The Dynamics of the Largest Cybersecurity Industrial Clusters:

San Francisco Bay Area, Washington D.C. and Israel

Tali Hatuka and Erran Carmel

TEL AVIV UNIVERSITY
Pursuing the Unknown

ICRC
Blavatnik Interdisciplinary
Cyber Research Center

KOGOD SCHOOL of BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC

Principal Investigators

Tali Hatuka (B. Arch., M.Sc., Ph.D.) is an architect, urban planner and associate professor at Tel Aviv University. Hatuka is the head and founder of the Laboratory of Contemporary Urban Planning and Design, an international center for investigating connections between the built environment and sociocultural dynamics. Hatuka's work focuses primarily on (1) the urban realm and society (i.e. public space, conflicts, technology) and (2) urban development and city design (i.e. industrial urbanism). She has researched and published regarding both issues in peer-reviewed journals, books, and edited volumes. She is the editor of The Digital City: Critical Dimensions in Implementing the Smart City, Planning, Technology, Privacy and Equality (2020). Her forthcoming book, *Places of Production: The City in the New Industrial Age* (Routledge, forthcoming), focuses on the impact of the fourth industrial revolution on societies, and is part of a larger project "Industrial Urbanism" (with Prof. Eran Ben Joseph, MIT), which was exhibited at MIT Museum in September 2014 (http://www.industrialurbanism.com/).

Erran Carmel is a Professor at American University's Kogod School of Business in Washington D.C. He is a former dean and former department chair. He leads the school's "Business in the Capital" initiative that researches regional businesses and regional policy. Carmel is known for his work on the globalization of technology work, and is the author of three books on this topic: *I'm Working While They're Sleeping: Time Zone Separation Challenges and Solutions* (2011); one of the first books on offshoring, *Offshoring Information Technology* (2005); and *Global Software Teams* (1999), which was the first on this topic and is considered a landmark in the field. He has well over 100 publications in journals, conference proceedings, book chapters, and reports. In the area of cybersecurity, he led a multi-year study for the U.S. Department of Defense in the early 2000s. He has been a Visiting Professor at University of Haifa (Israel), University College Dublin (Ireland), Universidad Adolfo Ibáñez (Chile), Beijing Normal University (China), and Ca'Foscari University of Venice (Italy).

Research Assistants

Antonio Mendoza was responsible for the geospatial analysis and developing the visualizations that support the empirical research. Mendoza, a planner from Mexico earned his master's degree in City Planning from MIT, specializing in international development and GIS analysis. He has held various research positions in non-governmental and academic institutions focusing on socio-economic development, resilience and governance on an urban scale.

Corbin Seligman, responsible for the literature review that supports the empirical research, received his B.A. in Economics and Geography from McGill University (2010). He spent nearly 10 years working in real estate, construction and related fields in Toronto, Canada. He is currently pursuing an M.Sc. at Tel Aviv University in the Faculty of Exact Sciences, Department of Geography.

The Dynamics of the Largest Cybersecurity Industrial Clusters:

San Francisco Bay Area, Washington D.C. and Israel

Tali Hatuka and Erran Carmel

January 2021

Language Editor: Shoshana Michael-Zucker

Graphic Designer: Rachel Freedman-Avital

The research and publication of this guide was supported by
the Blavtnik Interdisciplinary Cyber Research Center,
Tel Aviv University, Israel

Preface

The cybersecurity industry, driven by national security interests and private-sector protection, plays a critical role in our shared economic and cultural reality. The underlying premise of this report is that the cybersecurity industry does not emerge in a vacuum; rather it is influenced by environmental conditions present in a particular place and time. Thus, rather than using theory to analyze cybersecurity industry, this report uses field data to illuminate theory and policy with a focus on the relationship between economic development and physical environment.

The contribution and novelty of this report is threefold. First, the report assesses the key features of cyber companies; second, it defines related taxonomy and typologies of companies; third, it places the companies in a socio-geographical context. Empirically, this report focuses on both the distinct and the shared characteristics of the world's three largest regional cybersecurity ecosystems: Silicon Valley, Washington D.C., and Israel.[1] These three clusters each contain several hundred cybersecurity firms specializing in a wide array of products and services. Using the Cybersecurity150 as a gauge, approximately 32% of major firms are located in the San Francisco Bay Area (SFBA), 9% in metropolitan Washington D.C., and 12% in Israel.[2] These three regions are broadly defined in this project as industrial ecosystems for technology and innovation and, more specifically, as hubs of the cybersecurity sector.

This report is part of a broader project on the *Dynamics and Geography of the Cybersecurity Industry*, supported by the Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University. The information and discussion presented below are based on a review of existing literature; a wide-reaching data collection process conducted in 2018 and 2019 using industry databases, online literature, interviews and other sources; and Geographic Information Systems (GIS) analysis.

We are grateful to Antonio Jose Mendoza for meticulously preparing the GIS maps, to Corbin Seligman for his help with the literature review, and to Lee Ben Moshe for her great help with the illustrations and graphics. In addition, we thank the project research assistant Corbin Seligman at Tel Aviv University. At American University in Washington D.C., we thank the project research assistants Parth Tanna, Andre Jones, Hannah Farley, and Vinay Pedapati. We are grateful that some of this research was also supported by the Center for Business in the Capital at the Kogod School of Business at American University.

We hope this document will help cities and regions worldwide become more familiar with the cybersecurity industry, and the advantages and challenges of developing it as part of their holistic resiliency strategies.

Tali Hatuka and Erran Carmel
Tel Aviv and Washington, 2020

[1] Some other important cyber clusters the U.S. include New York City, Austin, San Diego, Boston, as well as San Antonio, Texas (because of U.S. Air Force Cyber Command) and Augusta, Georgia (because of U.S. Army Cyber Command). In the U.K., there are important clusters in London and the U.K. "cyber valley" around Malvern/Cheltenham.

[2] Based on the firms from the Cybersecurity 150 released in late 2019. Prior to that, the list was known as the Cybersecurity 500. On the shorter list, SFBA is more dominant; it accounted for only 24% on the 2018 list.

TABLE OF CONTENTS

Glossary & Abbreviations

Big3	The world's three largest cybersecurity clusters, which are used as case studies: San Francisco Bay Area, metropolitan Washington D.C. and Israel.
SFBA	San Francisco Bay Area, including the city of San Francisco, Oakland and Silicon Valley/San Jose
DC	Washington D.C. metropolitan region, including suburbs in Virginia and Maryland, extending to Baltimore
IL	The entire country of Israel, specifically the Tel Aviv Metropolitan Area
Pure-play	Private firms whose primary or sole business function is provision of products or services directly related to cybersecurity
IPO	Initial Public Offering
Mega-cluster	A large geographical area with a high number of firms.
Mesa-cluster	A large number of firms in a region.
Micro-cluster	Young, emerging clusters with small number of firms.
Sub-cluster	A notable geographical agglomeration of firms in a mega-cluster or mesa-cluster.
Hot zone	A dense geographical agglomeration of firms in a mega-cluster.

Executive Summary

This report offers a multi-disciplinary perspective on the cybersecurity industry. Conceptualizing **cybersecurity industry clusters as ecosystems**, we focus on three distinct mega-clusters: the San Francisco Bay Area, metropolitan Washington, D.C., and Israel. Benefits of clustering include: access to a pool of specialized labor, knowledge spillover, access to capital, and inter-organizational linkages. Research suggests that clusters' economics should be linked to their social dimensions and the configuration of the built environment. In addition, based on the empirical analysis, we suggest using a nuanced **taxonomy** of cybersecurity clusters using a spectrum of intensities: mega-, mesa- and micro-clusters, sub-clusters, and hot zones.

The Big3 clusters were catalyzed during the 1990s cybersecurity genesis – even before cybersecurity was recognizable as a distinct sub-industry within high-tech – and certainly well before the term "cybersecurity" was coined. All three cybersecurity clusters emerged as specialized clusters embedded within a larger high-tech ecosystem. At the same time, government was a key actor in facilitating the high-tech and defense ecosystems in each of these three regions. Cluster concentration remains high: the Big3 mega-clusters, hegemonic since their founding, together serve as headquarters for 53% of the largest and most influential global cybersecurity firms.

Cybersecurity industry dynamics. The industry can be viewed as a manifestation of two far-reaching relationship interplays: industry clustering processes and place (meaning, the industry's socio-spatial context). Regarding the first: there is some evidence of rapid industry consolidation — especially within the Big3 clusters (393 firms merged or acquired through 2018). However, the industry still remains quite fragmented because of the continued entry of new players and the breakup of some giant firms (e.g., Symantec). The second interplay is between place and social context, human capital, and institutions. Via comprehensive mapping, we show that cybersecurity clusters are situated in large, diverse urban regions, within complex, multi-modal transportation networks, with proximate universities, and layered on household income sectors.

Lessons for smaller clusters globally. Cybersecurity clusters (and sub-clusters) grow where one of two conditions exists: an anchor organization (such as the National Security Agency outside Washington) and/or where there is already a strong high-tech culture (as in Silicon Valley). Nurturing a new cybersecurity cluster is a long-term strategy, one that requires many years of patience (as in the Be'er Sheva sub-cluster in Israel). Local governments have been nurturing cybersecurity clusters specifically for about a decade with tax benefits, partnerships, and advocacy programs. However, these policies do not take place in a vacuum; rather, they are part of the ongoing competition between regions and cities. Thus, purposeful cluster growth requires more than a bundle of policies; it needs a cohesive strategic plan that structures a set of policies for nurturing the industrial ecosystem. Only with a holistic vision, which considers the social, economic and spatial context, can a cybersecurity cluster evolve and grow.

Finally, we identify three cybersecurity industry/cluster **challenges for the future**. First is the persistent cybersecurity workforce shortage—apparent in both countries covered in this report. The second challenge is the resiliency of these high-tech clusters as the hegemony of global cities is expected to diminish post-COVID-19, with the workforce migrating out of expensive and unhealthy urban areas. The third challenge is the durability of the cybersecurity industry itself. Are there too many cybersecurity firms? Will a new generation of technologies reconfigure these firms?

In sum, cyber industry cannot be understood in isolation, but only as part of a larger context. Although this industry has some unique features, cybersecurity clusters are not autonomous, and their emergence is connected to a wider technological infrastructure, and to a particular political urban and regional context.

Chapter 1

THE CYBERSECURITY INDUSTRY AS AN ECOSYSTEM

Chapter 1

THE CYBERSECURITY INDUSTRY AS AN ECOSYSTEM

Tali Hatuka and Erran Carmel

As digitization proliferates in all industries and all corners of the globe, cyber threats are becoming more frequent, sophisticated and costly. According to the World Economic Forum and McKinsey and Co., “a secure, robust cyber resilience environment spanning the public and private sectors would enable business and technology innovations, such as cloud computing and mobile Internet, to create between US$ 9.6 trillion and US$ 21.6 trillion in economic value between now and the end of this decade.”[3] As the quote indicates, the importance of cyber defense is clearly growing globally. Yet, typical for emerging industries, there is no international standard system for defining “cybersecurity,” nor an industry-wide classification for what constitutes a cybersecurity firm.[4] The 2018 UK Cyber Sector Report distinguishes cybersecurity firms from other companies based on nine distinct areas of activity and/or expertise, which their report refers to as “Taxonomy Components.”[5] This taxonomy centers on the unique behaviors of cybersecurity firms distinguishing them from firms in other sectors, and is part of a global effort to understand features and dynamics of the fast-growing cyber industry. Furthermore, the academic literature on the cybersecurity industry – as an industry – is still in its infancy.

The following introduction sets the stage for a broader multi-disciplinary perspective on the cybersecurity industry, which aims at linking the industry to business, social, economic, and geographical conditions. This brief introduction includes three parts. The first part describes with how the cybersecurity industry is studied in the existing literature. The second part presents the departure points and terminology used in assessing cybersecurity industry in this report, and the third and last part discusses the framework for analysis and the cases studied.

[3] Alan Marcus et al., “Risk and Responsibility in a Hyperconnected World” (World Economic Forum in collaboration with McKinsey & Company, January 2014), p. 26. http://reports.weforum.org/hyperconnected-world-2014/wp-content/blogs.dir/37/mp/files/pages/files/final-15-01-risk-and-responsibility-in-a-hyperconnected-world-report.pdf.

[4] Sam Donaldson, Christian Stow, and Jonathan Hobson, “UK Cybersecurity Sectoral Analysis and Deep-Dive Review” (Department for Digital, Culture, Media and Sport, June 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751406/UK_Cyber_Sector_Report_-__June_2018.pdf.

[5] Chapter 2 provides a detail discussion on cybersecurity “categories.” The taxonomy used in the UK report is primarily focused on “the economic contribution of the UK cybersecurity sector” and is an attempt to define the industry through a lens similar to that of “Standard Industrial Classification (CSM).” Donaldson, Stow, and Hobson, 2018.

1.1 Cybersecurity industry terminology and the existing literature

With cyberattacks becoming more frequent, more sophisticated and more costly, the cybersecurity industry is predicted to grow rapidly. Over the last decade, government-funded reports and academic studies have been written with the aim of better understanding this fast-growing industry. Generally, this body of literature focuses on two primary themes: economics and national security.

Economics: National and City Levels Economics is the departure point for the vast majority of literature on cyber clusters, recognizing them as an *engine for growth*. As Cohen et al. stated already in 2017, "the cybersecurity industry has the potential to function as a major driver of economic growth."[6] This approach tends to highlight the current and future number, age and size of firms; employment and compensation figures; and investment. The literature touches on potential policy interventions and areas requiring further research, often using return-on-investment (ROI) as justification for public and private investment in the sector.[7]

National Security: Governments, Public Sector and Private Enterprise. National security is another departure point in the literature on cyber clusters, addressing the increased attention nations are paying to investment in cybersecurity. Studies highlight the cost of cyberattacks to both the public and private sectors, calculating optimal levels of expenditure within firms as protection, as well as in the industry overall as investment. Thus, there is a wide consensus about the need to invest in combating cyberattacks in times of enhanced digitization processes, at all levels of government and in all corners of the globe. Awareness began at the turn of the millennium; in 2002, the U.S. Congress passed the Federal Information Security Management Act (FISMA) to require the government agencies to secure and defend agency systems that hold sensitive information.[8] More recently, the U.S. President's budget proposal for fiscal year 2019 included "$15 billion of budget authority for cybersecurity-related activities" which, according to the White House report, does not disclose additional spending on activities of a "sensitive nature."[9]

Methodologically, most studies on the cybersecurity industry analyze and assess public policy, current theory, and/or available quantitative data. The vast majority of literature focuses on economic figures such as gross production, employment and wages, size and number of firms, private and public sector revenue and investment, the financial cost of cyberattacks, and forecasted economic growth.[10] What this body of literature lacks is the socio-geographical context of the industry, and how the industry is associated with three key dimensions:

1. **The Built Environment.** There is almost no information about the built environment's influence on the cybersecurity industry or sector clustering. Key questions about the role of the city/local government in the

[6] Natasha Cohen et al., "Cybersecurity as an Engine for Growth" (New America, September 2017), newamerica.org.

[7] See for example, Cohen's paper provides a "starting point for local or national governments looking to expand their cybersecurity industry" (Cohen et al., 2017, p. 23). Moreover, a number of reports were developed for the primary purpose of promoting a specific cluster as an attractive place for investment by the private and public sector such as U.K. Midlands – Cyber Advantage by U.K. Department for International Trade (U.K. Trade) and U.S. Cybersecurity Clusters by Austrade.

[8] Tobi West and Zentner, Aeron, Managing Security Risks: An Assessment of U.S. Critical Cyber Infrastructure Protection (November 10, 2019). Available at SSRN: https://ssrn.com/abstract=3484552 or http://dx.doi.org/10.2139/ssrn.3484552

[9] "Cybersecurity Funding" (The White House, February 2018), p. 273. https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf.

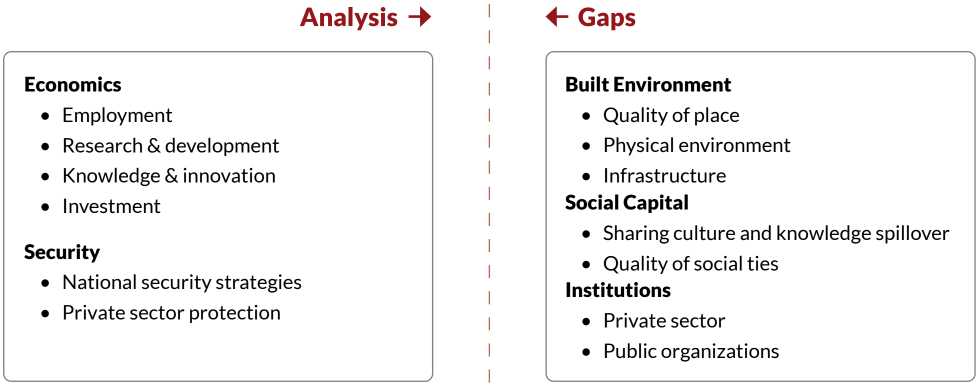
[10] Cohen et al. (2017, p. 2) state "the global cybersecurity market is expected to increase to $125 billion in 2020," while Austrade (2016, p.4) says that number should be US$ 170 billion this year. Austrade also notes the largest single funder of cybersecurity is the U.S. government, spending US$ 19 billion in 2017, followed by the banking sector, spending US$ 68 billion in the U.S. alone from 2016 to 2020 (Austrade, 2016, p. 4). The UK Cybersecurity Sector Analysis goes into impressive detail. The report segments firms based on whether they are fully dedicated to providing cybersecurity products and services; and how much "of their revenues and employment can be attributed to provision of cybersecurity products and services" (Donaldson et al., 2018, p. 5). They further categorize and analyze firms based on revenue; number of employees; average salary; location; and even how much they spend internally on cybersecurity functions (Donaldson et al., 2018, p. 42).

development of the cybersecurity cluster and the type of ecosystem that emerges in different contexts, are not addressed. Furthermore, other factors, like infrastructure and housing, are crucial for studying the growth in cybersecurity and its impact beyond industry's economics.

2. **Social Capital**. Societal characteristics that contribute to the growth of cybersecurity clusters, especially growing the cybersecurity workforce are not covered. Developing, attracting and maintaining a sufficient cyber labor force is a key concern at present, and will likely continue to be for the foreseeable future. Nations and cities that best meet the needs of top talent will have a significant advantage moving forward. It is also likely that culture plays a role in the development of the cybersecurity industry, but analysis of the subject is limited.

3. **Institutions and Organizations.** The cybersecurity sector does not exist in a vacuum. Complementary private sector producers and public institutions promote and accelerate growth. Generally, it is assumed economic activity is bolstered by proximate high-tech firms, which are also near national security facilities and research institutes. Strong associations with other sectors makes it difficult to isolate and examine individual cyber firms and/or the industry overall. The North American Industry Classification System (NAICS) still does not have a statistical code for cybersecurity firms so systematic study is challenging. Thus, there is a need to understand the dynamic between industry and institutions as an important first step toward assessing development, particularly in international analysis.

In sum, as shown in Figure 1, the literature review revealed the existence of extensive analysis on two predominant, overarching subjects. First, the economics of cybersecurity is studied using key indicators such as employment growth, investment in research and development, knowledge creation and innovation, and direct investment. Second, the literature examines cybersecurity as an element of both national security strategy and private sector protective measures. Further analysis for understanding cyber clusters should include: 1. The built environment: quality of place, physical environment, and infrastructure; 2. Social capital: workforce, sharing culture and knowledge spillover, and the quality and nature of social ties; 3. Institutions: with particular attention to both public organizations and the private sector. Addressing these gaps complements existing studies and will help define a standard taxonomy for the cybersecurity sector.



Analysis →

Economics
- Employment
- Research & development
- Knowledge & innovation
- Investment

Security
- National security strategies
- Private sector protection

← Gaps

Built Environment
- Quality of place
- Physical environment
- Infrastructure

Social Capital
- Sharing culture and knowledge spillover
- Quality of social ties

Institutions
- Private sector
- Public organizations

Figure 1.1 Analysis of and gaps in cybersecurity literature

1.2 Departure points for assessing contemporary cybersecurity industry

Addressing the gaps in the literature, the premises of this report are twofold: 1. The concept of clustering is significant for further understanding the cybersecurity industry, 2. Clustering can be defined on a spectrum of intensities.

Understanding cybersecurity as an industrial ecosystem. Clustering is a key concept for understanding the rapid development of cybersecurity. The line of reasoning is that, despite the borderless digital global economy, location matters more, not less. "Firms in a globalized knowledge economy are relying more and more on their local environment for aspects of their competitiveness."[11] The discourse on clustering associated with the works of Alfred Marshall, Michael Piore, Charles Sabel, and, most recently, Michael Porter, who describes clusters as "critical masses – in one place – of unusual competitive success in a particular field."[12] Accordingly, "increasing agglomeration of similar and related activity should be seen as a structural effect of globalization rather than some strange paradox."[13]

There are four key benefits of clustering: interfirm linkages, a pool of qualified, skilled labor, cost savings, and knowledge spillover. Individual clusters are important *hubs of specialized global production*. As the pace of innovation accelerates and more firms participate in a globally interconnected network, each segment of production – as well as associated business functions and services such as accounting, marketing – becomes ever more complex, leading to increasing firm specialization. "Clusters form not only due to interconnectivity between autonomous firms," but through a "restructuring of previously vertically-integrated production systems."[14] Individual firms focus on one particular point in production and rely on other firms in the network to complete other specialized tasks. Vertical dis-integration creates a snowball effect, deepening firms' reliance on each other. This process of strengthening interdependence is called the "*network effect*," referring to the increased value of an entire cluster, as well as the increased value of each firm within that cluster. With the subsequent addition of every new firm,[15] a webbed ecosystem of co-dependence and mutual benefit evolves.

Clusters on a spectrum of intensities. Clearly, clusters differ, in multiple ways: economically, culturally, geographically. Differences also could be found in the cluster itself, with varied density patterns. Current literature on cybersecurity, acknowledges differentiation among clusters and suggests a hierarchical order based on a number of variables, particularly the quantity of global cyber firms within the cluster. Yet, going beyond the quantity of firms and addressing the cyber security industry as an ecosystem, the following typology expands the understanding of variations.

