although Unit 8200 is the case this thesis will use as evidence when building out a broader conceptual theory, this thesis is not limited to a theory of Unit 8200. Instead, the theory built out in chapter four will be used throughout to help explain how all intelligence organizations might attract and retain top talent by leveraging organizational principles like signaling, social capital, and networks.

Finally, this thesis will conduct a comparative case study of the strategy and secrecy policy surrounding the human capital ecosystems of Unit 8200 and US NSA. This study will consider the effect of NSA experience in Silicon Valley, a primary labor market with which the NSA competes for talent, examining any apparent network effects and signaling value of NSA association, as well as whether this signaling value benefits the NSA itself in addition to its affiliates. This thesis will explore the human capital strategy of the NSA and Unit 8200 with a particular focus on secrecy policy and its enforcement. This thesis will seek to analyze the impact of secrecy and human capital strategy on the network effects and signaling value of NSA experience, in order to give context to what this means for both the NSA and the US technology sector. Through a comparison of two different human capital strategies in two different signals intelligence organizations, this thesis aims to gain leverage on the significance of secrecy and human capital to the strategy intelligence organizations in the cyber age.

Chapter 2: Conceptualizing Human Capital in Intelligence Organizations

This thesis endeavors to understand how intelligence organizations attract and make use of their human capital; i.e., highly technical knowledge workers. In order to gain leverage on this question, this project uses organization theory to examine how the human capital strategies of intelligence organizations manifest within the organizations themselves and in their public alumni networks. Reviewing the literature, it is clear that the human capital strategy for intelligence organizations is primarily an optimization problem. All intelligence organizations are unique and subject to their own limitations. However, two constraints are common across intelligence organizations: the need to manage secrecy and protect classified information; and second, the need to attract people with highly technical skillsets.[4] This chapter presents a broad overview of organization theory, specifically as it relates to social networks and their effects. To this end, this chapter will include an overview of signaling theory and social capital theory, as well as detail current understanding within organization theory of social networks and their effects. The intent of this chapter is to present a framework for conceptualizing the visible effects of human capital strategies in intelligence organizations and their networks.

[4] This chapter does not discuss in detail the breadth of literature on secret intelligence organizations. The literature on secrecy policy generally centers on the protection of citizens' rights to know and civil liberties. From a human capital perspective, writing on secrecy policy particularly in the United States concerns insider threat liabilities. The influence of secrecy policy to intelligence organizations' and operatives' signaling value represents a gap in the literature through which this project can contribute. For further reading on secrecy, the following sources are useful:
Lowenthal, Mark M.. *Intelligence: from secrets to policy*. Washington, DC: CQ Press, 2000.
O'Connell, Anne. "The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World." *California Law Review* 94, no. 6 (2006): 1655-1744.
Reducing Government Secrecy: Finding What Works. Steven Aftergood. *Yale Law & Policy Review*, Vol. 27, No. 2 (Spring, 2009), pp. 399-416

Organization Theory

Organization theory deals with the structure, culture and dynamics of organizations, and how these variables affect an organization's endogenous and exogenous impact in space. As sociologist Luther Gulick explains in "Notes on the Theory of Organization,"[5] the foundations of an organization's structure is its internal division of labor; this division involves both the internal hierarchy of labor and the actual work being completed by each individual. The efficacy of an organization's hierarchy and division of labor depends on the size of the organization and levels of uncertainty in its environment of productivity.[6] Organizations that operate in more uncertain environments require greater degrees of adaptability in order to remain effective organizations. This means that the barriers of hierarchy within an organization must be sufficiently low such that institutional change can be dynamic in real-time. At the same time, a legitimate balance of power must be maintained.[7] When understanding the makeup of Israel's Unit 8200 and the US NSA as intelligence organizations, neoclassical organization theory will be useful. The organizational assumptions, behaviors and cultures implicit to the organization based off of how the organization works will inform the impact of that organization's network. For example, understanding the organic nature of Unit 8200's network, its internal culture, its hierarchy and managerial practices as well as the organizational theory of the reserves influence will all inform the role of its human capital strategy, and in turn, the impact of the Unit 8200 alumni network on Israel's high-technology sector. Likewise, the NSA's characteristics and limitations should provide a basis for comparison and analysis within organization theory. The primary

[5] Shafritz, Jay M., and Philip H. Whitbeck. "Notes on the Theory of Organization." In *Classics of Organization Theory*. Oak Park, Ill.: Moore Pub. Co., 1978. 86-95.

[6] Shafritz, Jay M., Philip H. Whitbeck, and James D. Thompson. "Organizations in Action." In *Classics of organization theory*. Oak Park, Ill.: Moore Pub. Co., 1978. 287-301.

[7] March, James G., and Michael D. Cohen. "Leadership in an Organized Anarchy." In *Classics of Organization Theory*. Oak Park, Ill.: Moore Pub. Co., 1978. 385-399.

methodological tools used in this thesis will be taken from the doctrine of organization theory; namely, signaling theory, and network analysis. The sociological ideas of cluster genesis and population ecology also inform analysis of the impact of the Unit 8200 network on Israel's high-technology sector.

In organization theory, a "cluster" is a "'geographically proximate group of interconnected companies, suppliers, service providers and associated institutions in a particular field, linked by externalities of various types.' This definition indicates that a cluster is concentrated in a region… it may not be connected to only one industry but may include supply chains that connect firms of very different industries."[8] This describes Israel's regional technology sector as well as the US Silicon Valley, which both involve a high concentration of firms and organizations in a concentrated geographic location focused on high-technology. The saturation of the Unit 8200 and NSA alumni network within their respective regional technology clusters constitutes an associated institution that is not a competing technology firm, but a separate institution with certain institutional externalities that interact with the cluster environment at large. Silicon Valley and Israel's high-technology sector were chosen for analysis in this project not because they are examples of labor markets with which both Unit 8200 and the NSA compete for and interact with technical human capital talent.

Another important theoretical concept within organization theory is population ecology. Population ecology concerns the impact of environment on organizations. Network externalities in population ecology facilitate a greater flow of information exchange in an environment, affecting not only the organizations extant within that environment but the network itself. A sense of population ecology allows us to examine and identify the systems within an

[8] Blien, Uwe, and Gunther Maier. "The Starting Point." In *The economics of regional clusters: networks, technology, and policy*. Cheltenham, UK: Edward Elgar, 2008. 3.

environment that produce exchanges of labor, knowledge and information.[9] This sort of exchange is detailed in the hypothesis of this paper, wherein the Unit 8200 network within the environment of Israel's high-technology sector fosters and accelerates the velocity of exchange between these organizations. Understanding population ecology and cluster genesis together provides a sociological framework for thinking about the cases of the US NSA and the Unit 8200 networks within their high-technology labor markets.

Signaling

A central concept within organization theory relevant to this research project is signaling theory. Signaling theory in the labor market is generally understood as the phenomenon by which employers consider individuals in relation to their credentials in the labor market. In "Job Market Signaling," a classic 1978 paper in this field, author Michael Spence identifies elite universities as signalers in the job market.[10] In the face of uncertainty, e.g. an asymmetry of information between a prospective firm and an individual regarding an individual's capabilities, academic degrees can serve as positive signalers of a certain set of assumptions or skills the individual is likely to have. In other words, the signaler of an academic institution serves as a proxy metric of an individual's competence, indicating the likely possession of certain skillsets. Signaling theory is manifested in situations wherein a graduate from an elite institution, such as Stanford or Harvard, might be given greater consideration for a job than a candidate from a state college by virtue of the completion of that degree. My argument is that alumni status of Unit 8200 serves as a positive signaler in the Israeli high-technology industry, much like a degree from an elite academic institution might be signaling in the United States. Likewise, all

[9] Hannan, Michael T., and John Freeman. "The Population Ecology Of Organizations." *American Journal of Sociology* 82, no. 5 (1977): 929-964.
[10] Spence, Michael . "Job Market Signaling."*Quarterly Journal of Economics* 87, no. 3 (1978): 355-374.

intelligence organizations, including the US NSA, possess the capability to cultivate an elite signaling value association as employers of highly technical human capital labor. As documented in other organizations, such with elite schools, signaling value is a beneficial component to attracting top talent into intelligence organizations.

Networks

Networks are an important topic of study in organization theory because they compose the infrastructure of relationships in across society and with organizations. Relationships that are endogenous to an organization are considered informal in organization theory. Conversely, relationships that are exogenous to an organization are considered formal.[11] This thesis is interested in the analysis of networks formed by intelligence organization human capital. Particularly, this project will examine the formal and informal networks created by human capital around two intelligence organizations, and the associated signaling and network effects that these networks provide for their members. This analysis will be considered alongside an analysis of the human capital strategies of each organization case.

The effects of networks on their members are a widely studied topic of organization theory. Many network effects are well established in the literature and relate to the points of analysis of this thesis. This thesis holds that less stringent policies of secrecy, as they relate to human capital within intelligence organizations, contribute to the establishment of beneficial networks for affiliates and intelligence organizations themselves. This hypothesis holds that these network effects include enhanced social capital and signaling value associated with affiliation with an intelligence organization.

[11] Waldstrøm, Christian. *Informal networks in organizations: a literature review*. Aarhus School of Business, Department of Organization and Management, 2001.

This hypothesis is enforced by key findings in organization theory. First, a key idea in organization theory is that networks give social capital to their members.[12] This is because networks tend to be created around things that are desirable and exclusive.[13] Additionally, networks create environments of trust, where members often help each other out.[14] This creates a beneficial incentive for members to participate in desirable professional networks. It also creates an externality of networks that go beyond benefitting just the people who make up networks. The principle of assistance among network members contributes to the important role networks play in the development of high-technology industries.[15] And finally, networks cause status gradients in markets.[16] This means that networks create a credential for those who are part of the network, as networks themselves tend to be created around affiliations or characteristics that are desirable and exclusive. Because networks are seen as desirable, it benefits people who are in them, and in turn any affiliated organizations, because new members are incentivized to and benefit from being able to join.[17] When we think about the problem of intelligence organization human capital management, networks become a very important point of study for two reasons. First, networks are created and perpetuated by the strength of the relationships between their individual members, or nodes. Secrecy policy, particularly related to human capital, creates a friction around the establishment of a network by limiting its affiliating characteristics and potentially the richness of the interactions between members. And second, the credentials and status

[12] Burt, Ronald S. "The network structure of social capital." *Research in organizational behavior* 22 (2000): 345-423.

[13] Bourdieu, Pierre. "Social space and symbolic power." *Sociological theory* 7, no. 1 (1989): 14-25.

[14] Uzzi, Brian. "Social structure and competition in interfirm networks: The paradox of embeddedness." *Administrative science quarterly* (1997): 35-67.

[15] Ahuja, Gautam. "The duality of collaboration: Inducements and opportunities in the formation of interfirm linkages." *Strategic management journal* 21, no. 3 (2000): 317-343.
Owen-Smith, Jason, and Walter W. Powell. "Knowledge networks as channels and conduits: The effects of spillovers in the Boston biotechnology community." *Organization science* 15, no. 1 (2004): 5-21.

[16] Podolny, Joel M. "A status-based model of market competition." *American journal of sociology* (1993): 829-872.

[17] Podolny, Joel M., and Karen L. Page. "Network forms of organization." *Annual review of sociology* 24, no. 1 (1998): 57-76.

associated with networks of elite labor markets is a leveregeable asset for competitive firms. When we think about intelligence organizations as consumers of human capital, of which the best and brightest is a scarce resource, understanding intelligence organization networks are thus a crucial component to understanding the human capital strategies of organizations.

This study is interested in how intelligence organizations manage constraints to create optimal human capital strategies for attracting top talent. Non-intelligence organizations that need to attract top talent enjoy the benefit of working on non-national security critical work, and are thus more capable of speaking publically about their employees or workflows. As a result, the endogenous and exogenous networks of their labor pool are more easily leveraged to generate social status and prestige. Intelligence organizations must operate under conflicting prerogatives: they must construct effective human capital secrecy policy to manage extreme security liabilities, and they must sufficiently attract top talent to carry out their work. To examine these strategies, this thesis will first present a theoretical argument for intelligence human capital networks by presenting a theoretical framework of the example of Israel's Unit 8200. Then, this theoretical argument will inform the analysis of two cases of intelligence organizations very different approaches to human capital, the United States NSA and Israel's Unit 8200. Through these cases, this thesis hopes to better understand how intelligence organizations employ diverse strategies to attracting top technical talent.

Chapter 3: Working for the Surveillance State: the US National Security Agency

On a quiet thoroughfare off Interstate 280, a long row of non-descript office buildings sits off the street, their building facades further obscured by shady eucalyptus trees. They could easily go unnoticed but for the impressive cadre of luxury cars assembled in their parking lots, and the infamous zip code that betrays total anonymity. The road is Sand Hill, and the buildings are the flagship offices of some of the largest venture capital funds in Silicon Valley, each representing billions of dollars of funds under management.

The deceptive visage of Sand Hill Road is not unlike the scene at Oren Falkowitz' previous place of employment. The United States National Security Agency is concealed within long clusters of homogenous buildings in Fort Meade. The absence of a looming edifice gives no indication of the NSA's prominent role in national security, as the primary signals intelligence organization of the US Department of Defense.[18]

In 2012 when Falkowitz first sought out seed funding for his NoSQL[19] database startup SQRRL, he flew out to Silicon Valley constantly to meet with investors and attend startup events. Around the backside of one building, incubator office space housed a small mixer for enterprise software startup founders. Scruffy Californians in threadbare blue jeans and company t-shirts fraternized with older, more polished investors. Like usual, Falkowitz stood out in NSA classic white collar.

[18] "Organization of the Department of Defense." Organization Chart. *Department of Defense* (2012).

[19] NoSQL stands for "not only SQL databases" which are increasingly popular in big data applications.

In the beginning Falkowitz attended lots of these events. At first, he was dismayed to find a dearth of enterprise software founders in Silicon Valley with experience working in the industries for which they ostensibly created products. More puzzling to Falkowitz was that, on average, he was significantly more likely to come across other founders with experience in Israeli intelligence, specifically Unit 8200, than he ever was to come across founders with NSA experience. Falkowitz could not believe that the alumni of a small intelligence branch in the middle of the Middle East had penetrated Silicon Valley more fully than even the NSA itself, an American organization with much larger numbers.[20]

In many ways, Israel and the United States' national security environments are very similar. Both have similar national security interests, and the two countries regularly collaborate in intelligence.[21] It can be argued that the United States is Israel's biggest ally, and Israel is considered one of United States' biggest allies in the Middle East.[22] Additionally, both countries host impressive high-technology clusters, leading both to disproportionally contribute to global high-technology innovation. Israel leads the world in patents and Ph.D.'s per capita.[23] The United States and Israel lead the world in the highest number of engineers per capita.[24] Yet, the human capital serving the high-technology clusters in Israel and the United States have very different relationships to their respective intelligence communities.

This chapter presents one case study of an intelligence organization's approach to human capital, providing an analysis of the labor ecosystem surrounding the NSA and its relationship to the US high-technology sector. This case begins with an overview of the NSA and its projected

[20] The size of the IDF, its Intelligence Corps, or Intelligence Unit 8200 is not released by the IDF. The relatively smaller size and more limited resources of Unit 8200 compared to the NSA was alluded to in interviews with both directors of Unit 8200 interviewed to in this thesis.

[21] Greenwald, Glenn, Laura Poitras, and Ewen MacAskill. "NSA shares raw intelligence including Americans' data with Israel." *The Guardian*. Guardian News and Media, 12 Sept. 2013.

[22] "Is Israel Really America's Ally?." *Foreign Policy*. N.p., 20 June 2011.

[23] Israel Diplomatic Network. "Israel Innovation Report." Page 9.

[24] The Economist Newspaper. "Punching above its weight." The Economist. 10 November 2005.

challenges as cyber threats grow and alter the American national security landscape. This is followed by brief historical context regarding the development of the US high-technology sector and its relationship with the NSA. Finally, the NSA, its labor force, and alumni are analyzed in comparison with Unit 8200, operating from the case study framework put forth in Chapter 4.

This case demonstrates that the NSA represents an intelligence organization with a distinct approach to secrecy policy and human capital management. The NSA seeks to "home grow" its technical labor force with desirable skillsets, encouraging employees to devote their working lives to service to the organization. Policies of secrecy regarding organizational affiliation are strictly enforced and limit what employees and alumni can and cannot say about their intelligence affiliation, job training, and work experiences. These policies correlate with a dampened public presence of NSA alumni within the high-technology sector. The NSA's approach to attracting and making use of technical talent is not projected to scale proportionate to growing and evolving cyber security threats. To this end, this chapter highlights pain points to the NSA's current approach, impediments to its organizational adaptation, and calls into question the role and scope of secrecy in the human capital management of US intelligence organizations.

The Cyber Age

The central premise of this thesis is that as cyber threats increase, the necessity for cyber preparedness will require state intelligence organizations to adapt. The organizational change needed in intelligence organizations is profound, and chief to its success is a plentiful labor force of persons with technical skillsets.

Cyber- and computer-related jobs are increasing in all industries. According to the National Bureau of Labor Statistics, job growth for information security analysts and other computer engineering careers are slated to increase significantly faster than other employment areas for the foreseeable future.[25] These sorts of positions are highly technical, usually requiring advanced training including bachelors or other advanced degrees. A current dearth of qualified personnel to accommodate this job growth is already damaging business in the transition to the cyber age, as fewer and fewer business owners and IT professionals feel equipped to keep up with the security threats of a rapidly evolving domain.[26] The public sector's cyber needs are subject to the same challenges as those of the private sector; in the United States, where the military and Defense Department rely on a professional force, US intelligence organizations compete with private sector companies for the same labor force.

The introduction of the cyber world has transformed our way of life—it has become the forum through which we communicate, store information, and house our wealth. With this new domain of interaction comes a new prerogative for American intelligence organizations to not only have strong IT systems themselves but also to protect national interests and interests of American citizens in the cyber world. A key resource for the US government's ability to do this is human capital. A recent report by the CSIS Commission on cyber security argued that the cyber age will increasingly cause a human capital crisis in the US intelligence community, including the NSA. The report argued that the fundamental component to a successful cyber security strategy is not just the technologies themselves, but the right people in place in intelligence organizations to implement those strategies: "While billions of dollars are being spent on new technologies to secure the US Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine

[25] U.S. Bureau of Labor Statistics. "Summary: Computer and Information Technology Security Analysts." U.S. Bureau of Labor Statistics.
U.S. Bureau of Labor Statistics. "Summary: Computer and Information Technology Software Engineers." U.S. Bureau of Labor Statistics.

[26] "Study Reveals Cyber Security Teams are Bogged Down with Tactics Not Strategy." TEKsystems. October 16, 2014.

success."[27] Operating under this notion, the human capital strategies of intelligence organizations, and the associated incentive structures they create for attracting the best and brightest, cannot be underestimated when evaluating the effectiveness of 21st century national security strategies for intelligence organizations.

To be clear, cyber operations are not the only or even the primary workflow of the US Department of Defense, the NSA, or even IDF Unit 8200. But the proliferation of cyber workflows in intelligence organizations, and more broadly the introduction of the cyber domain, profoundly reveals the importance of human capital to the success of intelligence organizations—now more than ever. In this light, this chapter seeks to understand how the NSA currently attracts and makes use of technical talent, and if and how this strategy may be problematic as the cyber age advances.

The Agency

The National Security Agency is the primary signals intelligence and information assurance arm of the United States Government.[28] The agency was established in 1952 in response to the Brownell Committee Report, which found the contemporary processes for signals intelligence and processing ineffectual.[29] The creation of the NSA became the solution for more executive control over signals intelligence activities in the US government. From 1952 through its early years, the NSA functioned as a signals collection and analysis organization that worked across branches of the US Government and armed forces.[30] Early signals intelligence workflows drew upon more mathematical skillsets like cryptography. Overtime, signals intelligence

[27] Evans, Karen, and Franklin Reeder. "A Human Capital Crisis in Cybersecurity Technical Proficiency Matters." *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (2010): V. Print.
[28] "About NSA." NSA. http://www.nsa.gov/about/index.shtml (accessed May 27, 2014).
[29] George Washington University. "The National Security Agency: Declassified." The National Security Archive.
[30] *Ibid.*

workflows evolved alongside the Information Age, incorporating more and more computing activities. According to Bill Lin, the proliferation of computing workflows today renders the distinction between “cyber” and the analysis component of signals intelligence largely territorial.[31] Since 2009 the director of the NSA has also served as commander of US Cyber Command, which is housed at Fort Meade and seeks to coordinate cyber prerogatives between its parent node, US Strategic Command, and the Department of Defense.[32] Thus, the human capital from which the NSA is interested includes persons with technical and computing skillsets, capable of cyber work.

Case Limitations

This thesis is interested in understanding how intelligence organizations attract and make use of technical knowledge workers. A study that compares the human capital environment across intelligence organizations inevitably faces many limitations, as the manner in which intelligence is managed organizationally is different in different countries. Comparison between the two cases of this thesis is limited by the enormous differences between the two countries and their associated intelligence communities. The United States is a global superpower, geographically much larger, with more ethnic pluralism. Israel is a much smaller country, a geography where the technology industry and military activity functionally overlap. While the two countries share many of the same Middle Eastern intelligence interests, it follows that the United States has both the resources and the scope of power to support broader interests and activities.

[31] Interview, Bill Lin.

[32] "Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Cyber Military Operations." *The Secretary of Defense* (Declassified 2009): 1-3.

Comparison between US NSA and IDF Unit 8200 are equally limited by differences in the organizations themselves. It is reasonable to assume that Unit 8200 is significantly smaller than US NSA, commensurate with the size of country, GDP and resources. Unit 8200 conscripts its human capital, while the NSA recruits a professional force. Unit 8200 is housed within the Israel Defense Forces—rendering it a military organization. By contrast, the NSA is a subdivision of the Department of Defense. Although not technically military, it was conceived in order to improve upon a predecessor organization housed by the military, and in its founding directives included coordination with the military.[33] Today, US Cyber Command further underscores communication between the NSA and the military. Of course, the NSA is not the only intelligence organization in the United States, nor is it the only intelligence organization in the United States focusing on signals intelligence and cyber collection and analysis. Likewise, IDF Unit 8200 is not the only intelligence organization in Israel, nor is it the only intelligence organization focused on signals intelligence and cyber activity.

Despite significant difference, this thesis argues that Unit 8200 and US NSA bear sufficient similarities for a comparison between the two organizations to be suggestive. But similarity is not why the two cases were chosen. Especially in this day in age, human capital management is a huge issue for the NSA and the United States intelligence community at large. It is well understood that recruitment to the NSA is only projected to worsen, particularly as American intelligence organizations get larger and cyber threats become more serious.[34] Unit 8200 was chosen as a comparative case not because it faces a similar recruiting environment to the NSA; rather, it was chosen because the hypothesis of this study posits that an intelligence organization's human capital strategy, very similar to that used by Unit 8200, would support

[33] "National Security Council Intelligence Directive No.9: Communications Intelligence." *National Security Agency* (1950): 1-3.
[34] Interview, Bill Lin.

alleviating such a recruitment crisis in a free labor economy. While attracting top talent is an important issue in Israel, IDF Unit 8200 has the luxury of recruiting out of a draft. Instead, Unit 8200 is an interesting comparative case for its unusual relationship with its labor pool, and by courtesy, the high-technology industry. While the NSA is famously one of the most secretive organizations in the world, Unit 8200 appears to have a loosened policy of secrecy among its alumni.[35] This thesis argues that this loosened secrecy of Unit 8200's alumni contributes to the alumni of the units' striking ability to brand themselves and the unit itself. This phenomenon of signaling and branding is valuable for attracting technical talent in a knowledge economy. While this currently plays out in Israel, branding is a phenomenon of technical knowledge management that could also be beneficial in the recruitment of a professional force in a free labor market, such as is the case in the United States.

The Network

The NSA does not have a public network of alumni in the high-technology industry that compares to the public network of alumni of Unit 8200 in Israel's high-technology sector. Much of Israeli society is organized around military unit association (or lack thereof). As the vast majority of non-Arab Israelis spend the first few years of their working lives out of high school in the army, much of their initial adult connections are influenced by connections made in the army.[36] Given that most IDF units are not intelligence units and therefore not secret, these connections are a significant part of Israeli culture, work culture not excluded.[37] This is not true of the United States, where the military and intelligence community is a professional force.[38]

[35] George Washington University. "The National Security Agency: Declassified." The National Security Archive.
[36] These ideas are documented in the comparative case of this study.
[37] See empirical findings in the comparative case of this study.
[38] It should be reiterated here that not every citizen in Israel goes through the army. Muslim Israelis are neither conscripted nor permitted to enlist.

This cultural phenomenon is reflected in the lack of alumni organizations in the United States, including those that might be organized by the NSA or US Government, and more organic online groups such as through Facebook and LinkedIn.[39] As we see in Chapter 5 of this thesis, there are several alumni groups started by alumni online hosted through LinkedIn, Facebook, MeetUp, and other online forums, as well as a formal alumni association of Unit 8200 alumni (for which the identities of the group members are concealed to those outside the group), there is no such phenomenon for former NSA alumni.[40] At the time this thesis was published, a mere 484 employees listed their employment at the verified employer NSA on LinkedIn, a tiny fraction of what is thought to be the size of the organization.[41] This can be contrasted with the organizations on LinkedIn and Facebook for Unit 8200 for which there are thousands of members, for an organization much smaller than the NSA.[42]

The dearth of a public alumni network of NSA alumni in the US high-technology industry is both predictable and peculiar. Certain characteristics endemic to the United States limit the ability for NSA alumni to saturate the technology industry, but not to penetrate it. One primary component is sheer numbers. The NSA is estimated to employ 35,000-55,000 employees in total, including military and civilian employees.[43] The United States high-technology industry is considered the world leader, with an estimated market size of over $170

"Israel: Supreme Court Decision Invalidating the Law on Haredi Military Draft Postponement." *The Law Library of Congress: Research and Reports* (2014).

[39] Falkowitz, Oren. Personal Interview. Palo Alto, CA. 20 March 2014.

[40] As far as this research can tell, there exists no online or offline intentional network of NSA alumni. The existence of these groups was explored through research; additionally, no NSA alumni interviewed for this thesis was aware of the existence of any groups.

[41] "National Security Agency." LinkedIn. https://www.linkedin.com/company/1359?trk=prof-0-ovw-prev_pos (accessed April 15, 2014).

[42] A verified page or employer on LinkedIn deals with entity resolution; it is a way of making sure employer names on different profiles collect in the same place for data management purposes. Unit 8200 does not have a verified page on LinkedIn because the IDF does not formally discuss the unit, nor its internal unit number.

[43]"By the numbers: The NSA's super-secret spy program, PRISM." Foreign Policy.

billion for software and $240 billion for other Information Technology.[44] Furthermore, the US high technology industry is spread out across the geography of the United States, with strong clusters in Boston, New York, Seattle, and Silicon Valley.[45] These characteristics of the United States' Intelligence Community and its high-technology industry limit easily observable overlap from a bird's eye view. Yet as signals intelligence workflows involve more and more computing, the labor pool from which the NSA might draw upon looks similarly to that of the private high-technology sector: knowledge workers with highly technical skillsets. From the standpoint of labor economics, in a free labor market like in the United States, the NSA looks functionally like just another technology firm competing for employees from the same labor pool – a labor pool we already know possesses a growing labor shortage.

Looking at the high-technology industry from a top-level viewpoint, numbers and geography inhibit the NSA alumni population to have any significantly visible saturation. Yet NSA employees and those working in the high-technology industry have the same skillsets. This leaves the question, is there any beneficial professional network of NSA employees in the high-technology industry? If so, how do the members of this network interact with each other? How is it perpetuated? In the market economy, what does it mean to have worked at the NSA?

A lack of NSA alumni in the high-technology industry in the United States impedes any ability to conduct statistically significant quantitative analysis. However, there exist isolated cases of persons with NSA or other intelligence experience working in US high-technology clusters. In the case of the United States specifically, this thesis makes a distinction between the high-technology industry and technology companies that contract with the US government. This

[44] "SelectUSA." The Software and Information Technology Services Industry in the United States. http://selectusa.commerce.gov/industry-snapshots/software-and-information-technology-services-industry-united-states (accessed May 2, 2014).

[45]"American Cluster Innovation, Profiles from the 50 States." *Institute for Strategy and Competitiveness, Harvard Business School* (2008).

is because many of these contractors represent a large population of the Department of Defense labor force,[46] and for the purposes of this study are thus abstractly considered to be more a part of the intelligence community than the technology industry.

Oren Falkowitz, the founder of Sqrrl, is one such example of someone with NSA experience working in the US high-technology industry. In an interview, Falkowitz reflected that when he first founded Sqrrl in 2012, he was not sure he was going to leave the NSA for good. Falkowitz developed an idea for a big data company from his experience at the NSA. The decision to leave was relatively low-risk: he was sufficiently senior at the NSA to leave on good terms, with almost certain assurance he would be welcomed back should he decide to return. He didn't leave his team with any burnt bridges. All of these factors made it easier to leave, and eventually made it easier to break into the technology sector.

Falkowitz made a point to note that his case is unusual. He explained that usually the NSA encourages its employees to remain working at the NSA for the duration of their careers. Conversely, as a government job, it is very difficult to be fired from the NSA save an insider threat suspicion, which is rare. Those employees who do leave usually remain in the defense industry, opting to do similar jobs as defense contractors as a way of subverting lower government wages. When employees really leave, Falkowitz explained, "it's not exactly frowned upon, but it's not really received well." A significant impediment to a career network of persons with NSA experience working in high-technology is the small number of NSA alumni in circulation throughout a large and geographically dispersed technology industry.

[46] "Department of Defense's Use of Contractors to Support Military Operations: Background, Analysis, and Issues for Congress ." *Congressional Research Service* (2013): 2.

Falkowitz entered the technology industry by spending time in Boston and Silicon Valley. Boston was the original site of his company, and Silicon Valley was were the location of the venture capital funds from which he primarily sought funding.

"There really isn't a network of NSA alumni in the high-technology sector," explained Falkowitz, "There are cases of people who left the NSA to go into tech, but nothing is concentrated. If I wanted to seek connections of other NSA alumni in high-tech, I wouldn't have even known where to look."[47]

As an NSA alumni Falkowitz felt very much like an anomaly in Silicon Valley, which had its advantages and disadvantages. It was advantageous because "working at the NSA gave me some credibility that I knew what I was talking about in this [enterprise and data] space." [48] Experience in enterprise is rare for enterprise technology founders.[49] Even if investors did not know what Falkowitz did specifically in the NSA, he could speak to his experiences at the agency in a manner that would set him apart. Of course, this was contingent upon Falkowitz' willingness to identify himself as an alumni of the NSA.

"Most people are really uncomfortable saying that they're from the NSA…I don't really have a problem with it. Being from the NSA has been useful."[50]

Coming from an NSA background was also disadvantaging. According to Falkowitz, most people in technology do not understand the defense space, or what to think about someone who came out of it. Once Falkowitz ran a pitch meeting with one of the top venture capital funds in Silicon Valley. At the end of the meeting, which went very well, Falkowitz tried to supply references at the NSA to his potential investor. The investor politely took note of the references

[47] Falkowitz, Oren. Personal interview, 20 March 2014.
[48] *Ibid*.
[49] "Is the IT skills gap fact or fiction?." Enterprise CIO Forum. http://www.enterprisecioforum.com/en/question/it-skills-gap-fact-or-fiction.
[50] Falkowitz, Oren. Personal interview, 20 March 2014.

Falkowitz gave him, and then assured Falkowitz that he "knew a few guys at the NSA" to which he could make some calls.[51] This sort of due diligence in the American defense space seemed ridiculous to Falkowitz—the US NSA is a tens-of-thousands strong organization. It is unlikely that whomever the investor knew could speak to Falkowitz' work or even knew him. Furthermore, an insular culture of secrecy in the NSA would deter many of its members from speaking to another's work when cold-called.[52]

Despite Falkowitz' difficulty entering the technology industry initially, his own attitudes toward the agency and its human capital bode well for the creation of an alumni network were there more alumni around to be helped. Falkowitz noted that he would be more likely to help out someone with his or her high-technology career if they had NSA experience. Furthermore, Falkowitz would "probably" be more likely to hire someone with NSA experience at his own company than an equivalent candidate without NSA experience.[53] This is in part due to a shared experience of national service, but it is also due to the skillsets and experiences that Falkowitz knows the NSA provides, which would be useful to draw upon in his company.

No measurable public network of NSA alumni exists in the US high-technology industry that is analogous to the network of Unit 8200 alumni in the Israeli high-technology sector. This is in part due to unchangeable features of the United States and its high-technology environment: the US high-technology industry is extraordinarily large and geographically diverse, and the number of NSA alumni leaving the intelligence community is comparatively small. While a network may not be measurable, Falkowitz' story illustrates many of the realities impeding an

[51] Falkowitz, Oren. Personal interview, 20 March 2014.

[52] A further point to this is that there exists a specific office at the NSA that job recruiters should go through to verify the employment history and position of former or current NSA employees. This is outlined in the secrecy section of this case. Israel does not have the same infrastructure in place, as detailed in the comparative case of this thesis.

[53] Falkowitz, Oren. Personal interview, 20 March 2014.

observable NSA alumni network in the US high-technology industry. Falkowitz felt as if he would be welcomed back into the agency, though he conceded that others coming out of the NSA probably would not be able to return to their same job at the NSA after leaving, as it can take years to get promoted through what he sees as a strictly hierarchical system. This job insecurity associated with leaving the defense industry is reinforced by the agency's culture of loyalty, by which Falkowitz felt pressure to remain at the NSA for the duration of his career. However, the same culture of loyalty that pressures people to remain at the agency is also extant in Falkowitz' own attitudes toward other NSA alumni should he come across them in the technology industry—more likely to assist an NSA alumni with his career, and more likely to hire an NSA alumni given a desirable set of work experiences.[54] This attitude illustrates the building blocks of a potential network: willingness to help each other out, and valuable credentialing. The numerical and geographical limitations to an NSA network are real, but another major inhibitor to an American network is secrecy. While in Israel identification with Unit 8200 is technically illegal, many 8200 alumni identify anyway because it benefits their careers. By contrast, Falkowitz reports that many NSA alumni feel uncomfortable identifying with the agency. When NSA is not a mentioned part of work experience, it is not a "resume builder." [55] In the next section, this case examines the existing attitudes toward secrecy in the NSA and their utility.

Secrecy

As intelligence organizations, both the US NSA and IDF Unit 8200 deal with large amounts of sensitive information. In the NSA different security clearance levels are given to

[54] *Ibid.*
[55] *Ibid.*

different employees, which control the type and level of sensitive information to which each employee is privy. In order to work at the NSA, or at contracting companies embedded within the NSA, one must undergo extensive background checks proportional to the level of security clearance. Security clearances do two things: first, the clearance process protects against insider threat liabilities, and second, even the highest clearances usually compartmentalize information on a "need to know" basis—so no one knows too much. In the wake of the Snowden leaks, clearance levels are being re-evaluated for NSA employees and contractors alike, both in order to apply more stringent review processes regarding who gets security clearances, but also to silo information of higher sensitivity levels so no one, especially contractors, has "keys to the kingdom."[56] The Snowden leaks will likely make more stringent existing security measures, as insider threat strategies get reviewed and reevaluated.

This case is concerned with the secrecy policies of the NSA insofar as they limit the ability for ex-NSA members to self-identify as such professionally (i.e. to network), or for NSA experience in itself to carry social capital or signaling weight outside of the NSA and the US intelligence community. To this end, the siloing of sensitive information within the NSA and policies of identification are both salient pieces of information. In order to keep sensitive information compartmented it is not agency practice for members of the NSA with the same levels of clearance speak about what they were working on with each other across the agency.[57] This was manifest in Falkowitz' experience, when members across the agency were reluctant to identify themselves as NSA or vouch on behalf of Falkowitz, even while knowing Falkowitz to be NSA.

[56] "National Security Archive Electronic Briefing Book No. 24". *Declassified documents and Archive publications on U.S. Intelligence*. 2007-09-27

[57] Name Redacted. Personal Interview. 19 February 2014.

Three questions dictate the importance of secrecy to human capital management in intelligence organizations, and particularly that in the NSA. The first of these questions asks what the official policies are which dictate what members and alumni of the NSA are and are not permitted to say regarding their affiliation, position, and experiences with the NSA. A secondary question asks how these policies are enforced. The final piece involves whether or not members and alumni of the agency obey said policies.

According to declassified and unclassified etiquette documents, official policies by the NSA regarding human capital secrecy concern both conversational and formal association with the agency. In a declassified edition of the NSA employees' security manual, new employees are instructed to conform to a "far-reaching" but ambiguously defined policy of anonymity in casual conversation, in which they should neither confirm nor deny information about the agency, nor "draw attention to themselves."[58] This extends to conversations with friends and family. When employees are asked where they work, they are permitted to say they work at the Department of Defense. If pressed further, they may say the National Security Agency. They are not able to relay any information regarding the Agency's "mission, activities, or organization… or act mysteriously about the terms of …employment."[59] Any job titles when offered up in conversation should be non-descript, e.g. secretary, engineer, etc. If an employee holds a more specific job title, e.g. cryptanalyst, these personnel must respond to questions by saying their job title is something more general like "research analyst," so as not to betray any information about the mission or activities of the agency.[60]

Secrecy policy dictating casual conversation with family and friends extends into formal description of NSA experience and training. In policies regarding casual conversation there

[58] "Employee Security Manual." *Declassified. National Security Agency.*
[59] *Ibid*.
[60] *Ibid*.

exists evidence of dampened signaling and social capital value associated with NSA employment. The more specialized the work at the NSA, the less employees are permitted to speak about what it is they do. This suggests that the signaling value associated with said employee's work at the NSA is dampened because the policy deliberately makes the work sound less specialized than it is. For example, those who work with foreign languages are not permitted to discuss the languages with which they work.[61] Conversation policy also shows evidence of a dampened social capital value associated with NSA experience, as employees are ambiguously instructed not to "act mysteriously" about classified work, so as "not to draw attention to themselves." Evidence of dampened signaling and social capital effects extends into policies regarding formal association with the unit as well. This includes refraining from public discussion about the agency's activities and involvement in current events, but it also includes what can and cannot be said in a professional setting. For example, any job training provided by the NSA cannot be discussed if it touches on any classified work. This is problematic because significant training occurs with most specialized employees in-house in intelligence organizations,[62] and thus this policy limits discussion of skillsets a particular employee might have. The secrecy surrounding training can be starkly contrasted with IDF marketing of its elite intelligence units in Israel, including Unit 8200, which leads many to colloquially refer to Unit 8200 as equivalent to one of the best "schools" in the world.[63] A final policy limitation to formal association regards resumes and future job searches, where any resume job descriptions or

[61] *Ibid.*

[62] Mueller, Robert. Personal Interview. 28 April 2014.

[63] The Economist Newspaper. "MBAs are for wusses." The Economist. http://www.economist.com/node/16892040 (accessed May 1, 2014).

verification of employment by a prospective employer must be run through a specialized office at the NSA.[64]

Formal and informal identification with the unit is strictly limited by policy, which provides overt instructions for limiting the description, verification, and identification of job experience and titles in the NSA. However, secondary and tertiary to the question of policy is how these policies are enforced and if people follow them. There are two distinguishable ways that the NSA enforces secrecy policies. The first is enforcement after the point at which someone violates a policy. The second manner of enforcement is prevention. For this thesis, evidence of policy enforcement after the point of security violation is largely anecdotal. According to all former NSA employees interviewed for this thesis, the question of enforcement of these policies is a difficult question because any enforcement is quiet and confidential. However, enforcement of policy transgression could include termination of employment or the loss of security clearance. A secrecy policy violation could look like two things: either the failure to be diligent, or an insider threat. In the first case, this could look like someone bragging about their employment, acting "mysteriously" about the work of the NSA, drawing attention to themselves, or betraying the mission, activities or any classified information of the NSA. Here termination of employment is difficult, but the risk of inability renewing one's security clearance is more likely.[65] In the second case, behavior that breaks NSA's security policies that also resembles an insider threat can result in the termination of employment.

Enforcement of secrecy in human capital is much more apparent in the NSA's security clearance process. The NSA's process of hiring, for which there is admittedly little data, as well

[64] "Employee Security Manual." *Declassified. National Security Agency.*

[65] The evidence for this is tentative; it is just based off a consensus of those interviewed. However, some of those interviewed hadn't seen an instance in which it is enforced, because there isn't a strong tradition of people breaking the rules.

as the process for obtaining security clearances, represent a point of prevention for human capital secrecy liabilities. Questions surrounding the enforcement of secrecy liabilities are becoming more important in the wake of the Snowden revelations, including a full review by the Government Accountability Office of the entire security clearance process for both the NSA and other agencies in the intelligence community.[66] The 2013 report found that although secrecy clearances need reform, the cost of more stringent clearance requirements dramatically increases: "Underdesignating positions can lead to security risks; overdesignating positions can result in significant cost implications."[67] One recommendation made by Keith Alexander to the Senate Committee on Secrecy suggested that all employees must obtain a top secret security clearance before being allowed to read classified documents.[68] This small change, among many others suggested, has been estimated at a cost of over one billion dollars per year.[69]

Stringent policies exist at the NSA, not only for the management of sensitive information, but also for the identities and personal information for those employees privy to that information. These secrecy policies are intended to prevent human capital liabilities, such as an insider threat liability or the case in which an employee might be compromised by a foreign actor. While there is little data to back up how these policies are enforced, real consequences exist for those who do not follow them. The most glaring form of enforcement is prevention via the hiring and security clearance process, therefore, it follows that a large part of the selection of highly technical workers at the NSA includes not just the criterion of technical prowess but also the criterion of trustworthiness. Suspicion over insider threat liabilities is increasing in the wake of the Snowden

[66] "Actions Needed to Ensure Quality of Background Investigations and Resulting Decisions." *US Government and Accountability Office* (2014): 3.
[67] GAO report, "Personnel Security Clearances: Actions Needed to Ensure Quality of Background Investigations and Resulting Decisions." 11 February 2014
[68] "NSA Targets Systems Admins to Prevent Snowden-Type Leaks." Nextgov.
[69] "After Snowden, will the security clearance process finally change?." FedScoop. June 21, 2013.

disclosures, which cost the United States and its taxpayers billions of dollars and international and domestic trust.[70] The final component to the question of human capital secrecy is whether or not employees follow these policies. The data for this question is relatively unreliable and largely anecdotal. Noting the dearth of online alumni groups, meet ups, and online discussion boards of NSA alumni, while unscientific, is suggestive that obedience of these policies is embedded into the culture of the agency. It is also the primary contrastive point of this thesis, that there appears to be a stringently followed policy of human capital secrecy in the NSA, which is contrastive with how secrecy functions among Unit 8200 operatives and alumni.

Oren Falkowitz underscored this sentiment regarding public employee discussion of place of employment and job skills, “It’s really just not what’s done; people are very quiet and risk-averse.”[71]

The function of secrecy in the NSA’s human capital management is contrastive with how secrecy appears to function at Unit 8200. However, this difference does not indicate a free variable. Rather, it also highlights important limitations to the comparison of these cases, as well as some limitations to US intelligence community human capital management in general. As outlined in the NSA’s employee security manual, there exist a host of support via the Office of Security and other outlets within the organization to manage secrecy and aid employees in behaving according to protocol. This represents a large proportion of infrastructure dedicated to the preservation of an explicitly outlined security protocol. The result is a very different manifested human capital strategy.

Another important constraint to the NSA’s secrecy strategy is the ethnic pluralism within the NSA’s human capital pool, as well as its diversity of security interests. Former FBI Director

[70] Hagel, Chuck. "Department of Defense Press Briefing by Secretary Hagel and Gen. Dempsey from the Pentagon Briefing Room." Address, Pentagon Briefing Room from Department of Defense, June 26, 2013.
[71] Falkowitz, Oren. Personal interview, 20 March 2014.

Robert Mueller emphasizes this point. Mueller explained that as a global power, the United States will have more diverse intelligence interests and needs sets than smaller countries with more specific security objectives. These challenges are compounded by cultural heterogeneity in the labor pool from which the NSA recruits. Mueller explained that this is a stark contrast to most other intelligence communities in the world, and especially those of smaller countries like Israel. The Israeli intelligence community has more specific security objectives relevant to their region and commensurate with their resources. Unit 8200, like the rest of the Intelligence Corps and the IDF, conscripts secular, non-Arab Israelis. In addition their security interests are more narrowly defined, involving mostly their immediate and hostile neighbors. To subvert the insider threat liabilities associated with hiring employees with fluency in adversarial languages, news reports suggest that Jewish immigrants with ethnic backgrounds in countries like Iran and Iraq are conscripted into intelligence units in disproportionately large numbers.[72] The United States does not have it so easy.

Even if employees with fluency in these languages are trustworthy individuals who are eager to serve their country, their participation in certain immigrant or ethnic communities can be seen as a liability for the NSA, whose security protocols limits association with foreign nationals and membership in specific groups.[73] “Our security interests include the whole world, we need employees with fluency in almost every language,” explained Robert Mueller, former director of the FBI, who also noted: “It can be really hard to get someone a security clearance when they still have family in Syria.”[74] As explained by Mueller, even if Israeli Intelligence has a more immediate awareness of security threats, their labor pool does not have the same human

[72] "Israeli military fills up intel units with Iranian immigrants, report reveals - Diplomacy and Defense." Haaretz.com. January 9, 2014.
[73] “Employee Security Manual,” National Security Agency.
[74] Interview, Robert Mueller. 29 April 2014.

capital liabilities, and they do not deal with the same security limitations.

The NSA's inordinate focus on secrecy when recruiting and making use of human capital represents an imperfect labor market, where the ability to recruit top technical talent is impeded or affected by a secondary objective to ensure that those knowledge workers make secure additions to the US intelligence arm. But public intelligence agencies, even those that draw upon professional forces, do not function in a free labor market in a perfectly competitive way. While Chapter 5 suggested that loosely followed secrecy policies among Unit 8200 alumni might augment the signaling and social capital value of its associated intelligence work, the degree to which this is informative for the NSA is limited by the security constraints of a much larger, more diverse agency with broader security interests. In an age in which insider threat liabilities are of central concern, interrogating of the cost and benefit of secrecy strategies to the human capital pool, beyond mere costs, is important. In the following pages this case will consider the both the current strategy toward human capital recruitment in the NSA, and the apparent credential associated with NSA experience in the US high-technology community.

Current Strategy

Year after year, military academies are consistently ranked among the top institutions for public higher education, with some of the best and brightest in the country as their students.[75] Recruiting top students to the nation's military academies is something Colonel Charlie Miller thinks extensively about. The United States Military relies upon the academies' ability to recruit strong and intelligent leaders. And yet only 25% of graduating high school students meets the

[75] "National Liberal Arts College Rankings." U.S. News & World Report: News, Rankings and Analysis on Politics, Education, Healthcare and More.

basic physical requirements to be considered for military academy recruitment.[76] This means that the ability to take candidates with the requisite intellectual and leadership qualities is limited because the military must pull from a much smaller recruiting pool. As Colonel Miller becomes more and more involved in US Army Cyber Command, he has begun to think of cyber and signals intelligence recruitment in the same way: the available recruitment pool of top technical talent is made small by the need for those knowledge workers to meet basic secrecy requirements. Both the US military personnel and their civilian counterparts that make up the labor force of the NSA are professional, meaning that the NSA cannot just conscript those they think are the most smart and trustworthy. As the primary ammunition in the cyber age is knowledge power, the ability for the US to maintain leadership or punch at weight in the cyber domain depends on its ability to recruit competent technical knowledge workers commensurate with its security needs.

"Our response so far is that our cyber guys need to be homegrown—that they need to be trained in a rotational way," explained Colonel Miller.

The current human capital strategy for the civilian and military intelligence community is to "home grow" technical knowledge workers by providing specialized training in-house, and then encouraging those trained to remain at the agency for the majority of their careers. In a US Government and Accountability Office annual Strategic Human Capital Plan, a dearth of technical talent was highlighted as a key challenge to intelligence community human capital strategy:

> "Our war for talent is being fought in a labor market that is shrinking, the result of lower US birth rates, fewer college graduates (especially with technical degrees and foreign language proficiency). Add to that our requirement for some of the most esoteric skills, including… scientific disciplines and emerging technologies, as well as the most stringent suitability and security clearance requirements

[76] Miller, Charlie. Phone Interview. 3 February 2014.

> anywhere, and it is clear that the IC will face hyper-competition for the best and brightest."[77]

To address these concerns associated with the recruiting technical knowledge workers, the US Intelligence Community including the NSA has adopted a recruiting strategy that focuses on encouraging its members to stay for the duration of their careers. There are three primary reasons for this. The first is that the Intelligence Community is concerned about losing its leadership. "Everyone wants people to stay for the full 20 years," said Robert Mueller,[78] explaining that this is in part an effort to encourage leadership to stay. In a strictly hierarchical system, in which employees are tasked with working collaboratively on highly technical problems, it is critical for project management that the agency be able to maintain leadership within its workforce. As such, the agency's conventional viewpoint on this is to encourage those knowledge workers to remain at the agency through the point at which they would be valuable leaders.

Second, is the notion that security liabilities are better managed when there are fewer people involved in the intelligence community, and fewer people leaving. "The NSA even encourages its people to date each other," explained Bill Lin, a professor of electrical engineering and researcher who has worked extensively with the US intelligence community. Lin cited security concerns as a primary reason for the dearth of institutional churn in the NSA's human capital strategy.[79] The second reason is that there is an enormous sunk cost into each individual employee the NSA chooses to take on. Security clearances are estimated to cost

[77] "The Human Capital Strategic Plan." *US Government and Accountability Office* (2013): 5.
[78] Mueller, Robert. Personal Interview. Stanford, CA, 28 April 2014.
[79] Lin, Bill. Personal Interview. Stanford, CA, 26 February 2014.

thousands of dollars per employee in different intelligence agencies, and the process needs to be completely redone every few years.[80]

In addition to the cost of security clearances, enormous amounts of costly and sensitive in-house training is invested in advanced employees of the NSA. “A rotational program helps train people and provides some in-house churn, but a lot of sunk cost goes into training people, after which the IC wants people to stay,” explained Mueller.[81]

In the comparative case of this study, a very different cultural context for military training is presented. In Unit 8200 and other elite intelligence units in the Israel case, each person is given extensive skills training, and many leave the army after their service requirements end. The justification for this training can be better understood in an Israeli context, where the founding principles of the Israeli “peoples’ army” was to prepare Israeli citizens as well as productive soldiers. In this lens, army training is not considered a sunk cost into the career of a soldier, rather it is training invested into the economic output of Israeli citizens, most of whom become private sector contributors to the economy after army service. In the NSA, intelligence training is justified by the knowledge output within service.

Credential

This thesis makes the broad argument that enhancing the signaling and social capital value of intelligence service is beneficial for employees and alumni of intelligence agencies, but also the agencies themselves by helping to attract top talent. A particular recruiting challenge of national intelligence branches is secrecy, or the need to minimize the secrecy liability endemic to human capital. Secrecy also affects credentialing by limiting the amount of information that a

[80] Christensen, Michelle , and Frederick Kaiser. "Security Clearance Process: Answers to Frequently Asked Questions." *Congressional Research Service* 1 (2013).
[81] Mueller, Robert. Personal Interview. Stanford, CA, 28 April 2014.

particular employee can signal to other actors in the labor market about their skillsets and experiences. Thus, an ideal human capital strategy for intelligence organizations is one that would optimize these two concerns: the need to minimize security threats of sensitive information, and the need to reveal just enough information to establish national service work as a compelling credential. To interrogate this balancing act, it is important to develop an understanding of secrecy liabilities and the policies that are effective in containing them. Conversely, understanding how human capital signaling is affected by secrecy is also important. To examine the latter variable, we must first establish how the NSA job experience is seen or not seen as a positive credential in the high-technology labor market.

"There is no doubt that NSA could massively benefit from social capital and signaling," explained Robert Mueller. This is because both social capital and positive signaling value would aid in the ability for the NSA to attract and recruit top technical talent. Regardless of whether there exists a recruiting crisis in the US intelligence community or not, an enhanced social capital and signaling effect can aid in the recruitment of top technical knowledge workers, particularly in a competitive labor market.[82]

This thesis found no significant evidence to suggest that the NSA lacks a positive credentialing value commensurate with a generally high level of technical work.

"I think the general consensus in the [Silicon] Valley is that the NSA still does really complex work," explained Bandel Curano, managing director of Oak Partners in Palo Alto.[83] As such, Curano explained that he thought many NSA alumni would be received in the Silicon Valley labor market with the understanding that they were competent knowledge workers that probably have highly technical skillsets. However, there is a difference between the reputation of

[82] This framework is detailed more extensively in Chapter 2.

[83] Curano, Brandel. Personal Interview. Palo Alto, CA, 20 March 2014.

an agency and how that translates into the credentialing or signaling effects of a specific resume. Curano explained that the private sector moves quickly. A negative implication of this for those leaving the NSA might be confusion or disinterest in back-checking the skillsets of a prospective employee, when doing so requires working through a potentially slow and bureaucratic secrecy office.

Lieutenant Colonel Matthew Atkins, who studies how recruitment works within the US military and civilian intelligence community, reinforced the idea that current secrecy policies negatively impede the ability for NSA affiliates to effectively communicate their skills and competencies. Colonel Atkins argued that even if people have a baseline idea of what the NSA does and how this work is technical, that is minimally helpful if NSA operatives cannot communicate any specific training or experience that they received through the NSA with unclassified private sector value and application. Although it is difficult to answer, the question then becomes what the cost-benefit to human capital secrecy is to minimizing security liabilities.

However, secrecy policy is not the only factor limiting the potency of a positive credential from NSA experience in the US technology industry. Culture is also important to how NSA experience is viewed, and especially how this credentialing affects the NSA's ability to recruit top technical talent. A piece of this was alluded to in the earlier portion of this chapter, given the recent poor press from Edward Snowden. Almost all policy officials and members of the technology community interviewed for this thesis cited the Snowden disclosures, in addition to costing the American taxpayer billions of dollars, as shaping the reputation of the NSA as an unpatriotic place to work. This is reflected in the public discussion in the press, which reinforces the idea that the post-Snowden reputation of the NSA has accrued negative color.[84] This is problematic given that NSA's human capital strategy relies on a strong social capital value

[84] Hayden, Michael. "Beyond Snowden: An NSA Reality Check." *World Affairs Journal* (2014).

rooted in the ethos of serving one's country: "America's intelligence services continue to attract our Nation's best and brightest, idealistic individuals, both young and experienced, who want to serve their country" reads Objective 2.1 of the 2006 US National Intelligence Strategy's strategic human capital plan.[85]

Conclusion

This case finds that there lacks a public network of NSA personnel and alumni in the high-technology sector. Although the NSA draws a professional civilian and military force from a labor pool of highly technical workers, these knowledge workers do not necessarily overlap with those in the private high-technology sector. While NSA experience is generally seen as a positive indicator of technical skillsets, this is dampened on an individual signaling level by existing secrecy policies. Currently, human capital strategy in the US NSA airs on the side of protecting and preserving agency secrecy at the expense of a more public presence. This presents an area of further inquiry, as loosened secrecy policy on a human capital level might augment the signaling and social capital value associated with the agency. Although secrecy limitations are a critical component of the NSA's ability to maintain its operations, the cost-benefit of strengthening secrecy policy, particularly in the wake of the Snowden disclosures, should be weighed not only against increased monetary costs, but against the costs increased secrecy could have on the signaling and social capital value associated with the NSA, and in turn, successful human capital recruitment.