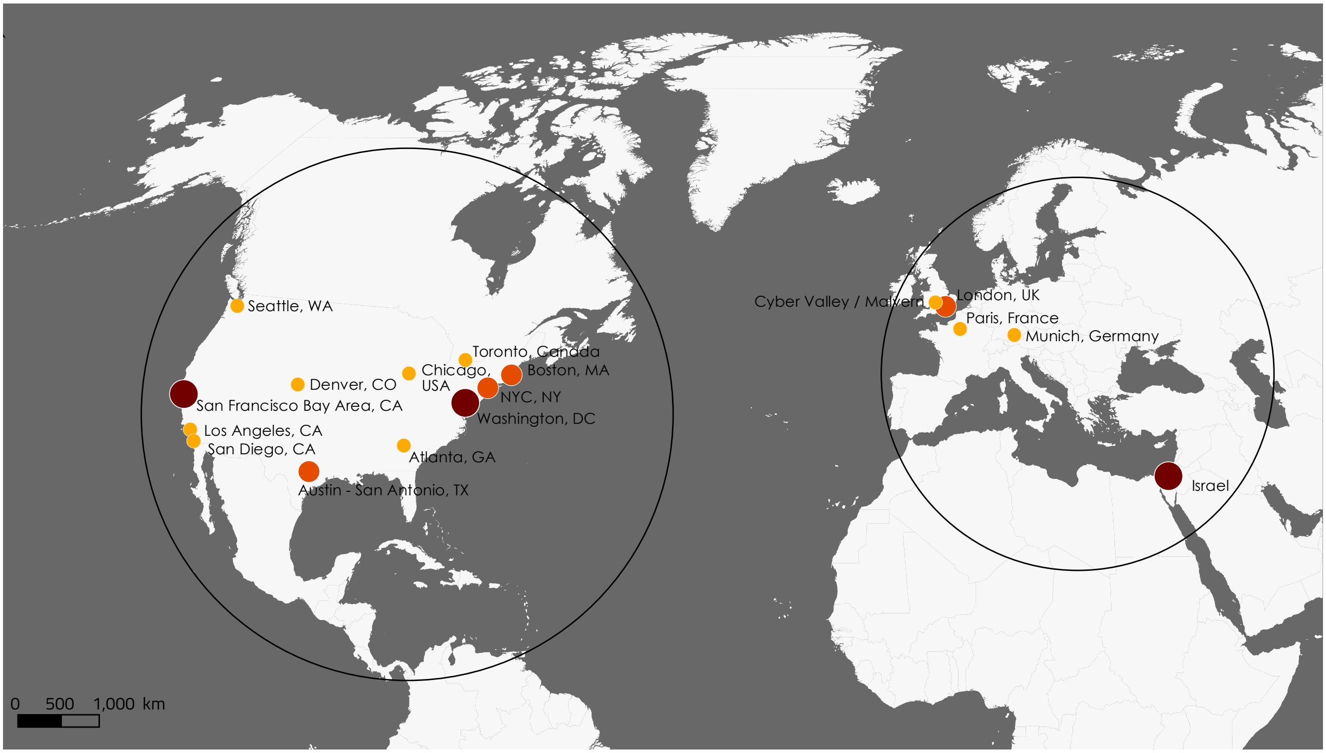
[11] Yama Temouri, "The Cluster Scoreboard: Measuring the Performance of Local Business Clusters in the Knowledge Economy," August 1, 2012, p. 6 https://doi.org/10.1787/5k94ghq8p5kd-en.

[12] Michael E. Porter, "Clusters and the New Economics of Competition," *Harvard Business Review* 76, no. 6 (December 11, 1998): 77–90, p. 78.

[13] Andres Malmberg, "Agglomeration," in *International Encyclopedia of Human Geography*, ed. Rob Kitchin and Nigel Thrift (Oxford: Elsevier, 2009), 48–53, p. 50. https://doi.org/10.1016/B978-008044910-4.00131-0.

[14] Malmberg, "Agglomeration."

[15] Michael L. Katz and Carl Shapiro, "Network Externalities, Competition, and Compatibility," *American Economic Review* 75, no. 3 (June 1985): 424.



Map 1.1 Location of main cybersecurity clusters in North America and Europe

● Mega-cluster

● Mesa-cluster

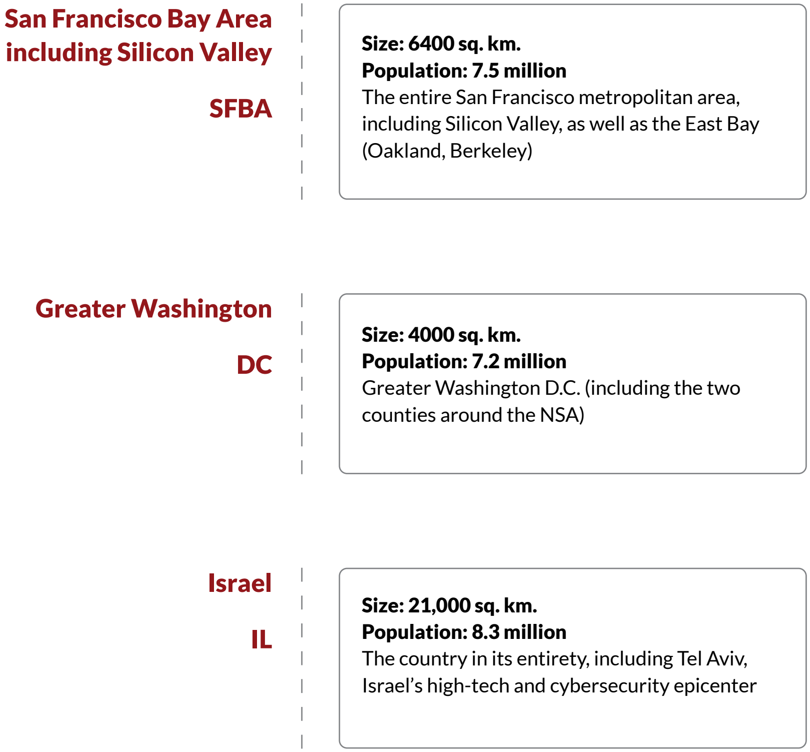
● Micro-cluster

Mega-cluster	(Tier 1 cluster) a large geographical area (at least 1000 km^2) with a high number of firms.
Mesa-cluster	(Tier 2 cluster) large number of firms in a region.
Micro-cluster	(Tier 3 cluster) young, emerging cluster with small number of firms.
Sub-cluster	A notable geographical agglomeration of firms within a mega-cluster or mesa-cluster. The number of firms is not necessarily large, but they have a distinct geographic location.
Hot zone	A dense geographical agglomeration of firms within a mega-cluster.

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)
©Laboratory for Contemporary Urban Design, Tel Aviv University

1.3 Questions and framework for analysis

Conceptualizing the **cybersecurity industry as an ecosystem**, this report focuses on three distinct mega-clusters: the San Francisco Bay Area ("SFBA"), metropolitan Washington, D.C. ("Washington" in the text, and "DC" in the figures), and Israel ("IL" in the figures). The three cybersecurity mega-clusters (Figure 1.2) share two important characteristics (Figure 1.3). First, and well-documented, is the *startup and high-tech innovation culture* that is a major growth driver for all three ecosystems. SFBA and Israel have thriving startup ecosystems, with associated substantial flow of risk capital and are heavily focused on products, while Washington exhibits a higher proportion of service-based firms (in Washington only 11% of cybersecurity firms are focused solely on products).[16] Second is the link between *human capital and national security*. Firms in Washington and Israel benefit directly and indirectly from their respective national governments' aggressive security and cyber-defense ecosystems. In Israel, this is often related to the military "unit 8200;" in Washington, it is frequently the National Security Agency (NSA).



San Francisco Bay Area including Silicon Valley

SFBA

Size: 6400 sq. km.
Population: 7.5 million
The entire San Francisco metropolitan area, including Silicon Valley, as well as the East Bay (Oakland, Berkeley)

Greater Washington

DC

Size: 4000 sq. km.
Population: 7.2 million
Greater Washington D.C. (including the two counties around the NSA)

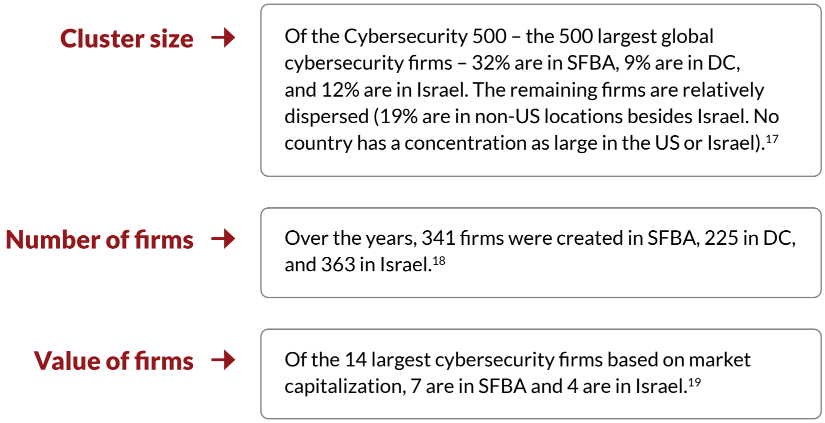
Israel

IL

Size: 21,000 sq. km.
Population: 8.3 million
The country in its entirety, including Tel Aviv, Israel's high-tech and cybersecurity epicenter

Figure 1.2 Geographic scale of three major cybersecurity clusters

[16] Erran Carmel, Bini Byambasuren, and Jonathan Aberman. *Cybersecurity Startup Founders in the Greater Washington Region: Prior Experience Required.* April 2018. Center for Business in the Capital, American University.



Cluster size →

Of the Cybersecurity 500 – the 500 largest global cybersecurity firms – 32% are in SFBA, 9% are in DC, and 12% are in Israel. The remaining firms are relatively dispersed (19% are in non-US locations besides Israel. No country has a concentration as large in the US or Israel).[17]

Number of firms →

Over the years, 341 firms were created in SFBA, 225 in DC, and 363 in Israel.[18]

Value of firms →

Of the 14 largest cybersecurity firms based on market capitalization, 7 are in SFBA and 4 are in Israel.[19]

Figure 1.3 Key measures of three major cybersecurity clusters

Using these cases, the report focuses on the following questions:

1. What were the catalysts and historical growth patterns of the cybersecurity industry in the Big3 clusters? (i.e., organic, top-down (government leadership), or hybrid [a combination of the two]).
2. How does national and regional economic policy influence development of a regional/local cybersecurity industry? (i.e. effect of consolidation within the sector, effect of policy and government activity on firms' choice of location and private-sector competition).
3. What is the interplay between industry characteristics (e.g., venture capital, acquisitions, pure-play firms) and clusters?
4. What are the geographic and social patterns associated with the areas of cybersecurity clusters?
5. What is the role of the urban context in the emergence of clusters and how does it influence their scale, intensity and/or development?
6. What are the key components of cybersecurity ecosystems?

In addressing these questions, the report continues as follows: Chapter 2 describes the evolution and typologies of the cybersecurity industry. Using quantitative economic data, the chapter analyses the evolution and categorization of the three mega-clusters. Chapter 3 provides geographical analysis of the three case studies, addressing the similarities and differences between these clusters. The report ends with Chapter 4, which summarizes the conclusions, and offers some policies for developing cybersecurity clusters as ecosystems.

[17] Cybersecurity 500 2017 List of Top Cybersecurity Companies https://cybersecurityventures.com/cybersecurity-500/

[18] Business in the Capital cybersecurity dataset, American University

[19] Bessemer Venture Partners, Israel Cybersecurity Landscape, https://www.bvp.com/cyber-security Figures are for Q1 2018

Chapter 2

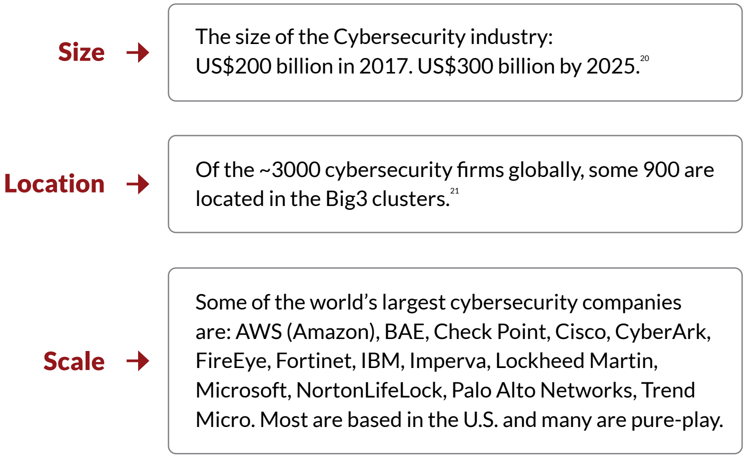
CYBERSECURITY INDUSTRY FEATURES AND EVOLUTION

Chapter 2

CYBERSECURITY INDUSTRY FEATURES AND EVOLUTION

Erran Carmel

This chapter describes the evolution of the cybersecurity industry using quantitative economic data. The key questions in this chapter are: what are the key stages in the evolution of this industry? What are the key industry typologies and firm categories? Addressing these questions, this chapter is divided into five sections. The first addresses the overall history of the sector, presented on a four-era evolutionary timeline. The second section presents the various product and service categories that have emerged and evolved within the industry. The third focuses on initial development and maturation of each one of the Big3 clusters. The fourth section then discusses cyber-industry economics and business fundamentals, outlining how firms tend to grow and expand. The chapter concludes with a look at the industry from a very different vantage point: as an innovation sector that is necessarily facilitated by significant government involvement.



Size →

The size of the Cybersecurity industry:
US$200 billion in 2017. US$300 billion by 2025.[20]

Location →

Of the ~3000 cybersecurity firms globally, some 900 are located in the Big3 clusters.[21]

Scale →

Some of the world's largest cybersecurity companies are: AWS (Amazon), BAE, Check Point, Cisco, CyberArk, FireEye, Fortinet, IBM, Imperva, Lockheed Martin, Microsoft, NortonLifeLock, Palo Alto Networks, Trend Micro. Most are based in the U.S. and many are pure-play.

Figure 2.1 Key industry figures and estimates

[20] CB Insights, 2019. Emerging market trends.

[21] 3000 is the estimate of AT&T's Thornton (ibid). 900 is from our data set of the Big3 clusters.

2.1 The Evolution of Cybersecurity Industry

The cybersecurity industry emerged in the 1980s and grew slowly through the 1990s, parallel to the birth of an historically monumental global communications network, the Internet. In the 1990s, the cybersecurity industry was initially known as "computer security" or "information security," and was not yet seen as a distinct industry unto its own. In fact, until 2007, American contractors of the U.S. Department of Homeland Security (DHS) were prevented from using the term "cybersecurity" as the subject itself was deemed sensitive.[22] In assessing the industry's evolution, four key eras can be identified (Figure 2.2):

Era 1: Embryonic. Early industry history is characterized by breakout firms. Key examples include McAfee for consumer-focused security which sold its first product in 1987; the Israeli firm, Check Point, known for software firewalls was founded in 1993; and Symantec, which began as a general software utilities firm and later transitioned into cybersecurity in the 1990s.[23]

Era 2: Distinct industry emerges. A distinct cybersecurity industry began to grow rapidly post 9/11, beginning in 2002, and marking the start of the second era. The U.S. began to focus more resources on thwarting threats from both hostile nation states and terrorist organizations. At the same time, malware became a growing global problem, causing extensive damage worldwide. The 2003 internet worm "Slammer," for example, was the first classic file-less flash worm able to spread to hundreds of thousands of computers within mere minutes.

Era 3: Rapid growth with abundant funding and specialization. This era was triggered by a significant increase in venture capital funding, picking up markedly in 2012. One possible catalyst for this wave of funding was an increase in major security breaches beginning around this time at the hands of both nation states and criminal organizations. The Stuxnet breach surfaced in 2010, for example, as did the Google breach by China that same year. More frequent breaches and corresponding industry growth led to increased demand for cyber-trained workers. As early as 2012, Burning Glass International found demand for cybersecurity employees in the 5 preceding years had grown 3.5 times faster than that for general technology workers and 12 times faster than the overall labor market.[24] Large-scale acquisitions began late in the second era and continued in third, when Intel bought SFBA-based McAfee in 2010 for a staggering US$7.7 billion, the biggest acquisition for Intel at the time. In 2013, Cisco Systems bought Washington-based Sourcefire for US$2.7 billion.[25]

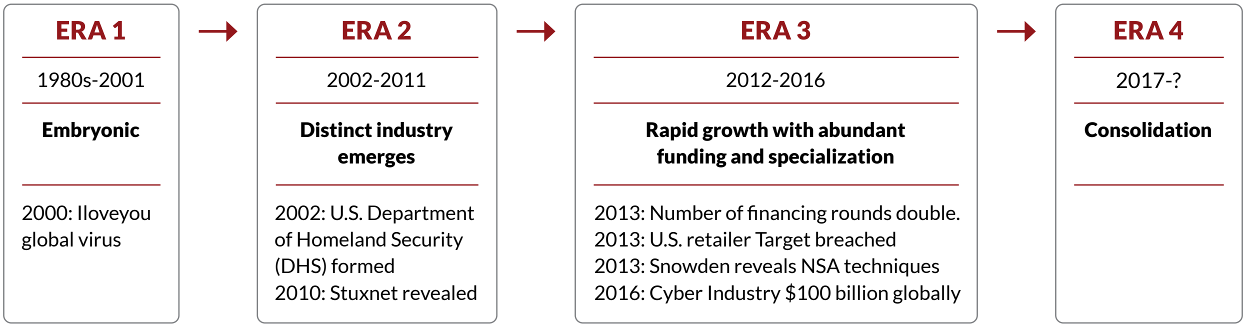
Era 4: Consolidation. Beginning in 2017, the previously red-hot cybersecurity growth moderated somewhat. There are several possible reasons for this: venture capitalists flocked to other opportunities; later-stage venture rounds of more established firms; market saturation, or an increase of stealth-mode startups that do not show up in industry data.

[22] George Schu, 2018, interview by authors.

[23] In fact, Symantec's transformation is an important component of the industry's evolution: many firms morphed into cybersecurity firms over time. Recent examples are A10 and Synopsys (Synopsys still does chip design, but is transitioning into a cybersecurity firm).

[24] Steve Johnson. Cybersecurity business booming in Silicon Valley, Mercurynews.com, 2013.

[25] Johnson, "Cybersecurity Business."



ERA 1

1980s-2001

Embryonic

2000: Iloveyou global virus

ERA 2

2002-2011

Distinct industry emerges

2002: U.S. Department of Homeland Security (DHS) formed
2010: Stuxnet revealed

ERA 3

2012-2016

Rapid growth with abundant funding and specialization

2013: Number of financing rounds double.
2013: U.S. retailer Target breached
2013: Snowden reveals NSA techniques
2016: Cyber Industry $100 billion globally

ERA 4

2017-?

Consolidation

Figure 2.2 Cybersecurity industry historical eras

Figure 2.3 shows annual startup formation during each of the four eras described above. It shows the yearly birthrate of cybersecurity firms, divided by cluster, over three decades. The dramatic increase in two of the three clusters (SFBA and Israel) in the last decade, especially in era, is notable. The increase is most pronounced in the Israeli cluster, which grew by fewer than 50 firms in 2000-2010, and by over 300 thereafter. In era 2, the early 2000s, the Washington cluster grew particularly quickly as a result of government demand; it subsequently plateaued, just as the other two clusters began to grow more rapidly.

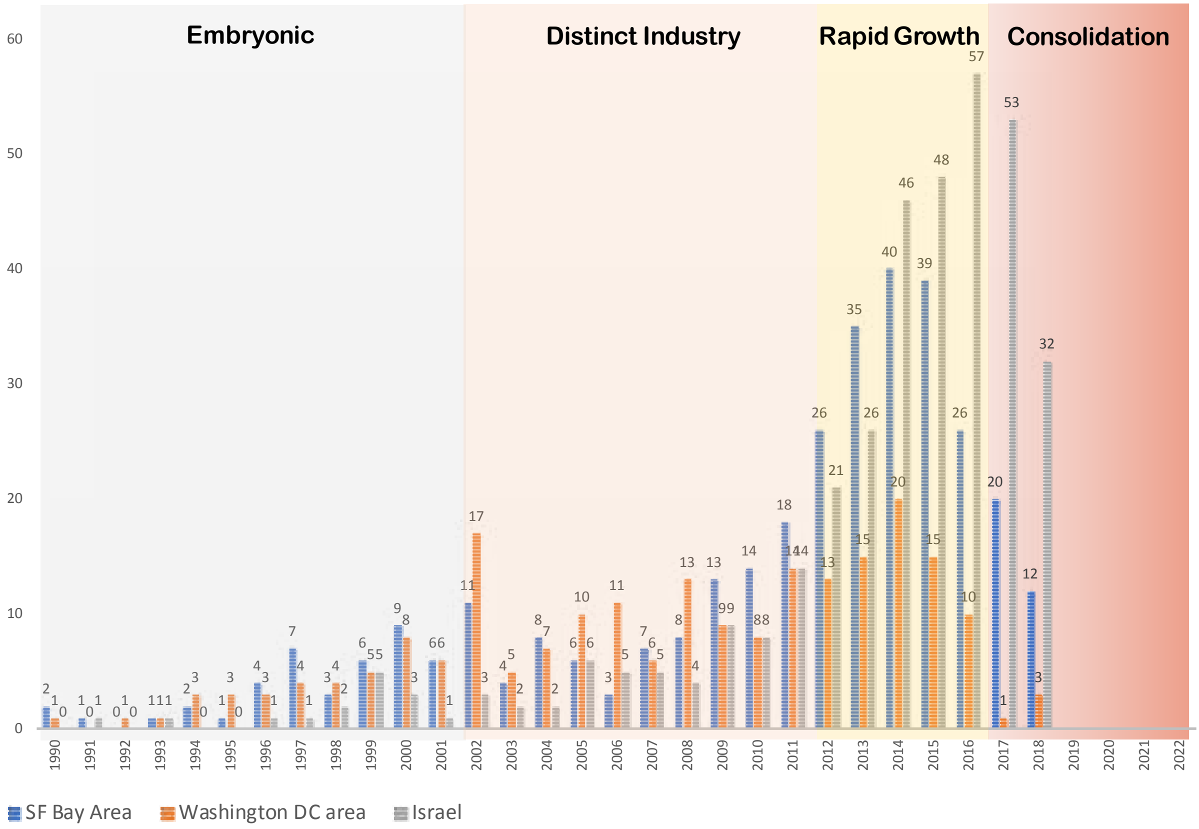


Figure 2.3 Timeline of cybersecurity startup births by cluster.[26]

[26] Note that 2018 is a partial year.

Two notable dynamics are taking place in the cybersecurity industry during this evolutionary process: rapid industry growth and significant consolidation.

- **Rapid Growth.** The global cybersecurity industry continues to grow at a fast pace. In 2018, 617 funding deals were successfully completed by private cybersecurity companies, representing a 40% increase in number of deals compared to 2015.[27] In 2019, four cybersecurity companies joined the global "unicorn club" of extraordinarily successful startups, with a valuation of over US$1 billion.

- **Consolidation.** Industrial maturity enhances processes of consolidation, creating giants which provide a broad range of products and services to a wide range of clients. As AT&T's Roger Thornton[28] stated, "There are 3000 firms today. Do we need that many? The industry is ready for more consolidation. The top 5 account for 10% of the sector's revenue." Thornton argues that this ratio is low and suggests further substantial consolidation lies ahead. Several of our interviewees also predict massive consolidation in the near future. For example, during a 2019 interview we conducted, one Israeli founder declared: "The hype is over in cyber! We've reached a steady-state. There will be only 10 firms by 2025." The pace of consolidation is increasing globally: In 2019 there were cybersecurity acquisitions totaling US$23 billion, including a particularly large acquisition valued at US$10.7 billion, in which both acquirer and acquired (Symantec) were in SFBA. That same year, there were 150 acquisition deals globally, up from just 45 in 2015.[29] Specifically, in the Big3 clusters, there were 186 cybersecurity acquisitions in all years combined (ending in 2019), representing 17% of all firms tracked in our Big3 dataset. SFBA leads with the greatest number and dollar volume of acquisition activity. We review this topic in more detail in Section 2.4.

[27] CB Insights database; The Increasingly Crowded Cybersecurity Unicorn Club, July 16, 2019.

[28] AT&T is an important cybersecurity services player. Interview is from Cyber Investing summit May 2019. Thornton was the VP of Products & Technology, AT&T Cybersecurity.

[29] CB Insights, 2019. Emerging Market Trends.

2.2 Industry typology and categorization

The global cybersecurity industry is characterized by particular firm characteristics and behaviors. With the aim of clarifying terminology, we introduce and define a set of typologies and categories:

Industry typology. Three types of cybersecurity firm have been identified: *Pure-play, Non-pure-play, and Non-cyber.*[30] This typology helps us understand the industry's scope using two key parameters: workforce and production. First, the cybersecurity workforce incorporates all three firm types, because they all employ cybersecurity workers. There are about one million cybersecurity workers in the USA as of 2020.[31] Second, cybersecurity industry production, that is producing cyber goods and services for consumption, includes only the first two types: pure-play and non-pure-play. Non-cyber firms, such as chocolate companies, do not produce cyber goods and services, but do hire cyber workers. Finally, the typology is useful when focusing solely on innovation and startup activity, in which case only one of the three types is of interest: much of the innovation takes place in pure-play firms.