[85] "The Human Capital Strategic Plan." *US Government and Accountability Office* (2013): 16.

Chapter 4: Network Effects

At 10:00pm on a quiet street in Ramat HaSharon, Israel, a ritzy suburb of Tel Aviv, a small horde of twenty-something, mostly male Israelis shuffle in and out of what is at street-view an unassuming limestone house. On its interior walls, tens of photos depict an elite Israeli intelligence official posing casually with multifarious international political leaders: Barack Obama, George Bush, Angela Merkel, the list goes on. A regimented corps of waiters weave through the crowd, handing out miniature remixes of traditional Middle Eastern *mezze*: “cake pops” with halva, schwarma “tacos,” fattoush cups. Techy words like “disrupt” and “Series A” pepper conversations spoken in a messy, hurried, English-Hebrew hybrid.

A quick survey of the room reveals the event an unofficial after party of the Ernst and Young Journey Conference 2013, the largest annual technology conference in the Middle East. The vast majority of the attendees are under the age of 35, all founders of Israeli high-technology startups and almost all alumni of IDF Unit 8200—a fact volunteered in conversation with abandon. Other attendees are few in number and one of two breeds: either foreign technology investors in town for the Journey conference, or decorated military commanders affiliated with the unit. In the corner, Brigadier General Pinchas Buchris, commander of Unit 8200 from 1997-2001,[86] introduces a young entrepreneur to a prominent Silicon Valley venture capitalist. The

[86] Perman, Stacy. "Chapter 4: Brains." In *Spies, Inc.: Business Innovation from Israel's Masters of Espionage*. Upper Saddle River, NJ: Pearson Education, 2010. All.

evening is highly exclusive, intimate, but hardly extraordinary—attendees interact casually, as if unit commanders routinely host events like this, connecting the best and brightest unit alumni with the slickest foreign investors eager to get their hands on "Silicon Wadi"[87] whiz kids.

This thesis investigates how elite signals intelligence units can develop policies and incentive structures to encourage the best and brightest technical minds to devote brainpower to national service. This chapter is the first of two chapters of the second comparative case of this thesis, detailing the human capital strategy, secrecy policy and network associated with the primary signals intelligence arm in the Israeli Intelligence Corps, IDF Unit 8200. The primary hypothesis of this case is that Unit 8200 has a human capital strategy that contributes to a publically observable network of alumni within Israel's high-technology sector. This network indicates a unique incentive structure embedded in the military organization of Unit 8200, and that lessons from this network can help inform how elite knowledge workers can be motivated to participate in national service. Operating from this premise, this chapter develops a theoretical framework for understanding the Unit 8200 network in the Israeli technology sector, both the function of the Unit 8200 network and how it is perpetuated. The second chapter of this case will detail empirical evidence of a Unit 8200 human capital ecosystem and strategy within Israel. This case argues that Unit 8200's network exists and is perpetuated due to a number of different factors, some of which are unique to Israel's case and some of which are distillable policies and incentives. Although this chapter focuses its argument on Unit 8200, it will serve as a general framework with which to contextualize the knowledge ecosystems surrounding other intelligence organizations, including the comparative case of this study, NSA.

[87] Hadar, Leon T. "Israel in the Post-Zionist Age: Being Normal and Loving It." *World Policy Journal* Vol. 16, no. 1 (1999): 76-86.

This chapter first introduces Unit 8200 as an intelligence organization and as a subunit of the Israel Defense Forces. Then, this chapter will go on to detail a theoretical framework for the unit's human capital strategy. This theoretical argument is composed of two parts. The first part of the theory seeks to explain the phenomenon of the Unit 8200 alumni network in the Israeli technology sector and how it is perpetuated. Central to this is the idea that Unit 8200 service experience is a positive signaler for those who hold alumni status. Thus, the second part of this theory investigates what exactly a Unit 8200 credential signals in the technology sector. This thesis argues that both components are relevant to understanding the ecosystem of intelligence organization human capital.

Unit 8200

Signals intelligence has long been a component of the IDF. The precursor to Unit 8200 was Unit 515, founded in 1952. This unit changed its name to Unit 848 shortly thereafter. After the Yom Kippur War, Unit 818 consolidated once again into Unit 8200. The Yom Kippur War was a turning point for Unit 8200, after which the capabilities and roles undertaken by Unit 8200 personnel became more significant to warfare. Unit 8200 especially contributed during the six-day war, providing significant intelligence on Egypt and Syria. After the six-day war the strategic importance of Unit 8200 was more recognized and the unit received significantly more funding. Today, the unit holds a central role in the intelligence division of the military, serving as the signals intelligence arm of the IDF.[88] Though Unit 8200 is a part of the Israel Defense Forces, as opposed to falling into a non-military of Israeli intelligence like the Mossad, Unit 8200 is most often compared to non-military signals intelligence organizations like the GCHQ in the United Kingdom and the NSA in the United States. In the Snowden documents, substantial

[88] Kahana, Ephraim. "Unit 8200." In *Historical dictionary of Israeli intelligence*. Lanham, Md.: Scarecrow Press, 2006. 295-298.

evidence suggested that Unit 8200 was the organizational counterpart in Israel with which the NSA shares intelligence, including “raw” signals intelligence, that is, sigint collected by the NSA but not yet analyzed by American analysts.[89] As cyber security and cyber threats become increasingly important points of concern in Israel, documents in the IDF suggest an expansion of Israel’s intelligence arm to accommodate the expansion of cyber focused forces.[90]

Part 1: The Unit 8200 Network

An Unenforced Policy of Secrecy

This section presents a theory for why there exists public network of Unit 8200 alumni within the Israeli high technology community. A premise of this section is that there does exist a public network of Unit 8200 alumni, evidence for which will be demonstrated in a later chapter. Operating from this premise, this theory suggests that a public network of Unit 8200 alumni is tolerated by the Israeli military because it benefits Unit 8200 itself, e.g. that the public knowledge of technical knowledge workers underlines the societal value of signals intelligence service, which is beneficial in the recruiting of top talent. Unit 8200 alumni are incentivized to declare their association with the unit in the private sector because it is a positive signaler that the alumnus possesses certain skillsets and networks. While formal policy dictates that alumni are not allowed to declare their association with the unit, there is little disincentive to declare association because doing so poses little risk of negative consequences, as the formal policy is rarely enforced. It is unlikely that the IDF is incapable of enforcing a policy of secrecy surrounding the identities of Unit 8200 alumni, and the public knowledge of Unit 8200 alumni is

[89] *The Guardian* (London), "NSA and Israeli intelligence: memorandum of understanding – full document," September 11, 2013.

[90] Israel Defense Forces. "IDF's First-Ever Cyber Defenders Make History - IDF Blog | The Official Blog of the Israel Defense Forces." IDF Blog The Official Blog of the Israel Defense Forces.

dangerous both to the security of the alumni and to the unit. These facts suggest that there is a positive benefit to the public network for Unit 8200 alumni for Unit 8200 itself.

Imagine a situation in which an alumnus of an elite intelligence unit applies for a job outside of the intelligence community. The human resources division of the desired company is civilian and not privy to classified intelligence work, nor is the technical recruiter sitting across the interview table. In this situation, how does the intelligence alumnus' application benefit from the work experience and skills gained during the applicant's years of service?

This is the difficult situation faced by alumni of Unit 8200 and other secret intelligence organizations on the private sector job market. Where other applicants might use their work skills and experiences to augment their applications, the secret status of the activities of intelligence organizations inhibits those possessing them from advertising them in the labor market. The prohibition of identifying unit affiliation at all, as is formally prohibited of Unit 8200 alumni, is doubly disadvantaging because it leaves years of work experience unaccounted for. As a signals intelligence organization, Unit 8200 is one of the "elite intelligence units" of the Israel Defense Forces, presumably engaging in highly technical activities.[91] These activities require advanced skillsets in electronics and computing to carry out.[92] If these skillsets were gained or employed at a technology company in the private sector, a job applicant would be able to describe them and specific projects freely. Job applicants benefit from declaring prior work experience and relevant skillsets.[93] Thus, not declaring intelligence agency affiliation or experiences puts intelligence unit alumni at a disadvantage in the job market. Because of this, Unit 8200 alumni are incentivized to declare their association with Unit 8200 because it signals

[91] Orpaz, Inbal. "'Preserving the madness' in IDF intelligence." Haaretz, September 26, 2013.
[92] "Signals intelligence." Princeton University. http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Signals_intelligence.html (accessed March 1, 2014).
[93] Spence, Michael. "Job market signaling." *The quarterly journal of Economics* 87, no. 3 (1973): 358.

to future employers that they possess certain skillsets and networks that would be desirable in an employee. In the high-technology sector, Unit 8200 experience would be more valuable than experience from a non-intelligence unit, because the technical skills gained from Unit 8200 work and training are relevant to technology work.

The incentive to declare association with Unit 8200 in the high-technology job market is exacerbated by the relatively small amount of risk posed in doing so. Although unit members are not technically permitted to publically identify affiliation, many do, suggesting that this policy is unenforced. It is unlikely that the Israel Defense Forces could not enforce this policy if it wanted to; as an intelligence collecting organization it would be easy for Unit 8200 itself to compile a list of those alumni who declare association public networking sites like Facebook or LinkedIn, or to compel technology companies to report any applicants who claim association.

The lack of repercussion for declaring public affiliation with Unit 8200 is particularly unusual given the clear risk associated with doing so for both alumni and Unit 8200 itself. As former intelligence soldiers, Unit 8200 alumni are privy to highly sensitive information. Amos Levinberg was a member of Unit 8200, taken as a prisoner of war by Syria during the 1973 war. While he was held captive, the Syrians managed to convince Levinberg that Israel was destroyed. In response Levinberg proceeded to reveal to his captors much of the sensitive information he knew as an 8200 officer, divulging so much information that he is known in Israel as the “singing soldier.”[94] This information dramatically hurt Unit 8200 during the 1973 war and thereafter. Today the story of the singing soldier is retold to Unit 8200 soldiers as a warning anecdote about the sensitivity of information dealt with by unit members. New Unit

[94] "The Spies Inside Damascus." Foreign Policy. http://www.foreignpolicy.com/articles/2013/09/19/the_spies_inside_damascus_mossad_syria (accessed February 10, 2014).

8200 members are told that the information disclosed by the singing soldier was so sensitive that it continues to damage the unit to this day.[95]

The story of the singing soldier illustrates just how dangerous it is for Unit 8200 to have the identities of their operatives and alumni public. By extension, it is also dangerous for the alumni themselves. The state of Israel, including its contested territories, is around the size of the state of New Jersey and bordered by enemy states including Syria and Lebanon.[96] Its technology hubs, like Herzliya Pituach, Tel Aviv and Haifa, are close to occupied and enemy territories. Erez, a Unit 8200 soldier with aspirations of someday working in technology, regularly volunteers his unit affiliation. Though he visits Jerusalem often, he is afraid to walk around the old city on Shabbat for fear of getting kidnapped in one of the Shuks.[97] Benjamin, another Unit 8200 alumnus, can understand Erez's concern. Benjamin once backed out of a hiking trip along the Israel National Trail for fear of capture. Despite this, his Unit 8200 affiliation is listed at the top of his resume. When asked why, Benjamin responded that "saying you're from Unit 8200 is like a golden ticket into the tech industry"—the same reasoning Benjamin wanted to be in Unit 8200 in the first place.[98]

Benjamin's response reveals that the incentive to declare Unit 8200 association in the technology sector outweighs the potential risks for doing so, suggesting that Unit 8200 has become an extremely beneficial credential in the workplace. That public declaration is unenforced by the IDF increases the benefit of this credential, as more and more successful technologists become associated with the unit. It is intuitive that the more a credential is seen as valuable, the greater the demand for such a credential will be. Thus, the more alumni are able to

[95] Name Redacted. Personal Interview. 18 February 2014.

[96] Central Intelligence Agency. "Israel." Central Intelligence Agency. https://www.cia.gov/library/publications/the-world-factbook/geos/is.html (accessed February 10, 2014).

[97] A shuk is an open market. Name Redacted. Personal Interview. 15 November 2013.

[98] Name Redacted. Personal Interview. 18 February 2014.

declare affiliation with Unit 8200 in the workplace, the more this benefits Unit 8200 itself by creating a demand for experience from that unit.

Republican theory is a theory of political participation positing that citizens are compelled toward military service in exchange for certain benefits of citizenship, such as social status, protection, and certain rights. In democratic societies this exchange is a delicate balance as public opinion toward the military can devalue service, rendering the exchange asymmetric.[1] This asymmetry is exacerbated when the value for military service bears less social prestige, as in modern Israel.[99] The natural strategy for rebalancing the republican contract between citizen and state is either to lessen the sacrifice of military service, or increase the returns associated with military service in accordance with changing values. Current military organization theory supports the idea that change is underway in the Israel Defense Forces, as the army is altering its reputation to respond to more modern values. As the paradigm of military service as a social rite of passage diminishes in Israeli society, and as the expansionist work of the IDF in contested territories has increasingly come into question, the IDF has adapted by moving toward an army with a more "professional ethos."[100]

When considering the semisecret status of Unit 8200's alumni network within the context of republican theory, the puzzle of tolerated semi-secrecy becomes more clear. More than any other unit in the IDF, Unit 8200 has garnered a reputation for economically successful alumni, a reputation that is perpetuated as the affiliations of more and more successful alumni become public. The incentive to declare affiliation with Unit 8200 is evidence of positive signaling; by

[99] Cohen, Stuart A. "Changing Civil–Military Relations in Israel: Towards an Over-subordinate IDF?." *Israel Affairs* 12, no. 4 (2006): 250.
For example, rapid economic growth and globalization in societies can devalue military service, because individualistic principles can become more important than market values. The phenomenon of changing republican contract has been evident at certain times throughout United States history. For example, around the end of the cold war citizens from stronger socioeconomic backgrounds trended toward a clear disinterest in serving in the military.[99]

[100] Cohen, Stuart A. "Changing Civil–Military Relations in Israel: Towards an Over-subordinate IDF?." *Israel Affairs* 12, no. 4 (2006): 250.

declaring association with the unit, alumni members reap increased return from military service in the form of increased social and market benefit. While public identities of alumni is a national security concern, this incentive is tolerated by the Israel Defense Forces because it makes military experience a tradeoff with an economic payoff, the sort of economic payoff that could benefit alumni of the unit for the duration of their working lives. In this context, the incentive structure created by the semisecret status of Unit 8200 is a highly adaptive move on behalf of the IDF to make the exchange between service in classified intelligence units attractive and desirable in the modern age. As post-materialist values of modern states continue to develop, the question of how to reconstitute military service becomes an increasingly relevant question. Likewise, as the global cyber security threat landscape becomes an increasingly pressing priority in military affairs, the incentive structures in place to attract top talent to secret intelligence work becomes a crucial issue in national security.

Brain Security is National Security

Positive economic growth increases the individualistic values of citizens. This means that as economies develop, in an effort to better their economic standing, the citizens of free market societies place individual priorities for economic mobility at a higher value. Despite numerous wars since the country's founding, Israel's economy has grown steadily. A huge facet of this growth has been the development of the high-technology sector in Israel. During the beginning of Israel's high-technology development in the 1990s, the country's GDP grew by 60% in one decade.[101] The high-technology sector in Israel is the fastest economic sector for growth, by a margin that continues to increase annually.[102] This margin is projected to increase commensurate with the growing importance of high technology in the global economy. This is especially true of Israel, as the greatest verticals for economic growth lie in exportation to foreign markets. 80% of Israel's high-technology products are exported to foreign markets.[103]

Current understanding of civil-military relations contends that civil interest groups are placing new pressures on the IDF. In recent years, sources of this civil pressure have included entering conscripts and their parents on military recruitment policies. The agendas of the interest groups regarding recruiting have been shaped in large part by the media reputation of the army and its various units.[104] Unit 8200 enjoys a growing and infamous presence in the domestic and international press, with a media reputation for conscripting only the smartest kids out of high school and churning out an alumni population of technology millionaires. The rising economic value of a Unit 8200 credential, which is perpetuated by the public reputation of its alumni network, suggests that this credential is a key part of the recruitment understanding of entering recruits and their parents. With the signaling value Unit 8200, conscription in the military bears with it the return of economic security and intellectual credentialing.

This theory contends that Unit 8200 is seen as elite and desirable in the Israeli economy, due to the rise of the technology sector and the value of a Unit 8200 credential for signaling

[101] "Economy." Israel Ministry of Foreign Affairs. http://mfa.gov.il/MFA/AboutIsrael/Economy/Pages/ECONOMY-%20Challenges%20and%20Achievements.aspx (accessed February 5, 2014).

[102] "Economy Sectors." Israel Ministry of Foreign Affairs. http://mfa.gov.il/MFA/AboutIsrael/Economy/Pages/ECONOMY-%20Sectors%20of%20the%20Economy.aspx (accessed February 5, 2014).

[103] "Economy: About." Israel Ministry of Foreign Affairs. http://mfa.gov.il/MFA/AboutIsrael/Economy/Pages/ECONOMY-%20Sectors%20of%20the%20Economy.aspx (accessed February 5, 2014).

[104] Levy, Yagil . "Who Controls the IDF? Between an "Over-Subordinate Army" and "a Military that has a State" ." The Open University of Israel Working Paper Series.

intelligence. Because of this, the perpetuation of the public network of Unit 8200 alumni benefits the increasing civil pressure from parents and conscripts directed at the recruitment policies of the IDF. This theory also contends that as the technology sector becomes a more powerful aspect of the economy, the sector itself and the knowledge workers that run it are themselves a powerful body with leverage over the military. Since its founding, a focus on improving the Israeli economy has been a central focus of IDF rhetoric. At certain times in Israeli history, the economic benefit of a strong military force has been emphasized to justify exorbitant defense spending. Today, as the IDF moves from away from a persona of nation building to a persona of a more professional army, the professional relationship between the army and the private sector is important. Thus, the rise of the technology sector presents an increasingly important source of civil pressure over the IDF. The credentialing value of Unit 8200 identification benefits technology knowledge workers within the private sector economy, rendering the public network of Unit 8200 positive for the health of the technology sector as a whole and therefore an objective of the technology's sector's strategic interests.[105]

An interest in catering to the free market, and specifically the technology sector, is a demonstrated priority of the Israeli government and by extension the IDF. In Prime Minister Netanyahu's speeches at both Israel's Cybertech Conference and at the Davos World Economic Forum in 2014, Netanyahu underlined the importance of maintaining a favorable economic environment for alumni of elite technology units.[106] The subtext of these statements was the notion that elite technology workers could graduate from elite intelligence units, begin companies in Israel, and then leave Israel if they found the market environment in Israel

[105] *Ibid.*

[106] Netanyahu, Benjamin. "Israel and the Global Economy." Speech, Annual Meeting 2014 from Davos World Economic Forum, Davos, January 23, 2014.
Netanyahu, Benjamin. "Cyber Security and the Future of Israel." Keynote speech, Cybertech from Israel Defense, Israel Ministry of Economy, Tel Aviv, January 28, 2014.

unfavorable. This is a huge national and economic security concern for Israel, as negative emigration of knowledge workers represents the loss not only of the economic value of that worker, but of the companies that worker created, and the potential value of that worker's descendants. Netanyahu's comments demonstrate an awareness of the grave security and economic concerns posed by the maintenance of a free market. This theory argues that this is evidence of the enormous leverage alumni of elite intelligence units, specifically Unit 8200, have over the Israeli government and the IDF. Formal policies of secrecy protect the national security of Israel by protecting sensitive intelligence information. Perpetuating a public network of Unit 8200 alumni that is favorable to the technology sector protects economic security by catering to a fickle, mobile, and economically well-endowed body of knowledge workers. Thus, the toleration of the public identities of Unit 8200 alumni is motivated by an incentive structure that favors recruitment policies, but that also appeases the civil interests of parents, conscripts, and the technology sector itself.

In the cyber age, brain security is national security. Cyber preparedness does not follow normal metrics of military strength, including size of GDP, size of force, or weapons stockpiles.[107] Instead, winners and losers in the cyber age are decided much more by the ability to capitalize and cultivate national brainpower. National service requirements are undermined by the ability of elite technology alumni to emigrate, taking enormous economic value with them. In a cyber threat environment, this brain drain represents not only economic loss but threats to national security. This underscores the need for Israel to maintain favorable recruitment incentives for elite units, particularly as cyber threats become more important. Israel's awareness

[107] Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no. 2 (2013): 7-40.

of rising cyber threats reinforces the notion that the maintenance of professional signaling for Unit 8200 is intentionally preserved to benefit not only alumni but also the IDF itself.

Part 2: The Unit 8200 Credential

Unit 8200 alumni are incentivized to declare their association with the unit in the private sector because there is a positive benefit to doing so. What is this positive benefit? In other words, what does a Unit 8200 credential mean? In and of itself, that a Unit 8200 credential is a positive enough signal to be worth declaring in the face of risks to physical harm and legal repercussion, is significant to understanding how a public network of Unit 8200 alumni exists and is perpetuated, and why this is positive for the recruiting efforts of the unit. The question of what exactly Unit 8200 signals is also relevant to understanding what incentive structures are in place to benefit the unit's recruiting policies. However, understanding more about what the Unit 8200 credential signals is helpful in understanding the more global phenomenon of how the unit's policies work to capitalize upon the brainpower resources available to it.

This part presents a theory for what exactly a Unit 8200 credential signals. It argues that declaring association with Unit 8200 is positive because it signals a perceived baseline level of intelligence. In addition, a Unit 8200 credential signals access to an exclusive network of alumni, and membership within close-knit social groups of other technical workers created during time in service. Finally, the Unit 8200 credential signals that those who possess it have certain experiences unique to the organizational characteristics of Unit 8200 itself.

Whiz Kids

When young people in Israel graduate from high school, national examinations help determine in which units they are placed. The Israel Defense Forces is relatively opaque about which criteria signal compatibility with which units, making it difficult to determine the baseline level of academic competencies possessed by members of various units. However, it is known that the IDF places students in units based off relative talents, and some units are more prestigious or elite than others.[108]

Zohar Zisapel is co-founder of RAD Group and often considered “the Bill Gates of Israel.”[109] An alumni of elite intelligence units himself, he often invests in and hires young entrepreneurs from Unit 8200. When considering new hires, Zisapel explained that he does not necessarily look for Unit 8200 or other elite unit alumni. However, having a Unit 8200 credential signals that the applicant has some baseline level of intelligence in order to get into the unit in the first place. Zisapel explained that everyone in Israel has to take the same national examinations. The kids who you knew were the smartest were the ones who got into Unit 8200 or other elite technology and intelligence units. This general understanding informs the perception that Unit 8200 alumni are smart, which can be a plus for someone’s resume.[110]

Imagine being the valedictorian of a high school class. All the smartest kids you know just got drafted to Unit 8200 or another elite intelligence unit. Likewise, all the smartest kids you knew wanted to get into Unit 8200. You do too; it would symbolize that you are smart. Your Jewish parents, rather than pushing you to get into the most elite college, are hoping you score well enough on a test to get drafted into “the whiz kid” unit.[111] The experience of getting drafted into the military informs a societal understanding those who get drafted into Unit 8200 service are intelligent. This understanding is perpetuated and institutionalized by the media, and also by

[108] "Creme de la creme: How the IDF Selects the Best of the Best for its Most Elite Units." IDF Blog The Official Blog of the Israel Defense Forces. http://www.idfblog.com/2013/08/11/creme-de-la-creme-how-the-idf-selects-the-best-of-the-best-for-its-most-elite-units/ (accessed March 1, 2014).

[109] "VoIP Alternatives." 25 Years of RAD Group: A Conversation with Zohar Zisapel. May 22, 2006.

[110] Zisapel, Zohar. Phone Interview. 5 February 2014.

[111] "Unit 8200 and Israel's high-tech whiz kids." UPI, June 4, 2012.

formal statements made by the Israeli government, the IDF and the Prime Ministers office lauding the elite nature of Israeli intelligence units.[112] This public reputation for Unit 8200 renders affiliation with Unit 8200 a sign of intelligence in the marketplace of knowledge workers.

The Golden Ticket

Having a Unit 8200 credential signals to the Israeli technology community that you are smart. However, affiliation with Unit 8200 also signals access to a special network. The network effects of a Unit 8200 credential are threefold. First, experience working in Unit 8200 ensures network externalities from living and working with other intelligent people during time spent in service. Second, inclusion in the Unit 8200 alumni network places alumni within a social network where social norms encourage assisting and helping out other members of the unit. And finally, Unit 8200 alumni status signals social capital, i.e. membership in an elite and exclusive group of technical knowledge workers.

Serving in Unit 8200 means working, living and eating with other members of the unit for the duration of military duty. As a result, there is an understanding by many in Israel that the bonds formed in the army are the closest friends one will have for life. In Israel, there is a cultural norm that you meet your lifelong base of friends from the army. The IDF is famous for its sense of military cohesion.[113] For Benjamin, going into the army was the first time he felt surrounded by a community of peers interested in the same problems and intellectual subjects he was interested in. Meeting his comrades for the first time rendered his military experience and its antecedent training course really powerful, not just for the accruement of skills, but as an

[112] Netanyahu, Benjamin. "Cyber Security and the Future of Israel." Keynote speech, Cybertech from Israel Defense, Israel Ministry of Economy, Tel Aviv, January 28, 2014.

[113] Siebold, Guy L. "The evolution of the measurement of cohesion." *Military Psychology* 11, no. 1 (1999): 5.

important milestone in his social maturity. “I was straight out of high school, and I loved it. It was like a really cool frat here in America,” explained Benjamin, who now attends an American university. Benjamin contended that the closest friends one makes in Israel come out of the army, not out of a collegiate experience.

This theory contends that a powerful component of Unit 8200’s network effects are the network effects solidified during the time many alumni first enter the army. Right out of high school, a cohort of intelligent and intellectually curious knowledge workers leave home for the first time and enter into a period of rigorous training and intellectual service. This liminal period parallels the first few semesters of college in the United States. Where a Stanford computer science student might find his or her intellectual home among other Stanford students for the first time, an 8200 operative might find his or her intellectual home among soldiers doing similar work with similar intellectual caliber, creating powerful bonds that come with an added bonding power of military cohesion.[114] There are two externalities to this facet of the Unit 8200 alumni network. First, when a Unit 8200 alumnus enters into the workplace, he or she comes armed with a deeply bonded network of other talented knowledge workers. This means that the Unit 8200 alumni network does not just exist within its professional environment, but has roots stemming from the alumni’s background and individual development. Secondly, the value of military service itself is enhanced by the close-knit nature of the intellectual community. As operatives live and work together, the intellectual payoff of military service is enhanced by a highly-interactive and concentrated group of people that produces a beneficial environment of idea exchange.[115] To this end, this thesis argues that Unit 8200 alumni have deep bonds with other alumni formed during service. These bonds help their careers later on, as well as enhance the

[114] *Ibid*.

[115] Ibarra, Herminia, and Steven B. Andrews. "Power, social influence, and sense making: Effects of network centrality and proximity on employee perceptions." *Administrative science quarterly* (1993): 277.

time spent in service by enriching the intellectual community of these units. Finally, promoting the formation of these relationships not only is beneficial to the future careers of alumni, but it aids in the performance of Unit 8200 as a whole by enhancing the performance of the force during service.[116]

Not only is a lasting network created among Unit 8200 operatives during service, but Unit 8200 alumni status sets a foundation for further network development in the private sector. This thesis argues that the organizational culture of Unit 8200 creates an environment in which Unit 8200 are inclined and normalized to help each other out in the army. This cultural ethos carries over into the public and private sector, where regardless of whether or not the alumni in question interacted during service, there exists a common attitude of teamwork and assistance. Organization theory finds that teamwork and familial-oriented cultures might be more strategic than firms with more individualistic cultures.[117] This thesis posits that a team-work based culture extant within Unit 8200 carries over into the private sector, creating an alumni environment wherein members of the Unit 8200 alumni network actively and dynamically strengthen the alumni network by forming new connections and helping each other out in the business world. This is good for the private sector by lowering the friction of doing deals, increasing the velocity of business in general.[118] This benefits the alumni by providing a dynamic network externality in active participation in the alumni network, enhancing alumni careers.

Unit 8200 alumni association is important for its signaling value, but also for its network effects. These network effects include those bonds solidified during military service, as well as

[116]MacCoun, Robert , and William Hix. "Unit Cohesion and Military Performance." *Sexual Orientation and U.S. Military Personnel Policy: An Update of RAND's 1993 Study*. Berke: UC Berkeley Law , 2012. 155-156. Print.

[117] Zahra, Shaker A., James C. Hayton, and Carlo Salvato. "Entrepreneurship in family vs. Non‐Family firms: A Resource‐Based analysis of the effect of organizational culture." *Entrepreneurship theory and Practice* 28, no. 4 (2004): 363-381.

[118] Tsai, Wenpin. "Knowledge transfer in intraorganizational networks: Effects of network position and absorptive capacity on business unit innovation and performance." *Academy of management journal* 44, no. 5 (2001): 996-1004.

the professional network perpetuated by a culture within Unit 8200 of assistance and teamwork that remains extant to the alumni population after they leave service. The final component of this thesis' network theory regarding Unit 8200 stems from the social capital associated with participation in this network. The Unit 8200 credential has a signaling value that signals to other members of the technology industry that Unit 8200 alumni are a smart group of people with a technical skillset. This signaling value interacts within the alumni network to produce a social capital effect; i.e., association with the Unit 8200 alumni network is cool and exclusive. This is useful for those members of the Unit 8200 network because it gives them social status, which aids in the value-creation of that knowledge worker throughout the course of his or her career.[119]

A Common Experience

This thesis is interested not only in how intelligence organizations like Unit 8200 attract and cultivate top talent, but how this talent is used by the organizations themselves. This is measured in part through analysis of the performance of these intelligence alumni in the private sector. To this end, the final component of the second part of this theory, regarding what a Unit 8200 credential means, concerns the unique experiences of Unit 8200 service common to alumni. Not much has been written regarding the organizational facets of Unit 8200 and how they translate into the mechanics of the Unit 8200 alumni population in the private sector, which is the gap in the literature that this thesis seeks to fill. However, the contributions of Unit 8200's case study are empowered by existent understanding of the function of certain organizational characteristics. Specifically, Unit 8200 and its alumni network simultaneously benefit from the

[119] Tsai, Wenpin, and Sumantra Ghoshal. "Social capital and value creation: The role of intrafirm networks." *Academy of management Journal* 41, no. 4 (1998): 464-476.

following facets of Unit 8200's organization: institutional churn, small group dynamics, intellectual cross-pollination, rapid prototyping, and common training.

IDF officers serve for a small number of years early on in their careers, usually before college, with a subsequent period of reserve duty. This creates an important ecosystem of intellectual cross-pollination. This thesis argues that the transfer and exchange of ideas facilitated by the structural design of unit 8200 itself is beneficial to the unit, especially as the unit engages in highly technical work. In other words, this thesis argues that reserve duty and a flat organizational structure combine to produce an environment of symbiotic knowledge exchange with the private sector as knowledge workers jump back and forth between the private sector and the military. The knowledge exchange created by reserve duty is boosted by a unique labor structure to Unit 8200 itself where Unit 8200 operatives work in small and constantly changing teams. Finally, the short full-time spent in the military by each knowledge worker, roughly correlate to the terms of national service, produces broad-based institutional churn that is beneficial to cyber work. Institutional churn, small group dynamics, and intellectual cross-pollination enrich the intellectual environment of Unit 8200 itself, rendering the organization more equipped to handle ill-defined problems, i.e. highly-technical problems faced by modern cyber organizations. Finally, common training courses in the military reduces the friction for knowledge workers to work together in and out of the private sector by equipping knowledge workers from the same training courses the same basic pedagogy.

Conclusion

This thesis investigates how intelligence organizations attract construct effective human capital strategies in the face of the need to attract top talent and maintain secrecy policies. This question is approached in part by examining the publicity and network of organization alumni in the private sector. This chapter develops a theory proposing that there exists a public network of Unit 8200 alumni in the high technology sector. This network is perpetuated by alumni of Unit 8200 because there is a positive benefit to the alumni for doing so. The network is tolerated by the Israel Defense Forces because its associated externalities benefit also the unit itself. The positive benefits of association with Unit 8200 for alumni themselves are unique and threefold. First, Unit 8200 carries with it a positive signaling value that alumni from this unit are smart and possess certain technical skillsets. Second, Unit 8200 association includes access to a special and valuable career network. And finally, Unit 8200 experience involves a certain set of common experiences that enhance the network and the credential of Unit 8200 itself. In addition, these common experiences indicate a unique manner and ability for Unit 8200 as an organization to take advantage of top technical talent in intelligence work. Although this chapter focuses on the example of Unit 8200, the argument it constructs highlights important features of the extraorganizational and intraorganizational human capital networks in intelligence organizations. In the following two chapters, this framework will be compared against empirical data from both Unit 8200 and US NSA in order to better understand how specific human capital strategies and secrecy policies function in the attraction and maintenance of a labor pool of highly technical knowledge workers.

Chapter 5: 8200 יחידה, Yehida Shmoneh-Matayim

On the landing site for 8200 Entrepreneurship and Innovation Support Program (EISP), an introductory video showcases participant testimonials alongside a heavy techno beat.[120] One of the most popular startup incubators in Israel, it is not closed to Unit 8200 alumni only; it just uses the name of the unit as its trademark. Unlike the traditional incubator model, which takes a cut of startup profits later on, EISP is non-profit, originally conceived of by members of the private and independent 8200 Alumni Association.

"The entrepreneurship program was conceived as a way for us, the 8200 alumni association, to see how we can assist the younger generation," explains Nir Lempert, chairman of the 8200 Alumni Association.

Its supporters' logos are stamped prominently on the websites front page, including leading firms in the finance and technology industry like Ernst and Young Israel and host of venture capital funds. On their own websites, the 8200 EISP logo is often stamped as a sign of community involvement.

"I am an alumnus of the unit," testifies Ernst and Young Israel Chairman Ronen Barel, "And if there is an opportunity, and this certainly is, to give back to the place that gave me so much, then I'm happy to be here."

[120] "The Entrepreneurship and Innovation Support Program." 8200 EISP. http://www.eisp.org.il/ (accessed March 6, 2014).

"The true melting pot of the Israel hi-tech industry are the technological military units, with 8200 as the leader," croons donor Hanina Brandes, founding partner of Naschitz Brandes law firm.

The 8200 EISP program is interesting because it illustrates many of the hypotheses that this thesis holds about the Unit 8200 network's impact in the technology sector. The Unit 8200 name does not denote an incubator of unit alumni founders, but is instead used to add social capital to the incubator by explicitly drawing a connection between the incubator and the unit. One donor sees the Unit as the "leader" of IDF technological units, which in turn carry social capital themselves. Another donor makes sure to identify his own affiliation to the unit before giving testimony himself. The entire model is philanthropic, where alumni of the unit and their associated firms justify their involvement by saying it is "giving back." Put a different way, alumni seem to be eager to help each other out. By opening their doors to non-unit alumni the program attempts to spread the ethos of Unit 8200 across society, and in turn, reinforce its brand.

This case argues that there exists a publically observable network of Unit 8200 alumni in the Israeli high-technology sector and that this network carries with it positive benefits for its members, including positive credentialing, social status, and access to an supportive network. This case also argues that this public network is correlated with an unenforced policy of human capital secrecy surrounding Unit 8200 in the high-technology sector. This chapter is the second chapter of this case study, and provides qualitative and quantitative evidence of a public network within Israel's high-technology sector. First, this chapter will look at qualitative evidence to suggest a public network of Unit 8200 alumni in Israel's technology sector. Then this chapter will examine Israel's human capital secrecy policies for Unit 8200 and other units in the Intelligence Corps. This chapter will go on to discuss the results of a social networking survey taken by members of the technology community, and how these results support this thesis' hypotheses. This chapter will conclude with a discussion of these results.

Qualitative Evidence of the Network

There is extensive evidence of a public network of Unit 8200 on the Internet. Unit 8200 alumni, or those who publically identify as such, have independently organized themselves into several groups online both closed and open. On LinkedIn, for example, there are three primary unit 8200 alumni groups. The first is associated with the unit 8200 Alumni Association, the same that cofounded the 8200 EISP incubator program: "8200 Fellowship – Israeli IDF."[121] Although this group is closed, several details are publically available. The group was created in April of 2008, and current 7,800 members are a part. This coheres with this thesis' hypothesis that Unit 8200's identity and the identities of its members have become significantly more public in recent years, correlating with the rise of software and computing services as an increasingly important facet of knowledge economies.[122] Like other LinkedIn groups, in order to request membership you must submit a request through the group's administrators, both of whom publically advertise their membership within the 8200 Alumni Association. Someone already within the group must approve your request. This provides reasonable assurance that someone within the Unit 8200 network verifies some connection of all members to Unit 8200 or its alumni association. Listed on the group page, outsiders of the group can see all members of their network (1st, 2nd, and 3rd degree connections) who are also members of the group. This is true of all closed groups on LinkedIn.

[121] LinkedIn. "8200 Fellowship - Israeli IDF." LinkedIn. http://www.linkedin.com/groups/8200-Fellowship-Israeli-IDF-84086/about (accessed April 1, 2014).

[122] This phenomenon is documented in earlier chapters of this thesis.

The other two main groups on LinkedIn include "Independent 8200 Alumni"[123] and "The 8200 Alumni Developers Group."[124] The former is an open group founded in 2012 with 390 members.[125] The latter is a private group with 206 members, founded in 2013. It is a subgroup of the group "Developers in Israel." It is the only subgroup of this group that is associated with a unit of the military; the other twelve are associated with certain skillsets like Java or C++.[126] There is no verified employer page on LinkedIn for Unit 8200, because the identity of the unit itself is technically secret. This can be contrasted with the NSA in Chapter 6, which does have a verified employer page on LinkedIn.

In addition to LinkedIn groups, there exist other groups online including those on Facebook and the 8200 Alumni Association itself. One Facebook group, "8200 Fellowship – Israeli IDF" contains 1,171 members and shares the same group administrators as the LinkedIn group with the same name.[127] Although it is a closed group, meaning that someone already in the group must approve your request to join, the group members are public and searchable. The 8200 Alumni Association itself is another online, closed group.[128] It is not affiliated with Unit 8200 itself, but is rather a private organization in Israel started by alumni.[129] It is closed, meaning that a special login is required in order to access the website. Through this association, any alumni could verify the identities of any other alumni instantaneously, as each alumni can see the members of other alumni online. According to all Unit alumni interviewed for this thesis, while in the army information is siloed such that one operative could not verify the identities of all

[123] LinkedIn. "Independent 8200 Alumni." LinkedIn. https://www.linkedin.com/groups/Independent-8200-alumni-4260738/about (accessed April 2, 2014).

[124]LinkedIn. "The 8200 Developers Group." LinkedIn. http://www.linkedin.com/groups/8200-developers-group-7413276/aboutFind a website by URL or keyword... (accessed May 31, 2014).

[125] *Ibid.*

[126] *Ibid.*

[127] Facebook. 8200 Fellowship - Israeli IDF. https://www.facebook.com/groups/370330037734/ (accessed April 1, 2014).

[128] 8200 Alumni Association. "8200 Alumni Association." 8200. http://www.8200.org (accessed March 4, 2014).

[129] Nadav, Inbar. Personal Interview. 17 October 2013.

other 8200 members who might be working on different teams. The alumni association shows that this is different once Unit 8200 members become alumni and join these groups; at that point, they have immediate access to all alumni also in the group whether they served with them or not.

Unit 8200 is estimated to be significantly smaller than any intelligence organization in the United States, as just one unit of an already small intelligence corps. Thus, with reasonable certainty the representation of 7,800, or 390, or 206 alumni in an online organization represents a large population of Unit 8200 alumni in circulation in the technology industry. In a private interview with one 8200 alumni, this thesis found that estimates for the size of Unit 8200 are a tiny fraction of its sister network in a place like the United States.[130] Consider the possibility then that Unit 8200 is 1,000 people. If this number were multiplied by around 12 (accounting for 36 years of peoples' working lives after the army, assuming all alumni of the unit stay for three years and subsequently enter the Israeli technology industry), then the estimate of Unit 8200 alumni in the technology sector would be 12,000. If this were the case, the public network of Unit 8200 alumni represented by these online groups is an extremely significant percentage of the total alumni population.

It should be noted here that despite the fact that these groups are closed, it is still possible to reconstruct a picture of what the broader network looks like, and reconstructing a picture of those in a closed online group is a relatively simple thing to do technically. So, even joining a closed group risks your identity as a Unit 8200 alumni getting out, especially for cyber adversaries. Simple machine learning techniques can reverse engineer a picture of the network through the network's nodes, given an initial known sample of people in the network. One 8200 alumni interviewed for this thesis, Ben, said he did this exact exercise with his friends after just having been drafted into 8200, because he wanted to see who else got in and because he was

[130] This is an estimate from a former Unit 8200 officer as part of an anonymous interview.

bored.[131] When asked if others in the unit would know how to do this, Ben responded that they 'definitely would,' or if not, they [as 8200 members and alumni] would be aware that it was at least possible. Thus, this thesis assumes that Unit 8200 alumni are aware that they are making their identities somewhat publically discoverable even when they are joining closed groups online. This is also true of participation in social networks in general, which connect individuals via nodes to friends in their networks.

While many alumni of elite Israeli intelligence organizations appear to join these public groups, not everyone coming out of Unit 8200 are comfortable joining alumni groups, closed or open. Nir, an economics researcher and 8200 alumnus, explained that he is not a member of the 8200 Alumni Association because it seemed like a security liability: "No way are they getting my email."[132] However, these aforementioned groups represent a significant population of Unit 8200 alumni who prioritize benefiting from an online network. An important component of this is what exactly is illegal and not illegal regarding human capital secrecy and Unit 8200. This will be discussed within the next section.

Human Capital Secrecy in Unit 8200

Formalized evidence of official secrecy policy for the IDF Intelligence Corps is extremely difficult to come by. This thesis was unable to find any unclassified resources detailing secrecy policies applicable to Unit 8200 alumni or the alumni of other intelligence units. However, this thesis was able to verify human capital secrecy policy for Unit 8200 through an interview with a former director of Unit 8200.[133] The identities of all brigadier generals who direct Unit 8200 are secret, thus the first name of the director will not be reprinted here. The

[131] Name Redacted. Personal Interview. 18 February 2014.
[132] Name Redacted. Personal Interview. 30 March 2014
[133] Name Redacted. Personal Interview. 17 October 2013.

director explained that human capital secrecy policy is extremely important to security liability management of the unit. Especially given the close proximity of Israel's adversarial neighbors, the risk of a Unit 8200 member being captured is a real one. As such, it is not technically permissible for Unit 8200 alumni to say they are from the unit, instead they can say that they are in "intelligence." It is not appropriate to publically identify oneself with the unit as either a current member or as an alumnus, resumes and job interviews included. These policies are made explicitly clear to all operatives of Unit 8200. Of those interviewed for this thesis who were both members of Unit 8200 and who publically identified themselves as such, all understood what was and was not against the rules. Of those rules they broke, many responded with the justification that "everyone did." The director explained that secrecy policy is not public because the Intelligence Corps is very secretive in general, and there does not exist the infrastructure to manage this sort of information in the unit. People know the rules, and the security threats are so real in Israel that people know the rules and are aware of the risks that could come from being unscrupulous. Although not publically advertised, Unit 8200 policy makes clear that public association with the unit whether in a professional or social setting is not permissible. Despite these policies, sufficient evidence online suggests that this is widely not followed. In the next section results from this social networking survey will be analyzed in order to better understand the features of the Unit 8200 alumni network, and the benefits members of the network reap in the technology sector by participation.

Survey Results

This thesis deployed a survey to members of the high-technology sector in Israel that asked questions about unit affiliation and its impact on individual careers in the technology sector. The survey was intended to confirm or support this thesis' hypothesis that Unit 8200 members enjoy positive signaling value and social capital through affiliation with the unit in the technology sector, and that this social capital and credentialing represents positive incentives for Unit 8200 alumni to disregard formal secrecy policy and associate themselves with the unit in their professional lives. The survey was deployed via a snowball sample to an initial sample of members of the technology sector, including alumni of Microsoft Junction incubator, Birthright Excel Alumni Group, and alumni of Elevator Fund. In addition, a link to the survey was advertised on the twitter account of TechAviv. Members of the Israeli technology community and Israeli society were encouraged to take the survey, whether or not they had served in the IDF, national service, or intelligence corps. This thesis divides the results data into two groups, those who identify as having served in intelligence and those who have not. Immediate limitations of the control groups should be noted here. The survey responders self reported their unit affiliation, and responded to the survey anonymously. Many members of the technology community contacted saying that they were uncomfortable taking the survey because of the questions asked, or mentioned that the questions asked were illegal. This thesis holds that many intelligence alumni declined to take the survey because it violated their sense of secrecy policy compliance. However, this thesis holds that a refusal to take the survey does not signify complete compliance with secrecy policy in general, it could be true that these members of the technology community identify with Unit 8200, or other units in the Intelligence Corps or IDF in other capacities. Thus, the results of this survey are limited.

--Secrecy

This thesis hypothesizes that alumni from Unit 8200 and the intelligence corps, while not technically permitted to associate with their units, would do so in a professional setting because it could benefit them professionally. Evidence from the survey supports this hypothesis. When asked, “Would you be comfortable stating your unit affiliation on this survey?” only 37% of intelligence alumni responded yes, while 63% responded no.

Figure 1: Intelligence Community Job Disclosure for Survey

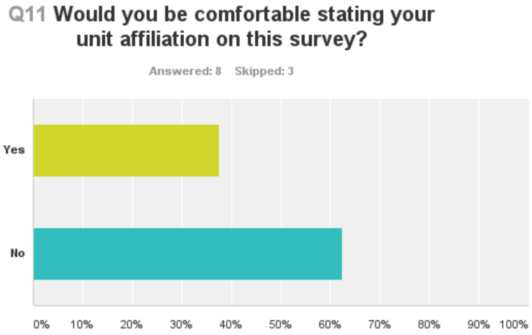
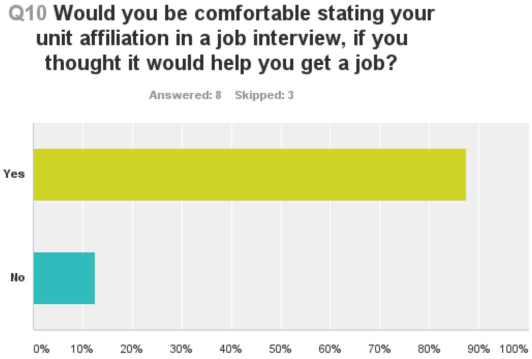


Figure 2: Intelligence Community Unit Disclosure for Job Interview



However, when asked “Would you be comfortable stating your unit affiliation in a job interview, if you thought it would help you get the job?,” 88% of intelligence alumni responded positively while 12% responded negatively. For the non-intelligence group, 53% responded that they would be comfortable stating their unit affiliation on the survey, while 93% responded that they would be comfortable stating their unit affiliation in a job interview if they thought it would help them get a job. This result suggests that mention of unit affiliation is broadly volunteered in professional settings for both groups. However, the result is particularly striking among intelligence alumni operating under more stringent secrecy rules.

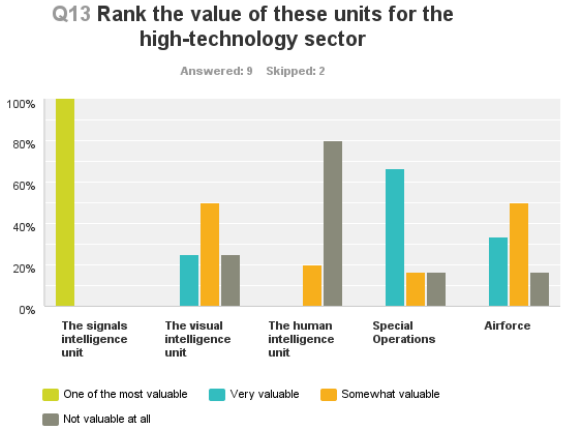
--Unit 8200

This survey did not ask respondents to personally identify whether or not they belonged to IDF Unit 8200. However, respondents were asked to force-rank the value of the signals intelligence unit (Unit 8200) against other intelligence units, and other areas of the army that traditionally hold social prestige.[134] Respondents were asked to rank the signals intelligence unit against the visual intelligence unit, human intelligence unit, special operations and air force in terms of their value for the high-technology sector. In the intelligence group, 100% of respondents listed the signals intelligence unit as "one of the most valuable." 25% of intelligence respondents said that the visual intelligence unit was "very valuable," 66% said that special operations was "very valuable," and 33% said air force was "very valuable." In the non-intelligence group, 53% cited the signals intelligence unit as "one of the most valuable" and 35% cited it as "very valuable." In the non-intelligence group, Special Operations and air force were second and third most cited by respondents as "one of the most valuable." These results say that when forced to choose, both intelligence alumni and non-intelligence alumni in the technology industry in Israel see the signals intelligence unit as one of the most valuable. These results suggest that the signals intelligence unit is seen as one of the most valuable in the technology industry across the industry, and that this viewpoint is particularly pronounced among intelligence alumni themselves. However, there are a few limitations to this question. First, while Unit 8200 is the signals intelligence unit of the IDF, Unit 8200 as a name was not stated on the survey. "Signals intelligence," and additionally "visual intelligence" and "human intelligence"

[134] Inbar, Efraim. "Israel's small war: The military response to the Intifada." *Armed Forces & Society* 18, no. 1 (1991): 29-50.

may not have been understood by all respondents fully, as the survey was administered in English.

Figure 3: Intelligence Community Views on Unit Value



To further examine the significance of Unit 8200 in the high-technology sector, participants were asked “how much preference do you believe employers give to alumni of the signals intelligence unit?” In response to this question, 30% of intelligence responders said “a lot of preference” while the other 70% of intelligence responders said “a good amount of preference.” No respondents in the intelligence group stated that the alumni of the signals intelligence unit received “a small amount of preference” or “no preference” at all. Comparing this with the non-intelligence group, 45% responded saying that “a lot of preference” was given to alumni of the signals intelligence unit by employers. 41% from this group said that they were given “a good amount of preference” and 14% said “a small amount of preference.” No respondents from this group stated that they were given no preference by employers.

Finally, respondents were asked to weigh in, on a scale of 1-10 (with 10 being the most advantageous and 1 being the least advantageous), how much advantage affiliation with the signals intelligence unit provides its members for success in the high technology sector. 54% of respondents overall responded with an eight, nine, or ten. 20% of respondents from intelligence responded with an eight, nine, or ten, and 33% responded with seven. In the non-intelligence group, 53% responded with an eight, nine, or ten.

These results are all caveated by the small sample size of the survey in general, and by a language barrier. Because the survey was administered in English and Unit 8200 was not directly named, results could be skewed as people may have misunderstood what the signals intelligence unit meant, particularly in the non-intelligence group. However, these results show clear trends within this data set, arguing that both intelligence and non-intelligence alumni and members of the high-technology sector see Unit 8200 as an elite unit that is one of the most valuable units in the high technology sector. There are also clear trends that both groups see Unit 8200 as advantageous for a professional career in technology, a credential that provides its holders significant preference from employers. This information supports this thesis' hypothesis that Unit 8200 is a uniquely valuable signaler in the high-technology sector, one that benefits those who publically associate themselves with it.

--Social Capital

A central hypothesis of this thesis is that Unit 8200 alumni and other intelligence alumni enjoy social status in the technology sector. A third hypothesis is that Unit 8200 affiliation is a positive signaler of technical credential and job experience. Significant evidence from the survey supports both these hypotheses. Both intelligence alumni and non-intelligence alumni responded that military unit affiliation is a significant factor in their professional lives. However, intelligence alumni responded saying that unit affiliation was more important to advancing their career than even their college degree. Survey participants were asked to rank the importance of the following characteristics to advancing their career: military unit affiliation, college degree, civilian work experience, military work experience, and IDF training course. In the non-intelligence group, prior civilian work experience was most cited as “one of the most important” or “very important” factors. This was followed by unit affiliation and college degree, both of which were ranked “one of the most important” by 20% of responders, and “very important” by 37% and 29% of respondents respectively.

Figure 4: Intelligence Community Importance of Experiences for Career Advancement

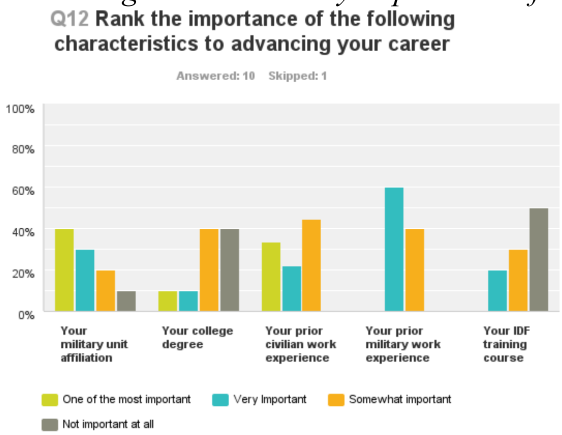
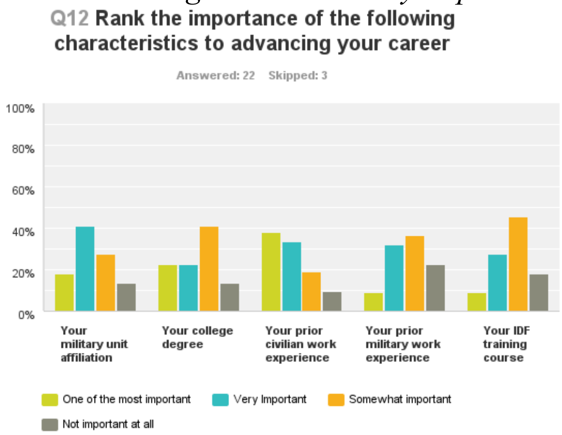


Figure 5: Non-Intelligence Community Importance of Experiences for Career Advancement



This suggests that unit affiliation in general is important to career networking in Israel, as is work experience and college degree. In the intelligence group, military unit affiliation was listed as “one of the most important” characteristics by 40% of respondents and “very important” by 30%. This characteristic was followed by prior civilian work experience, for which 33% of respondents cited as "one of the most important," and 22% cited as "very important." Only 10% of respondents from the intelligence group cited college degree as "one of the most important" characteristics, with another 10% citing it as "very important." These results suggest that unit affiliation, college degree and work experience all matter in the technology sector. However, for intelligence community alumni, unit affiliation matters significantly more than even college degree. This is much different from the non-intelligence group, which cites college degree as a very important characteristic for their careers.

To further examine the social capital value of intelligence work, the survey asked respondents to rank the social status their respective units had in high technology. Among non-intelligence respondents, only 9% responded saying that their unit had the most social status of any IDF unit in technology. 27% responded with "a significant amount," 23% responded with "some amount," and 41% responded with "not much at all." Of those who responded with "the most of any IDF unit" or "a significant amount," 50% were from the air force. In the intelligence group, 50% of responders responded that their unit had "the most [social status] of any IDF unit." 20% responded with "a significant amount," 30% responded with "some amount," none responded with "not much at all." These results suggest that intelligence unit affiliation carries with it social status within the high-technology industry, but so do existing units such as the air force.