Pure-Play → Cybersecurity Firms	Mostly engaged in cybersecurity. Most of the pure-play firms derive 100% of their revenues from cybersecurity. Most of these firms are product firms and many of these are startups. Check Point and Symantec (Symantec was broken up in late 2019)[32] are two large Pure-Plays. Other American examples: Mandiant, Darktrace, FireEye, and Qadium. The Pure-Plays can be subdivided by specialty category (see further below) such as threat detection or end-point security. As a young industry there is a great deal of M&A activity.
Non Pure-Play → Cybersecurity Firms	Firms which sell cybersecurity products and services, but this activity is not their main activity or source of revenues. Examples are: Oracle, IBM, Cisco, Microsoft, as well as some services firms in U.S. national security such as Booz, ICF, Blue Canopy. Also, some IT and consulting services firms such as Accenture or EY.
Non Cybersecurity Organizations →	Organizations engage in cybersecurity activities and many hire cybersecurity workers to protect their assets, but they do not derive revenues from cyber. Examples: hospitals, military, chocolate companies, airlines, schools, JP MorganChase.

Table 2.1 Industry typologies

Industry Categorization. The broader cybersecurity industry can be broken down into several categories or specialties. Many of the firms are considered innovative product firms, which develop new cybersecurity products as their core activity. The categories in Table 2.2 are dynamic: the industry evolves quickly in response to the new attack vectors that malicious actors develop relentlessly.

[30] Our typology is consistent with other studies. Aggarwal and Reddie (2018a, b), discussed below, use different terminology for a similar typology: for "Pure-play cybersecurity firms" they use the term "cybersecurity firms;" for "Non-pure-play cybersecurity firms," "internet technology firms;" and for "Non-Cyber," "internet-adjacent." We do note one exception: they include tech firms that have cybersecurity services *embedded* inside their offerings in their second category. We do not consider such firms as cybersecurity firms because they derive small or zero revenue from cybersecurity.

[31] Cyberseek, Cybersecurity Supply/Demand Heat Map, 2020. https://www.cyberseek.org/heatmap.html

[32] Symantec recently went through major changes. Its consumer-focused division was renamed NortonLifeLock and moved to Arizona. The business-focused cybersecurity services division was sold to Broadcom and soon after that to Accenture to serve as part of Accenture's Managed Security Services

Anti-Fraud Security	Protection against deception for unfair or unlawful gain, which includes credit card theft, data break-ins, identity theft, and cyberbullying.
Application Security	Protection of websites and applications.
Behavior Detection	Uses a combination of observation, casual conversation, directed conversation, and response evaluation.
Blockchain	Specialized security for blockchain applications.
Cloud Security	Policies, technologies, and controls deployed to protect data, applications, and cloud infrastructure.
Crowdsourcing	Platforms for teams of good-faith hackers who test security as adversaries.
Cryptography	Focused on specific cryptographic technology solutions, sometimes in hardware.
Data Security	Protection of data from unauthorized access and data corruption.
Deception Security	Detection, analyses, and defense against zero-day and advanced attacks, often in real time.
Enterprise Security	Broad security for organizations, including security operations, detection/mitigation, web browser and email protection, DDoS mitigation, and supporting DevSecOps.
Hardware Security	Focus on hardware solutions to cybersecurity threats.
ICS Security	Security solutions for Industrial Control Systems (ICS): typically related to critical infrastructure, Supervisory Control and Data Acquisition (SCADA) systems.
Identity Management	Identifying, authenticating, and authorizing access to applications, systems or networks by associating user rights and restrictions with established identities.
IoT Security	Safeguarding connected devices and networks in the Internet of Things.
Mobile Security	Protection of smartphones, tablets, laptops and other portable computing devices, as well as the networks they connect to.
Multi-Category	Companies which operate in more than one category where no particular category is considered primary.
Network/Endpoint Security	Protection of corporate/organization networks by focusing on network devices (endpoints), including monitoring their status, activities, software, authorization and authentication
Privacy	Privacy protection for consumers.
Risk Remediation	Remedying damage done by bad actors.
Threat Intelligence	Identification of possible threats (e.g., from log files or the dark web) and then presenting them in an actionable format.
Transportation	Specific solutions for protecting private cars, other vehicles, airplanes, drones, marine... anything that moves.

Table 2.2 Categories used in dataset with brief descriptions

Note two important notes regarding Table 2.2. First, each category encompasses a diverse, distinct, and constantly evolving set of competing firms. For example, Samatani et al. (2019)[33] estimate that there a total of 91 firms globally in the *Threat Intelligence* category alone, although some of these are larger firms that participate in multiple vertical categories, not only Threat Intelligence. They note that 34 of these 91 firms are based in SFBA (our own data shows 37, close enough to be comfortable).

Second, firms' classification by category is fluid because their primary activities change over time, and many firms operate in multiple categories. The distribution of firms belonging to each category is not evenly distributed in the Big3 clusters (Figure 2.4). IoT security, for example, is most prominent in Israel with 38 firms versus only 21 in the two American clusters combined, though this is likely temporary. Israeli firms have tended to be agile in finding successful niches like IoT. SFBA dominates in the broader categories of cybersecurity, like cloud and endpoint security. The presence of consulting and multi-sector firms in Washington, on the other hand, dwarfs the other two regions. Washington's 38 consulting and 37 multi-sector firms outnumber the other two clusters combined.

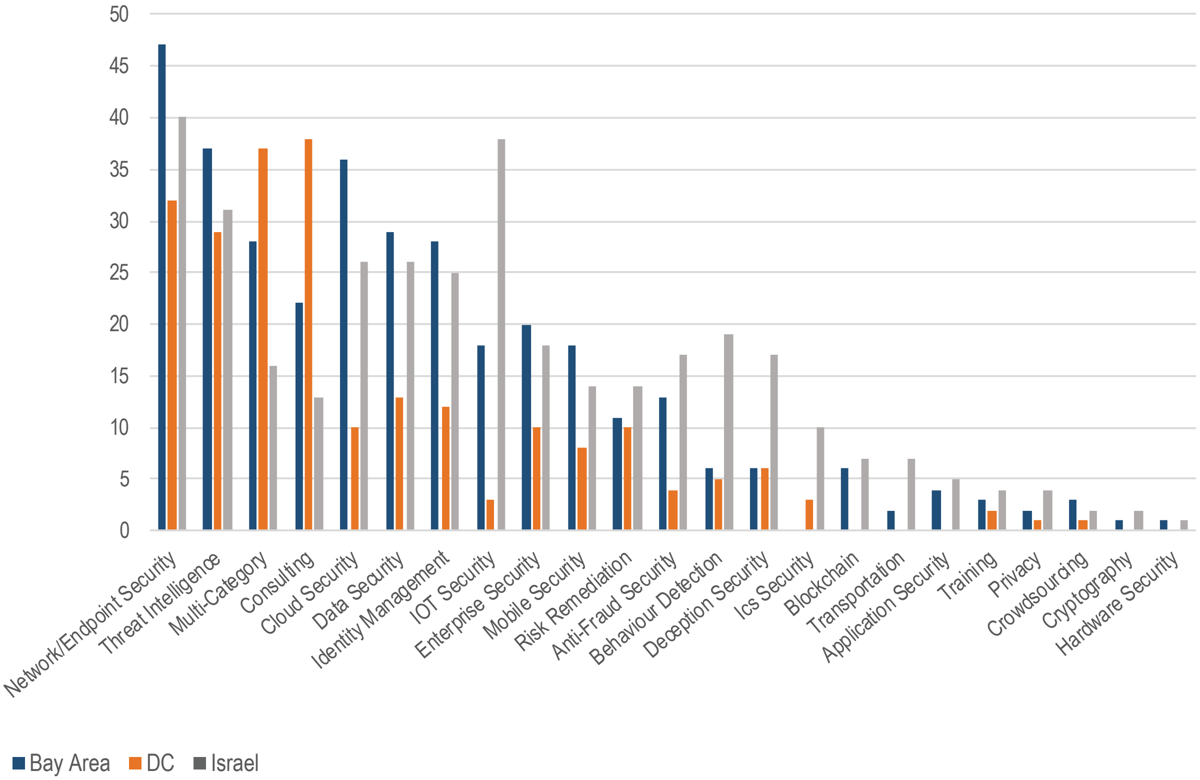


Figure 2.4 Cybersecurity firms in each cluster classified by primary business operation.[34]

Service Categories. Service firms are those which design, install, monitor, react, and support client cybersecurity needs. A majority of venture capital flows to pure-play product firms, especially in SFBA and Israel, yet most of the industry's workforce is dedicated to services. Moreover, much of that workforce is outside the Big3 clusters. Many of the technology giants operate substantial cybersecurity service businesses. Tech giants typically do not break

[33] Sagar *Samtani*, Maggie *Abate*, Victor *Benjamin*, and Weifeng *Li*. "Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective" Palgrave Handbook of International Cybercrime and Cyberdeviance, Springer, 2019.

[34] Source: Business in the Capital cybersecurity dataset, American University.

down their cybersecurity units' numbers, but a sample of those that do speaks to their size. Cisco, for example, sold US$1.75 billion in cybersecurity services (2016) representing about 3% of its global revenues.[35] In 2015, IBM had 8000 employees working in cybersecurity globally, with revenues of US$2 billion).[36] When EMC published its cybersecurity revenues in 2014 after acquiring RSA, they stood at US$1 billion.[37]

One of the largest cybersecurity services categories is *Managed Security Service Providers* (MSSP). These firms provide relatively routine maintenance support for client companies of all sizes that choose to outsource their cybersecurity needs. According to Cybersecurity Ventures, there are 44 large MSSPs total, including many familiar names, such as Accenture, DXC Technology, IBM, Verizon, BT, CenturyLink, Trustwave, NTT, Secureworks, and Wipro.[38] Many service firms, including many MSSPs, have set up enormous cybersecurity centers known as Security Operations Centers (SOCs). Each SOC employs many cybersecurity specialists. AT&T, for instance, has 8 SOCs around the world, mostly located in the U.S., one of which was recently completed in the Washington area to service the needs of the U.S. Federal Government. Fireye has 7 SOCs in the U.S.

It is worth mentioning that only five of the 44 MSSPs are based in one of the Big3 clusters. Why are these firms not physically located in the geographic centers of cybersecurity innovation? One likely reason is that MSSPs tap the less expensive cybersecurity workers who specialize in more routine cybersecurity network maintenance and client service activities. Thus, their activity is often located in cities with a lower cost of labor, like Blue Bell, Pennsylvania, or Colorado Springs, Colorado.

2.3 Clusters roots and history

The industry's evolution is further concretized by presenting the historical narratives of each one of the Big3. These narratives will serve to aid understanding of the ecosystems' emergence and their future trajectories.

- **San Francisco Bay Area Cluster History**

The origins of the SFBA cybersecurity cluster are in the foundation built by the larger high-tech industry, the famed Silicon Valley. Its evolution began in the days of Fairchild Semiconductor in the 1950s and 1960s and the many spin-offs that emerged at the time, through to contemporary technology heavyweights like Apple and Google.

Initial development of the SFBA cybersecurity cluster was also influenced by early success of firms such as McAfee and Symantec. McAfee sold its first product in 1987, and was initially focused on the consumer security market. The firm was later acquired by Intel, also headquartered in Silicon Valley. Symantec[39] began as a general software utilities firm and subsequently transitioned into cybersecurity in the 1990s. By the early 2010s, McAfee and Symantec had grown their service and product offerings to include those related to firewall and antivirus protection. By 2013, Symantec had an impressive 150 products and thus began to "rationalize" its product line. Competition for these two giants then intensified. Among their largest competitors were other SFBA tech goliaths Cisco and HP, as well as a large new wave of cybersecurity startups.

SFBA is at the heart of the global cybersecurity industry. As early as the turn of the millennium, the area was displaying signs of a maturing industry: firms began to consolidate through mergers and acquisitions. In some

[35] Cisco annual report 2016

[36] IBM annual report 2018; Steve Morgan, Meet The World's Largest Pure-Play Cybersecurity Companies, Forbes, Apr 20, 2016

[37] Joe Panettieri. Dell-EMC: Keep or Sell RSA Security? Channel e2e.com, Feb 11, 2016

[38] Steve Morgan, "Directory Of Managed Security Service Providers (MSSPs) To Watch In 2020," *Cybersecurity Ventures*, Feb. 20, 2020 https://cybersecurityventures.com/managed-security-service-providers-mssps/

[39] As noted above, Symantec was acquired recently.

significant deals at this early stage both the acquirer and the acquired were headquartered in SFBA. One key example is the 2003 acquisition of Netscreen by Juniper for US$3.5 billion. Both of these firms were headquartered in Sunnyvale, in the heart of Silicon Valley. Another important transaction saw Intel purchase McAfee for US$7.6 billion in 2010. Again, both firms were headquartered in Silicon Valley.

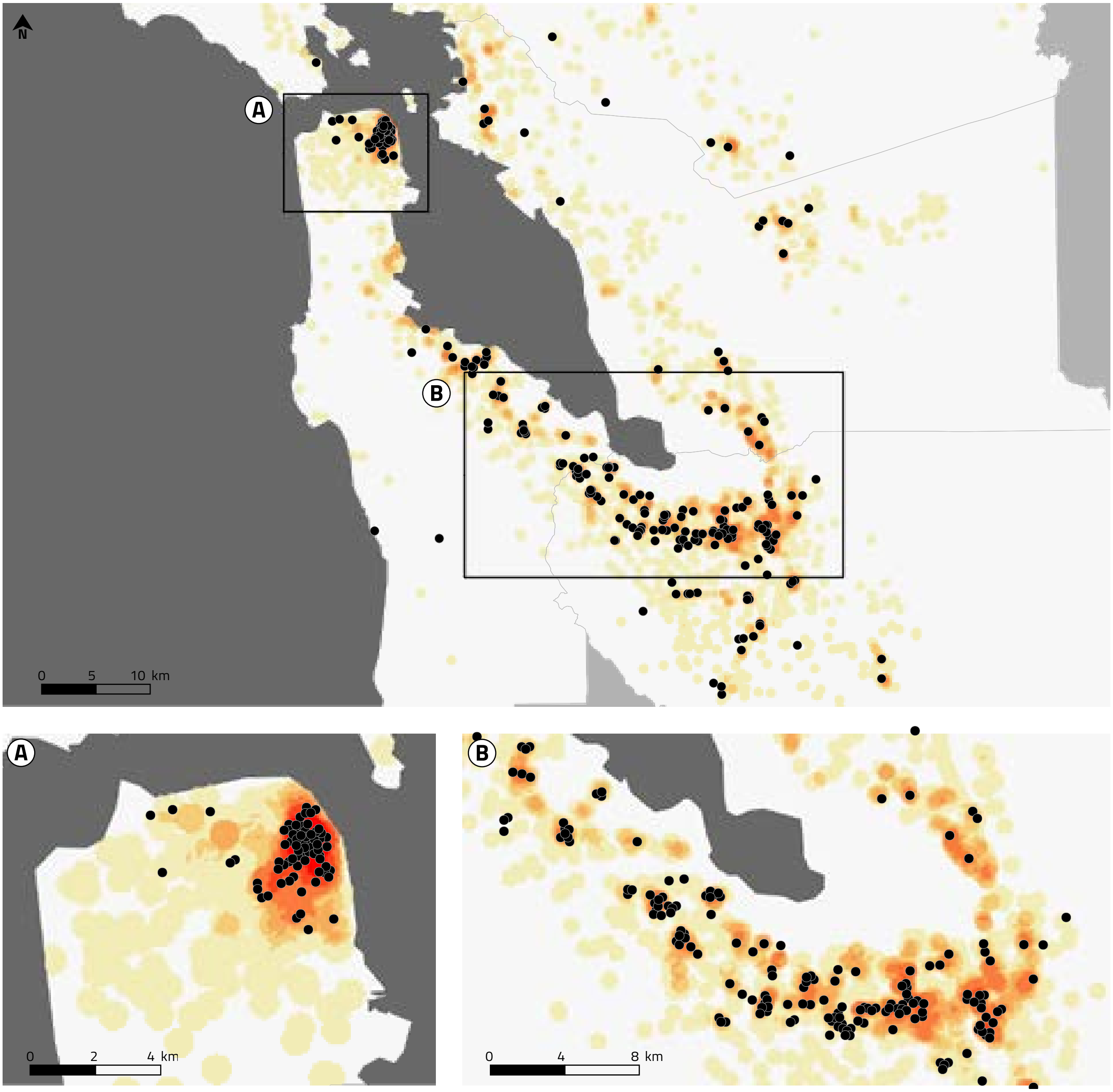
Regarding the industry's regional collaboration, the cybersecurity industry has long shared threat knowledge through ISACs and ISAOs, and training through organizations such as ISC^2 but has lagged behind other high-tech industries in creating formal industry-specific lobbying groups and professional associations. One exception in SFBA is the annual RSA conference, which first took place in San Francisco in 1991. By the late 1990s it had grown into an important magnet for all cybersecurity-related businesses in the IT field.[40]

SFBA cybersecurity firms are distributed geographically much like the rest of the high-tech industry in the region, as shown in Map 2.1. Cluster development began mostly in Silicon Valley, which is located at the southern end of San Francisco Bay, about 50 km (30 miles) from San Francisco. By 2013, however, SFBA high-tech startup activity began to display a clear bimodal distribution pattern between downtown San Francisco and Silicon Valley.[41] Major tech firms established themselves in the City of San Francisco, including the likes of Twitter, Yelp, Airbnb, Uber, and Salesforce. While most cybersecurity firms established early on remain in the Silicon Valley area, particularly the largest ones, some cybersecurity startups did follow this geographic trend. Important cybersecurity firms in the City of San Francisco include Expanse, Forgerock, Bugcrowd, Okta, and Hacker1.

Map 2.1: San Francisco Bay Area Overlay of cybersecurity firms in relation to general high-tech firms distribution. Black dots are cybersecurity firms. Map A is a close-up of the City of San Francisco; the red area in the heatmap is downtown. Map B is a close-up of the heart of Silicon Valley that includes the headquarters of Google, Apple, Facebook, Intel, Netflix, and many more recognized firms. Source: Business in the Capital cybersecurity dataset, American University; US Bureau of Labor Statistics for high-tech firms.

[40] In 1993, it became an annual event and was renamed the RSA Data Security Conference. Finally, by 2000, it took on the name of "RSA Conference." It has always been held in the San Francisco Bay Area.

[41] Richard Florida, 2013. "Why San Francisco May Be the New Silicon Valley" *CityLab*, August 5, 2013 https://www.citylab.com/life/2013/08/why-san-francisco-may-be-new-silicon-valley/6295/



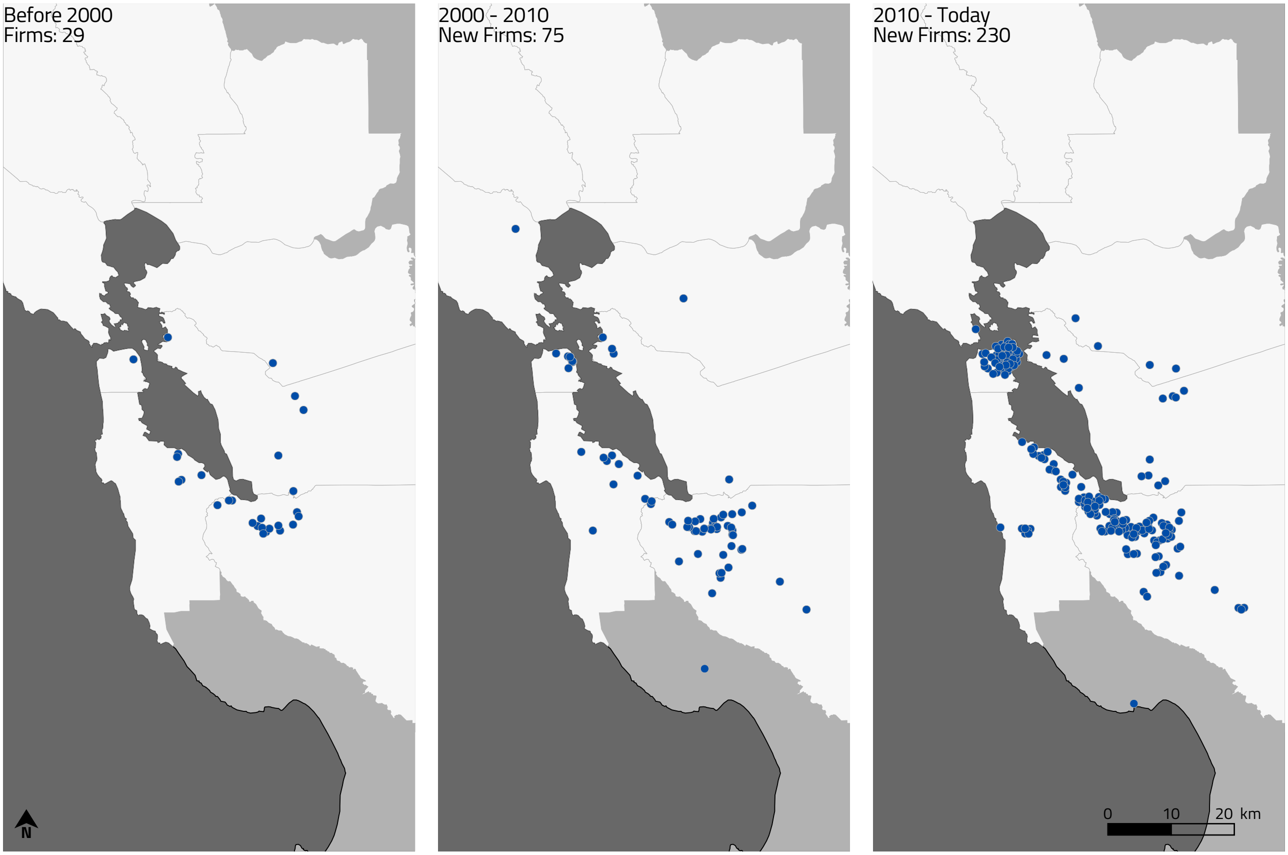
Map 2.1 SFBA-headquartered cybersecurity firms in relation to general high-tech firm distribution

High Tech Firms per sq. km.

🟨	1 - 5
🟧	5.1 - 10
🟧	10.1 - 20
🟥	20.1 - 50
🟥	50.1 - 100
🟥	100.1 - 508

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)

Map 2.2 illustrates growth of the SFBA cybersecurity cluster as well as the emergence of hot zones,[42] based on the year each firm was founded. Before 2010, the majority of firms were founded in southern SFBA, Silicon Valley. While the valley cluster is still larger, a ballooning of cybersecurity firms in downtown San Francisco after 2010 is evident. It is likely a reflection of migration patterns toward living in city centers, compounded by the onerous commute between the city and Silicon Valley.



Map 2.2 SFBA-headquartered pure-play cybersecurity firms by year founded

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)

[42] A “hot zone” is a dense geographic agglomeration of firms within a mega-cluster, as noted in Chapter 1.

• Washington D.C. Cluster History

The Washington D.C. cybersecurity industry owes its origin to its history as a center for national security and defense. The local defense and technology ecosystem began developing during World War II. At that time, under urgent wartime pressure, the Pentagon building was built hurriedly. From that point on, it has been commonly said that all aspects of U.S. national defense emanate from the Pentagon. The U.S. emerged from WWII as a global superpower with a vast and growing network of both private sector and government defense expertise. A significant portion of this network was located within driving distance of the Pentagon. Vannevar Bush is a prime example. Bush was the influential defense visionary widely considered to be the “spiritual father” of the World Wide Web: He spent the decade after the war in Washington.[43]

The defense industry formed in communities surrounding Washington D.C. such as Arlington, Falls Church, Tysons Corner, and later, further out near Dulles airport. At the end of World War II, none of the largest private aerospace and defense firms were headquartered in the Washington area, but key firms slowly migrated their headquarters there in subsequent years. Of the five largest American defense contractors, three moved their headquarters to Washington, including General Dynamics in 1990; Lockheed in 1995; and Northrop Grumman in 2011. The other two are not headquartered in the D.C. region, but have established major local operations, Raytheon in 1995, and Boeing in 2017. In the 1980s, U.S. federal government employment shrunk while government contracting doubled, spelling significant opportunity for private contractors.[44]

The first private defense consulting contractors were established near the Pentagon in the 1950s.[45] Subsequently, many major government contractors from across the country relocated to the Washington region in order to be close to the Pentagon, e.g., CACI moved its headquarters from Los Angeles to Washington in the 1970s. Others opened major divisions close to the Pentagon, including CSC and PRC in the 1960s, and SAIC in 1970, all from California. These firms represent critical components of the Washington D.C. *national security ecosystem*, which we define as, “the regional network of government entities and commercial contractors that work together for the protection of the nation.”

The U.S. Department of Defense and other agencies in the national security ecosystem began to protect their own information systems in the 1980s. However, there was little private sector cybersecurity startup activity until after the turn of the century. Regarding startup formation and industry maturation, development of the Washington cluster differed from that of Silicon Valley, at least in this early stage. One major difference was that Washington cybersecurity startup founders were in large part incubated within the national security ecosystem,[46] a relative rarity in SFBA. Significant industry demand was created by increased government contracting. Most major contracts in the early years went to large, well-known, Washington-based government consultancy contractors, such as Booz Allen. Then, primarily between 2010 and 2012, most major defense giants with headquarters or major presence in Washington began either buying or building in-house commercial cybersecurity operations; Boeing, Lockheed and General Dynamics among them. These firms had historically focused on services. During that time, many smaller regional cybersecurity firms that originated as service providers transitioned into being pure-play cybersecurity product firms.

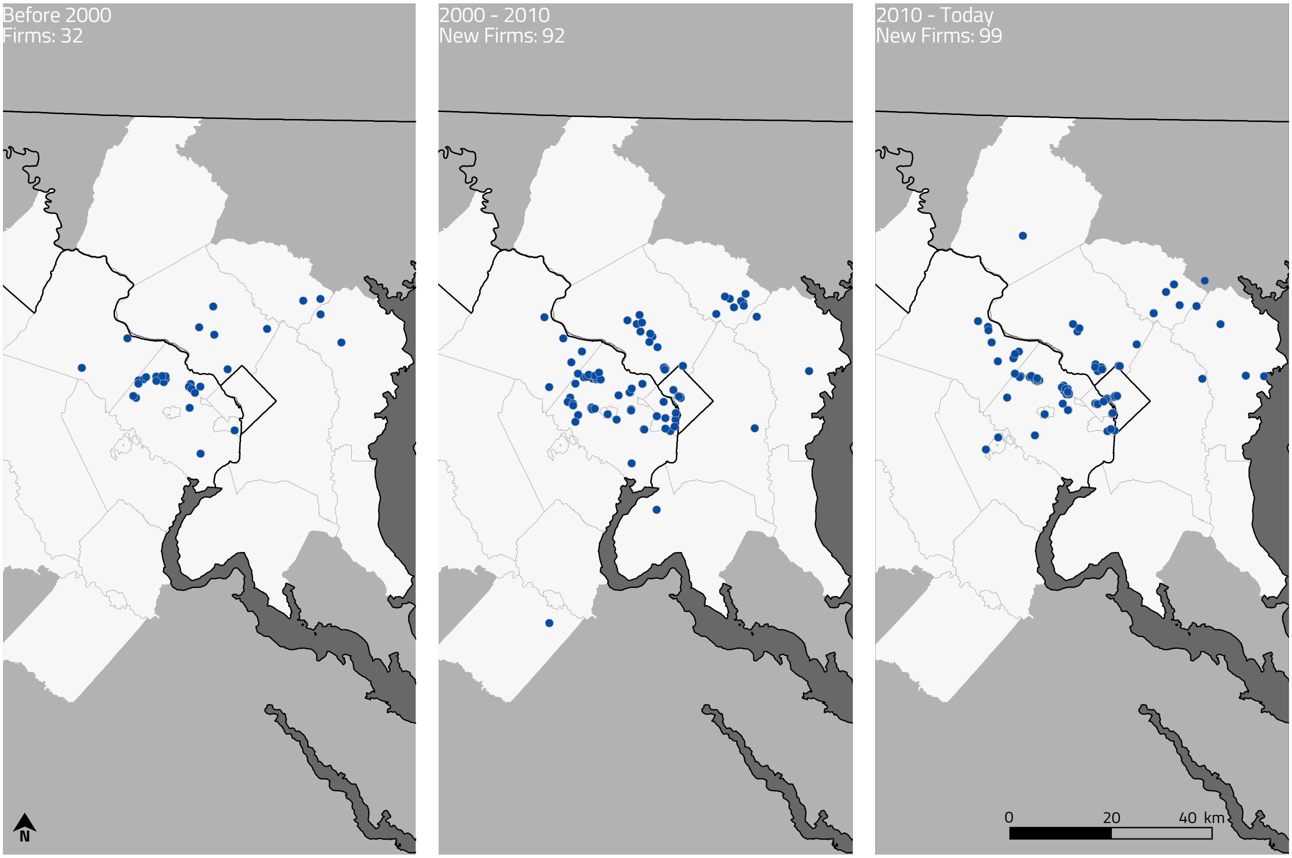
[43] Paul Ceruzzi, 2008. “Internet Alley: high technology in Tysons Corner 1945-2005” Cambridge: MIT Press.

[44] Feldman, M. P., J. Francis and J. Bercovitz (2005), “Creating a Cluster While Building a Firm: Entrepreneurs and the Formation of Innovative Clusters.” *Regional Studies*, 39: 129–142.

[45] Paul Ceruzzi, “Internet Alley.”

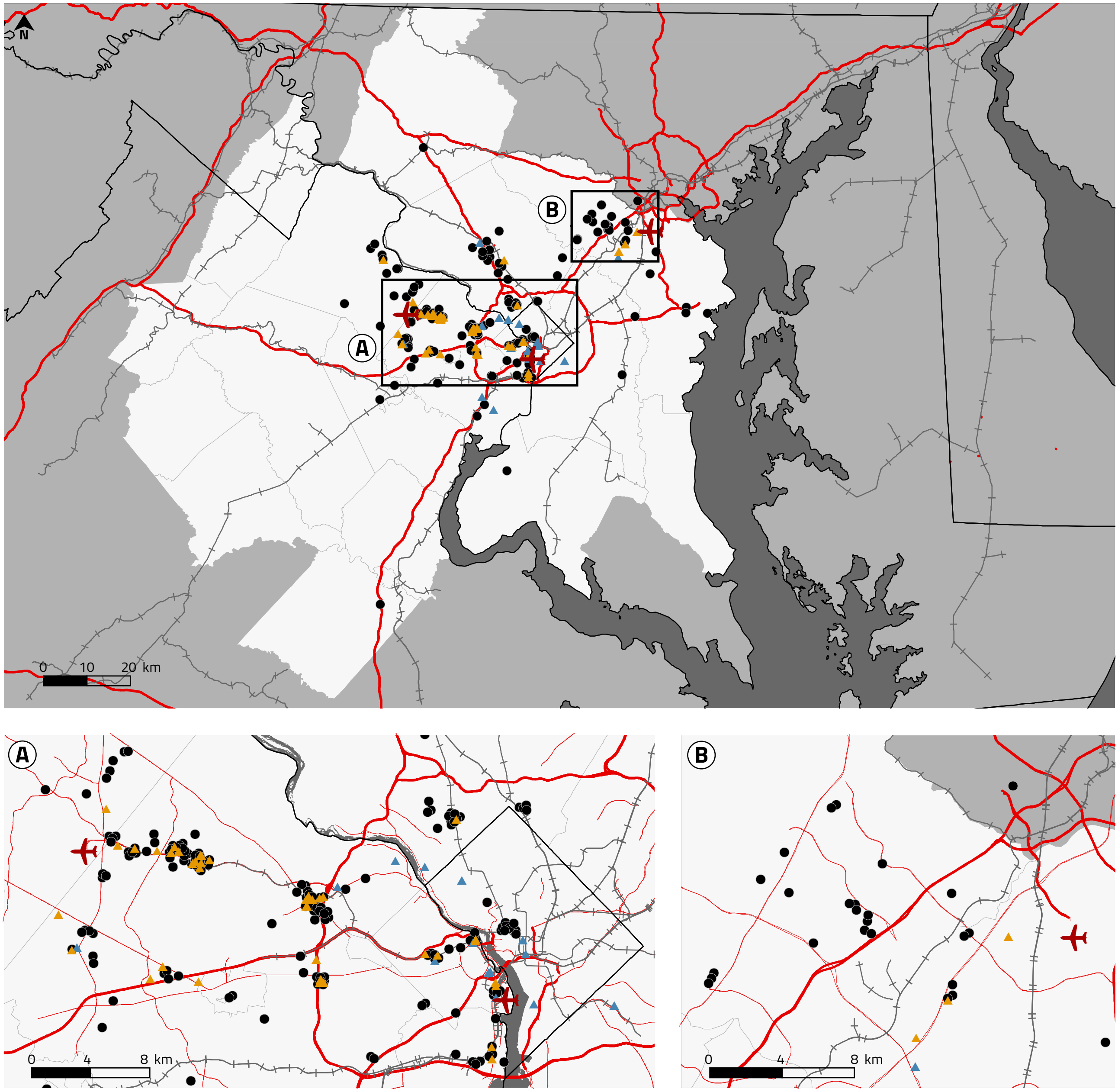
[46] Erran Carmel, Bini Byambasuren, and Jonathan Aberman. *Cybersecurity Startup Founders in the Greater Washington Region: Prior Experience Required.* April 2018. Center for Business in the Capital, American University.

Map 2.3 contextualizes the growth of the Washington cluster geographically, including the emergence of sub-clusters, based on the year each firm was founded. Overall, however, the distribution pattern in each decade is fairly similar to its predecessor and there does not seem to be a time-based pattern on the clustering of firms in the Washington cluster. Note that, compared to clusters in Israel and SFBA, the Washington cluster has the highest ratio of firms founded prior to the turn of the millennium.



Map 2.3 Washington-headquartered pure-play cybersecurity firms by year founded

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



Map 2.4 Washington-headquartered pure-play cybersecurity firms, national security organizations and large defense contractors

● Cybersecurity Company

▲ Private National Security / Cyber

▲ US Government National Security

Highway / Primary Road

Railway

Major Airport

State Boundary

County Limit

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University (Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)

Map 2.4 illustrates the interplay between U.S. national security and the cybersecurity industry. It overlays three organizational types: U.S. national security organizations, such as the U.S. Department of Defense at the Pentagon; large defense contractors such as Booz Allen; and pure-play cybersecurity firms. The map displays the clustering that is predominantly located due west of Washington D.C., along the corridor toward Dulles International Airport. Map A is a close-up of this so-called "Dulles corridor" where most defense and cybersecurity firms are concentrated.

Many cybersecurity workers and startup founders began their careers at the U.S. National Security Agency (NSA) in Fort Meade, Maryland. Many other cybersecurity workers work or have previously worked for similar co-joined entities such as the U.S. Cyber Command and the Defense Information Systems Agency. As a result, Maryland has a particularly high concentration of cybersecurity experts and software programmers. Founders of several innovative startups share this heritage. Three noteworthy examples based in the Maryland suburbs of Washington D.C. include: Trusted Information Systems, which pioneered the firewall in the 1980s; Sourcefire, a key firm for detecting network intrusions; and Tenable, which created a successful platform to measure cybersecurity risk.[47] The U.S. Federal Government and associated agencies based heavily in the D.C. metropolitan area help make the region a major component of the U.S. cybersecurity industry, spending approximately US$14 billion on cybersecurity in 2016 and US$19 billion in 2017.[48]

Map 2.4.B is a close-up of the sub-cluster of cybersecurity firms that emerged around the NSA in Fort Meade, midway between Washington and Baltimore. This sub-cluster, made up of Fort Meade, Annapolis Junction, Colombia, and other suburban communities, is of interest because it was clearly seeded by an anchor organization. According to our data, the sub-cluster has roughly 25 firms, as of this writing, is still growing rapidly and employing thousands of workers.

• Israel Cluster History

Similar to SFBA, the Israeli cybersecurity cluster grew from roots in the larger Israeli high-tech cluster, colloquially known as "start-up nation."[49] Against the odds, Israel has become one of the world's foremost high-tech innovation clusters.[50] According to Engel and Del-Palacio,[51] one of this cluster's greatest strengths is that it is an "Innovation Super-Cluster," meaning that it fosters inter-industry crossover and collaboration between fields such as military applications, biotechnology, and medical devices. "Israel is not simply a set of industrial clusters where the innovation advantage is industry specific."[52] One commonly-cited metric of accomplishment is the number of companies a given nation has listed on the high-tech heavy NASDAQ. By this measure, Israel consistently ranks in the top tier of countries worldwide.[53] Thus, the Israeli cluster milieu, similar to that of Silicon Valley, is where the Israeli cybersecurity industry was born and developed.

The origin of the Israeli cybersecurity industry is showcased by its most successful firm, Check Point, with its firewall software product. Check Point was founded in 1993 and almost immediately became a global symbol of computer security in the new internet age. Check Point notably paved the way in financing for other Israeli startups. Check Point received venture capital early on, and within just three years launched an IPO on the

[47] Ron Gula, 2017. "Maryland needs you to create the next great cybersecurity company." *Washington Business Journal*. Nov 28, 2017

[48] Austrade, "US Cybersecurity Clusters," 2016. https://www.austrade.gov.au/ArticleDocuments/5085/US-Cyber-Security-Clusters.pdf.aspx

[49] Dan Senor and Saul Singer, *Startup Nation: The Story of Israel's Economic Miracle* (New York, NY: Twelve, 2009).

[50] Jerome S. Engel and Itxaso del-Palacio, "Global Clusters of Innovation: The Case of Israel and Silicon Valley," *California Management Review* 53, no. 2 (February 2011): 27–49, https://doi.org/10.1525/cmr.2011.53.2.27.

[51] Engel and Del-Palacio, "Global Clusters of Innovation."

[52] Engel and Del-Palacio, "Global Clusters of Innovation."

[53] Catherine de Fontenay, C. and Erran Carmel, 2004. Israel's Silicon Wadi: The forces behind cluster formation. In Bresnahan, T. Gambardella, A. and Saxenian, A. (eds.) *Building High Tech Clusters*, Cambridge University Press.

NASDAQ exchange, which raised the then-impressive sum of US$67 million. Like many Israeli tech companies, Check Point was founded by young tech entrepreneurs. Most of the firm's founders and pioneer employees were trained through their experience in Israel's elite 8200 military intelligence unit, somewhat analogous to the American NSA.

Other Israeli firms from that era include Arx, Radguard, Finjan, and Netguard. Nearly all of these companies were acquired, except for Radguard which collapsed in the global recession of 2001. Memco, another example, was purchased for US$400 million in 1998. For over 25 years, Check Point has stayed independent, and grown to become not only one of the largest and most successful high-tech firms in Israel, but one of the largest cybersecurity firms in the world. CyberArk, founded in 1999, is another Israeli firm that remains independent, growing and expanding considerably alongside Check Point.

Several Israeli and American firms are spin-offs started by former employees of Check Point, mimicking the incubator role played by Fairchild Semiconductor in Silicon Valley. Founders and employees of Check Point went on to establish some of the largest and most influential cybersecurity firms in the world, including Palo Alto Networks, Illusive Networks, Sentinel One, and Imperva, among others. Three of these firms are headquartered in Silicon Valley.

During the rapid growth period of era 3, the Israeli cybersecurity industry grew far more dramatically than the other two clusters, rocketing in start-up creation. For several years during that era, the nationwide cybersecurity startup launch rate stood at an astounding three to four firms per month.

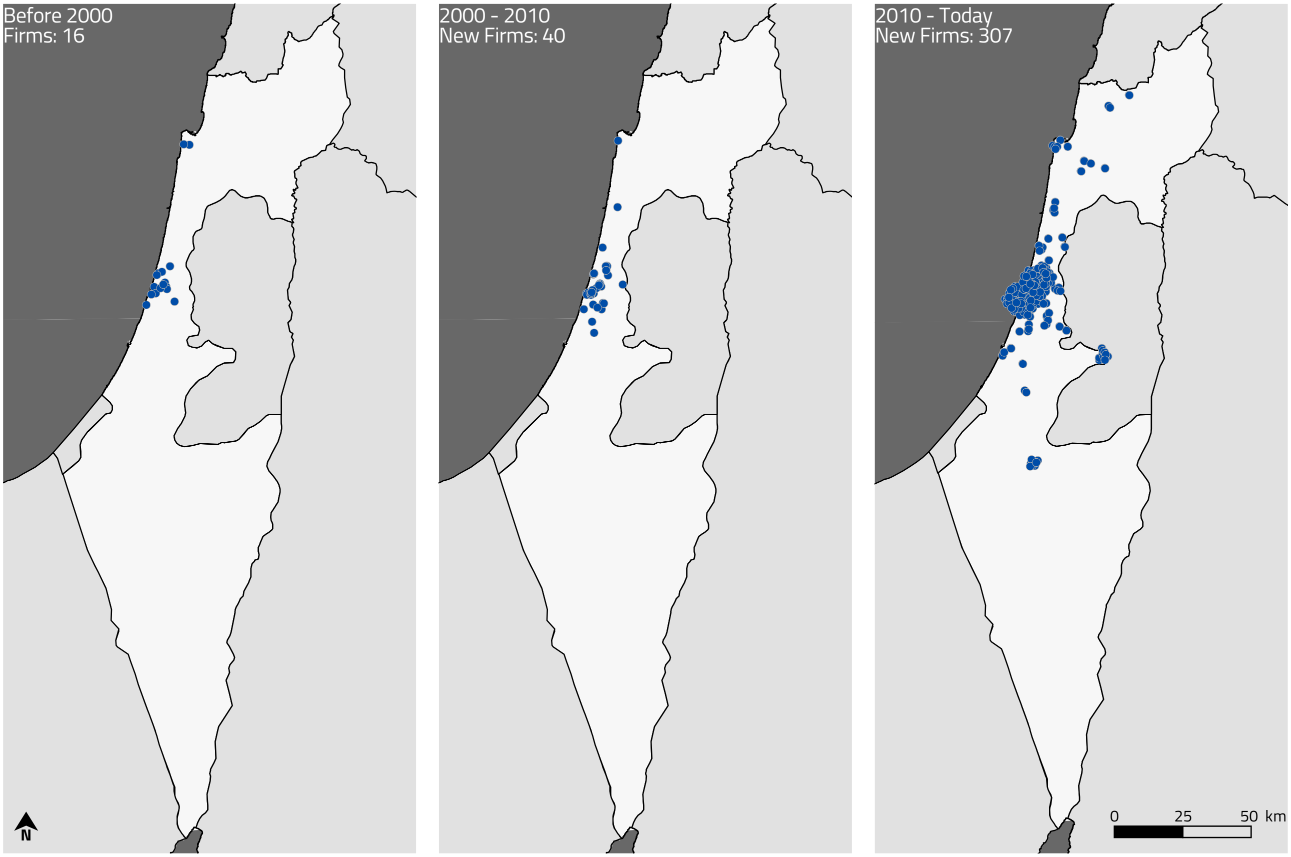
The sub-cluster in Be'er Sheva, in the south of Israel, is of particular interest. The Israel maps in Chapter 2 and Chapter 3 magnify this small cluster because, unlike other formations in the Big3 clusters, which are somewhat organic, it is a deliberate cybersecurity sub-cluster. Geographically, the cluster straddles a major regional train station. Ben-Gurion University, one of Israel's principal universities, is south of the tracks; just north of the tracks is the high-tech park, and some cyber and military bases. All three elements are within walking distance of each another.

This deliberate cybersecurity cluster was born in 2014 when the Prime Minister declared "Be'er Sheva will not only be the cyber capital of Israel but one of the most important places in the cybersecurity field in the world."[54] This was followed by grand plans to move major national and military cyber units to Be'er Sheva. Some cyber firms and divisions have been in Be'er Sheva since 2014 and even before. But the numbers have been small when measured by number of workers, number of firms, capital raised, and overall influence. A major setback began when the Israeli military repeatedly delayed relocating its cyber assets from Tel Aviv to Be'er Sheva.[55]

[54] Irad Schmair, November 11, 2019. "In the South They Dream Of Silicon Valley, Start-Ups Remain in the Center." The Marker (in Hebrew). And Authors' interviews 2018.

[55] Schmair, 2019; Authors' interviews.

Map 2.5 illustrates growth of the Israeli cybersecurity cluster based on the year each firm was founded. Firms tend to be younger than those found in SFBA and in Washington. Nearly all firms founded before the turn of the millennium are located in metropolitan Tel Aviv.[56] Minor scattering takes place after 2010 as a handful of mostly less-influential firms are founded in other Israeli cities, Be'er Sheva,[57] Haifa, and Jerusalem.



Map 2.5 Israel-headquartered pure-play cybersecurity firms by year founded

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)

©Laboratory for Contemporary Urban Design, Tel Aviv University

[56] Formally, the City of Tel Aviv is "Tel Aviv-Jaffa"

[57] Be'er Sheva, one of Israel's largest cities, is also sometimes written as Beersheba.

2.4 Size, money, and consolidation

In order to better understand the variations between the cybersecurity clusters, this section examines quantitative data concerning the Big3 clusters using data on company size, venture capital, and consolidation.

- **Company Size: Workforce, Revenues, and Valuations**

How many people are employed by the cybersecurity firms in this study? In order to set approximate boundaries for this analysis, we use Cyberseek (2020), which estimates that nearly one million people involved in cybersecurity work in the U.S., and also that there were 504,000 job openings in 2019.[58] However, we emphasize that many of these workers are employed by non-cybersecurity organizations, which is largely outside the scope of this chapter.

The median firm size for pure-play firms in the Big3 (Figure 2.5), by number of employees, is approximately the same in all three clusters: at 31, 31, and 25 for the SFBA, Washington, and Israel clusters respectively. All three regions are weighted downwards, in terms of size, by a disproportionate number of startups, which tend to be quite small, there are 171 firms have fewer than 10 employees, accounting for 19% of the total firms in the dataset.

SFBA-based firms have by far the greatest number of employees. Our data for SFBA firms shows a total of 92,000 employees.[59] This total is heavily weighted by a handful of behemoth firms, each with many thousands of workers globally, including Fortinet with 5100 employees; Palo Alto Networks with 5300; McAfee with 7600; Juniper Networks with 9400; and Symantec (before its break-up) with 11,800 employees. In the other two clusters, total employment in pure-play firms is roughly 20,000.