Respondents were also asked to rank on a scale of 1-10 (with 10 being the most impactful and 1 being the least impactful), the advantage that service in their respective units provides for a career in the technology sector. In the intelligence group, 70% of respondents gave a ranking of eight, nine, or ten. In the non-intelligence group, the results were much more distributed. 32% responded with a one, two, or three, indicating that they viewed that their unit provided little advantage on the high-technology sector. 29% responded with a ranking of eight, nine, or ten. Of those who responded with an eight, nine, or ten, 60% were from the air force, a division of the army traditionally holding social prestige in Israel.[135] Advantage in the technology sector correlates with how respondents viewed the impact alumni from their unit had in the technology sector. When asked to rate, on a scale of 1-10 (with 10 being the most impactful and 1 being the least impactful) the impact alumni from their respective units have on the high-technology sector, 66% of respondents from the intelligence group ranked an eight, nine, or ten, and 89% responded with a rank of seven or above. In the non-intelligence group, only 29% responded with a ranking of eight, nine, or ten. By contrast, 42% responded with a one, two, or three.

--Credential

As established in Chapter 3, the benefits of skillsets learned in active service and those learned in training courses on the Israeli economy are historically lauded parts of army service by Israeli military officials. This thesis holds that the skills learned in technical units of the IDF as well as in their associated training courses are very valuable in the high-tech sector. When asked to rank the importance of skillsets learned in military training courses for respondents' everyday professional lives, 40% of respondents said that training course skillsets were "very important," and 30% of respondents said "somewhat important." When asked the same of skillsets learned in active service, 30% of intelligence alumni responded with "one of the most important," while 50% responded with "very important." In the non-intelligence group, 17% responded saying that training course skillsets were "one of the most important," and 21% responded saying that they were "very important." 61% responded saying that they were either "somewhat important" or "not important at all." When asked about the skillsets learned in active

[135] *Ibid*.

service, 26% of non-intelligence respondents said that skillsets from active service were "one of the most important" factors in their everyday professional lives, while 43% responded saying that they were very important. These results suggest that military training courses are more valuable for those from intelligence units after they leave the army. Military service in general is seen as valuable by both groups.

--Network

Finally, this survey looked at the presence and strength of Unit 8200's human capital network itself in Israel's high-technology sector. This thesis hypothesizes that intelligence alumni, and particularly alumni of Unit 8200, have access to a beneficial professional network of alumni in the high-technology sector, one in which members of the intelligence units are more likely to encounter other intelligence alumni in their professional lives, and where members of their network regularly helps other members of the network professionally. To interrogate this hypothesis, the survey asked respondents how often they encounter someone from their unit in their professional lives. Only 4% of the non-intelligence group responded saying "very often," and 39% responded saying "somewhat often." When asked how often they collaborated with someone from their unit on a project, 9% of the non-intelligence group responded with "very often" while only 22% said "somewhat often." In the intelligence group, 40% of respondents said that they encountered someone from their unit in their professional life "very often," and 50% of intelligence respondents said that this happens "somewhat often." Of intelligence respondents, 10% of respondents said that they collaborate with someone from their unit on a project "very often," and an additional 70% of respondents said that they collaborate with someone from their unit on a project "somewhat often." When asked "how likely are alumni from your unit to help out other members of the unit professionally?," 50% of intelligence respondents said “very likely,” and another 50% responded as “somewhat likely.” No intelligence respondents said “not very likely” or “not likely at all.” Among non-intelligence responders, 45% responded saying that alumni from their units were “very likely” to help out other members of the unit professionally. 27% of non-intelligence responders said that members of their unit were only “somewhat likely” to do so, 18% responded with “not very likely” and 9% responded with “not likely at all.”

Figure 6: Intelligence Community Professional Collaboration With Comrades from Own Unit

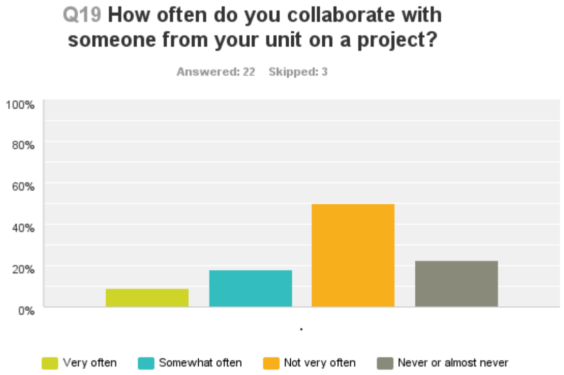
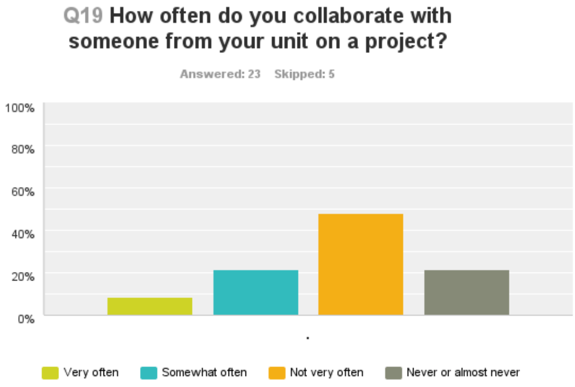


Figure 7: Non-Intelligence Community Professional Collaboration With Comrades from Own Unit



Finally, respondents were asked to rank on a scale of 1-10 (with 10 being the most important and 1 being the least important) how important unit affiliation is to their ability to network professionally. In the non-intelligence group, 40% of respondents responded with an eight, nine, or ten. By contrast, 44% of non-intelligence respondents gave a rank of one, two, or three. Of non-intelligence responders who gave a rank of eight, nine, or ten, 40% came out of the air force.

These results confirm the notion that military affiliation is an important component of Israeli society, and professional networks are colored according to military affiliation regardless of which unit someone is or is not an alumni. However, these survey results suggest that there could be an enhanced networking effect among intelligence alumni in the technology sector, where members of intelligence alumni networks might feel as though they are more supported in the technology industry than those in non-intelligence alumni networks. A little over a quarter of total respondents to take this survey were alumni of intelligence units. As mentioned at the beginning of this survey, this could be due to a selection bias, where fewer intelligence alumni elected to take the survey due to security concerns of taking a survey online. This ratio of intelligence to not intelligence does not necessarily reflect relative penetration of technology alumni in technology generally. This networking evidence from the survey suggests that in fact intelligence alumni are more likely to encounter other intelligence alumni in technology in their professional lives, and more likely to collaborate with them on projects. However, all of these findings should be further explored with a larger sample size.

Conclusion

This case finds that overall, evidence available supports the hypotheses of this thesis regarding secrecy and the Unit 8200 network in the high-technology sector in Israel. There exists extensive evidence of a public network of Unit 8200 alumni online and in independently initiated alumni groups, with a significant proportion of estimated alumni in the high-technology sector participating in these groups. Although it is illegal for Unit 8200 and other intelligence alumni to identify their affiliation with their respective units, evidence from the survey suggests that they are significantly likely to break this rule if it could advance their professional careers. Evidence from the survey suggests that Unit 8200 alumni enjoy a specific level of advantage and social capital in the technology sector, and that this signaling value is recognized by members of the technology industry generally and especially other intelligence alumni. Finally, survey results suggest that alumni of intelligence units are more likely to see themselves as part of more saturated and supportive career networks in the high-technology industry, in which alumni of the same unit are more likely to help others from their networks out, and where alumni are more likely encounter and collaborate with each other in the high technology industry.

Given the small sample size of this survey, the takeaways from these results are only suggestive. However, they do support the hypotheses of this thesis and elucidate clear areas of further research, including more stringent work on the relative social networks of unit alumni in technology, and how willing unit alumni are to transgress secrecy policy and under what circumstances.

Chapter 6: Conclusion

In an effort to understand how differences in secrecy policies and human capital strategies impact intelligence organizations' ability to attract top talent, this thesis compares the value of two different approaches to human capital management and secrecy in intelligence organizations. Through a critical examination of the empirical data surrounding two different intelligence organizations and their respective human capital strategies and networks, this thesis demonstrates the value of less stringent policies of secrecy in the attraction and retention of top technical knowledge workers to intelligence organizations.

Grounded in the literature from organization theory, this thesis held that the human capital strategies of intelligence organizations optimize over two competing constraints when attracting and making use of human capital: first, the need to manage secrecy policy and protect sensitive intelligence information; second, the mission-critical necessity to attract the best and brightest knowledge workers. Operating from the disciplinary framework provided by this theory, the strength and development of endogenous and exogenous networks of organizational affiliates enhances the social capital and signaling value associated with intelligence organizations. This social capital and signaling value not only benefits the affiliates of these intelligence organizations, it benefits the organizations themselves by creating positive incentives to devoting time to service. Additionally, secrecy policies which limit the information intelligence personnel can and cannot say about their affiliation, skills and job training inhibit the development and strength of these networks, dampening their associated social capital and signaling values. Because of this, less stringent policies of human capital secrecy aid in the attraction and maintenance of top talent in intelligence organizations.

To provide empirical evidence for this argument, this thesis conducted a comparative case study of two different intelligence organizations via qualitative social network analysis. Each case was chosen to represent two different approaches to human capital management and secrecy policy. In the first case, the US National Security Agency illustrated one human capital ecosystem with an obeyed, tighter policy of secrecy with regard to human capital management. This case critically analyzed the human capital networks surrounding this intelligence organization, demonstrating evidence of a dampened networks within its human capital ecosystem, and in turn, dampened signaling and social capital effects associated with these networks. In the second case, IDF Unit 8200 illustrated a different human capital ecosystem in which policies of secrecy surrounding what affiliates and alumni of Unit 8200 were and were not allowed to reveal about their affiliation, skills, and job training from experience with the unit remained relatively unenforced. Empirical data from the human capital ecosystem of Unit 8200 alumni showed a strong and cohesive set of endogenous and exogenous networks surrounding with the unit, as well as powerful signaling and social capital value associated with the network and the unit itself. This thesis argues that the differences in secrecy policies and human capital strategies directly contribute to manifest differences in NSA's and Unit 8200's human capital ecosystems. Furthermore, this thesis argues that human capital secrecy policy directly contributes to intelligence organizations' abilities to attract top technical knowledge workers.

Theoretical Implications and Areas of Further Research

While loosened policies of human capital secrecy enables intelligence organizations to more effectively attract top technical knowledge workers to devote time to national service, the extent to which these organizations can leverage loosened human capital secrecy to the benefit of their recruitment strategies should still be informed by each individual organization's particular limitations and challenges. Human capital secrecy policies are contributing factors in the development of strong endogenous and exogenous human capital networks around intelligence organizations, and in turn their associated network effects; yet other factors contribute to the establishment of these networks as well. In the case of the NSA, size and geography inhibit the establishment of tight exogenous networks of NSA affiliates in the high-technology industry. This is compounded by a secrecy policy informed by a more demographically pluralistic labor pool, which informs a policy of tighter human capital secrecy via a perceived concern of greater human capital security liabilities. These limitations contribute to a current debate within the US Intelligence Community over a tightening of security clearance policies. As established in Chapter 3, the security reforms suggested are estimated to cost additional billions of dollars per year.

The NSA case raises important questions about the role and efficacy of tighter secrecy policy. At an organizational size in which "it is unclear whether secrecy scales,"[136] the question for security policy reform should take into account the true efficacy of security clearance policies, including the human capital incentives they encourage or inhibit. Loosened secrecy policy as it relates to what employees can and cannot say about their job training and experiences can dampen the ability of intelligence organizations to attract top talent. Additionally, the findings of this thesis suggest that there could be hidden talent attraction costs in the cost-benefit analyses of new security policies. An area of further study thus involves further research into

[136] Lute, Jane Holl. Personal Interview. Stanford, CA, 26 February 2014 (See Chapter 3 for additional information.)

both the precise human capital effects of the implementation of different secrecy policies, and the scalability of secrecy policies, particularly in an age of online forums and social media.

In the case of Israel Unit 8200, a limited security bureaucracy correlated with empirical evidence of a relatively unenforced policy of secrecy surrounding what affiliates and alumni of the unit were and were not allowed to say about their affiliation, job training, or experiences. This unenforced secrecy policy correlated with a much more public network of Unit 8200 affiliates with a strong associated network effects including signaling and social capital value. As with the NSA case, other factors contributed to Unit 8200's manifest human capital ecosystem than just the unit's human capital strategy. A conscripted IDF anticipates churn, resulting in a large number of alumni of elite units like Unit 8200 entering the workforce. Furthermore, the strategic culture of the IDF and its traditional role in society helps balance the sunk cost of investing job training into members of the unit who only stay for a short time, only to leave and benefit from a strong professional network the high-technology private sector. Although evidence from this thesis suggests that these network effects are beneficial for Unit 8200 and affiliates, their enormous value in the private sector raises concerns in the Unit 8200 over leadership loss, or their ability to encourage top technical talent to make professional military careers after mandatory service. Finally, the security liabilities associated with unenforced policies of human capital secrecy, and a resulting public network of Unit 8200 are real and points of concern among unit leadership. An area of additional study for the Israel case involves further research into the security liabilities endemic to the public network of intelligence alumni and affiliates within broader Israeli society and the high-technology community. The Israel case also underscores the need to better understand effects of the dynamic relationship between growing high-technology economies and cyber intelligence organizations, as well as any maladaptive leadership loss that results from enhanced social capital and signaling value of intelligence experience in these competitive labor markets.

Bibliography

8200 Alumni Association. "8200 Alumni Association." 8200. http://www.8200.org (accessed March 4, 2014).

"About NSA." NSA. http://www.nsa.gov/about/index.shtml (accessed May 27, 2014).

"Actions Needed to Ensure Quality of Background Investigations and Resulting Decisions." *US Government and Accountability Office* (2014): 3.

"After Snowden, will the security clearance process finally change?." FedScoop. June 21, 2013.

Ahuja, Gautam. "The duality of collaboration: Inducements and opportunities in the formation of interfirm linkages." *Strategic management journal* 21, no. 3 (2000): 317-343.

[1]"American Cluster Innovation, Profiles from the 50 States." *Institute for Strategy and Competitiveness, Harvard Business School* (2008).

Atkins, Matthew. Interview by author. Personal interview. Stanford, CA, May 4, 2014.

Ben. Interview by author. Personal interview. Stanford, CA, February 2, 2014.

Blien, Uwe, and Gunther Maier. "The Starting Point." In *The economics of regional clusters: networks, technology, and policy*. Cheltenham, UK: Edward Elgar, 2008. 3.

Bourdieu, Pierre. "Social space and symbolic power." *Sociological theory* 7, no. 1 (1989): 14-25.

Buchris, Pinchas. Interview by author. Personal interview. Tel Aviv, Israel, October 17, 2013.

Burt, Ronald S. "The network structure of social capital." *Research in organizational behavior* 22 (2000): 345-423.

"By the numbers: The NSA's super-secret spy program, PRISM." Foreign Policy.

Central Intelligence Agency. "Israel." Central Intelligence Agency. https://www.cia.gov/library/publications/the-world-factbook/geos/is.html (accessed February 10, 2014).

Charney, Scott. Interview by author. Personal Interview. Stanford, CA, May 1, 2014.

Christensen, Michelle , and Frederick Kaiser. "Security Clearance Process: Answers to Frequently Asked Questions." *Congressional Research Service* 1 (2013).

Cohen, Stuart A. "Changing Civil–Military Relations in Israel: Towards an Over-subordinate IDF?." *Israel Affairs* 12, no. 4 (2006): 250.

"Creme de la creme: How the IDF Selects the Best of the Best for its Most Elite Units." IDF Blog The Official Blog of the Israel Defense Forces. http://www.idfblog.com/2013/08/11/creme-de-la-creme-how-the-idf-selects-the-best-of-the-best-for-its-most-elite-units/ (accessed March 1, 2014).

Curano, Bandel . Interview by author. Personal interview. Palo Alto, CA, March 20, 2014.

"Department of Defense's Use of Contractors to Support Military Operations: Background, Analysis, and Issues for Congress ." *Congressional Research Service* (2013): 2.

Div, Lior. Interview by author. Personal interview. Tel Aviv, Israel, October 17, 2013.

The Economist Newspaper. "MBAs are for wusses." The Economist. http://www.economist.com/node/16892040 (accessed May 1, 2014).

The Economist Newspaper. "Punching above its weight." The Economist. 10 November 2005.

"Economy." Israel Ministry of Foreign Affairs. http://mfa.gov.il/MFA/AboutIsrael/Economy/Pages/ECONOMY-%20Challenges%20and%20Achievements.aspx (accessed February 5, 2014).

“Employee Security Manual.” *Declassified. National Security Agency.* 14 April 1994.

"The Entrepreneurship and Innovation Support Program." 8200 EISP. http://www.eisp.org.il/ (accessed March 6, 2014).

Erez. Interview by author. Personal interview. Tel Aviv, Israel, October 15, 2013.

"Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Cyber Military Operations." *The Secretary of Defense* (Declassified 2009): 1-3.

Evans, Karen, and Franklin Reeder. "A Human Capital Crisis in Cybersecurity Technical Proficiency Matters." *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* x (2010).

Facebook. 8200 Fellowship - Israeli IDF. https://www.facebook.com/groups/370330037734/ (accessed April 1, 2014).

Falkowitz, Oren. Interview by author. Personal interview. Palo Alto, CA, February 19, 2014.

Fishelson, Yaron. Interview by author. Personal interview. Stanford, CA, April 10, 2014.

GAO report, “Personnel Security Clearances: Actions Needed to Ensure Quality of Background Investigations and Resulting Decisions.” 11 February 2014

George Washington University. "The National Security Agency: Declassified." The National Security Archive.

Greenwald, Glenn, Laura Poitras, and Ewen MacAskill. "NSA shares raw intelligence including Americans' data with Israel." *The Guardian*. Guardian News and Media, 12 Sept. 2013.

Hadar, Leon T. "Israel in the Post-Zionist Age: Being Normal and Loving It." *World Policy Journal* Vol. 16, no. 1 (1999): 76-86.

Hagel, Chuck. "Department of Defense Press Briefing by Secretary Hagel and Gen. Dempsey from the Pentagon Briefing Room." Address, Pentagon Briefing Room from Department of Defense, June 26, 2013.

Hannan, Michael T., and John Freeman. "The Population Ecology Of Organizations." *American Journal of Sociology* 82, no. 5 (1977): 929-964.

Hayden, Michael. "Beyond Snowden: An NSA Reality Check." *World Affairs Journal* (2014).

Holl Lute, Jane. Interview by author. Personal interview. Stanford, CA, February 26, 2013.

"The Human Capital Strategic Plan." *US Government and Accountability Office* (2013).

Ibarra, Herminia, and Steven B. Andrews. "Power, social influence, and sense making: Effects of network centrality and proximity on employee perceptions." *Administrative science quarterly* (1993): 277-303

Inbar. Interview by author. Personal interview. Tel Aviv, Israel, October 16, 2013.

Inbar, Efraim. "Israel's small war: The military response to the Intifada." *Armed Forces & Society* 18, no. 1 (1991): 29-50.

"Is the IT skills gap fact or fiction?." Enterprise CIO Forum. http://www.enterprisecioforum.com/en/question/it-skills-gap-fact-or-fiction.

"Is Israel Really America's Ally?." *Foreign Policy*. N.p., 20 June 2011.

Israel Defense Forces. "IDF's First-Ever Cyber Defenders Make History - IDF Blog | The Official Blog of the Israel Defense Forces." IDF Blog The Official Blog of the Israel Defense Forces.

“Israel: Supreme Court Decision Invalidating the Law on Haredi Military Draft Postponement." *The Law Library of Congress: Research and Reports* (2014).

"Israeli military fills up intel units with Iranian immigrants, report reveals - Diplomacy and Defense." Haaretz.com. January 9, 2014.

Kahana, Ephraim. "Unit 8200." In *Historical dictionary of Israeli intelligence*. Lanham, Md.: Scarecrow Press, 2006. 295-298.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no. 2 (2013): 7-40.

Levy, Yagil . "Who Controls the IDF? Between an "Over-Subordinate Army" and "a Military that has a State" ." The Open University of Israel Working Paper Series.

Lin, Bill. Interview by author. Personal interview. Stanford, CA, February 26, 2014.

LinkedIn. "The 8200 Developers Group." LinkedIn. http://www.linkedin.com/groups/8200-developers-group-7413276/aboutFind a website by URL or keyword... (accessed May 31, 2014).

LinkedIn. "8200 Fellowship - Israeli IDF." LinkedIn. http://www.linkedin.com/groups/8200-Fellowship-Israeli-IDF-84086/about (accessed April 1, 2014).

LinkedIn. "Independent 8200 Alumni." LinkedIn. https://www.linkedin.com/groups/Independent-8200-alumni-4260738/about (accessed April 2, 2014).

Lowenthal, Mark M.. *Intelligence: from secrets to policy*. Washington, DC: CQ Press, 2000.

MacCoun, Robert , and William Hix. "Unit Cohesion and Military Performance." *Sexual Orientation and U.S. Military Personnel Policy: An Update of RAND's 1993 Study*. Berke: UC Berkeley Law , 2012. 155-156. Print.

March, James G., and Michael D. Cohen. "Leadership in an Organized Anarchy." In *Classics of Organization Theory*. Oak Park, Ill.: Moore Pub. Co., 1978. 385-399.

Mike. Interview by author. Personal interview. Palo Alto, CA, February 19, 2014.

Miller, Charlie. Interview by author. Phone interview. Stanford, CA, February 3, 2014.

Mueller, Robert . Interview by author. Personal interview. Stanford, CA, April 28, 2014.

Nadav. Interview by author. Personal interview. Tel Aviv, Israel, October 17, 2013.

"National Liberal Arts College Rankings." U.S. News & World Report: News, Rankings and Analysis on Politics, Education, Healthcare and More.

"National Security Agency." LinkedIn. https://www.linkedin.com/company/1359?trk=prof-0-ovw-prev_pos (accessed April 15, 2014).

"National Security Archive Electronic Briefing Book No. 24". *Declassified documents and Archive publications on U.S. Intelligence*. 2007-09-27

"National Security Council Intelligence Directive No.9: Communications Intelligence." *National Security Agency* (1950): 1-3.

Nelson, Landy T. Interview by author. Personal interview. Stanford, CA, March 18, 2014.

Netanyahu, Benjamin. "Cyber Security and the Future of Israel." Keynote speech, Cybertech from Israel Defense, Israel Ministry of Economy, Tel Aviv, January 28, 2014.

Netanyahu, Benjamin. "Israel and the Global Economy." Speech, Annual Meeting 2014 from Davos World Economic Forum, Davos, January 23, 2014.

Nir. Interview by author. Personal interview. Stanford, CA, March 3, 2014.

"NSA Targets Systems Admins to Prevent Snowden-Type Leaks." Nextgov.

O'Connell, Anne. "The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World." *California Law Review* 94, no. 6 (2006): 1655-1744.

Orpaz, Inbal. "'Preserving the madness' in IDF intelligence." Haaretz, September 26, 2013.

Owen-Smith, Jason, and Walter W. Powell. "Knowledge networks as channels and conduits: The effects of spillovers in the Boston biotechnology community." *Organization science* 15, no. 1 (2004): 5-21.

Panetta, Leon. "Remarks by Secretary Panetta on Cyber Security to the Business Executives for National Security, New York City." Address, Business Executives for National Security from Department of Defense, New York City, October 11, 2012.

Perman, Stacy. "Chapter 4: Brains." In *Spies, Inc.: Business Innovation from Israel's Masters of Espionage*. Upper Saddle River, NJ: Pearson Education, 2010. All.

Podolny, Joel M. "A status-based model of market competition." *American journal of sociology* (1993): 829-872.

Podolny, Joel M., and Karen L. Page. "Network forms of organization." *Annual review of sociology* 24, no. 1 (1998): 57-76.

Reducing Government Secrecy: Finding What Works. Steven Aftergood. *Yale Law & Policy Review*, Vol. 27, No. 2 (Spring, 2009), pp. 399-416

Secrecy and Levy, Yagil, and Shlomo Mizrahi. "Alternative Politics and the Transformation of Society–Military Relations The Israeli Experience." *Administration & Society* 40, no. 1 (2008): 25-53.

"SelectUSA." The Software and Information Technology Services Industry in the United States. http://selectusa.commerce.gov/industry-snapshots/software-and-information-technology-services-industry-united-states (accessed May 2, 2014).

Shafritz, Jay M., and Philip H. Whitbeck. "Notes on the Theory of Organization." In *Classics of Organization Theory*. Oak Park, Ill.: Moore Pub. Co., 1978. 86-95.

Shafritz, Jay M., Philip H. Whitbeck, and James D. Thompson. "Organizations in Action." In *Classics of organization theory*. Oak Park, Ill.: Moore Pub. Co., 1978. 287-301.

Shochat, Eden. Interview by author. Phone interview. March 1, 2013.

Siebold, Guy L. "The evolution of the measurement of cohesion." *Military Psychology* 11, no. 1 (1999): 5.

"Signals intelligence." Princeton University. http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Signals_intelligence.html (accessed March 1, 2014).

Spence, Michael . "Job Market Signaling."*Quarterly Journal of Economics* 87, no. 3 (1978): 355-374.

"The Spies Inside Damascus." Foreign Policy. http://www.foreignpolicy.com/articles/2013/09/19/the_spies_inside_damascus_mossad_syria (accessed February 10, 2014).

Tsai, Wenpin. "Knowledge transfer in intraorganizational networks: Effects of network position and absorptive capacity on business unit innovation and performance." *Academy of management journal* 44, no. 5 (2001): 996-1004.

Tsai, Wenpin, and Sumantra Ghoshal. "Social capital and value creation: The role of intrafirm networks." *Academy of management Journal* 41, no. 4 (1998): 464-476.

"Study Reveals Cyber Security Teams are Bogged Down with Tactics Not Strategy." TEKsystems. October 16, 2014.

"Unit 8200 and Israel's high-tech whiz kids." UPI, June 4, 2012.

U.S. Bureau of Labor Statistics. "Summary: Computer and Information Technology Security Analysts." U.S. Bureau of Labor Statistics.

Uzzi, Brian. "Social structure and competition in interfirm networks: The paradox of embeddedness." *Administrative science quarterly* (1997): 35-67.

"VoIP Alternatives." 25 Years of RAD Group: A Conversation with Zohar Zisapel. May 22, 2006.

Waldstrøm, Christian. *Informal networks in organizations: a literature review*. Aarhus School of Business, Department of Organization and Management, 2001.

Zahra, Shaker A., James C. Hayton, and Carlo Salvato. "Entrepreneurship in family vs. Non-Family firms: A Resource-Based analysis of the effect of organizational culture." *Entrepreneurship theory and Practice* 28, no. 4 (2004): 363-381.

Zisapel, Zohar. Interview by author. Phone interview. Tel Aviv, Israel, February 5, 2014.

APPENDIX I: Interview List

Israel Unit 8200

[1] Benjamin. Interview by author. Personal interview. Stanford, CA, February 2, 2014.
Former Unit 8200 officer, current computer science undergraduate.

[2] Buchris, Pinchas. Interview by author. Personal interview. Tel Aviv, Israel, October 17, 2013.
Brigadier General and former Director of Unit 8200. Former General Manager of Israel Ministry of Defense. Advisor and seed investor in several security and high-technology companies, former managing director of companies in Israeli telecom, oil and gas, and private equity.

[3] Div, Lior. Interview by author. Personal interview. Tel Aviv, Israel, October 17, 2013.
Former member of Unit 8200. Founder and CEO of CyberReason.

[4] Erez. Interview by author. Personal interview. Tel Aviv, Israel, October 15, 2013.
Former officer of Unit 8200. Current computer science undergraduate in the United States.

[5] Fishelson, Yaron. Interview by author. Personal interview. Stanford, CA, April 10, 2014.
Veteran of non-intelligence unit in the Israel Defense Forces.

[6] Inbar. Interview by author. Personal interview. Tel Aviv, Israel, October 16, 2013.
Former leadership in elite subunit of Unit 8200. Technology consultant and cyber security expert. Hacker headhunter for high-technology companies, including CheckPoint Technologies.

[7] Nadav. Interview by author. Personal interview. Tel Aviv, Israel, October 17, 2013.
Brigadier General and former Director of Unit 8200.

[8] Nir. Interview by author. Personal interview. Stanford, CA, March 3, 2014.
Former member of Unit 8200. Current economics researcher.