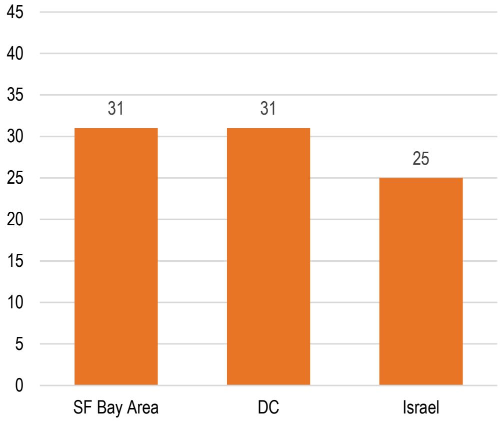


Figure 2.5 Cybersecurity firm size: Median number of employees in pure-play firms by cluster.[60]

Company size is also measured by revenue. SFBA cybersecurity firms totaled nearly US$26 billion in revenue in 2018, led by established players such as Symantec (US$4.8 billion), Juniper Networks (US$4.7 billion), and McAfee (US$2.4 billion). The median revenue per company is roughly the same in all Big3 clusters[61] as seen in Figure 2.6b.

[58] Cyberseek 2020 Cybersecurity Supply/Demand Heat Map. https://www.cyberseek.org/heatmap.html. Note that the heat map uses data from 2018-2019. Workforce includes those who require cybersecurity knowledge but are not officially cybersecurity workers.

[59] Estimating the SFBA workforce at these firms is not straightforward. Many of the company workers are not in the SFBA but around the globe. Furthermore, many workers in pure-play firms, such as salespeople and accountants, are not cybersecurity professionals. Also, there is the issue of contractors; in the larger SFBA cybersecurity firms, a 1:1 ratio of full-time and contract workers is not uncommon.

[60] Source: Business in the Capital cybersecurity dataset, American University.

[61] In each cluster, there was data for more than 100 firms; specifically, there were 242 in SFBA, 125 in Washington and 168 in Israel.

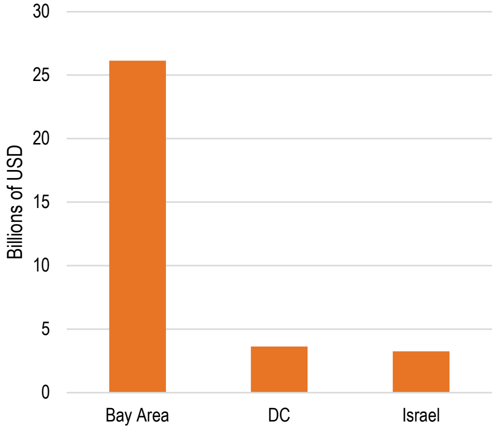


Figure 2.6a Total firm revenue by cluster (2018)[62]

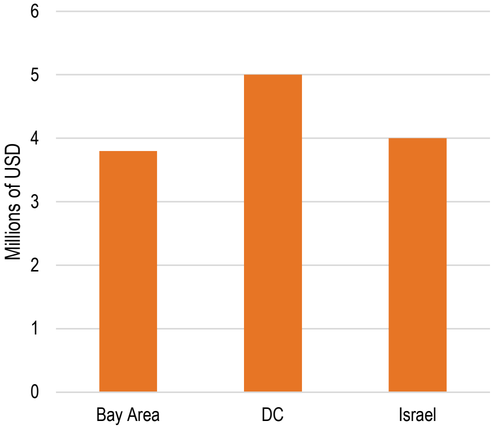


Figure 2.6b Median firm revenue by cluster (2018)[63]

Finally, company size can be measured by valuation, which represents a firm's net worth either based on their stock price or a professional estimate. The handful of firms with publicly traded equity in the Big3 clusters had a combined value of US $138 billion,[64] of which most of the firms (12 of 16), and most of the value, are in SFBA. These 16 firms tend to be larger, more influential firms.

To get a sense of the not-insignificant impact of younger firms, it is useful to look at unicorns. Unicorns are young firms assessed at over US$ one billion. In early 2019, before the coronavirus pandemic, there were 308 unicorns globally in all areas, and six were SFBA cybersecurity firms. One of the cybersecurity unicorns, Crowdstrike, launched an IPO later that year.

- **Venture Capital and IPOs**

In order to launch and grow, new companies need investments. Startups in all industries typically raise funds through venture capital and public equity. Figure 2.7 compares the amount of venture capital raised by cybersecurity firms in each of the Big3. All three clusters raise large amounts of capital by global standards, but the hegemony of SFBA is evident with US$13 billion in venture capital raised; more than twice Washington and Israel combined.

A successful IPO is a marker of a company's growth and success, although many firms do not choose this path. Thirty-seven cybersecurity companies "went public" in the Big3 clusters between 1996 and 2019. A timeline is presented in Figure 2.8. As the graph shows, the number of IPOs peaked in 1999 during the "Dot-Com" period, followed by minimal activity after the 2001 recession. The dearth of IPOs despite industry growth after 2010 reflects broader preference for exit via M&A, including purchase by private equity firms. Relatively few cybersecurity firms are traded publicly. In 2013, for example, three cybersecurity firms launched an IPO: FireEye, Barracuda Networks, and Gigamon. Of these, only FireEye remains a publicly-traded company, while the other two have since privatized.

[62] Source: Business in the Capital cybersecurity dataset, American University.
[63] Source: Business in the Capital cybersecurity dataset, American University.
[64] Computed on May 6, 2020, after the initial coronavirus crisis crash.

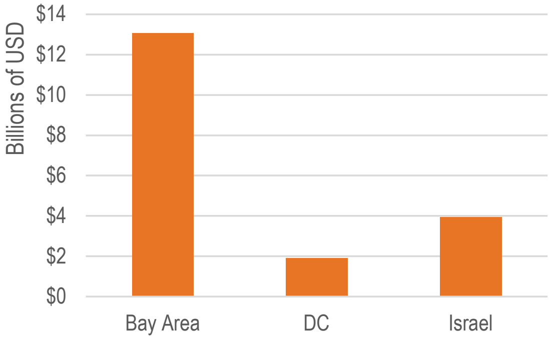


Figure 2.7 Cybersecurity firm venture capital funds raised, cumulative through Q3 2018.[65]

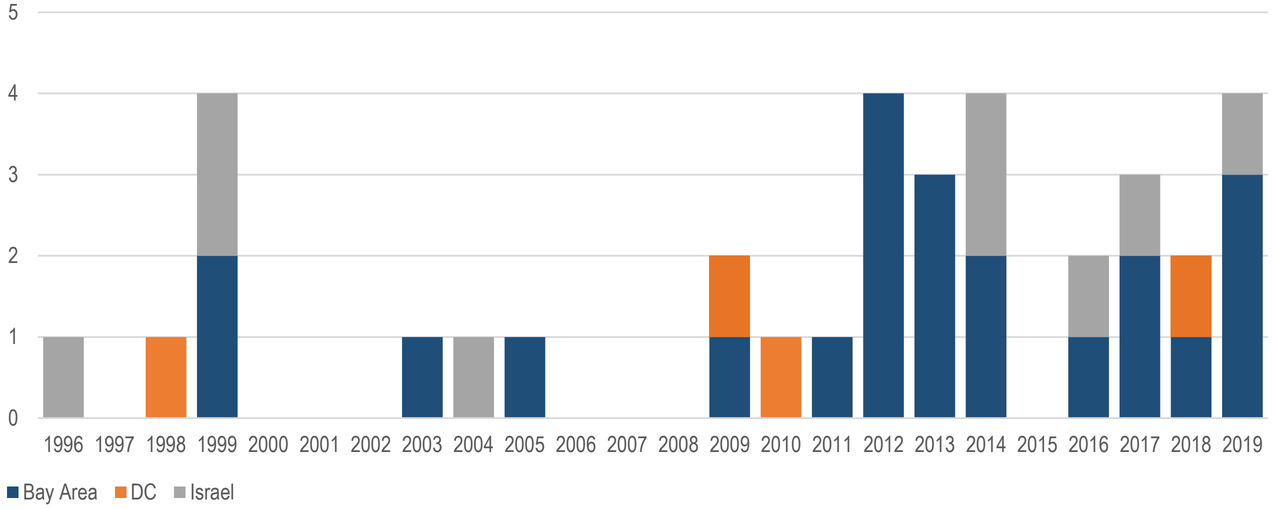


Figure 2.8 Number of cybersecurity firm IPOs by year. (note: 2019 is a partial year).[66]

[65] Source: Business in the Capital cybersecurity dataset, American University.

[66] Source: Business in the Capital cybersecurity dataset, American University.

- **Consolidation**

A key to understanding of an industry is assessing where it is on the historical consolidation curve. Young industries are fragmented while mature industries, such as automobiles, have a few giants. Deans et al. (2002)[67] write that "most industries progress predictably through a clear consolidation life cycle." Their *Industry Consolidation Life Cycle* suggests that the cybersecurity industry is in Stage 2 (of 4 stages) since the major players still do not have more than 50% of the global market share. Nonetheless, there is currently significant consolidation activity.

Figure 2.9 shows extensive acquisition activity of cybersecurity firms based in the Big3 clusters. In all years, these firms acquired 393 cybersecurity firms around the world. Figure 2.9a shows the acquisitions made by firms headquartered in the Big3 clusters. Figure 2.9b shows the 186 firms that were acquired by firms in the Big3 clusters, in all years.

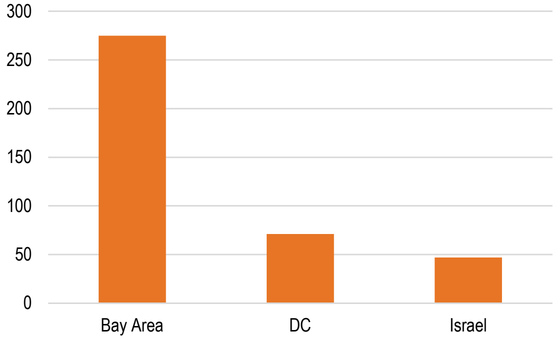


Figure 2.9a Number of acquisitions made by cybersecurity firms with HQ in given cluster. Cumulative for all years. Acquired firms are both inside and outside the three clusters.[68]

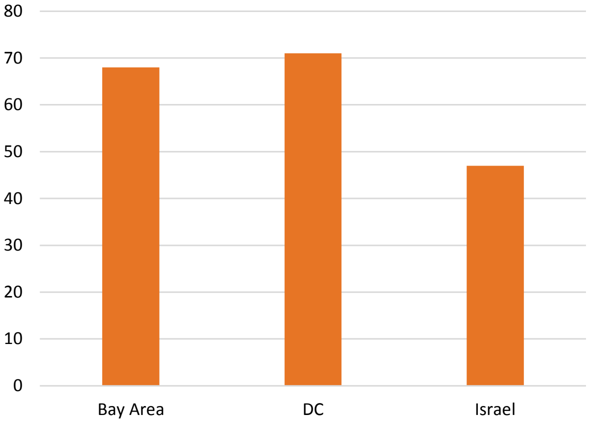


Figure 2.9b Number of acquired firms by cluster. Cumulative for all years.[69]

[67] Graeme K. Deans, Fritz Kroeger and Stefan Zeisel, "The Consolidation Curve" *Harvard Business Review*, December 2002.

[68] Source: Business in the Capital cybersecurity dataset, American University.

[69] Source: Business in the Capital cybersecurity dataset, American University.

Table 2.3 provides insight into which larger, more established companies are acquiring cybersecurity startups based in each of the Big3 clusters. A total of 18 companies in our database made more than one acquisition. This table highlights the five most active buyers of cybersecurity firms in each cluster. Note the top five companies are exactly the same in both the SFBA and Israel clusters; and that, conversely, there is no overlap whatsoever with those making acquisitions in Washington. For both American clusters, four of the top five buyers are located within the given cluster. In Israel, on the other hand, four of the five top buyers are based in SFBA.

Acquiring company	# Firms Acquired in **Bay Area**
⬜ Palo Alto Networks	4
⬜ Symantec	3
⬜ Thoma Bravo	3
🟥 Check Point	2
⬜ Cisco	2

Acquiring company	# Firms Acquired in **Washington D.C.**
⬜ Converged Security Solutions	2
🟥 FireEye	2
⬜ KEYW Corp	2
⬜ Akima	1
⬜ Altamira	1

Acquiring company	# Firms Acquired in **Israel**
🟥 Palo Alto Networks	8
🟥 Symantec	6
⬜ Check Point	5
🟥 Thoma Bravo	4
🟥 Cisco	3

🟥 Acquiring company located in different cluster

⬜ Acquiring company located in cluster

Table 2.3 Top 5 acquiring firms in each of the Big3. Cumulative for all years. (2018).[70]

2.5 Summary: patterns of industry development

The important findings concerning two of the key questions posed above, historical growth and policy, are summarized here.

Beginning with historical growth. Cybersecurity has existed as a distinct industry for only about 20 years. But even before the industry became recognizable, while still in its very early years, it spawned the Big3 clusters, each with a somewhat unique origin. However, all three cybersecurity clusters emerged as *specialized clusters* embedded within a larger ecosystem. That is, inside the hegemonic innovation cluster of SFBA, inside the defense and high-tech network of Washington, and inside the "start-up nation" ecosystem in Israel.

The rapid growth period of the industry beginning around 2012 was triggered by a combination of two factors: major network breaches and increased venture capital funding. Notable is the particularly dramatic growth of the SFBA and Israel clusters during era 3. The Israeli cluster grew by fewer than 50 firms between 2000 and 2010, and by over 300 in the decade thereafter. However, the three clusters did not all grow evenly. In the early 2000s, era 2, the Washington cluster grew quickly as a result of government demand for cybersecurity products and services and subsequently plateaued while the other two clusters grew substantially.

The second question dealt with how to understand cybersecurity in order to make better policy. In this study, the focus is on what those in business known as Pure-play firms, whose primary business activity, and source of revenue, are cyber-related products or services. The cybersecurity industry has a typical high-tech mix of innovative pure-play firms plus non-pure-play firms that offer cybersecurity products and services as part of a broader list of offerings. Firm behavior changes rapidly as new external threats continue to emerge, metastasize

[70] Note: 2019 is a partial year. Source: Business in the Capital cybersecurity dataset, American University.

and evolve. Thus, firm categorization is fluid, as their focus changes rapidly to meet changing market demands, and with it, their categorization. Further, many firms are in multiple categories at any given time. All the Big3 clusters contain a diverse, extensive set of firms which engage in a broad spectrum of cybersecurity businesses. There is some regional specialization, such as IoT in Israel, or consulting and multi-sector firms in Washington. However, these examples are somewhat of an exception: the Big3 are all encompassing.

The median size of firms based in each of the Big3 is roughly the same, whether based on employment or revenue. Firm workforce size ranged from a median of 25 to 31 employees, while median revenue ranged from US$3.5 to 5 million per company. However, other dimensions highlight the dominance of the SFBA cluster over the others. First, SFBA cybersecurity companies employ approximately 92,000 people, more than double the other two clusters, which have roughly 20,000 employees each, combined. Second, the overall valuation of SFBA companies is much larger than the other two clusters, 87% of the combined value is in SFBA. Third, SFBA companies raised US$13 billion in cumulative venture capital funding, again more than the other two clusters combined.

Of interest when making policy decisions is the story of industry consolidation. The cybersecurity industry in general — the Big3 clusters specifically — is consolidating at a rapid pace but still remains quite fragmented, relegating it to Stage 2 (of 4) of the consolidation curve. Worldwide, 393 firms altogether have been acquired by larger and more established Big3 cybersecurity firms. A total of 186 cybersecurity firms within the Big3 were the target of acquisitions from 2003 through 2019.

Chapter 3

THE CYBERSECURITY INDUSTRY AS AN ECOSYSTEM

Chapter 3

THE CYBERSECURITY INDUSTRY AS AN ECOSYSTEM

Tali Hatuka and Corbin Seligman

“Industrial Ecosystem” is a key concept often used to describe innovative clusters. The concept posits that production and innovation in a particular place form a multifaceted network that encourages mutually beneficial relationships and exchanges between and among participating entities. The industrial ecosystem is nurtured by the region’s economy and organizations, which are viewed as a complex, interconnected structure. This economic and policy perspective tends to prioritize organizational structure over the spatial, cultural and social features that create a particular incubator, which contributes to the development of the economic/industrial ecosystem. This claim does not imply that each dimension in the environment influences the ecosystem directly, but rather that complex relationships between the social, spatial, cultural, and political play a major role in forming the ecosystem in the first place. This dynamic that contributes to the formation of the ecosystem has been given different names, such as “buzz,” “flavor,” “feel,” “atmosphere,” and “character,” all referring to the multilayered relations between people, practices and built forms associated with innovative clusters.

Yet, over the last decade there is a growing recognition of the role of spatial context and urban morphology, and that “creative clusters are not randomly distributed, they are entwined with the morphologies of particular places; such clusters cannot be reduced to economics any more than they can be reduced to morphology.”[71] Viewing context as a major actor in the evolution of innovation clusters is the point of departure for this chapter, which focuses on the role of the environment in the development of the Big3 cybersecurity clusters. Following these ideas, the aims of this chapter are twofold: 1. **Placing the Big3 cybersecurity clusters in spatial, social and institutional context**; 2. **Mapping clusters’ intensities**, shifting from a monolithic view to an aggregate, more tuned spatial view of the clusters.

The chapter includes three sections. The first addresses theoretical concepts and defining attributes of clusters. The second section provides analysis of the three case studies: the San Francisco Bay Area (SFBA), Washington D.C. metropolitan region (DC), and the Israel (IL); and presents their distinguishing characteristics with a focus on infrastructure, social capital and institutions. The third section provides a more direct comparison of the similarities

[71] Stephen Wood and Kim Dovey, “Creative Multiplicities: Urban Morphologies of Creative Clustering,” *Journal of Urban Design* 20, no. 1 (January 1, 2015): 52–74, p. 52 https://doi.org/10.1080/13574809.2014.972346.

and differences between these clusters, and concludes with a discussion of their evolution and an examination of the cluster type they represent (i.e. organic, top-down, or hybrid).

3.1 Clusters: definitions and development

Generally, the term "cluster" refers to a group of similar things or people positioned or occurring closely together.[72] Yet, the analysis of clusters has varied from one discipline to the other.

From the economic perspective, a cluster is a "concentrated density of firms within a geographic region"[73] that is categorized or characterized by a particular product or service,[74] and often develops hierarchical relationships with other clusters that can span worldwide. In many clusters, the model of participation is based on the **triple helix**, theorized by Henry Etzkowitz and Loet Leydesdorff in the 1990s,[75] to describe the interactions between universities, industries and governments. The triple helix is considered a means to enhance **social networks** within the cluster that encourage: (1) cross-sector relationships between academia, industry and government; (2) cross-scale relationships between new entrepreneurs and larger, established firms, as well as all firm sizes in between; and (3) up- and down-stream relationships between suppliers and producers.[76] These three features – density of firms, the triple helix model, and the social networks within in the cluster – generate numerous competitive advantages. They allow firms within the cluster to become highly-specialized and increasingly efficient and effective, each firm honing in on a specific segment of production (i.e. one point on the supply chain).[77] Thus, companies within a given cluster are often dependent on the greater network – and on many firms and organizations within it – to fulfill other specialized segments of production. As Allen Scott writes, regional economic clusters can be "caught up in structures of interdependency stretching across the entire globe."[78] When competing on a global stage, non-codified or tacit knowledge becomes increasingly valuable, because it is difficult to (re)produce and impossible to imitate.[79] Thus, one of the core elements of clusters is **interdependency**, which relies on and strengthens network innovation and, in turn, enhances growth through collaboration.

Economic development strategies are often comprised of policies or initiatives that aim to enhance these and other productive efficiencies in order to stimulate regional economic growth. The primary goal of these policies is to identify and further develop economic clusters in select metropolitan areas.[80] Wolman and Hincapie list several

[72] A. Malmberg, "Agglomeration," in *International Encyclopedia of Human Geography*, ed. Rob Kitchin and Nigel Thrift (Oxford: Elsevier, 2009), 48–53, https://doi.org/10.1016/B978-008044910-4.00131-0.

[73] Sam Donaldson, Christian Stow, and Jonathan Hobson, "UK Cybersecurity Sectoral Analysis and Deep-Dive Review" (Department for Digital, Culture, Media and Sport, June 2018), p. 56 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751406/UK_Cyber_Sector_Report_-__June_2018.pdf.

[74] Julie Brown and Micha Mczyski, "Complexcities: Locational Choices of Creative Knowledge Workers," *Built Environment* 35, no. 2 (June 24, 2009): 238–52, https://doi.org/10.2148/benv.35.2.238; Thomas A Hutton, "Spatiality, Built Form, and Creative Industry Development in the Inner City," *Environment and Planning A: Economy and Space* 38, no. 10 (October 1, 2006): 1819–41, https://doi.org/10.1068/a37285; Norma M Rantisi, Deborah Leslie, and Susan Christopherson, "Placing the Creative Economy: Scale, Politics, and the Material," *Environment and Planning A: Economy and Space* 38, no. 10 (October 1, 2006): 1789–97, https://doi.org/10.1068/a39210.

[75] Henry Etzkowitz, "Triple Helix Clusters: Boundary Permeability at University—Industry—Government Interfaces as a Regional Innovation Strategy:," *Environment and Planning C: Government and Policy*, January 1, 2012, https://doi.org/10.1068/c1182.

[76] Tali Hatuka, "Facing Forward: Trends and Challenges in the Development of Industry in Cities," *Built Environment* 43 (March 6, 2017): 145–55, https://doi.org/10.2148/benv.63.3.145.\\uc0\\u8221{} {\\i{}Built Environment} 43 (March 6, 2017

[77] Brown and Mczyski, "Complexcities."; Hutton, "Spatiality, Built Form, and Creative Industry Development in the Inner City."; M Rantisi, Leslie, and Christopherson, "Placing the Creative Economy."

[78] Allen J. Scott, *The Cultural Economy of Cities: Essays on the Geography of Image-Producing Industries* (SAGE, 2000) p. 29.

[79] Filippo Celata and Raffaella Coletti, "Place-Based Strategies or Territorial Cooperation? Regional Development in Transnational Perspective in Italy," *Local Economy* 29, no. 4–5 (June 1, 2014): 394–411, https://doi.org/10.1177/0269094214533903

[80] Alex Burfitt and Stewart Macneill, "The Challenges of Pursuing Cluster Policy in the Congested State," *International Journal of Urban and Regional Research* 32, no. 2 (2008): 492–505, https://doi.org/10.1111/j.1468-2427.2008.00784.x.

policies and tools that governments should use in support of these strategies. These include supporting "expansion through recruiting companies that fill gaps in cluster development," organizing "supply chain associations," and representing "cluster interests before external organizations such as regional development partnerships, national trade associations, and local, state, and federal governments."[81]

From urban geography perspective, a cluster is "a socio-spatial assemblage of people, buildings and activities without any necessary center, boundary or scale."[82] Additionally, the production processes of some service-sector firms depend on infrastructure in a fixed, physical location. As such, **proximity** increases the productivity of companies within a given network by driving innovation and stimulating new business. Physical proximity fosters personal relationships, creating a social environment in which it is "*safer to take risk*" due to the "*socialization of sharing*."[83] Proximity is also associated with **density**, which has the effect of making face-to-face meetings easier, as well as increasing the frequency of ad hoc, informal and often chance encounters in public space.[84] Moreover, firms derive an advantage from being proximate to a diverse range of complementary industries.[85] **Diversity** is considered an important, if not critical, component of the system.[86] Firms in a given network typically benefit from efficiencies created by **shared infrastructure**, including transportation infrastructure; business networks; research facilities; academic institutions and training facilities; a critical mass of clientele; and complimentary industries and services. The underlying premise of this approach is proximity to firms in the same or related industries improves firms' access to specialized workers, suppliers, and customers, and also to the institutions that support their work, such as universities and research centers. **Skilled labor** becomes more specialized as a cluster develops. Training an equivalent workforce in a different location becomes increasingly difficult and costly, reinforcing the cluster's gravitational pull and industry dominance. Similarly, the cost of other specialized inputs is often greatly reduced relative to locations outside the cluster. As such, **social capital** is an especially important aspect of clusters. A sufficient supply of skilled labor and intellectual capital are among the most critical features of successful clusters.[87]

Paths and trajectories for cluster development can vary greatly. A cluster can grow organically or develop through intentional, often top-down actions taken by local governments. Either way policies play a major role in their development. Focusing on the national level, Aggarwal and Reddie[88] examined the role of government in cybersecurity. The authors identified several market failures that require government attention and action, beginning with concerns about **imperfect markets**. In Japan, for example, the cybersecurity industry has grown slowly due to dependence on large firms with strong ties to government ministries, as well as the practice of top-down policymaking. In the United States, on the other hand, there is a plethora of companies of all sizes. In Israel, the government created overall umbrella organizations such as the Israel National Cyber Directorate, which merged and incorporated several other units, including the Cyber Emergency Response Team, with an annual budget of

[81] Harold (Hal) Wolman and Diana Hincapie, "Clusters and Cluster-Based Development Policy," *Economic Development Quarterly* 29, no. 2 (May 1, 2015): 135–49, p. 141, https://doi.org/10.1177/0891242413517136.

[82] Wood and Dovey, " Creative Multiplicities," p. 54

[83] Wood and Dovey, " Creative Multiplicities."

[84] Michael L. Katz and Carl Shapiro, "Network Externalities, Competition, and Compatibility," *American Economic Review* 75, no. 3 (June 1985): 424.

[85] Howard Wial Krueger Susan Helper, and Timothy, "Locating American Manufacturing: Trends in the Geography of Production," *Brookings* (blog), November 30, 1AD, https://www.brookings.edu/research/locating-american-manufacturing-trends-in-the-geography-of-production/.

[86] Teis Hansen and Lars Winther, "Innovation, Regional Development and Relations between High- and Low-Tech Industries," *European Urban and Regional Studies* 18, no. 3 (July 1, 2011): 321–39, https://doi.org/10.1177/0969776411403990.the inferior growth of the European Union (EU)

[87] Natasha Cohen et al., "Cybersecurity as an Engine for Growth" (New America, September 2017), newamerica.org.

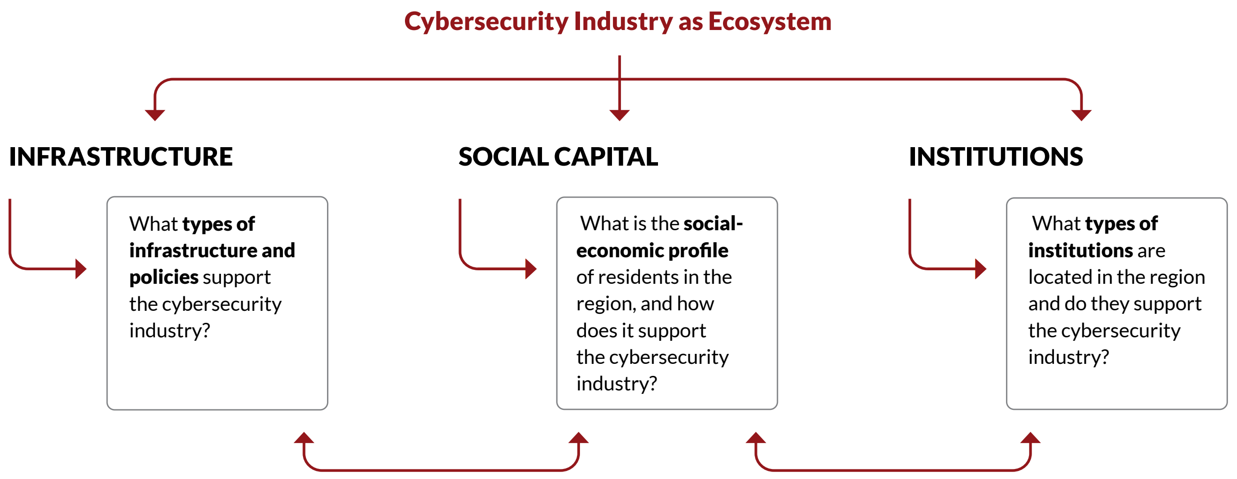
[88] Vinod Aggarwal and Andrew Reddie, "Comparative industrial policy and cybersecurity: a framework for analysis" Journal of Cyber Policy. vol. 3, no. 3 (2018): 291–305; 445–46.

roughly US$60 million.[89] The second market failure is factor adjustment, especially **labor shortages**. In the U.S., human capital-related programs subsidize cybersecurity education through the Federal Cybersecurity Workforce Strategy, National Initiative for Cyberspace Education, CyberCorps, and Cybersecurity Education and Training Assistance Programs (CETAP). These initiatives are insufficient; we noted above that there is a persistent labor shortage. There are half a million unfilled cybersecurity positions in the U.S. – equivalent to half of the existing workforce. The third market failure deals with **agglomeration effects**. Here, governments' stated desires and proactive actions help create clusters. The fourth market failure is the set of **national security prerogatives**, when governments create policies designed to enhance "industrial independence." In many countries, national security priorities have led to efforts to discriminate against foreign IT products. The U.S., for instance, has instituted several export controls on cybersecurity services and products. In all countries there are strong influences between private cybersecurity firms and national security agencies, often via cybersecurity experts with a professional background in national security. Aggarwal and Reddie summarize their outlook of governments' role in the cybersecurity sector: "As countries pursue industrial policy in cybersecurity, conflict is nearly inevitable among firms and governments over access to markets."[90] They project that cybersecurity markets will likely become even more localized and protected.

Yet policies of the national government must be viewed in the context of local policies. No matter how clusters develop, they are located in a concrete place and environment that is characterized by co-location benefits and efficiencies that include among others: local culture, informal knowledge spillover and information sharing, supportive and shared infrastructure, institutions, establishment of the place as a "brand," and attraction to the area of additional resources such as people, capital and other firms. Yet, the key question is not why the cluster evolved in a particular location, but how the environment served as an incubator for the cybersecurity ecosystem. More specifically, what **types of infrastructure and policies** support the cybersecurity industry? What is the **social-economic profile** of residents in the region, and how does it support the cybersecurity industry? What **types of institutions** are located in the region and do they support the cybersecurity industry?

[89] The budget is for the year 2017. Ziv. A, 2018. "What Went Wrong With Israel's Cybersecurity Agency," *Jerusalem Post*, Aug 29, 2018.

[90] Aggarwal and Reddie, "Comparative industrial policy," p. 302.



Cybersecurity Industry as Ecosystem

INFRASTRUCTURE

What **types of infrastructure and policies** support the cybersecurity industry?

SOCIAL CAPITAL

What is the **social-economic profile** of residents in the region, and how does it support the cybersecurity industry?

INSTITUTIONS

What **types of institutions** are located in the region and do they support the cybersecurity industry?

Figure 3.1 Conceptual analytical framework

Focusing on the urban dimensions of clusters, the next section places the Big3 cybersecurity clusters in spatial, social and institutional context, and maps the intensity of the clusters. These assessments will be used to further reflect on the particular attributes of the cybersecurity clusters.

3.2 Cybersecurity ecosystems: San Francisco bay area, Washington D.C., and Israel

This section addresses these questions by juxtaposing three key factors: infrastructure, social capital and institutions with firms spatial spread in the Big3 cybersecurity clusters.

a. San Francisco Bay Area: A Hybrid Cluster

A case of private sector entrepreneurialism and public support strategy

The San Francisco Bay Area (SFBA) cybersecurity cluster spans from the City of San Francisco in the north to San Jose in the south, through San Mateo and Santa Clara counties. SFBA cyber firms are not distributed evenly throughout the region. There are two distinct “hot zones” within this mega-cluster. The first stretches from Palo Alto, southward to San Jose, at the south end of San Francisco Bay, covering an area about 110 sq. km (42.5 sq. miles). Better known as Silicon Valley, this hot zone contains 127 cyber firms that employs over 60,000 people in the region and globally. The second hot zone is a highly concentrated area in downtown San Francisco, covering approximately 5 sq. km (1.9 sq. miles) that are home to 62 cyber firms. Map 3.1 depicts clustering of cybersecurity firms in SFBA segmented by size, as measured by number of employees; the hot zones are visible in magnifications A and B. All firms with more than 1,000 employees and a significant majority of those with more than 100 employees are located in Silicon Valley, rather than in the City of San Francisco. As noted in Chapter 2, many of the largest firms are clustered at the southern end of the valley, near Mountain View, Cupertino and the San Jose airport. As in Washington, firm size seems to be inversely correlated with proximity to the city center; the larger the firm, the more likely it is to be outside the dense city core.

Viewing the cybersecurity industry in wider set of variables, including infrastructure, social capital and institutions, the following points emerged.

Infrastructure and policy. The SFBA is a contiguous, highly-developed urban region concentrated around San Francisco Bay in northern California, on the west coast of the United States. It has an exceptionally diverse population of over 7 million, with nearly 50% of inhabitants being of Asian, African, Hispanic or Pacific Islander descent. The City of San Francisco is the center of the second largest urban agglomeration in California and fifth largest in the United States.[91] SFBA consists of several municipalities, including the City of San Francisco, Mountain View, Oakland and San Jose. It is connected by a complex system of roads and highways, rail corridors, the BART (Bay Area Rapid Transit) network, CalTrain, several ferry lines, and three international airports. Map 3.2 presents major transportation infrastructure (i.e. highways and primary roads; rail corridors; and airports), and cybersecurity firm locations. Map 3.2A shows the hot zone in downtown San Francisco. The cybersecurity cluster generally follows the transportation corridor of highways and railroads that follow the narrow stretch of terrain southward from San Francisco to San Jose, between the Bay's edge and the Santa Cruz mountain range.

Well before the emergence of cybersecurity, local and federal government policy supported cultivation and development of Silicon Valley as a tech hub. In 1980, for instance, "a shift in Federal government policy (the Bayh–Dole Act or Patent and Trademark Law Amendments Act) permitted universities to pursue ownership of their inventions."[92] This enhanced collaboration between entrepreneurs, investors and other private sector players in commercializing government research through universities. Stanford and UC Berkeley were particularly successful at capitalizing on this change in policy, strengthening the local tech industry through increased patent filing, capital and skilled labor. Yet, apart from generally supportive policy, government played a limited role in early cluster development. Scholars have noted that it is more beneficial for governments to support new business ventures directly than through policy, particularly firms with a competitive advantage in innovation.[93] As discussed in Chapter 2, support for the embryonic-phase in SFBA came in the form of government and military defense spending, allowing for the establishment and success of local anchor firms, such as Fairchild Semiconductor.

Once the high-tech cluster was established in the Silicon Valley area, the City of San Francisco became "an important site for considering the various tactics of venture-backed firms in influencing public policy in a variety of areas."[94] Local tech firms influence and are influenced by municipal politics and planning policy. For example, former San Francisco Mayor Ed Lee's pro-technology stance was linked to campaign donations from tech firms and entrepreneurs. His administration made a concerted effort to attract technology firms into the city through policies such as creating a tax haven in neighborhoods with chronic under-investment. In order to take advantage of the tax incentive, firms are required to "give back" through "Community Benefit Agreements (CBA)" with the city, which "commit them to make practical contributions to the local area." TechSF is another example of a supportive local initiative, set up by city hall to retrain workers to fill lower paid jobs in the tech industry.[95] Thus, the pro-technology municipal administration in San Francisco became a critical element recent growth of the tech industry. And the growth has been strong: By 2015, 40% of high-tech unicorns worldwide were located in the City of San Francisco, compared to 23% in the Valley.[96]

[91] "Bay Area Census -- Bay Area Data," accessed April 30, 2020, http://www.bayareacensus.ca.gov/bayarea.htm.

[92] Jerome S. Engel, "Global Clusters of Innovation: Lessons from Silicon Valley," *California Management Review* 57, no. 2 (February 1, 2015): 36–65, p. 40, https://doi.org/10.1525/cmr.2015.57.2.36.

[93] Casper, "New Technology Clusters."

[94] Donald McNeill, "Governing a City of Unicorns: Technology Capital and the Urban Politics of San Francisco," *Urban Geography* 37, no. 4 (May 18, 2016): 494–513, p. 508, https://doi.org/10.1080/02723638.2016.1139868.

[95] McNeill, "Governing a City of Unicorns."

[96] McNeill, "Governing a City of Unicorns."

All these dynamics in the larger high-tech setting are mirrored in the cybersecurity industry, illustrated in Map 2.2 in Chapter 2. The map shows exponential growth in the cyber industry in downtown San Francisco over the last decade.

Social capital. Flexibility and adaptation are integrated into the sociocultural and structural dynamics of the tech sector and its associated industries in SFBA. Cross- and inter-sector collaboration and innovation, as AnnaLee Saxenian highlights, allows Silicon Valley firms to flourish while those on Route 128 near Boston declined.[97] Highly experienced individuals and firms regularly mentor, work with, and invest in younger entrepreneurs and start-ups.[98] Collaboration follows the triple helix model, and there is overlap not only in the private sector, but between and among private firms, government, and academic institutions as well, each frequently playing the traditional role of the other. In SFBA, large multinational firms and startups, as well as government and academic institutions are themselves actors in the social structure. While Silicon Valley cannot be characterized as the typical spatially-proximate, urban, or "close-knit civil society" described in much literature on agglomeration, it *is* the product of institutionalized, intentional, and socially acceptable actions taken by individuals, private companies, government and academic institutions to achieve the common objectives of "innovation and its commercialization."[99]

The City of San Francisco is a dense urban environment, a critical ingredient for startups in their infancy. Online networks and media are important at later stages, but when firms initially launch "spatial social networks are crucial to reproducing the dynamics of adoption at a city scale."[100] Investors have "increasingly focused their attention on the rapid growth in potential investment returns offered by youth-oriented social media 'early adopters,' which in turn is reflected by the locational choice of San Francisco over the suburban Valley" [101] and in software, the designers have become "more urbanized by disposition." The city is an important place for tech companies to grow during early phases before proliferating.[102] Tech firms, particularly those in social media, choose to locate in San Francisco due to its high ratio of early adopters.[103] Local social dynamics and demographics thus factor into locational decisions of technology firms, especially new ventures. The large tech population not only supports startups as early adopters of products, but also serves as a large pool of highly skilled and highly mobile labor, an essential input for tech firms at every stage and scale.

Spatial distribution of education and income relative to that of cybersecurity firms is visualized on Map 3.3, which displays distribution of SFBA population with at least a Bachelor's degree, and Map 3.4, which shows distribution of median household income; both include locations of cyber firms. Silicon Valley is a sprawl of mostly suburban single-family homes with office parks distributed in various locations. The downtown San Francisco hot zone sits between traditionally poor neighborhoods and those that are highly gentrified. There are some suburban, low-density areas proximate to the Silicon Valley cluster with median incomes higher than US$ 200,000.

The maps show similar patterns of segregation. The two cyber hot zones (downtown San Francisco and Silicon Valley) straddle between highly educated, high income areas and low academic achievement, less affluent areas.

[97] AnnaLee Saxenian, Regional Advantage (Harvard University Press, 1996).

[98] Peter Cohan, "How Cambridge and Silicon Valley Became Startup Hubs," *Forbes*, July 18, 2017, https://www.forbes.com/sites/petercohan/2017/07/18/how-cambridge-and-silicon-valley-became-startup-hubs/#2b6525fa37a7.

[99] Stephen S. Cohen and Gary Fields, "Social Capital and Capital Gains in Silicon Valley," *California Management Review* 41, no. 2 (January 1, 1999): 108–30, https://doi.org/10.2307/41165989.

[100] Jameson L. Toole, Meeyoung Cha, and Marta C. González, "Modeling the Adoption of Innovations in the Presence of Geographic and Media Influences," *PLOS ONE* 7, no. 1 (January 19, 2012): e29528, p. 8 https://doi.org/10.1371/journal.pone.0029528.

[101] McNeill, "Governing a City of Unicorns." p. 498.

[102] Toole, Cha, and González, "Modeling the Adoption of Innovations in the Presence of Geographic and Media Influences."

[103] McNeill, "Governing a City of Unicorns."

Institutions. Institutions played a major role in the ongoing development of the SFBA high-tech cluster.[104] The federal government finances government laboratories in the region, such as Lawrence Berkeley, Lawrence Livermore National Laboratory and the Stanford Linear Accelerator; in addition to direct investment in many private firms.[105] Substantial, long-term federal financial support into SFBA through aerospace, military and defense "can be considered as a crucial catalyst for the subsequent emergence of this techno-centric innovation cluster."[106] Government is "an essential catalyst" for stimulating growth through direct investment, as a major consumer, and through funding research and development. In Silicon Valley and other economic clusters around the world, the evidence of government intervention playing a central role is unmistakeable.[107]

Leading post-secondary research institutions were established in SFBA, and have taken proactive roles in cultivating the local high-tech sector.[108] UC Berkeley and Stanford University both integrated business, research, and education into their programs in the early 1900s, "with Stanford taking the lead in commercialization of telephone, electronics, and computer technologies."[109] The private sector has historically been a major source of post-secondary regional research funding. The Stanford Research Park, for example, was established in 1951 – a joint project with large corporations such as General Electric, IBM, Eastman Kodak, Lockheed, Varian, and Hewlett-Packard.[110] By 2011 Stanford alumni had "created 39,900 companies with $2.7 trillion in revenue, and 5.4 million jobs."[111] Universities, particularly research-intensive institutions, are "anchors of technology clusters."[112]

Map 3.5 shows the locations of major post-secondary institutions and transportation infrastructure. On the regional map, the location of universities corresponds somewhat to the cybersecurity hot zones, but not in the East Bay (Oakland and Berkeley). Proximity does not indicate influence or causality, but rather suggests that universities and cyber firms share advantageous environmental characteristics.

The high-tech industry advocates for its local interests through formal networks. Sf.citi, for example, was founded in 2012 as a non-profit business league representing San Francisco's tech firms. It is essentially a chamber of commerce meant "to encourage member firms to make pro-bono interventions in the city's urban infrastructures."[113]

[104] When William Hewlett and David Packard founded HP, for example, their MIT professor Frederick Terman secured them with Defense Department contracts. Cohan, "How Cambridge and Silicon Valley Became Startup Hubs." Other noteworthy early examples include Varian, Fairchild Semiconductors, and Lockheed Martin, which became the largest employer in the Valley during the Cold War and the "Space Race." Engel, "Global Clusters."

[105] Engel, "Global Clusters Global Clusters." For further reading see also Chapter 2, Cluster roots history.

[106] Engel, "Global Clusters of Innovation."

[107] Josh Lerner, *Boulevard of Broken Dreams: Why Public Efforts to Boost Entrepreneurship and Venture Capital Have Failed--and What to Do About It* (Princeton University Press, 2012).

[108] Stephen B. Adams, "From Orchards to Chips: Silicon Valley's Evolving Entrepreneurial Ecosystem," *Entrepreneurship & Regional Development* (March 9, 2020): 1–21, https://doi.org/10.1080/08985626.2020.1734259.

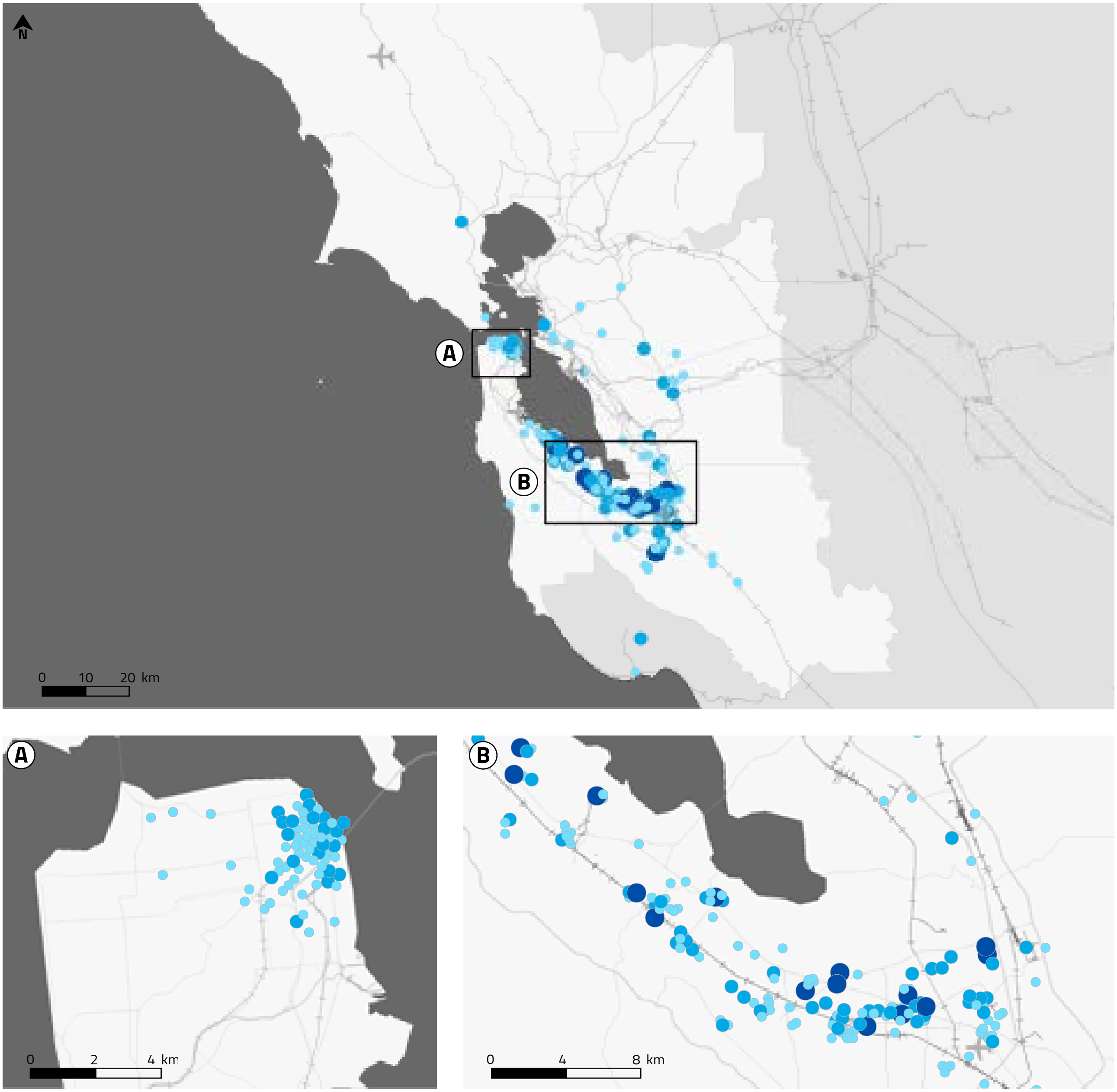
[109] Engel, "Global Clusters of Innovation," p. 39.

[110] The park is now home to over 150 firms with more than 23,000 employees. These firms specialize in electronics, software, biotechnology, and other high-tech fields. In addition to publicly funded research labs, "many major corporations also created R&D centers either because they were headquartered in the Valley (like Hewlett-Packard or Cisco) or because they wanted their researchers close to the center of innovation and commercialization (like IBM, Xerox, and Samsung)."

[111] Cohan, "How Cambridge and Silicon Valley Became Start-up Hubs."

[112] Casper, "New-Technology Clusters and Public Policy."

[113] McNeill, "Governing a City of Unicorns," p. 502.