[9] Shochat, Eden. Interview by author. Phone interview. March 1, 2013.
Former member of an elite intelligence unit. Founder of Face.com, acquired by Facebook. Founder and Managing Partner of Aleph Capital.

[10] Zisapel, Zohar. Interview by author. Phone interview. Tel Aviv, Israel, February 5, 2014.
Founder of RAD Group. Former director of elite intelligence unit. Prolific high-technology investor.

United States National Security Agency

[1] Atkins, Matthew. Interview by author. Personal interview. Stanford, CA, May 4, 2014.

Hoover Institution National Security Affairs Fellow researching intelligence recruitment. Intelligence officer, US Airforce.

[2] Charney, Scott. Interview by author. Personal Interview. Stanford, CA, May 1, 2014. Corporate Vice President, Microsoft Trustworthy Computing Group. Former employee of the US Intelligence Community.

[3] Curano, Bandel . Interview by author. Personal interview. Palo Alto, CA, March 20, 2014. Managing Partner, Oak Investment Partners.

[4] Falkowitz, Oren. Interview by author. Personal interview. Palo Alto, CA, February 19, 2014. Former NSA employee. Co-founder and CEO of Sqrrl.

[5] G. Interview by author. Personal interview. Stanford, CA, April 15, 2014.
Current NSA scholarship student and computer science undergraduate.

[6] Holl Lute, Jane. Interview by author. Personal interview. Stanford, CA, February 26, 2013. Former Deputy Secretary of Homeland Security.

[7] Lin, Bill. Interview by author. Personal interview. Stanford, CA, February 26, 2014. Computer and electrical engineering researcher and professor. Worked with the United States' Intelligence Community throughout course of career.

[8] Mike. Interview by author. Personal interview. Palo Alto, CA, February 19, 2014.
Former NSA employee. Founder of venture-funded big data startup.

[9] Miller, Charlie. Interview by author. Phone interview. Stanford, CA, February 3, 2014. Special Assistant, OCSA. US Army Cyber Command.

[10] Mueller, Robert . Interview by author. Personal interview. Stanford, CA, April 28, 2014. Former Director of the US Federal Bureau of Investigation.

[11] Nelson, Landy T. Interview by author. Personal interview. Stanford, CA, March 18, 2014. Colonel, US Army. US Army Strategist.

APPENDIX B: Survey and Responses

1. .		
Answer Options	Response Percent	Response Count
I understand the above information.	100.0%	38
answered question		38
skipped question		2

2. Did you serve in the IDF?		
Answer Options	Response Percent	Response Count
Yes	90.0%	36
No	10.0%	4
answered question		40
skipped question		0

3. What was the highest rank you achieved?	
Answer Options	Response Count
	38
answered question	38
skipped question	2

Question 3, Responses:

Number	Response Date	Response Text
1	May 11, 2014 7:02 PM	n/a
2	May 11, 2014 7:12 AM	Sergent first class
3	May 9, 2014 7:33 AM	Sergeant first class
4	May 3, 2014 1:33 PM	lieutenancy
5	May 1, 2014 11:37 AM	Major
6	Apr 29, 2014 10:06 AM	Captain
7	Apr 28, 2014 1:56 PM	First Sargent
8	Apr 28, 2014 12:09 PM	major
9	Apr 28, 2014 11:59 AM	First Sargeant
10	Apr 28, 2014 7:56 AM	Staff sergeant
11	Apr 28, 2014 7:47 AM	Sergeant
12	Apr 28, 2014 7:43 AM	Lieutenant
13	Apr 28, 2014 6:52 AM	First Sargent
14	Apr 28, 2014 6:49 AM	captain
15	Apr 28, 2014 6:08 AM	Officer
16	Apr 23, 2014 5:37 PM	Lieutenant
17	Apr 23, 2014 4:54 AM	Captain
18	Apr 22, 2014 5:11 PM	rasar

19	Apr 15, 2014 1:30 PM	ltc
20	Apr 14, 2014 11:19 PM	סמל ראשון
21	Apr 10, 2014 7:52 AM	Staff sergeant
22	Apr 9, 2014 8:34 AM	Major
23	Apr 8, 2014 5:26 PM	Lieutenant
24	Apr 8, 2014 9:39 AM	lieutenant
25	Apr 7, 2014 7:57 PM	First Sergeant
26	Apr 6, 2014 4:22 PM	Staff sergeant
27	Apr 6, 2014 2:59 PM	Sargent
28	Apr 6, 2014 8:58 AM	Captain
29	Apr 6, 2014 7:25 AM	Lcdr
30	Apr 6, 2014 7:06 AM	COL
31	Apr 6, 2014 1:00 AM	Officer
32	Apr 5, 2014 10:16 PM	sergeant (samal)
33	Apr 5, 2014 9:33 PM	First Sergeant
34	Apr 5, 2014 8:57 PM	First Sergeant
35	Apr 5, 2014 8:09 PM	Captain
36	Apr 5, 2014 7:50 PM	Lieutenant
37	Apr 5, 2014 7:35 PM	Sergeant major
38	Apr 5, 2014 7:20 PM	Major

4. For how many years did you serve?	
Answer Options	Response Count
	38
answered question	38
skipped question	2

Question 4, Responses:

Number	Response Date	Response Text
1	May 11, 2014 7:02 PM	n/a
2	May 11, 2014 7:12 AM	3
3	May 9, 2014 7:33 AM	3
4	May 3, 2014 1:33 PM	3
5	May 1, 2014 11:37 AM	8
6	Apr 29, 2014 10:06 AM	4.1
7	Apr 28, 2014 1:56 PM	3
8	Apr 28, 2014 12:09 PM	5.5
9	Apr 28, 2014 11:59 AM	3
10	Apr 28, 2014 7:56 AM	3
11	Apr 28, 2014 7:47 AM	2
12	Apr 28, 2014 7:43 AM	4
13	Apr 28, 2014 6:52 AM	3
14	Apr 28, 2014 6:49 AM	4
15	Apr 28, 2014 6:08 AM	3
16	Apr 23, 2014 5:37 PM	6
17	Apr 23, 2014 4:54 AM	9
18	Apr 22, 2014 5:11 PM	1 year + 10 years reserves (still active)

19	Apr 15, 2014 1:30 PM	5
20	Apr 14, 2014 11:19 PM	3 years and 4 monthes
21	Apr 10, 2014 7:52 AM	2
22	Apr 9, 2014 8:34 AM	18
23	Apr 8, 2014 5:26 PM	5.5
24	Apr 8, 2014 9:39 AM	3 years
25	Apr 7, 2014 7:57 PM	3
26	Apr 6, 2014 4:22 PM	3
27	Apr 6, 2014 2:59 PM	2
28	Apr 6, 2014 8:58 AM	5
29	Apr 6, 2014 7:25 AM	9
30	Apr 6, 2014 7:06 AM	25
31	Apr 6, 2014 1:00 AM	4
32	Apr 5, 2014 10:16 PM	2
33	Apr 5, 2014 9:33 PM	3
34	Apr 5, 2014 8:57 PM	3
35	Apr 5, 2014 8:09 PM	4.5
36	Apr 5, 2014 7:50 PM	5
37	Apr 5, 2014 7:35 PM	5
38	Apr 5, 2014 7:20 PM	7

5. If you served, what year did you join the IDF?	
Answer Options	Response Count
	38
answered question	38
skipped question	2

Number	Response Date	Response Text
1	May 11, 2014 7:02 PM	n/a
2	May 11, 2014 7:12 AM	2003
3	May 9, 2014 7:33 AM	2003
4	May 3, 2014 1:33 PM	1993
5	May 1, 2014 11:37 AM	1995
6	Apr 29, 2014 10:06 AM	Intelligence
7	Apr 28, 2014 1:56 PM	1999
8	Apr 28, 2014 12:09 PM	1992
9	Apr 28, 2014 11:59 AM	1980
10	Apr 28, 2014 7:56 AM	1994
11	Apr 28, 2014 7:47 AM	1994
12	Apr 28, 2014 7:43 AM	1991
13	Apr 28, 2014 6:52 AM	2002
14	Apr 28, 2014 6:49 AM	2003
15	Apr 28, 2014 6:08 AM	2001
16	Apr 23, 2014 5:37 PM	1995
17	Apr 23, 2014 4:54 AM	1998
18	Apr 22, 2014 5:11 PM	2003
19	Apr 15, 2014 1:30 PM	1982

20	Apr 14, 2014 11:19 PM	2006
21	Apr 10, 2014 7:52 AM	2010
22	Apr 9, 2014 8:34 AM	1993
23	Apr 8, 2014 5:26 PM	2009
24	Apr 8, 2014 9:39 AM	2006
25	Apr 7, 2014 7:57 PM	2005
26	Apr 6, 2014 4:22 PM	2005
27	Apr 6, 2014 2:59 PM	2004
28	Apr 6, 2014 8:58 AM	2005
29	Apr 6, 2014 7:25 AM	2005
30	Apr 6, 2014 7:06 AM	1977
31	Apr 6, 2014 1:00 AM	2008
32	Apr 5, 2014 10:16 PM	2007
33	Apr 5, 2014 9:33 PM	2007
34	Apr 5, 2014 8:57 PM	2005
35	Apr 5, 2014 8:09 PM	2006
36	Apr 5, 2014 7:50 PM	2005
37	Apr 5, 2014 7:35 PM	2004
38	Apr 5, 2014 7:20 PM	2004

6. My military unit can best be described as		
Answer Options	Response Percent	Response Count
Part of the Intelligence Corps	28.2%	11
Not part of the Intelligence Corps	15.4%	6
Combat Unit	30.8%	12
Airforce	12.8%	5
Other	12.8%	5
	answered question	39
	skipped question	1

7. Are you working or have you worked in the high-technology industry?		
Answer Options	Response Percent	Response Count
Yes	82.5%	33
No	17.5%	7
	answered question	40
	skipped question	0

8. If you work or have worked in high-technology, what best describes your job?

Answer Options	Response Percent	Response Count
Research and Development	14.7%	5
Finance	0.0%	0
Venture Capital	5.9%	2
Startup (technical role)	29.4%	10
Startup (non-technical role)	41.2%	14
Medium to Large technology company	8.8%	3
	answered question	34
	skipped question	6

9. Describe the impact you believe that service in the most elite signals intelligence unit has on members' future high tech career?

Answer Options	Response Count
	29
answered question	29
skipped question	11

Question 9, Responses:

Number	Response Date	Response Text
1	May 11, 2014 1:45 PM	I did not serve due to medical issues and it has negatively impacted my career.
2	May 9, 2014 7:33 AM	It has a significant impact and a lot of my friends who served in elite intelligence units work nowadays in the high tech industry
3	May 3, 2014 1:33 PM	Some experience but mainly creditably and network (similar to ivy league graduates)
4	May 1, 2014 11:37 AM	Very high
5	Apr 29, 2014 10:06 AM	Technical background in a startup-like environment
6	Apr 28, 2014 1:56 PM	I learned a lot in the army
7	Apr 28, 2014 12:09 PM	N/A
8	Apr 28, 2014 7:56 AM	The army service, in computers/IT related capacity, provides a rare opportunity for people with no experience, to be involved in real life, enterprise level IT projects. This would provide a stepping stone for pro IT jobs as a civilian later on. Or at least have been in my case
9	Apr 28, 2014	none

	7:47 AM	
10	Apr 28, 2014 7:43 AM	I think regardless of the unit, IDF alumni are educated to think out of the box, do much with less budget, and sometimes work in the "gray area". Regarding intelligence corps etc - of course it's quality manpower that is drafted to intel, but mostly it's all just the Israeli parallel of ivy league fraternities and alumni clubs - the retired intelligence officers know and help each other, some of them are investors themselves or hold key positions in VCs, etc...
11	Apr 28, 2014 6:49 AM	Dealing with pressure and taking hard descitions
12	Apr 28, 2014 6:08 AM	Better improvisation skills
13	Apr 23, 2014 5:37 PM	it is an enabler for their career, and the best school.
14	Apr 23, 2014 4:54 AM	Provides technical knowledge and skills, strong and relevant network, confidence in one's abilities and potential, and reputation
15	Apr 22, 2014 5:11 PM	Good at working together on large scale technical projects.
16	Apr 15, 2014 1:30 PM	Very big impact
17	Apr 14, 2014 11:19 PM	The creativity abilitties due to lack of resources Nd the fact that you are being thrown to the water in an early age, kind of force you to think different and deal with the situation. Also mostly people's life depend in your decisions, which force you to increase the ability of responsibility..
18	Apr 10, 2014 7:52 AM	For me, nothing (:
19	Apr 9, 2014 8:34 AM	Indoctrination for solving problems
20	Apr 8, 2014 5:26 PM	Te unit is almost an high tech company of its own, it gives you experience and drives you towards creativity and entrepreneurship. Also, being an officer allows you to gather management and personal skills early on in your life
21	Apr 8, 2014 9:39 AM	The members of the intelligence unit learn to work under a lot of pressure with deadlines. They learn how to work with people, the 'Know How' of a big concern. In addition, I think that those units make the people who serve there a Sense of being capable to do things.
22	Apr 6, 2014 4:22 PM	There's no doubt that for many years now, quite a few leaders in successful high tech companies have had rich military background, especially intelligence related. The military service teaches you to think outside the box, and gives you the tools to deal with all sorts of situations that you encounter in the real world.
23	Apr 6, 2014 7:06 AM	very high impact
24	Apr 5,	most of the people that work in the high ranked position in high tech are

	2014 10:16 PM	usually people that served in thw 8200 unit (like me) and it is a big impact on their carrer and the way they are percieved by others.
25	Apr 5, 2014 9:33 PM	Members get the best tools for working with the most advanced technology and the knowledge that any person seeking career in high-tech needs to have.
26	Apr 5, 2014 8:57 PM	I'm not sure since the unit i served at is a field combat unit, it seems like these retired from the intelligence unit usually go for hight-tech while we, strong and masculine men from combat unit, have to go to Uni before, so we can learn how to oprate a computer...
27	Apr 5, 2014 8:09 PM	During the service we get to expose to many different technologies and we get the opportunity to be part of technological team , to join various of courses and to lead an important projects which gives us the advantage in a future high tech career
28	Apr 5, 2014 7:50 PM	It is the perfect training ground to learn the world of high technology needs and capabilities. In a young age, Israeli soldiers are given the platforms and the go ahead to work on high level project which are backed financially to ensure freedom of operation
29	Apr 5, 2014 7:35 PM	Experience, Desire, excellent

10. Would you be comfortable stating your unit affiliation in a job interview, if you thought it would help you get a job?		
Answer Options	**Response Percent**	**Response Count**
Yes	91.3%	21
No	8.7%	2
answered question		23
skipped question		17

11. Would you be comfortable stating your unit affiliation on this survey?		
Answer Options	**Response Percent**	**Response Count**
Yes	47.8%	11
No	52.2%	12
answered question		23
skipped question		17

12. Rank the importance of the following characteristics to advancing your career					
Answer Options	One of the most important	Very Important	Somewhat important	Not important at all	Response Count
Your military unit affiliation	9	12	9	4	34
Your college degree	6	8	13	7	34
Your prior civilian work experience	11	10	9	2	32
Your prior military work experience	2	13	14	5	34
Your IDF training course	3	9	13	9	34
				answered question	34
				skipped question	6

13. Rank the value of these units for the high-technology sector					
Answer Options	One of the most valuable	Very valuable	Somewhat valuable	Not valuable at all	Response Count
The signals intelligence unit	17	6	2	0	25
The visual intelligence unit	2	8	5	5	20
The human intelligence unit	0	3	6	7	16
Special Operations	4	7	6	3	20
Airforce	3	5	7	5	20
				answered question	33
				skipped question	7

14. On a scale of 1-10 (10 being the most impactful and 1 being the least impactful), rate the advantage that service in your unit provided you for a career in the technology sector.										
Answer Options	1	2	3	4	5	6	7	8	9	10	Response Count
.	4	3	3	1	2	2	5	3	8	3	34
									answered question		34
									skipped question		6

15. How important are the skillsets you learned in your military training course to your everyday professional life?					
Answer Options	One of the most important	Very important	Somewhat important	Not important at all	Response Count
.	5	9	13	6	33
				answered question	33
				skipped question	7

16. How important are the skillsets you learned in active service to your everyday professional life?

Answer Options	One of the most important	Very important	Somewhat important	Not that important at all	Respons e Count
.	9	15	5	4	33
				answered question	33
				skipped question	7

17. How much social status does your unit have in high-technology?

Answer Options	The most of any IDF unit	A significant amount	Some amount	Not much at all	Response Count
.	7	8	8	9	32
				answered question	32
				skipped question	8

18. How often do you encounter someone from your unit in your professional life?

Answer Options	Very often	Somewhat often	Not very often	Never or almost never	Response Count
.	5	14	10	4	33
				answered question	33
				skipped question	7

19. How often do you collaborate with someone from your unit on a project?

Answer Options	Very often	Somewhat often	Not very often	Never or almost never	Response Count
.	3	12	12	6	33
				answered question	33
				skipped question	7

20. On a scale of 1-10 (with 10 being the most impact and 1 being the least impact), how much impact do alumni from your unit have in the high-technology labor force?

Answer Options	1	2	3	4	5	6	7	8	9	10	Response Count
.	5	3	3	2	1	2	4	7	3	3	33
										answered question	33
										skipped question	7

21. How much preference do you believe employers give to alumni of the signals intelligence unit?

Answer Options	A lot of preference	A good amount of preference	A small amount of preference	No preference	Response Count
.	13	16	3	0	32
				answered question	32
				skipped question	8

22. How likely are unit alumni from your unit to help out other members of the unit professionally?

Answer Options	Very likely	Somewhat likely	Not very likely	Not likely at all	Rating Average	Response Count
.	15	11	4	2	1.78	32
					answered question	32
					skipped question	8

23. On a scale of 1-10 (with 10 being the most important and 1 being the least important), how important is your unit affiliation to your ability to network professionally?

Answer Options	1	2	3	4	5	6	7	8	9	10	Response Count
.	2	6	3	1	2	3	3	6	6	1	33
										answered question	33
										skipped question	7

24. On a scale of 1-10 (with 10 being the most advantageous and 1 being the least advantageous), how much advantage does your unit affiliation give you for success in the high-technology sector?

Answer Options	1	2	3	4	5	6	7	8	9	10	Response Count
.	4	7	4	0	2	1	5	8	1	1	33
										answered question	33
										skipped question	7

25. If you did not serve in the signals intelligence unit, on a scale of 1-10 (with 10 being the most advantageous and 1 being the least advantageous), how much advantage do you think this affiliation provides its members for success in high tech sector?

Answer Options	1	2	3	4	5	6	7	8	9	10	Response Count
.	1	2	2	1	3	4	5	8	4	3	33
										answered question	33
										skipped question	7

APPENDIX C: Survey Responses

Figure 1: Intelligence Community Job Type

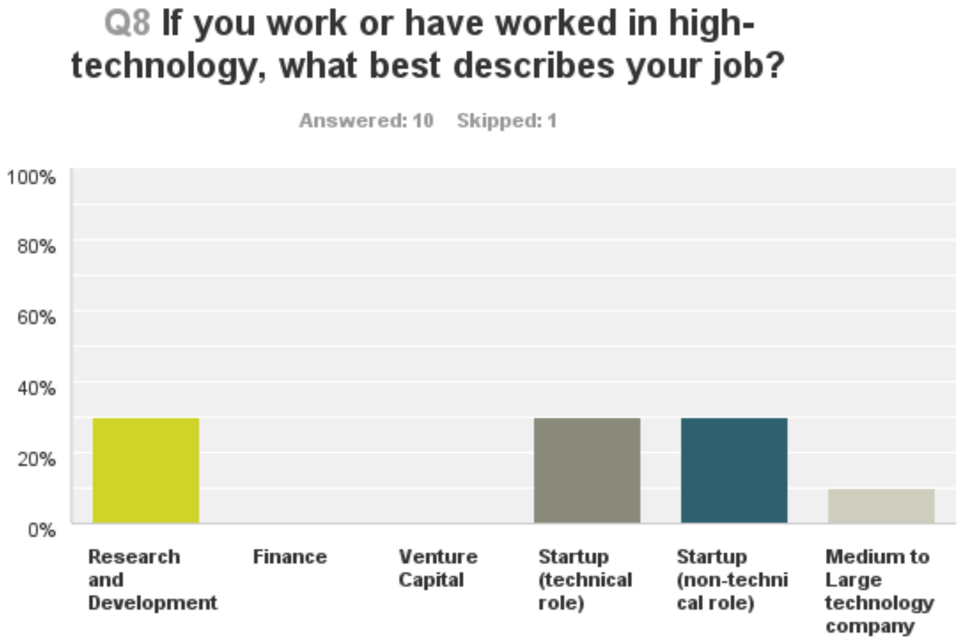


Figure 2: Intelligence Community Unit Disclosure for Job Interview

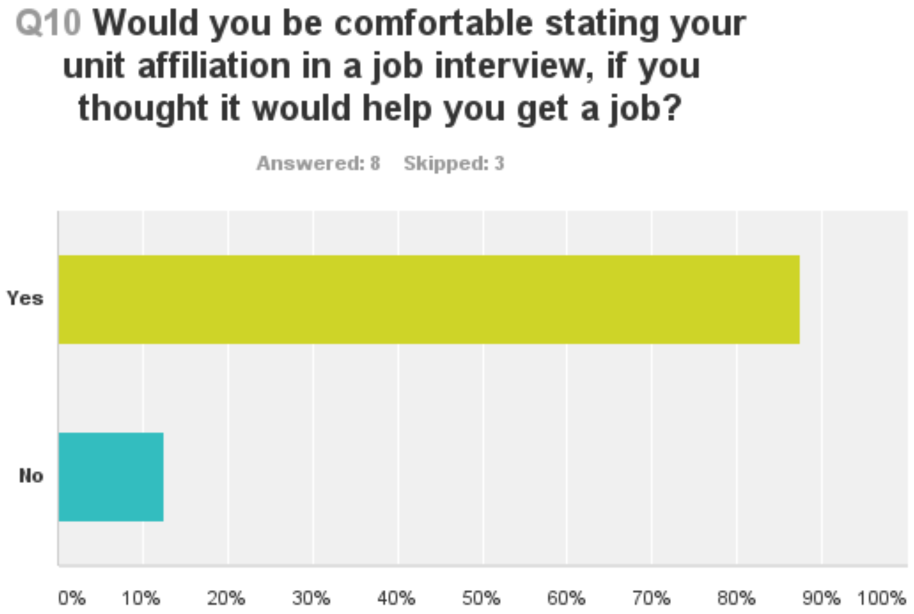


Figure 3: Non-Intelligence Community Job Disclosure for Survey

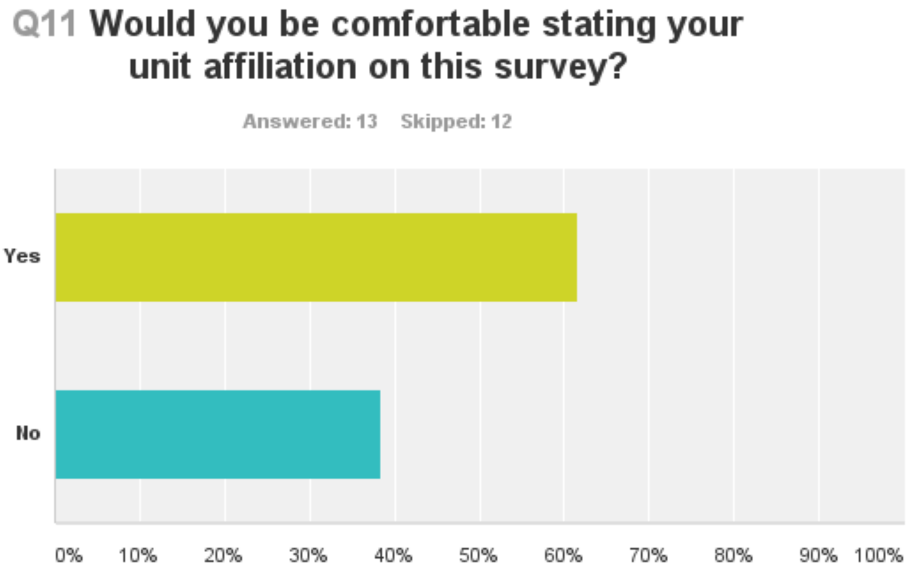


Figure 4: Intelligence Community Job Disclosure for Survey

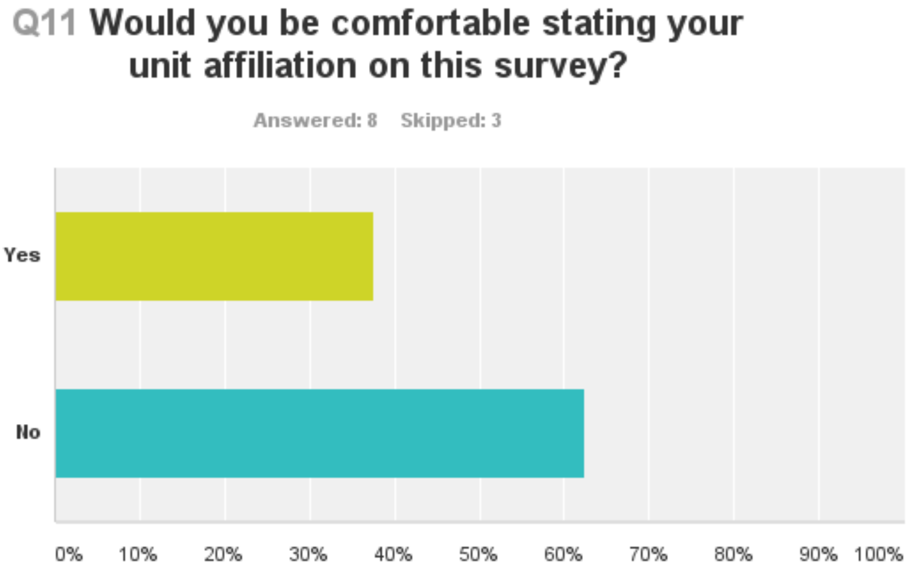


Figure 5: Intelligence Community Importance of Experiences for Career Advancement

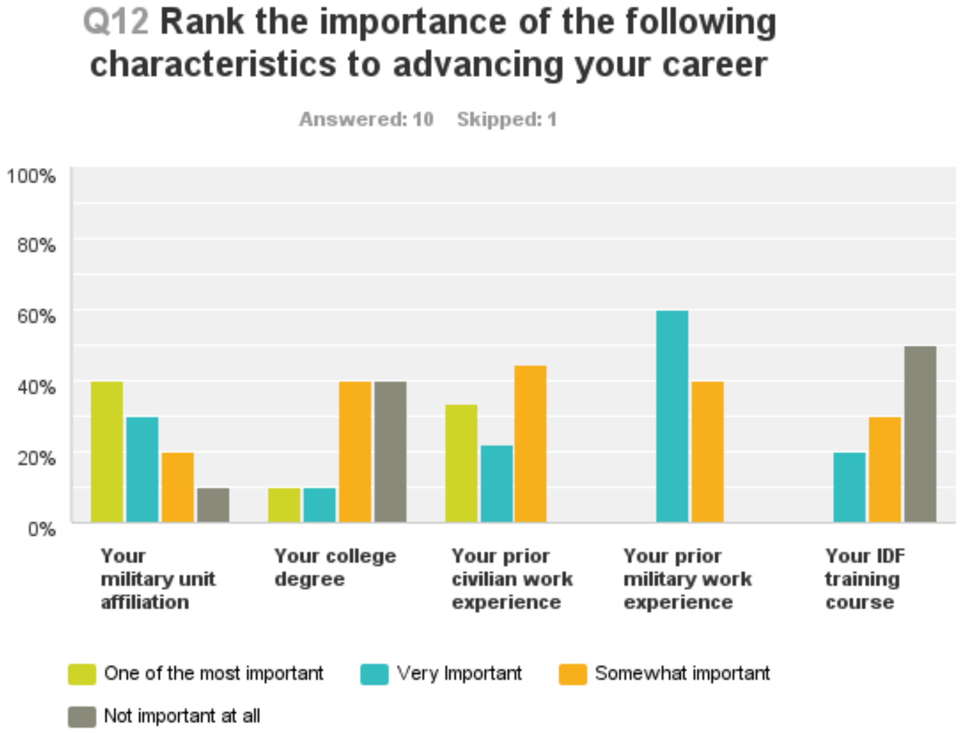


Figure 6: Non-Intelligence Community Importance of Experiences for Career Advancement

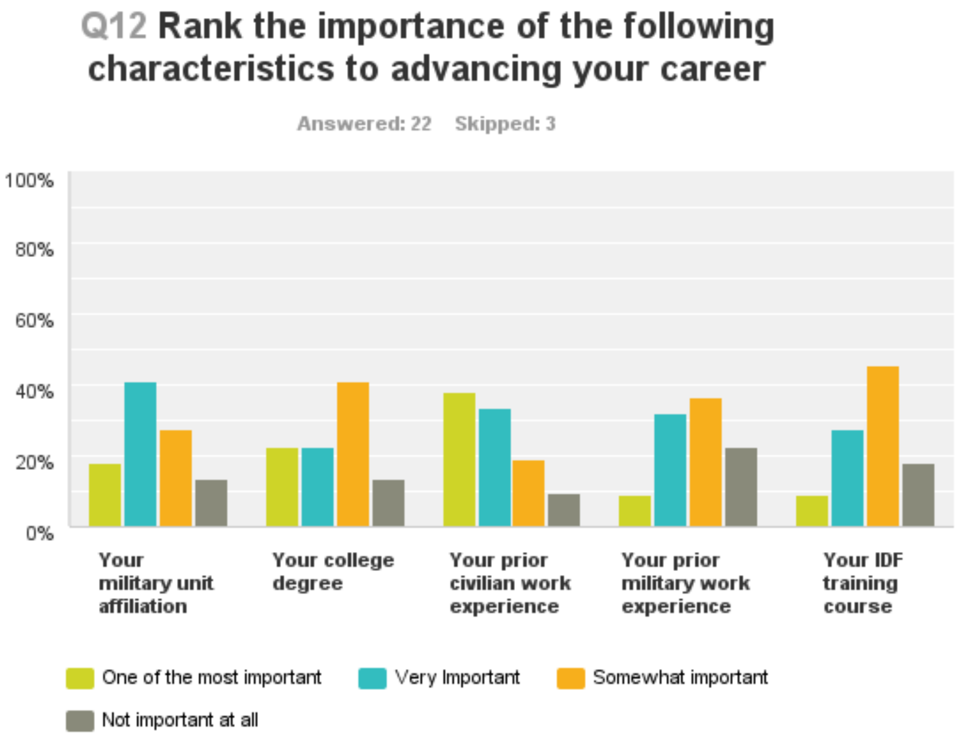


Figure 7: Non-Intelligence Community Views on Unit Value

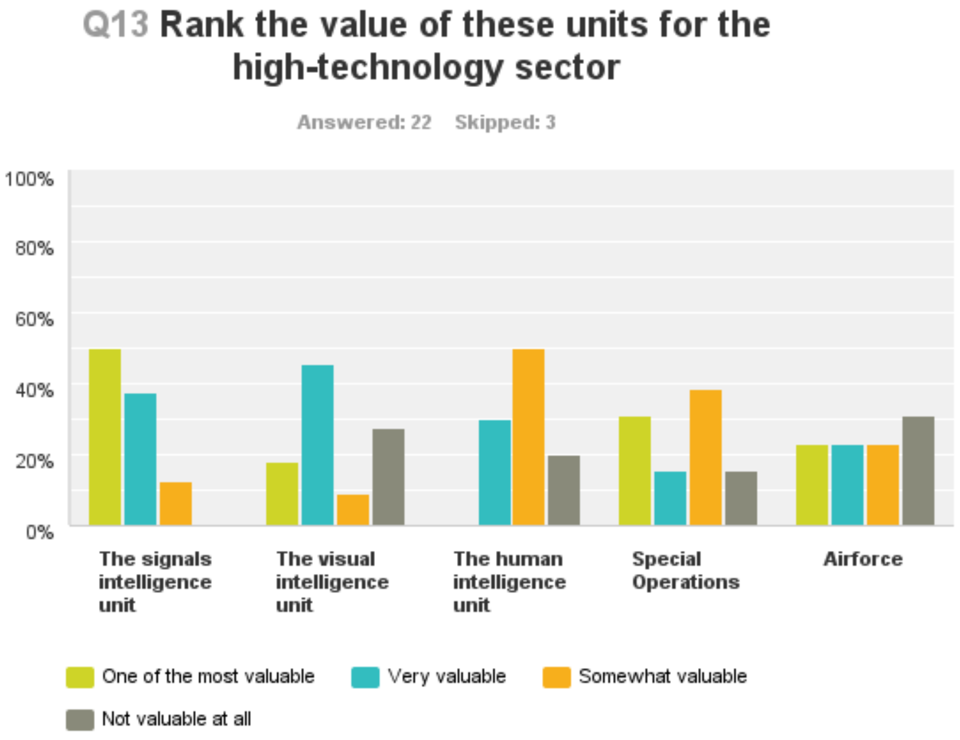


Figure 8: Intelligence Community Views on Unit Value

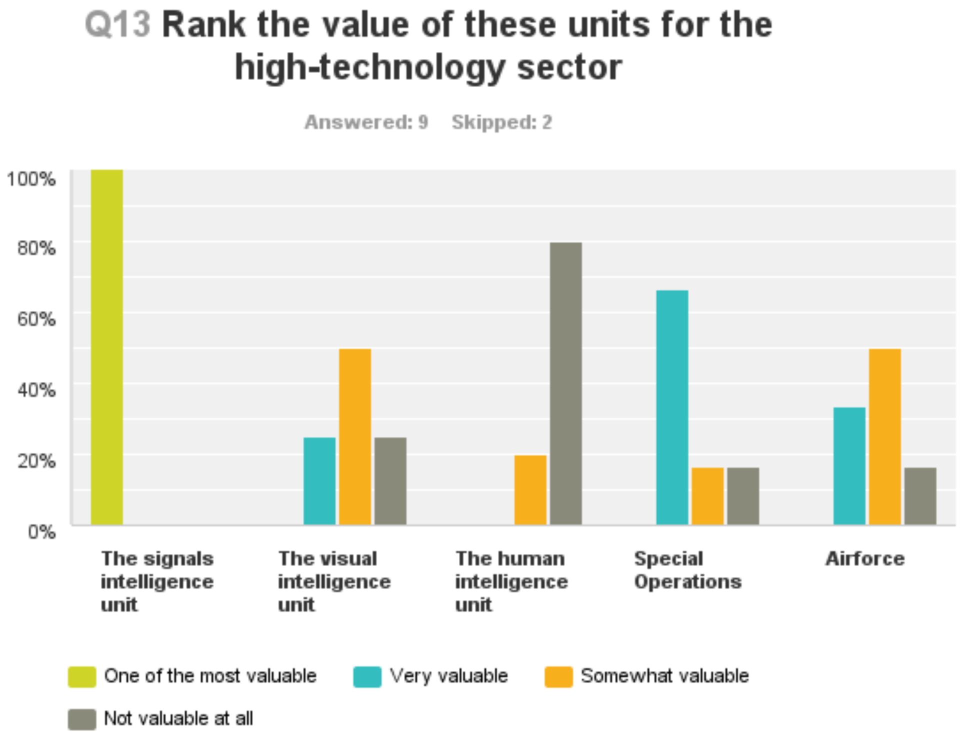


Figure 9: Intelligence Community Views on Own Unit Value

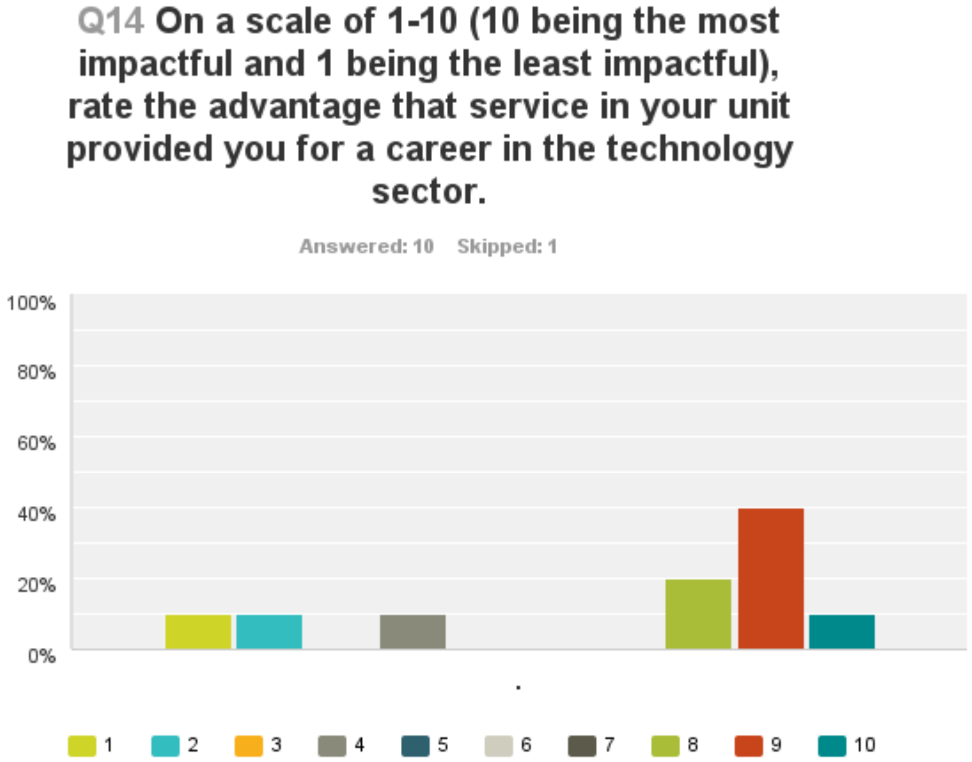
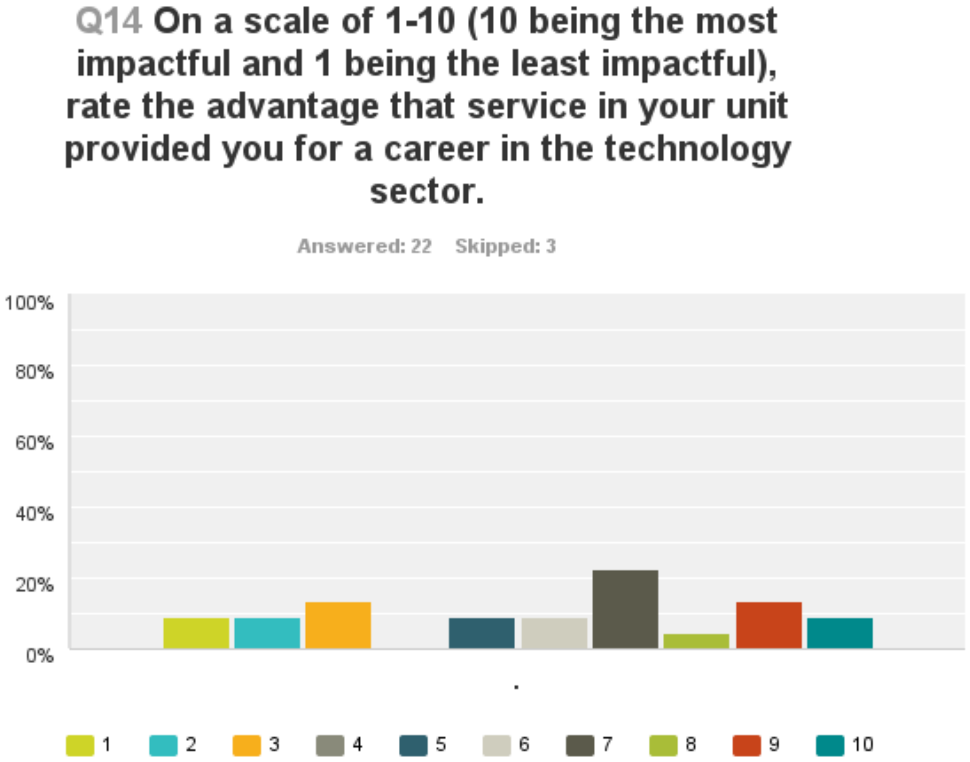
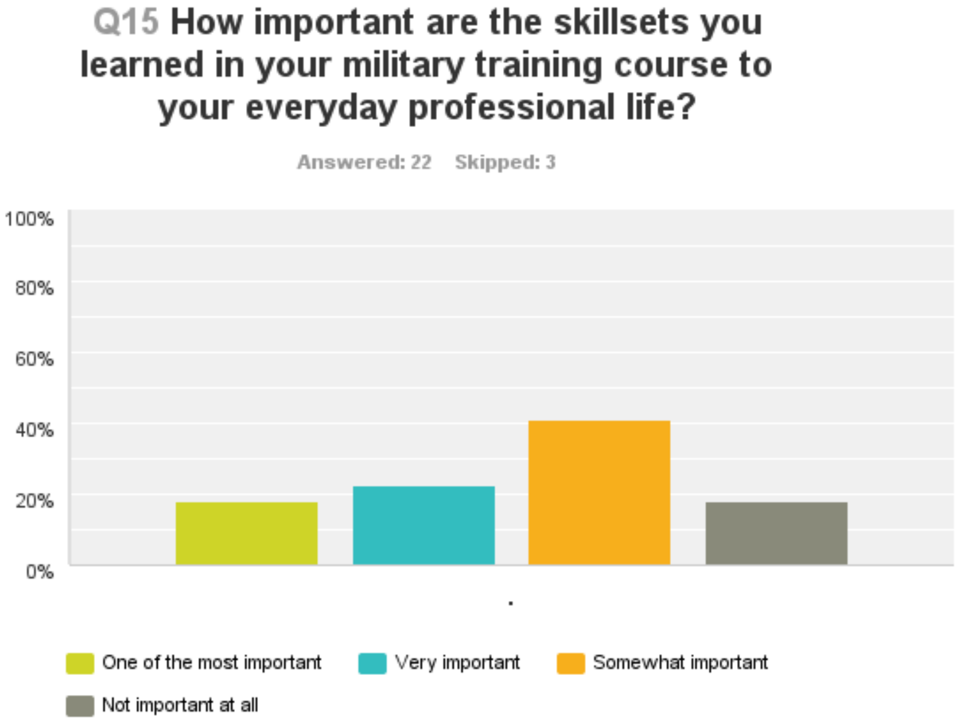


Figure 10: Non-Intelligence Community Views on Own Unit Value



Q14 On a scale of 1-10 (10 being the most impactful and 1 being the least impactful), rate the advantage that service in your unit provided you for a career in the technology sector.

Figure 11: Non-Intelligence Community Views on Value of Skillsets Learned in Training



Q15 How important are the skillsets you learned in your military training course to your everyday professional life?

Figure 12: Intelligence Community Views on Value of Skillsets Learned in Training

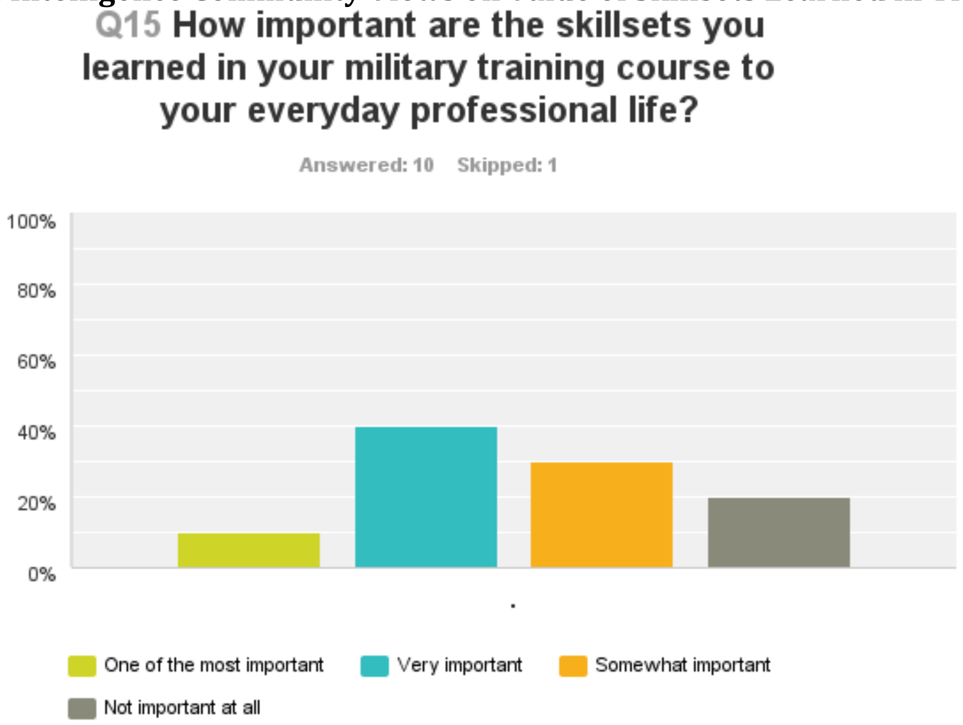


Figure 13: Non-Intelligence Community Views on Value of Skillsets Learned in Own Unit

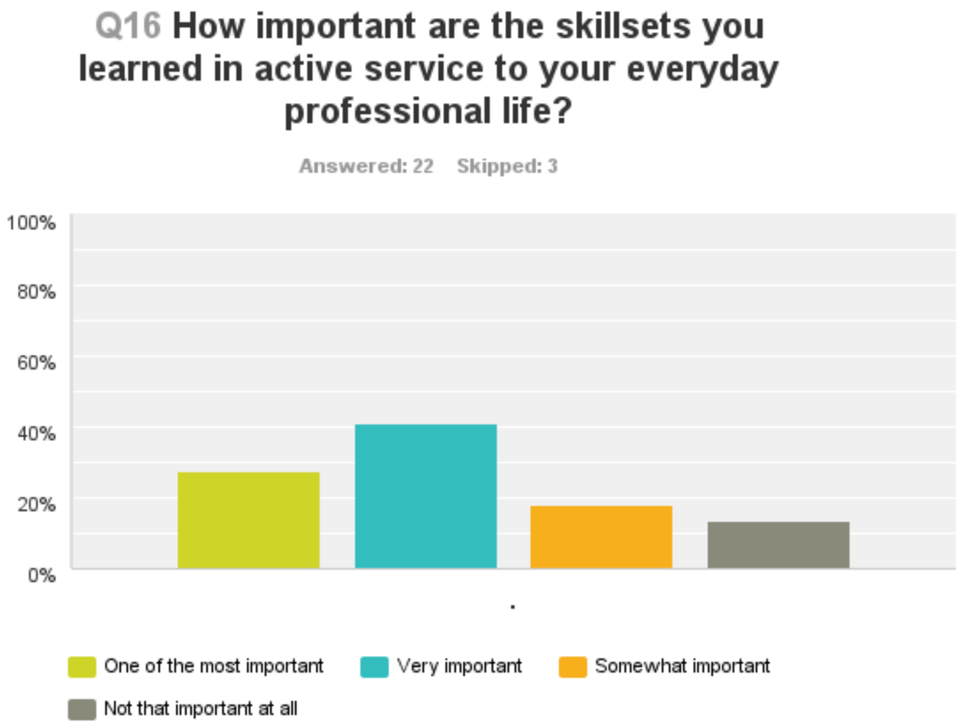


Figure 14: Intelligence Community Views on Value of Skillsets Learned in Own Unit

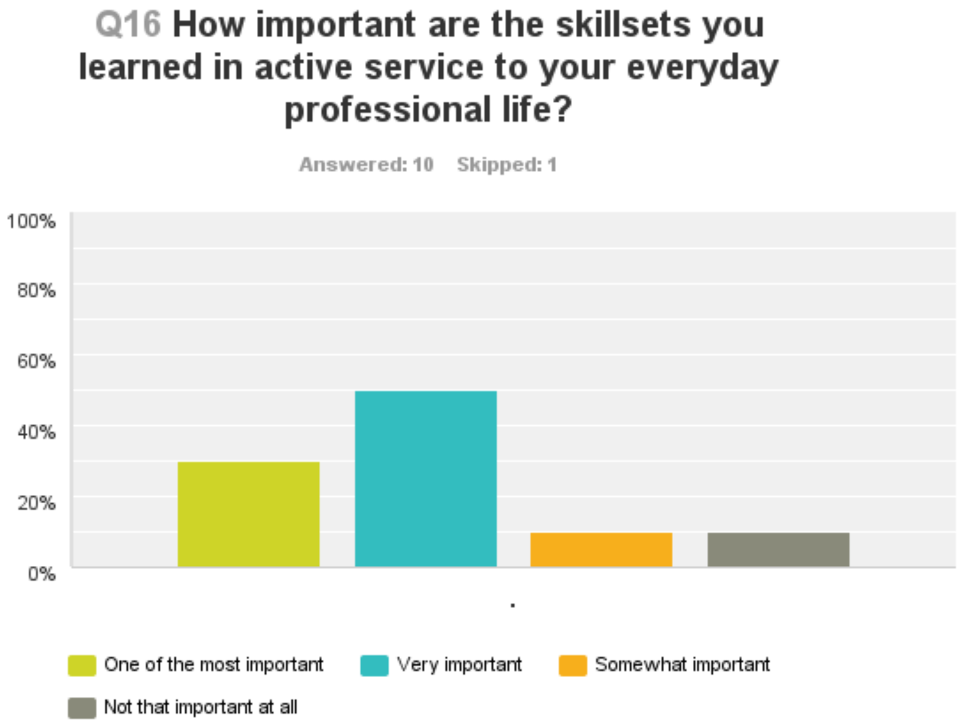


Figure 15: Intelligence Community Views on Social Status of Own Unit

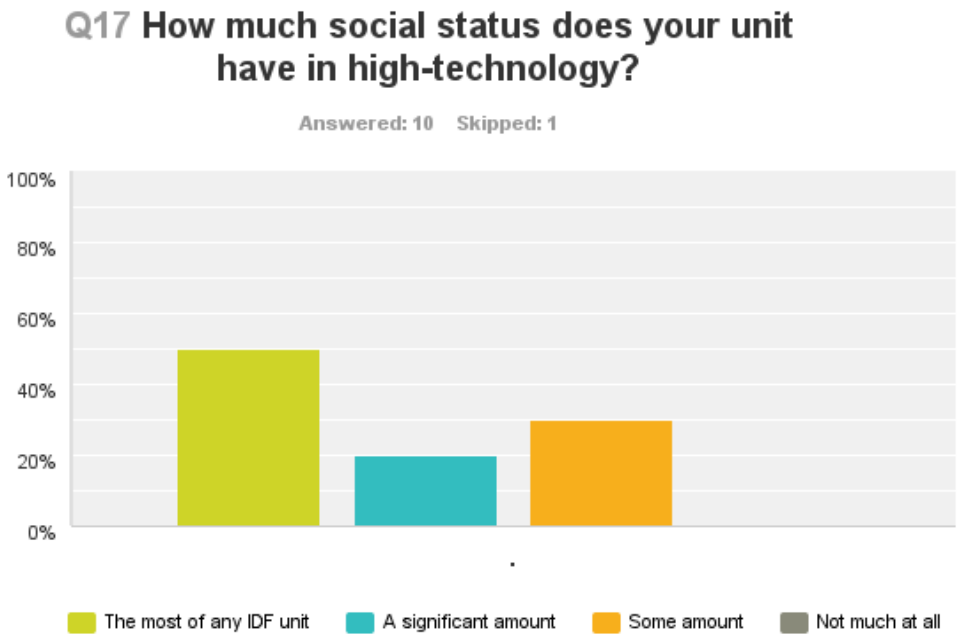


Figure 16: Non-Intelligence Community Views on Social Status of Own Unit

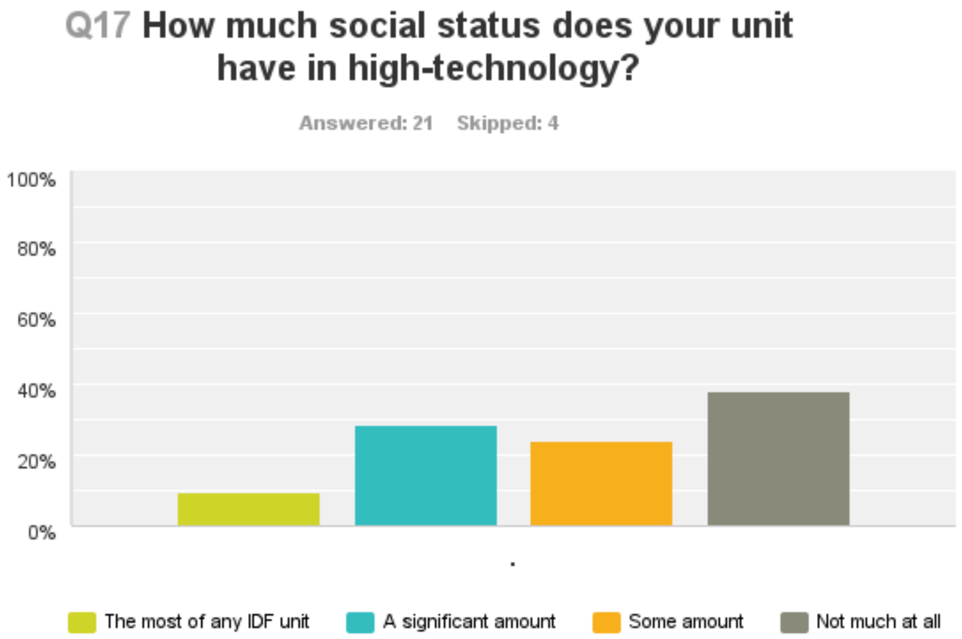


Figure 17: Intelligence Community Professional Encounters With Comrades from Own Unit

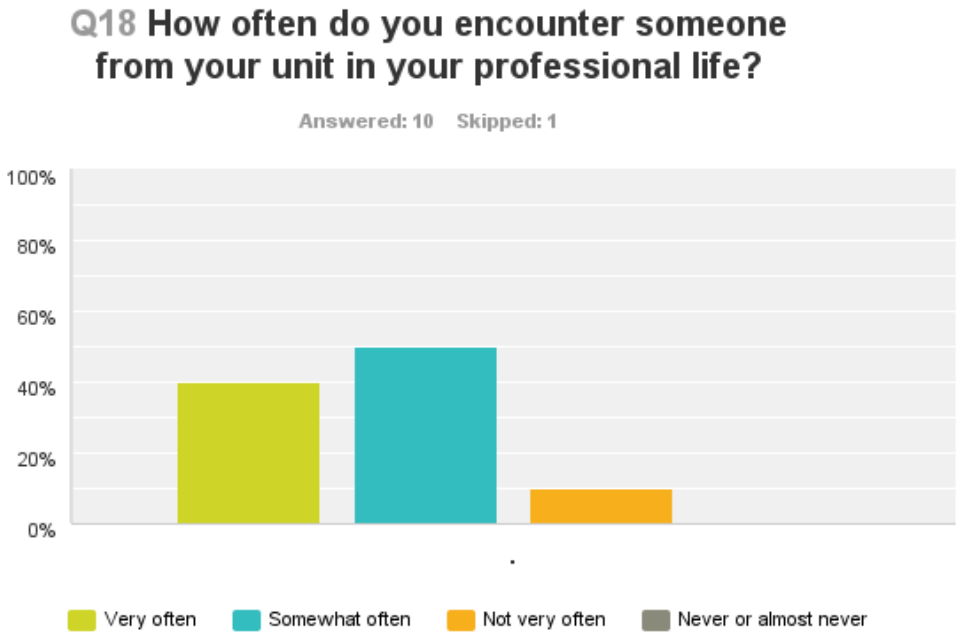


Figure 18: Intelligence Community Professional Collaboration With Comrades from Own Unit