Map 3.1 SFBA-headquartered pure-play cybersecurity firms by number of employees

Number of Employees

● 1-100

● 101-1,000

● 1,001+

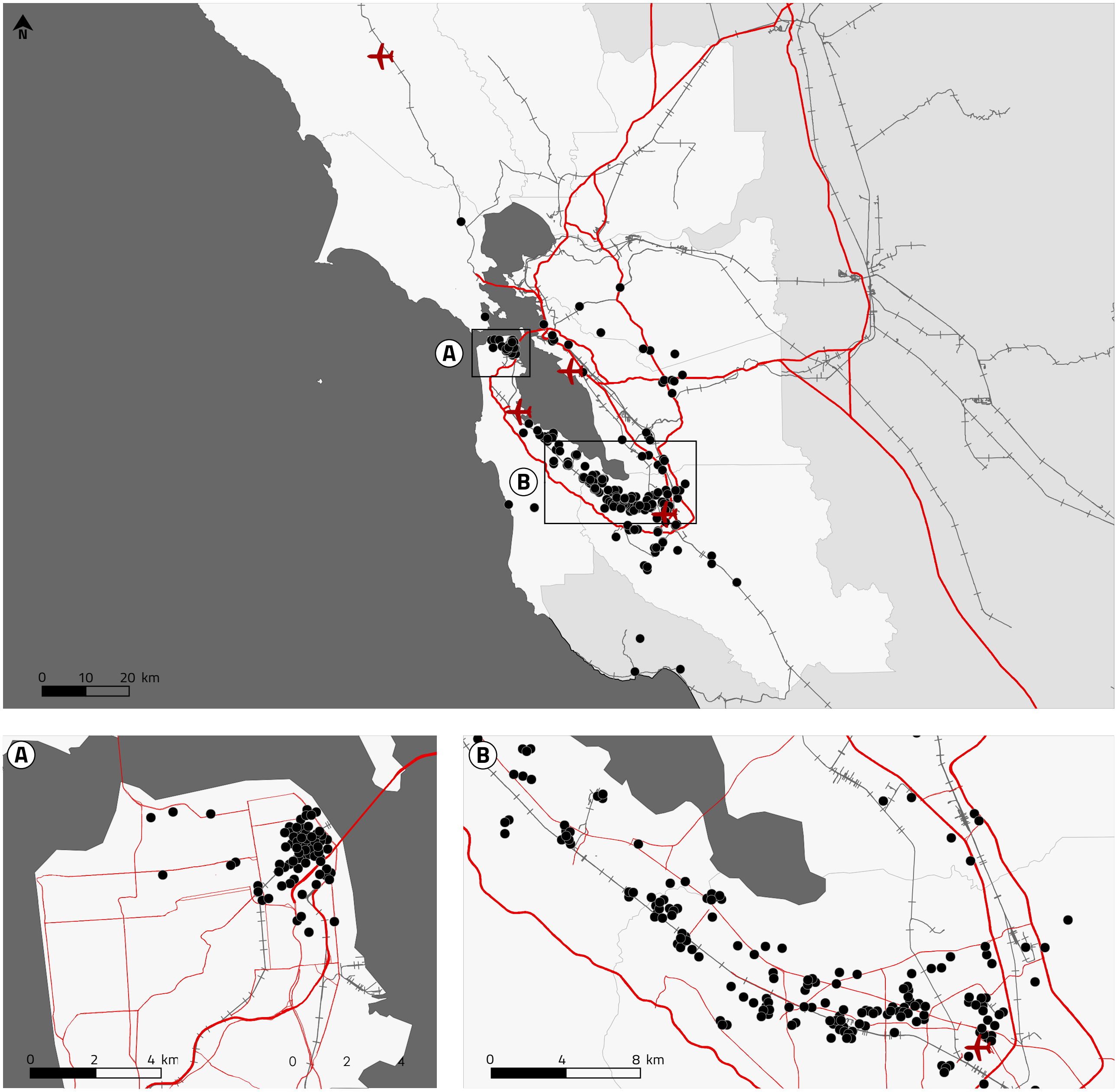
Highway / Primary Road

Railway

Major Airport

Country Limit

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



Map 3.2 SFBA-headquartered pure-play cybersecurity firms & transportation infrastructure

● Cybersecurity Company

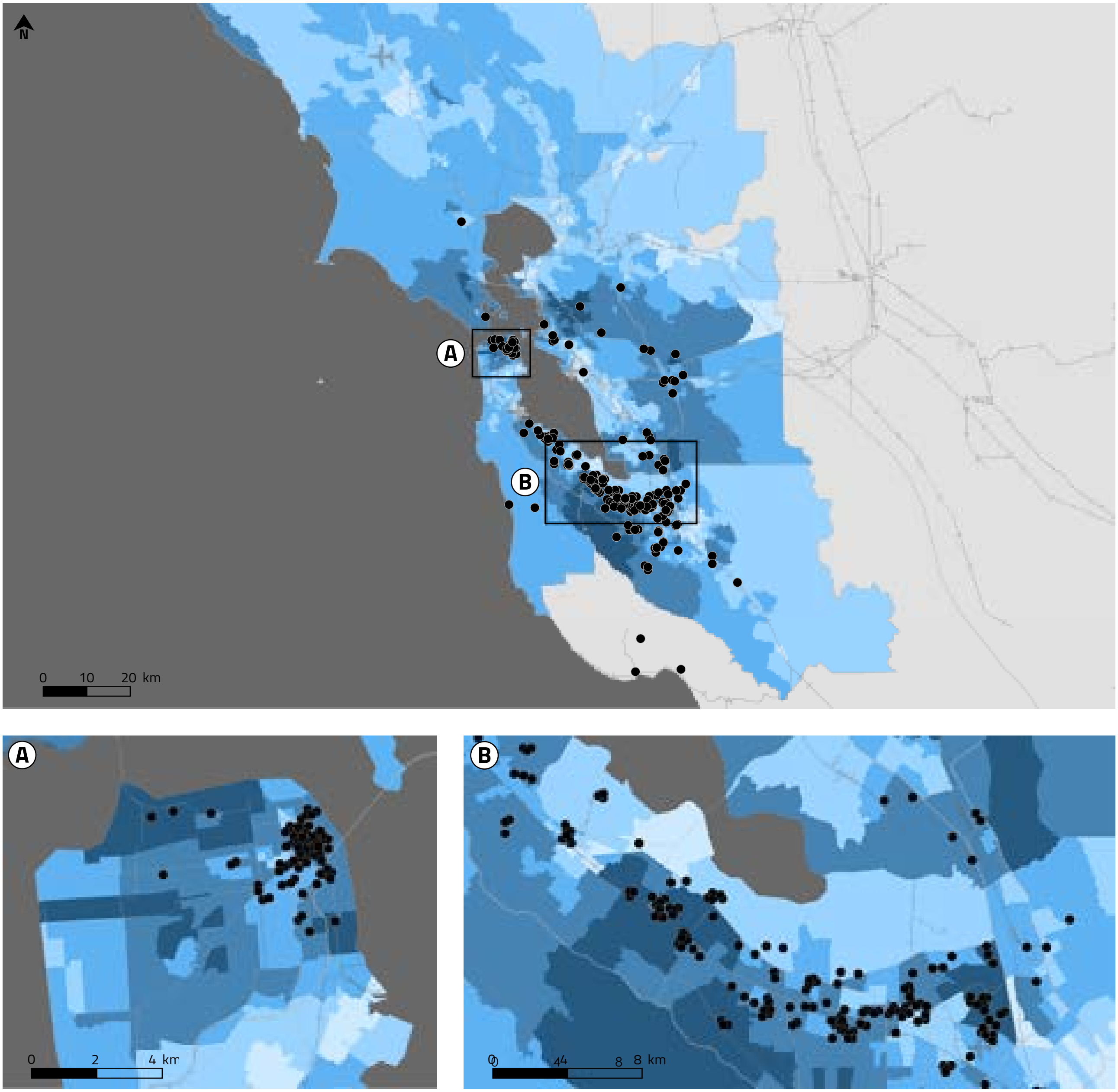
— Highway / Primary Road

┼─┼ Railway

✈ Major Airport

□ County Limit

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



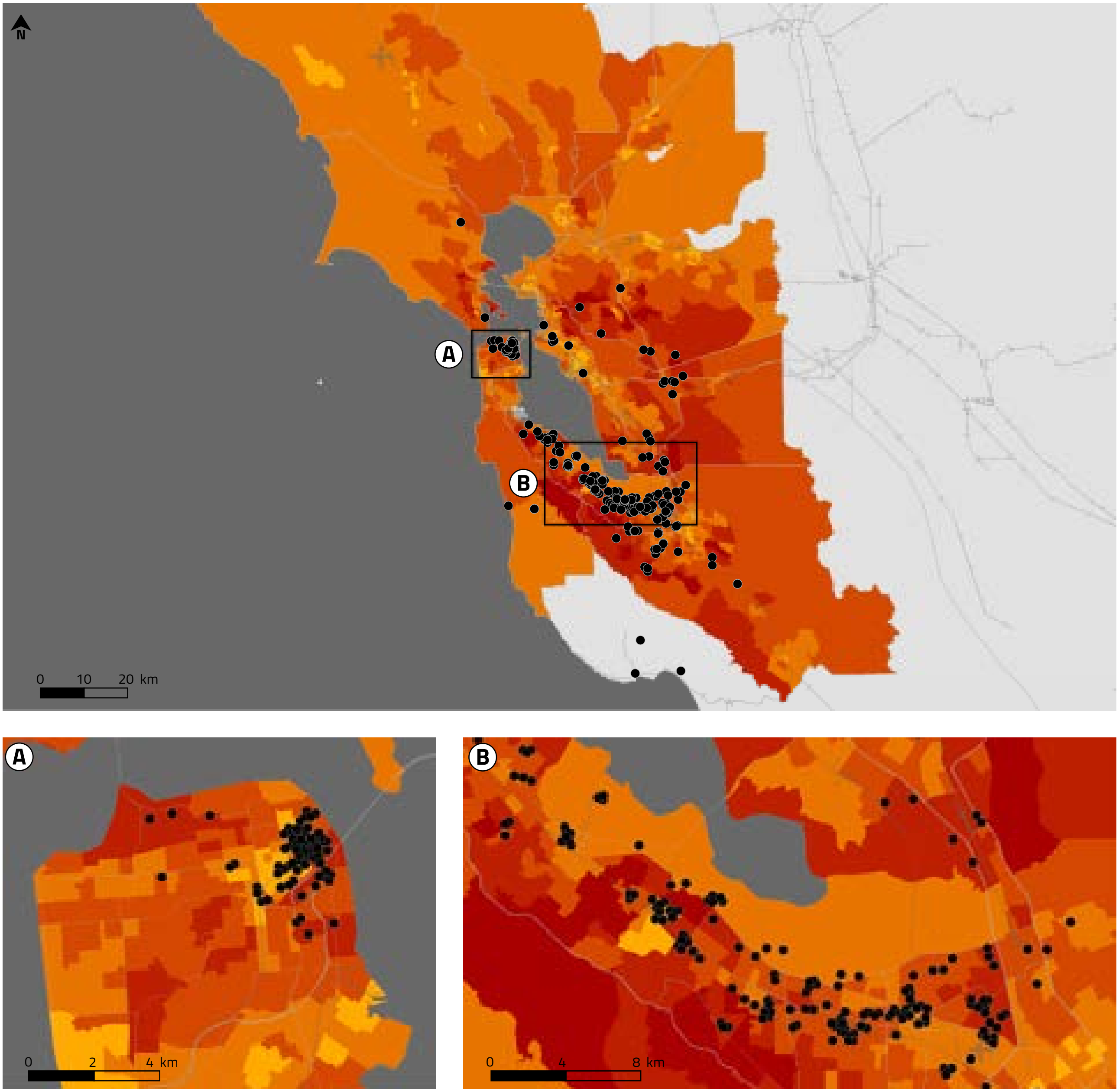
Map 3.3 SFBA-headquartered pure-play cybersecurity firms & academic achievement

Pop. with Bachelor's Degree or Higher

▢	0% - 20%
▢	21% - 40%
▢	41% - 60%
▢	61% - 80%
■	81% - 100%

●	Cybersecurity Company
—	Highway / Primary Road
┼	Railway
□	County Limit

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



Map 3.4 SFBA-headquartered pure-play cybersecurity firms & socioeconomic status

Household Median Income ($/year)

🟨 Below 50,000

🟧 50,001 - 100,000

🟧 100,001 - 150,000

🟥 150,001 - 200,000

🟥 Above 200,001

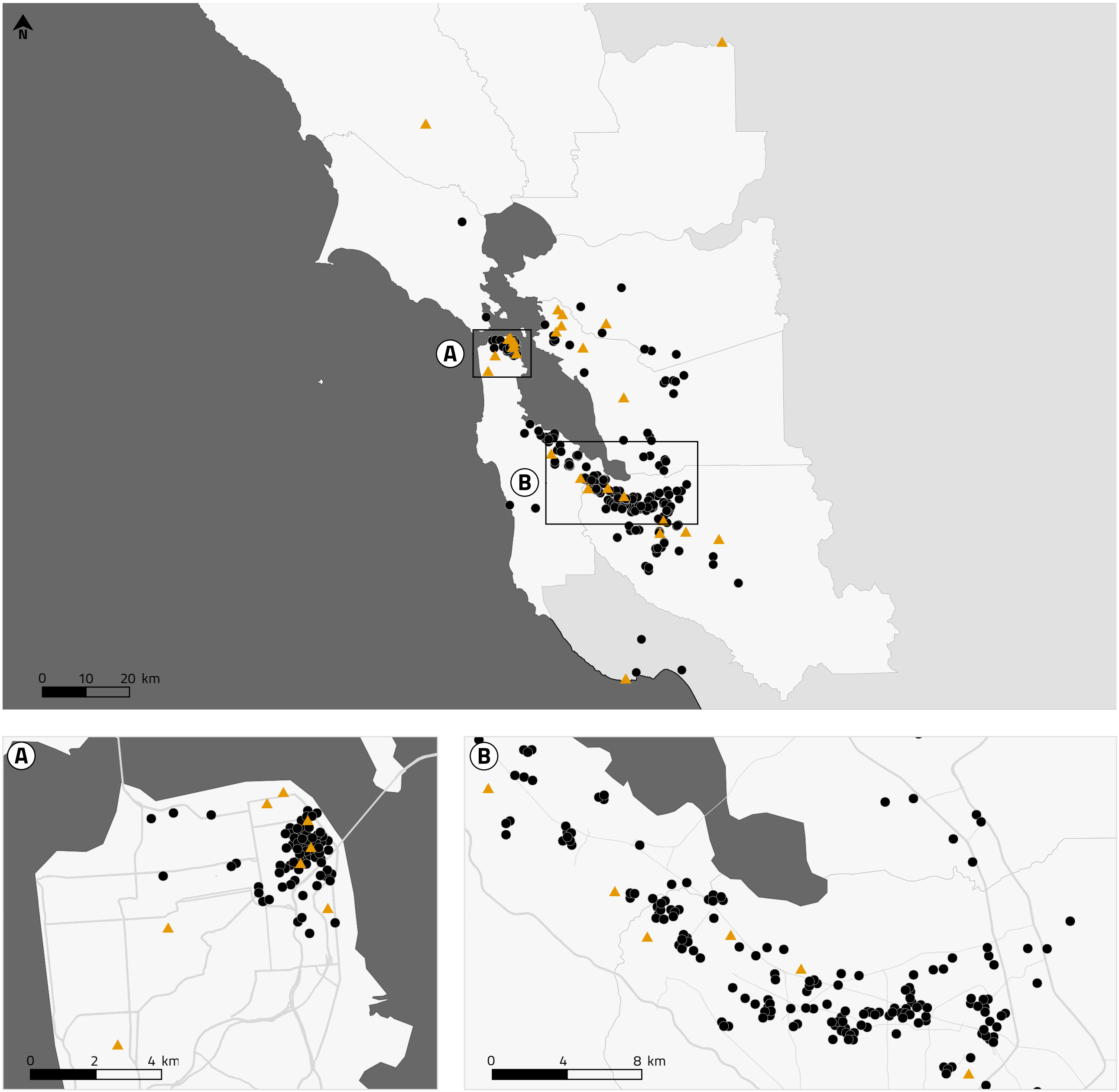
● Cybersecurity Company

— Highway / Primary Road

┼ Railway

□ County Limit

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



Map 3.5 SFBA-headquartered pure-play cybersecurity firms & post-secondary institutions

● Cybersecurity Company

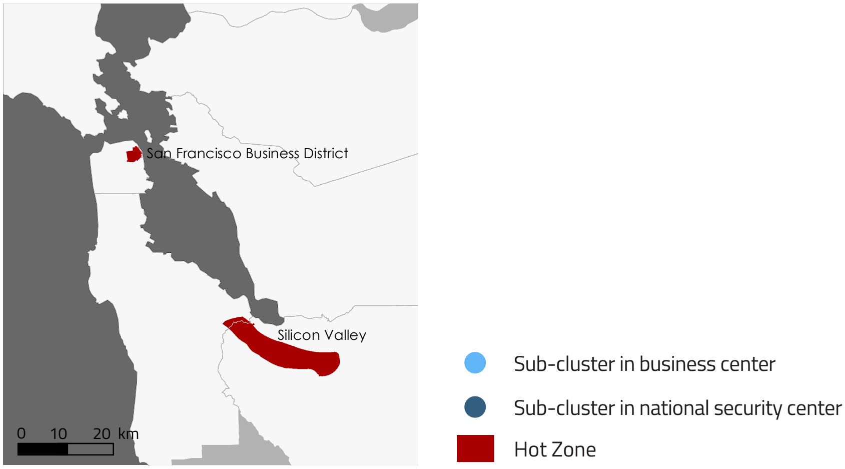
▲ Postsecondary Institutions

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)

Table 3.1 summarizes key features of the SFBA cluster. Academic culture, production diversity, and high connectivity all contribute to the stability and ongoing growth of the cluster. Collaboration between government, the private sector and several top-tier academic institutions has been – and continues to be – paramount to industry growth. Government and military presence and investment played a significant role in fostering initial establishment of major technology companies in SFBA. Thus, the SFBA cybersecurity cluster cannot be isolated from its context in the broader high-tech cluster, nor from its historic connections to military and government influence.

SAN FRANCISCO BAY AREA

The San Francisco Bay Area (SFBA) cybersecurity cluster spans from the City of San Francisco in the north to San Jose in the south, through San Mateo and Santa Clara counties. There are two distinct "hot zones" in this cluster: The first stretches from Palo Alto, California southward to San Jose at the south end of San Francisco Bay covering an areaof approximately 110 sq. km. The second hot zone is a highly concentrated area in Downtown San Francisco of approximately 5 sq. km.


San Francisco Business District
Silicon Valley
0 10 20 km
● Sub-cluster in business center
● Sub-cluster in national security center
🟥 Hot Zone

INFRASTRUCTURE

Key Cities & Transportation

- Bay area is home to over 7.5 million inhabitants and includes several large municipalities, namely San Francisco, San Jose and Oakland.
- Complex network of highways, railways, public transportation, shipping and three international airports.

Industries & Services

- San Francisco Bay Area is a banking and financial hub, as well as a center for food processing, manufacturing, culture and media.

SOCIAL CAPITAL

Socioeconomic

- Culture of risk-taking, collaboration and entrepreneurialism.
- Cross-sector collaboration.
- Top spot for VC funding in the USA.

INSTITUTIONS

Government & Military

- Government presence. Significant investment and support from government and military.
- Government contracts helped establish pillar firms and kick-start cluster development.

Research & Education

- Two top-tier academic institutions Stanford University and UC Berkeley supply skilled labor to tech industry.
- Collaborative, multi-sector research labs and institutions.

Table 3.1 Features of Bay Area cybersecurity ecosystem

b. Washington D.C. Region: a top-down cluster

A case of cluster formation as a direct result of major government and military presence

Washington D.C. and the surrounding metropolitan area (referred to as "Washington" in this section) represents the 5th largest regional economy in the United States.[114] This cybersecurity cluster stretches from Dulles International Airport in Virginia, through the District of Columbia to Maryland suburbs approaching Baltimore. The Washington-Arlington-Alexandria (DC-VA-MD-WV)[115] metropolitan statistical area (MSA) is home to approximately 7.2 million inhabitants (see Figure 1.2), over 50% of whom are of African, Asian or Hispanic descent.[116] As the capital, the region is home to a large number of government agencies including a large military and defense ecosystem. As with SFBA, cybersecurity firms in the Washington cluster are not distributed evenly. However, unlike SFBA there is no distinct hot zone in Washington, rather there are sub-clusters situated in neighborhoods throughout the region. The most notable sub-clusters are located in Reston, Tysons Corner, and Ballston running east-west along Interstate 66 and Route 267 which connects Washington D.C. with Dulles International Airport. Another sub-cluster, noted in Chapter 2, is in close proximity to the NSA offices. Map 3.6 shows cybersecurity firms in Washington, based on firm size, as measured by number of employees. Nearly all the cybersecurity firms are in the Maryland and Virginia suburbs, and not in Washington D.C. proper. Three of the largest firms, each with more than 1,000 employees, are located about 25 km outside the city, visible in magnification 3.6A (bottom left).

Viewing this cybersecurity industry growth in wider set of variables, including infrastructure, social capital and institutions, the following points emerged.

Infrastructure and policy. Map 3.7 illustrates major transportation infrastructure, specifically highways and primary roads, rail corridors, and airports. The most important cybersecurity company distribution runs east-west along Interstate 66 and Route 267 connecting Washington D.C. with Dulles International Airport. This concentration is evident in magnification 3.7A, along with important sub-clusters that tightly follow rail lines and highways in Reston, Tysons Corner, and Ballston. Figure 3.7B depicts the sub-cluster stimulated by NSA with approximately 25 firms. These firms are scattered in office parks throughout this suburban area. While rail connectivity is often an important factor for attracting high-tech and cyber firms, the east side of Washington D.C. hosts no cybersecurity firms, despite having many Metro mass-transit lines. Several interstate highways run through and around Washington as well as rail corridors, bus routes and the capital region mass-transit network. East coast rail lines connect Washington to key cities including Baltimore, Philadelphia, and New York. There are three major international airports in the region.

At the local policy level, metropolitan Washington, as one of the major U.S. high-tech clusters, has encouraged and facilitated high-tech business to locate and expand in the region. But the region is splintered politically between three jurisdictions (Washington D.C., which is not a state, Virginia, and Maryland), and within the latter two, it is also divided on the county and city levels. Each of these political entities usually operates independently to bring high-tech in general – and cybersecurity specifically – to their region. For example, the Economic Development units of the state of Maryland (until 2019) and Fairfax County, Virginia, have specific officers who specialize in cybersecurity enticement. Each also has attractive tax programs, such as the Cybersecurity Investment Incentive Tax Credit, Maryland, which provides a refundable income tax credit to those who invest in local cybersecurity firms.[117]

[114] "District of Columbia : Mid–Atlantic Information Office : U.S. Bureau of Labour Statistics," accessed May 3, 2020, https://www.bls.gov/regions/mid-atlantic/district_of_columbia.htm#tab-2.

[115] Our analysis does not precisely follow MSA boundaries

[116] "Census Profile: Washington-Arlington-Alexandria, DC-VA-MD-WV Metro Area," Census Reporter, accessed July 21, 2020, http://censusreporter.org/profiles/31000US47900-washington-arlington-alexandria-dc-va-md-wv-metro-area/.

[117] "Maryland Cyber Tax Credit | Maryland Department of Commerce," accessed July 21, 2020, https://commerce.maryland.gov/fund/programs-for-businesses/cyber-tax-credit.