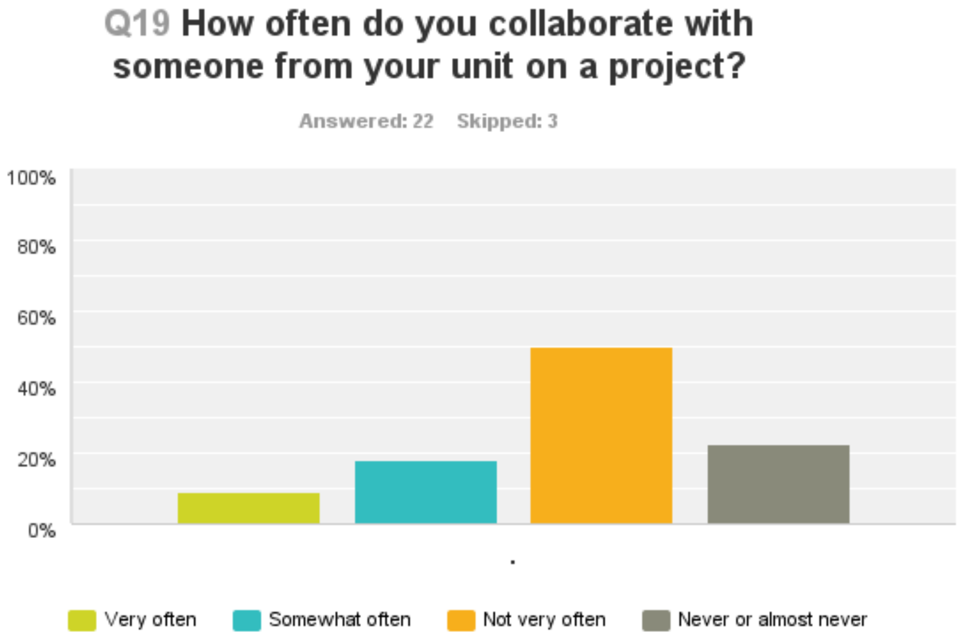


Figure 18: Non-Intelligence Community Views on Own Unit Alumni Impact on High-Tech Labor Force

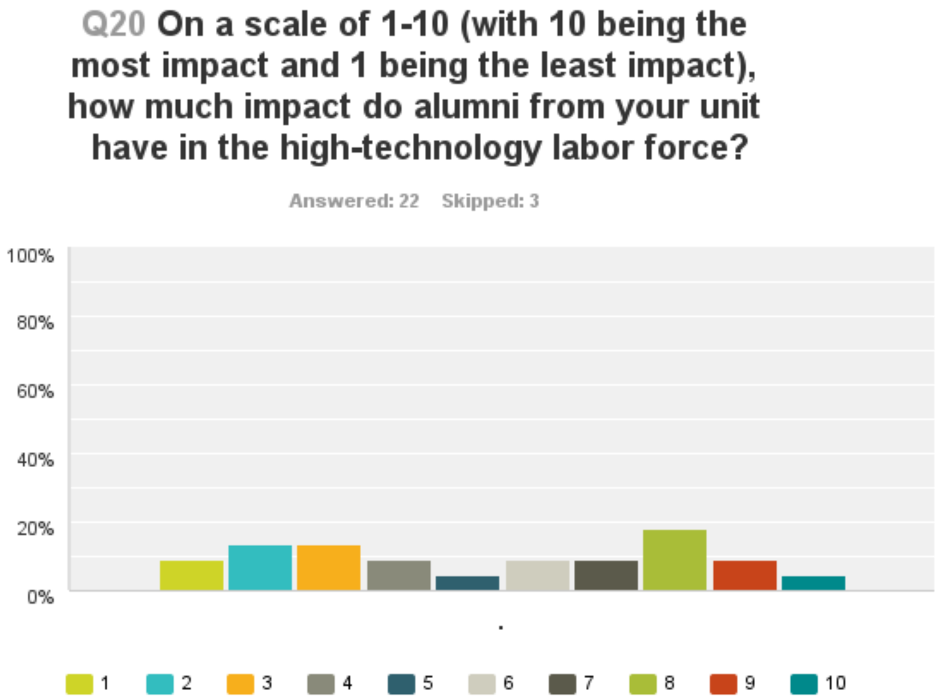


Figure 19: Intelligence Community Views on Employers Preference to Unit 8200

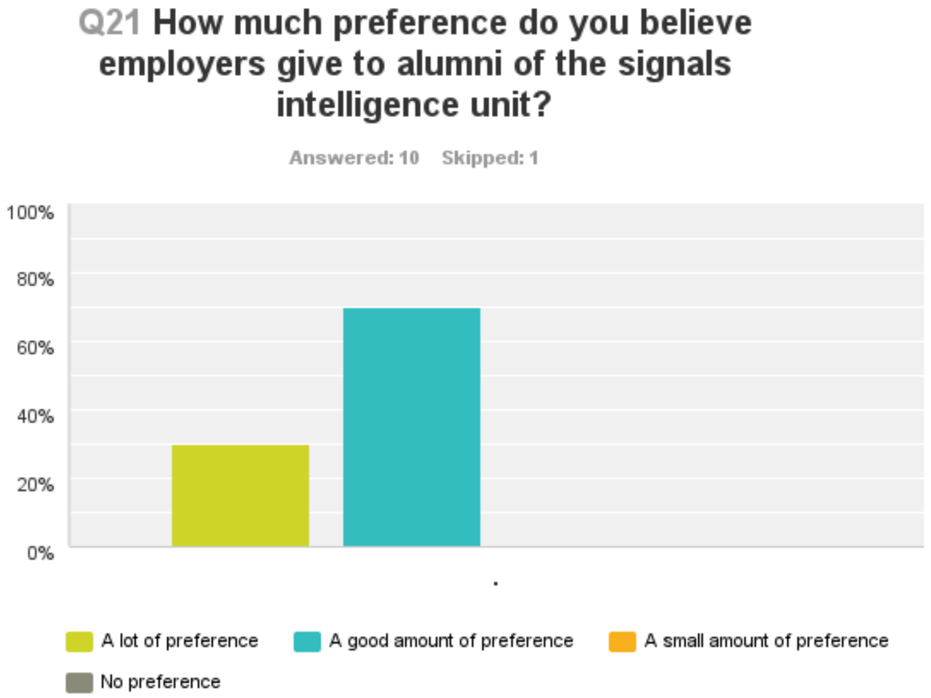


Figure 20: Non-Intelligence Community Views on Employers Preference to Unit 8200

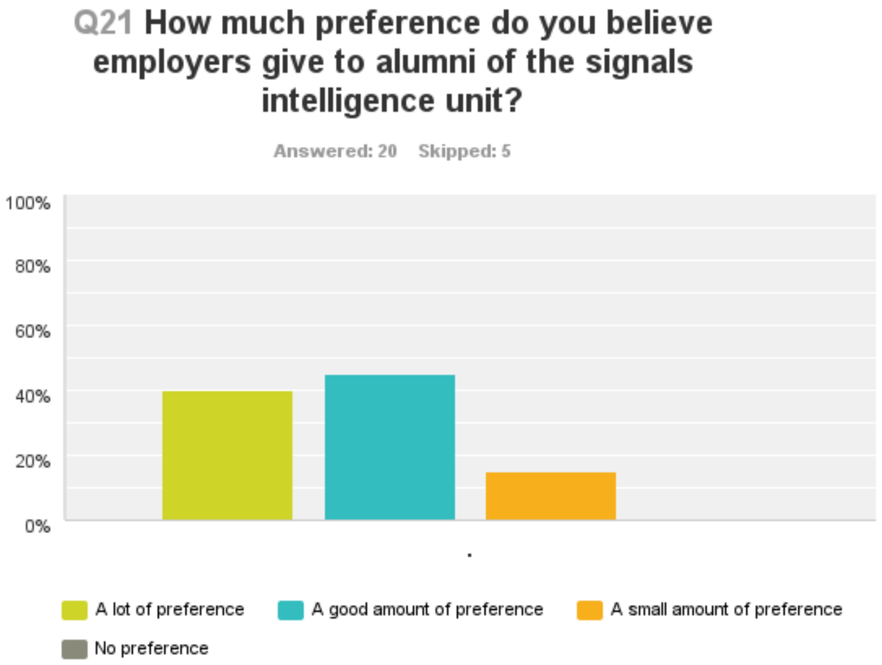


Figure 21: Intelligence Community Views on Impact of Unit Affiliation on Networking

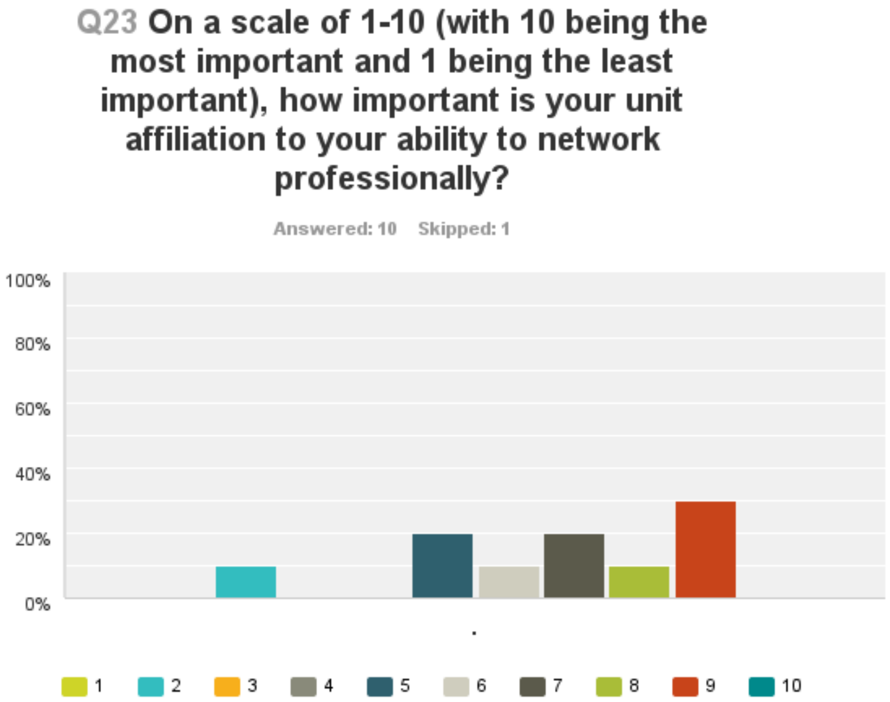


Figure 22: Intelligence Community Views on Own Unit Affiliation Impact on Success

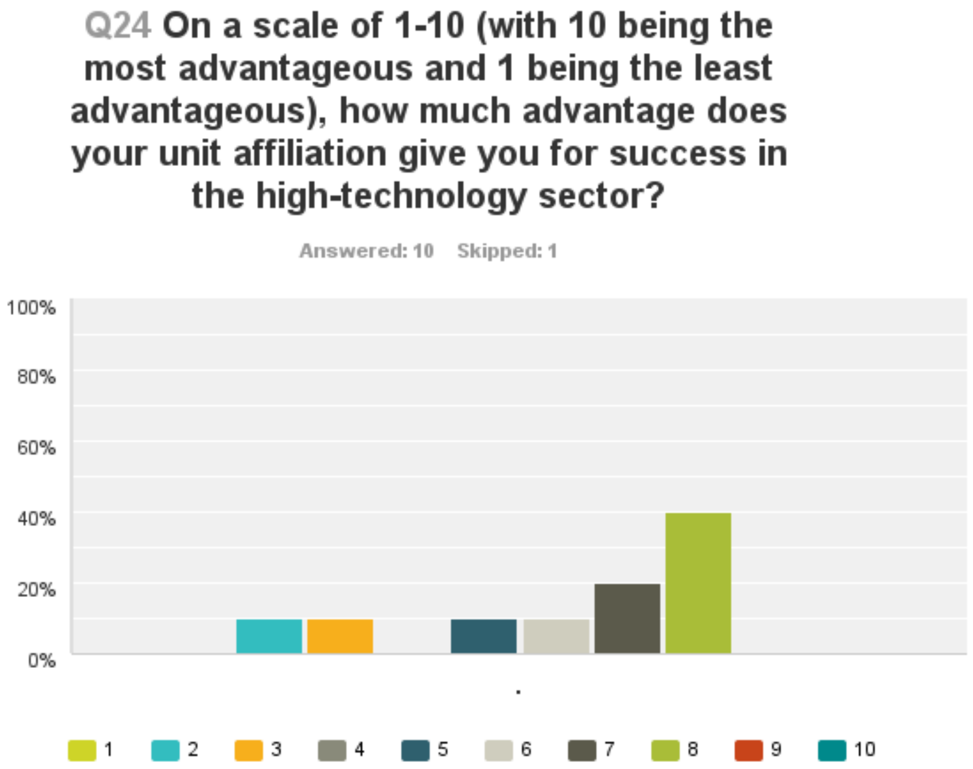


Figure 23: Intelligence Community Views on Impact of Unit 8200 Affiliation on Success

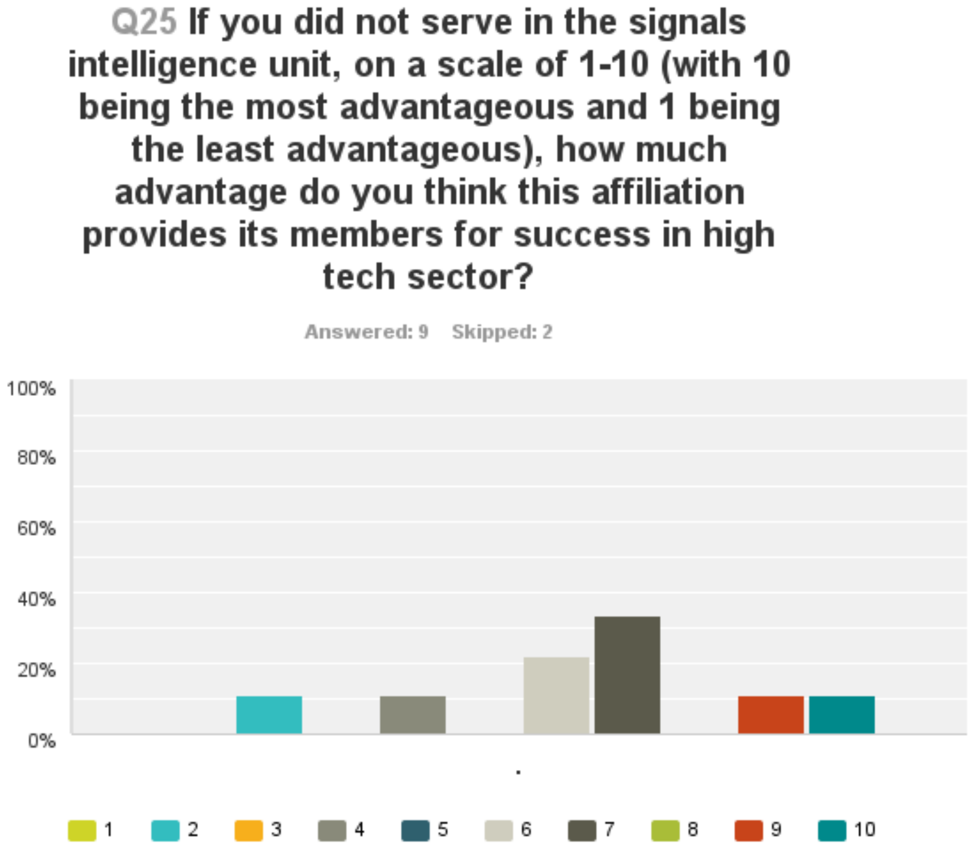
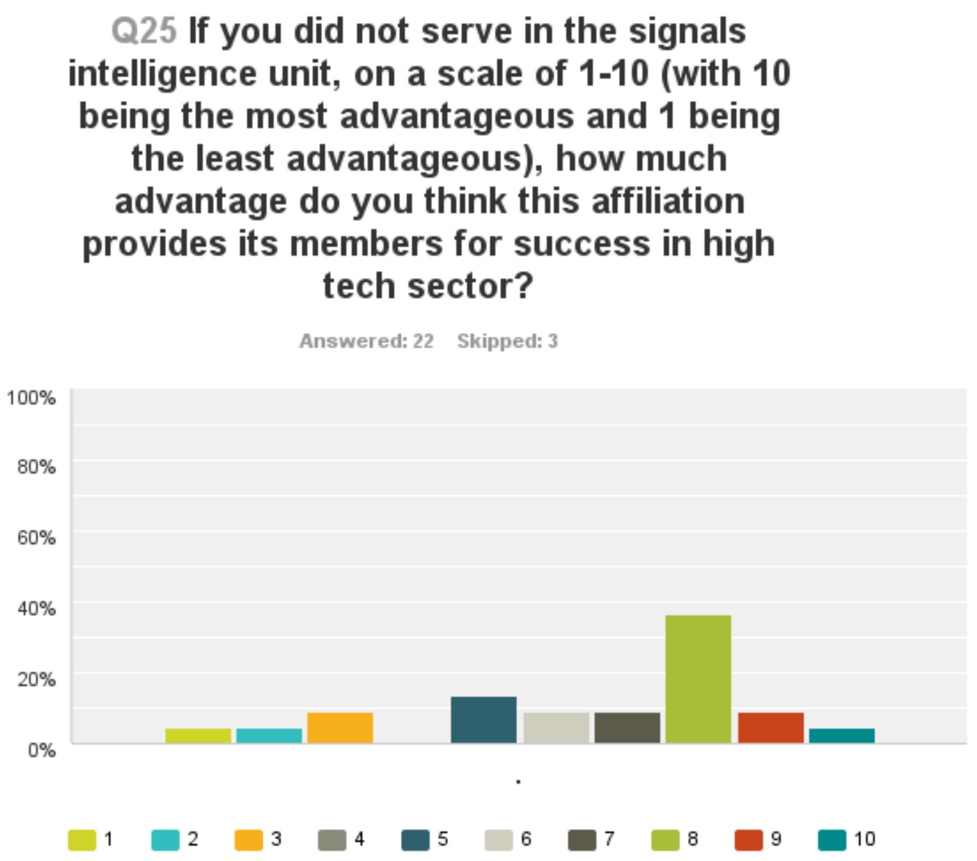


Figure 24: Non-Intelligence Community Views on Impact of Unit 8200 Affiliation on Success



Q25 If you did not serve in the signals intelligence unit, on a scale of 1-10 (with 10 being the most advantageous and 1 being the least advantageous), how much advantage do you think this affiliation provides its members for success in high tech sector?

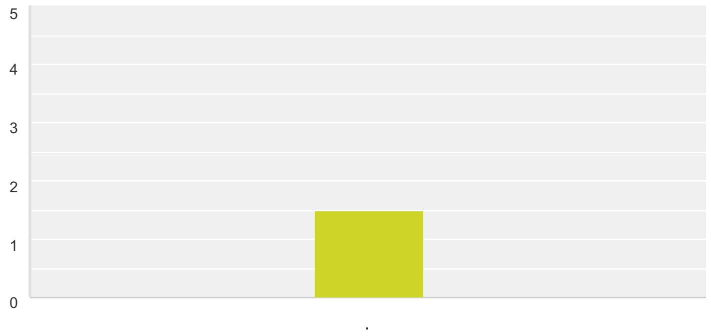
Answered: 22 Skipped: 3

Figure 25: Intelligence Community Likelihood of Professional Helping Members of Own Unit

IDF in High-Technology

Q22 How likely are unit alumni from your unit to help out other members of the unit professionally?

Answered: 10 Skipped: 1



	Very likely	Somewhat likely	Not very likely	Not likely at all	Total	Average Rating
.	50.00% 5	50.00% 5	0.00% 0	0.00% 0	10	1.50

Figure 26: Non-Intelligence Community Work in High-Technology Industry

Q7 Are you working or have you worked in the high-technology industry?

Answered: 25 Skipped: 0

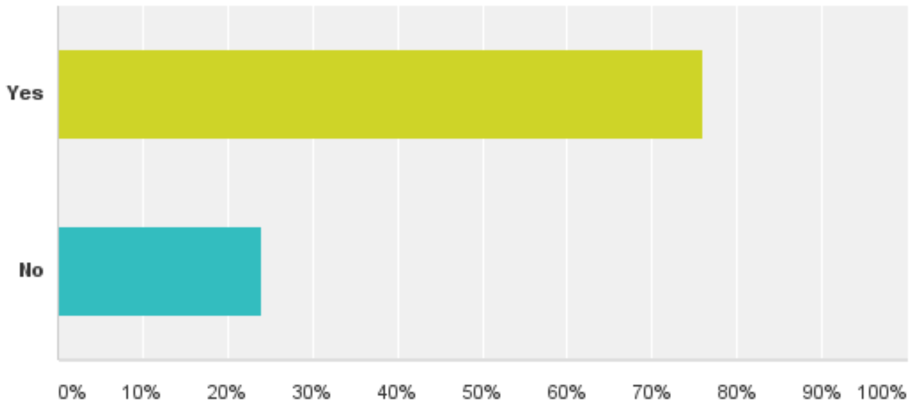


Figure 27: Non-Intelligence Community Type of Work in High-Technology Industry

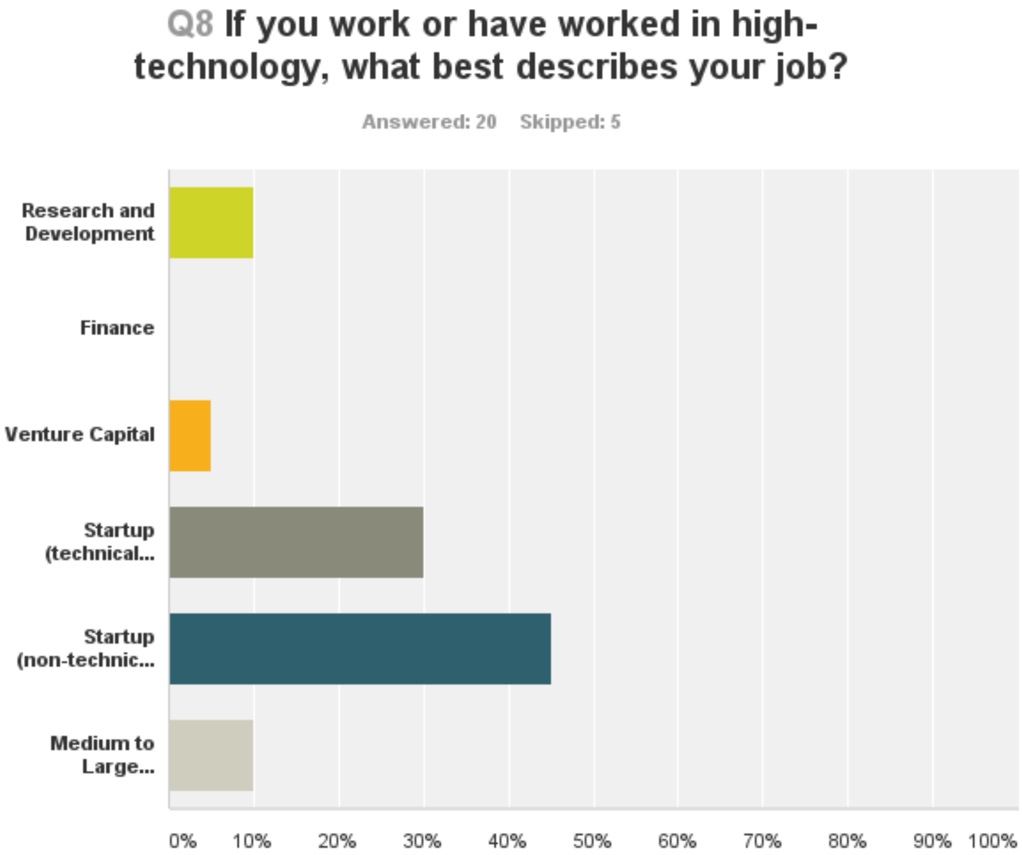


Figure 28: Non-Intelligence Community Unit Disclosure for Job Interview

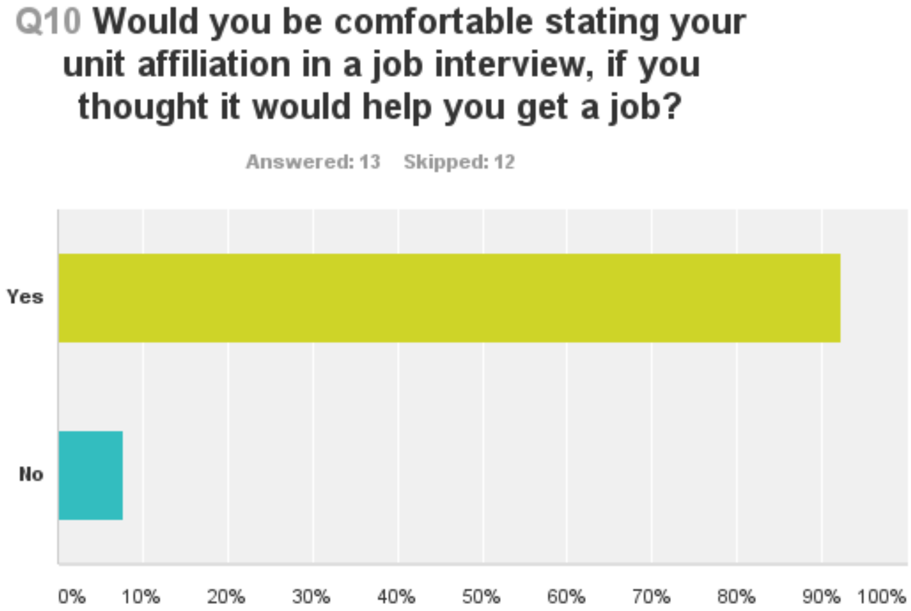
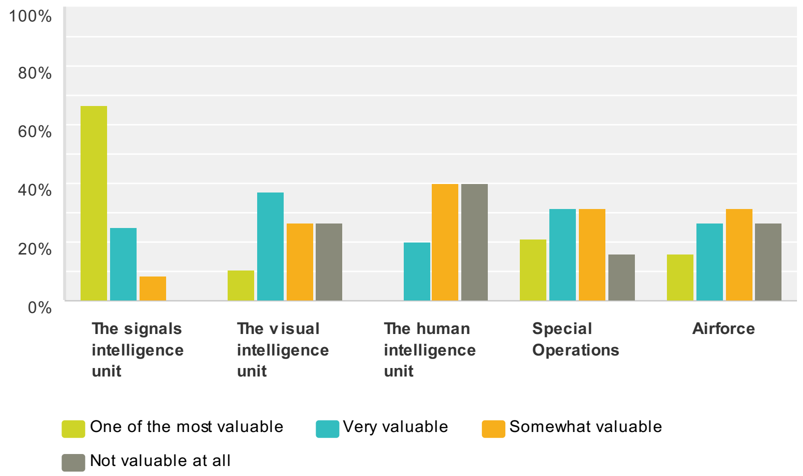


Figure 29: Unit Value in High-Technology Sector (All Respondents)

IDF in High-Technology

Q13 Rank the value of these units for the high-technology sector

Answered: 31 Skipped: 6



	One of the most valuable	Very valuable	Somewhat valuable	Not valuable at all	Total
The signals intelligence unit	**66.67%** 16	**25.00%** 6	**8.33%** 2	**0.00%** 0	24
The visual intelligence unit	**10.53%** 2	**36.84%** 7	**26.32%** 5	**26.32%** 5	19
The human intelligence unit	**0.00%** 0	**20.00%** 3	**40.00%** 6	**40.00%** 6	15
Special Operations	**21.05%** 4	**31.58%** 6	**31.58%** 6	**15.79%** 3	19
Airforce	**15.79%** 3	**26.32%** 5	**31.58%** 6	**26.32%** 5	19