Not all efforts are focused on enticement. Some of the local efforts are focused on tech/cyber workforce development, such as Virginia's the Cyber Veterans Initiative that gives those who have served in the military access to cyber training, apprenticeship, employment and financial support to accelerate their transition into the cyber workforce.[118] Some offer also "personalized business counseling"[119] to help small businesses succeed, such as the City of Washington D.C.'s Department of Small and Local Business Development. The city's Inclusive Innovation Fund aims to grow the city's opportunity sectors, including smart cities, data, and security technology by "enabling access to capital by under-represented entrepreneurs."[120]

Over the years, there have been some efforts to coordinate Washington regional policies related to taxation, economic and industry workforce (e.g., Greater Washington Partnership, Greater Washington Initiative [now defunct], and the Metropolitan Washington Council of Governments), but these efforts are minor relative to the powerful pull of local interests. The failure of the region to come together during the bidding for Amazon HQ2 in 2017, illustrates this.[121] Firms and NGOs are aware of the competition and compete for favorable tax and other incentives, such as the relocation of the U.S. National Science Foundation from Arlington to neighboring Alexandria.[122]

Social Capital. Washington D.C. was designed and built according to a grand capital city master plan created in the 1700s. The federal government has maintained a strong physical, political, cultural and economic presence ever since, often being directly involved with city planners, architects and engineers. The U.S. government directly administered the District for much of its history.[123] The presence of the American "command and control center" is not only reflected in Washington's urban morphology, but also manifests in "close interactions between government, administration, non-profits and the private sector," creating a "unique economic geography."[124] This triple helix cultural-economic dynamic (which also characterizes SFBA, as mentioned earlier) require geographic proximity, influencing firms' and organizations' location selection. Washington is a major defense-services center and general knowledge hub that has been able to diversify its economy "into industry sectors that are ancillary but less dependent on government contracting."[125] The unrivaled government presence and military spending in Washington provides not only capital and consistent business, but also trained professionals, with many new firms founded by people with substantial military or government security experience, and the firms' primary business operations often directly service government agencies. Nearly three out of four local cybersecurity firms were founded by individuals with prior experience in national security and "*a substantial majority of the region's cybersecurity business emerged without venture capital.*"[126]

Port Covington in Baltimore is a US$5.5 Billion example of local cyber industry-related physical infrastructure development. "Port Covington Set to Become a Global Cybersecurity Hub • Port Covington," *Port Covington* (blog), accessed July 21, 2020, https://pc.city/press_release/port-covington-set-to-become-a-global-cybersecurity-hub/.

For further reading about the initiative with a focus on the housing see, Gillian Rathbone-Webber, "Introduction to the Port Covington Development Project and Affordable Housing Symposium," *University of Baltimore Journal of Land and Development* 6, no. 2 (2017 2016): 153–54.

[118] "Cyber Veterans Initiative - Secretary of Technology," accessed July 21, 2020, https://www.cybervets.virginia.gov/.

[119] "DC Procurement Technical Assistance Center | Dslbd," accessed July 21, 2020, https://dslbd.dc.gov/service/dc-procurement-technical-assistance-center.

[120] "Inclusive Innovation Fund," DC Economic Strategy, 2020, https://dceconomicstrategy.com/initiatives/inclusive-innovation-fund/.

[121] Thompson, D. "Amazon's HQ2 Spectacle Isn't Just Shameful—It Should Be Illegal," *The Atlantic Monthly*, November 2018.

[122] David Kaufmann and Fritz Sager, "How to Organize Secondary Capital City Regions: Institutional Drivers of Locational Policy Coordination," *Governance* 32, no. 1 (2019): 63–81, https://doi.org/10.1111/gove.12346.

[123] Stephen J. McGovern, *The Politics of Downtown Development: Dynamic Political Cultures in San Francisco and Washington, D.C.* (University Press of Kentucky, 2014).

[124] Sven Conventz et al., *Hub Cities in the Knowledge Economy: Seaports, Airports, Brainports* (Routledge, 2016).

[125] Conventz et al. *Hub Cities*, p. 226

[126] Carmel, E. Byambasuren, B. and Aberman, J. *Cybersecurity Startup Founders in the Greater Washington Region: Prior Experience Required*. April 2018. Center for Business in the Capital, American University, p. 9.

Washington D.C. also has the highest ratio of female owned high-tech firms of any city in the country (18.57%) and also exhibits the highest growth rate of female-owned firms (9.27%). Women-owned firms are also the largest in Washington as measured by number of employees. [127] This may be due, in part, to government contracts providing opportunities for women and minorities. In-turn, this could attract additional women and minority entrepreneurs to the region.

Washington has a relatively highly educated and high-income population, with its mean in each category being approximately 50% higher than the national average.[128] Map 3.8 displays pure-play cybersecurity firms relative to population with at least a Bachelor's degree and Map 3.9 displays cyber firms relative to socioeconomic status. Cybersecurity companies are clustered along commercial arteries, but groupings of firms are found in the neighborhoods of Bethesda, Courtyard, Ballston, Tysons Corner, and Reston, all areas with highly educated, relatively wealthy populations.[129]

Institutions. The Washington cybersecurity market is rooted in robust government and military presence. Washington's biggest buyer of technology is the U.S. Federal government. The U.S. Federal cybersecurity market is projected to reach US$22 billion by 2022. It has been growing rapidly, at 12% CAGR, and most of those dollars stay in the Washington region.[130] There are numerous laboratories and research universities in Washington at the "forefront of scientific advancement."[131] However, in contrast to the early evolution of Silicon Valley, where Stanford University played a key role, the Washington high-tech industry developed without direct support of a major research university.[132] Despite being home to a number of high-profile universities, there is limited evidence of their direct contribution to early growth of the local technology sector. Economic development was never a primary objective for John Hopkins University in nearby Baltimore, for example, standing in sharp contrast to the likes of MIT in Boston and Stanford in Silicon Valley. Accordingly, Johns Hopkins has "not generated highly visible economic benefit for the local area."[133] The direction of influence in Washington seems to work the other way: once entrepreneurial success and a sizeable industry were established, universities began developing programs to meet growing demand for skilled labor.[134] Washington boasts a significant number of academic and research institutions as seen in Map 3.10. Despite the high number of institutions and graduates in the region, there seems to be less of a spatial correlation between universities and cyber clustering in Washington than in SFBA and Israel.

[127] Heike Mayer, "Segmentation and Segregation Patterns of Women-Owned High-Tech Firms in Four Metropolitan Regions in the United States," *Regional Studies* 42, no. 10 (December 1, 2008): 1357–83, https://doi.org/10.1080/00343400701654194.

[128] "Census Profile."

[129] While best known for its government and military institutions, other, often complementary industries also make up a significant part of the diverse local economy creating a regional nucleus of economic production. Slightly more people in Washington are employed in specialized professional and business services than are employed directly by government. A large percentage of people are employed in trade and transportation, education and health, and in leisure and hospitality, "Washington, DC Area Economic Summary" (U.S. Bureau of Labour Statistics, April 8, 2020).

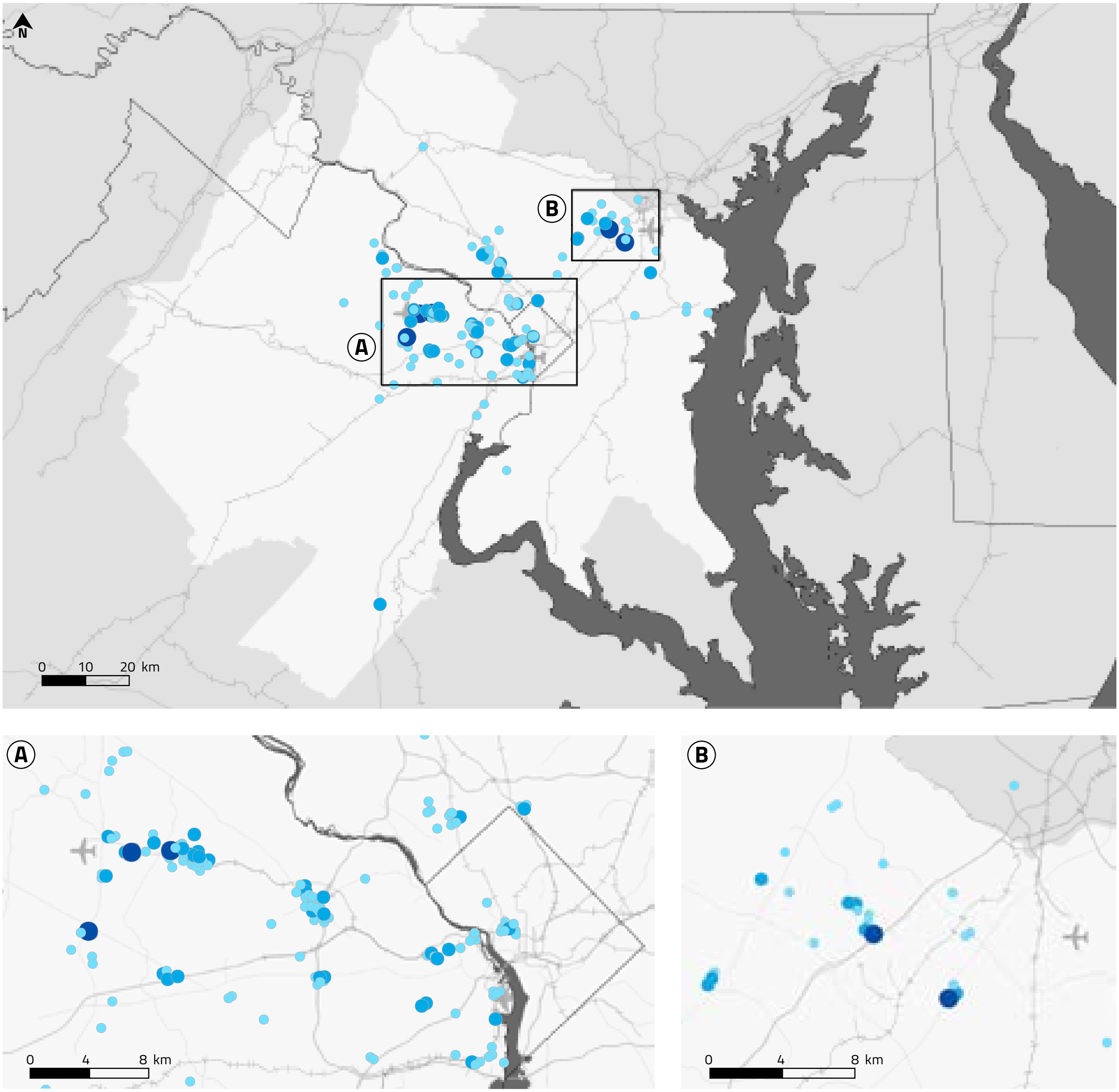
[130] See also map 2.4 (Chapter 2) which shows that the Washington D.C. Metropolitan Area is home to a large number of government agencies, institutions, and arms-length defense contractors, in addition to a host of agencies, NGOs and other institutions. Erran Carmel, Bini Byambasuren, and Jonathan Aberman. *Cybersecurity Startup Founders in the Greater Washington Region: Prior Experience Required.* April 2018. Center for Business in the Capital, American University. p. 11.

[131] Edmund J. Zolnik, "The Role of Postdoctoral Fellows in Technology Transfer: Evidence from the National Capital Region of the USA," *International Journal of Knowledge-Based Development* 1, no. 3 (January 1, 2010): 158–75, https://doi.org/10.1504/IJKBD.2010.035657.

[132] Heike Mayer, "What Is the Role of Universities in High-Tech Economic Development? The Case of Portland, Oregon, and Washington, DC," *Local Economy* 21, no. 3 (August 1, 2006): 292–315, https://doi.org/10.1080/02690940600808362.

[133] Maryann Feldman and Pierre Desrochers, "Research Universities and Local Economic Development: Lessons from the History of the Johns Hopkins University," *Industry & Innovation* 10, no. 1 (March 2003): 5–24, p. 20 https://doi.org/10.1080/1366271032000068078.

[134] Mayer, 2006.



Map 3.6 Washington-headquartered pure-play cybersecurity firms by number of employees

Number of Employees

● 1-100

● 101-1,000

● 1,001+

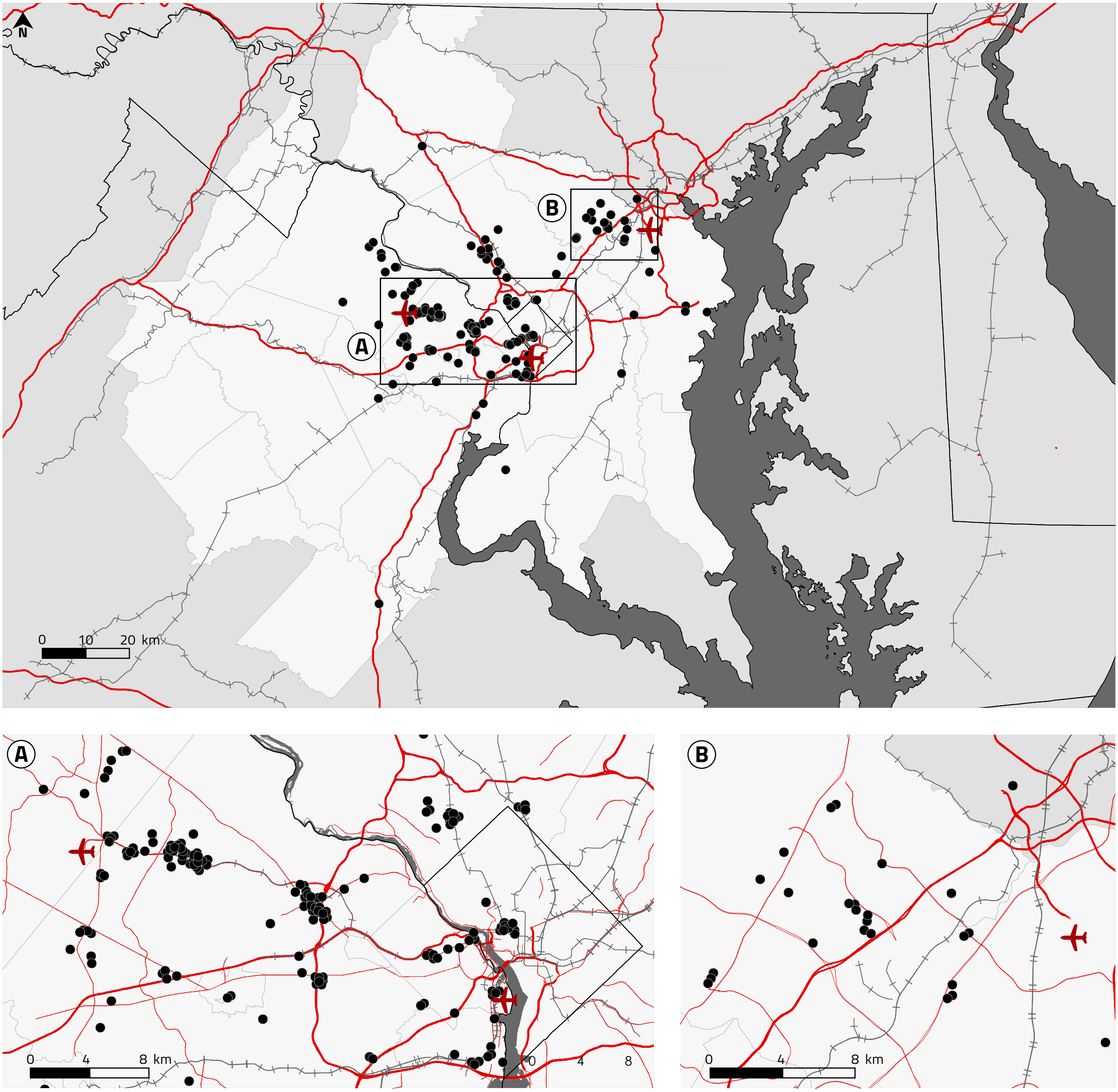
Highway / Primary Road

Railway

Major Airport

State Boundary

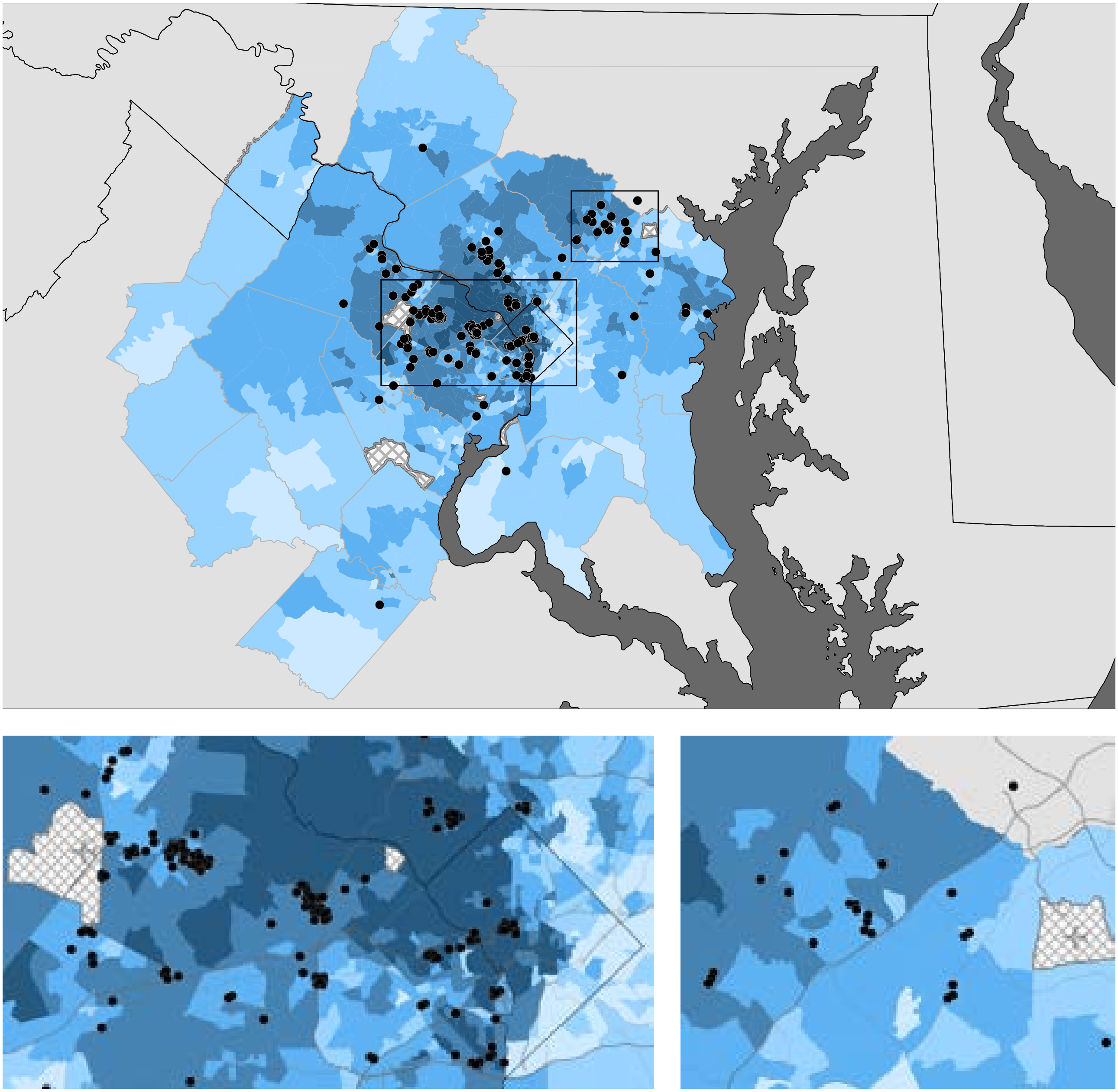
Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



Map 3.7 Washington-headquartered pure-play cybersecurity firms & transportation infrastructure

●	Cybersecurity Company
—	Highway / Primary Road
┼─┼	Railway
✈	Major Airport
—	State Boundary
□	County Limit

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



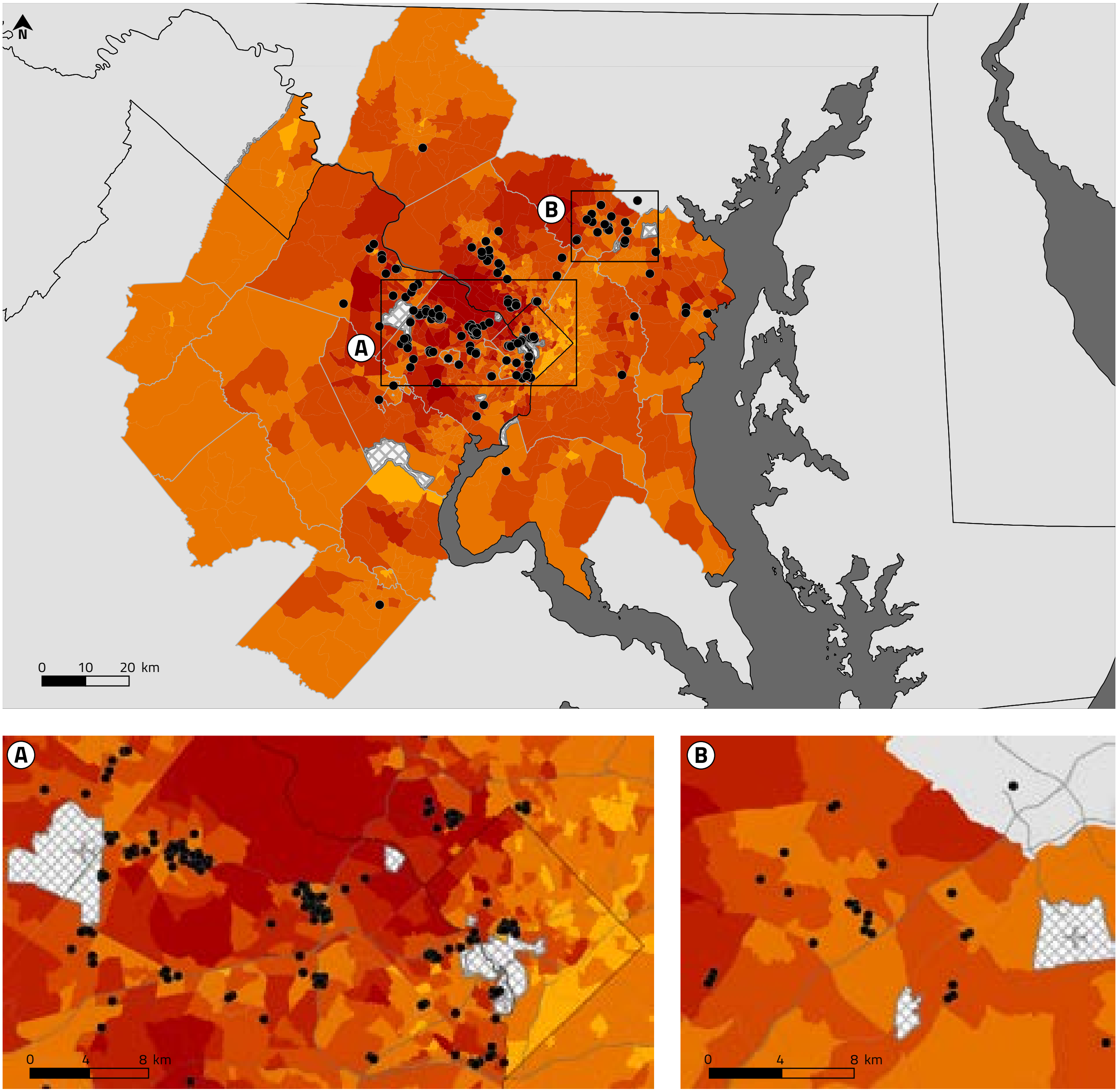
Map 3.8 Washington-headquartered pure-play cybersecurity firms & academic achievement

Pop. with Bachelor's Degree or Higher

▨	0% - 20%
▨	21% - 40%
▨	41% - 60%
▨	61% - 80%
▨	81% - 100%
▩	NA

●	Cybersecurity Company
─	Highway / Primary Road
┼	Railway
━	State Boundary
□	County Limit

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)

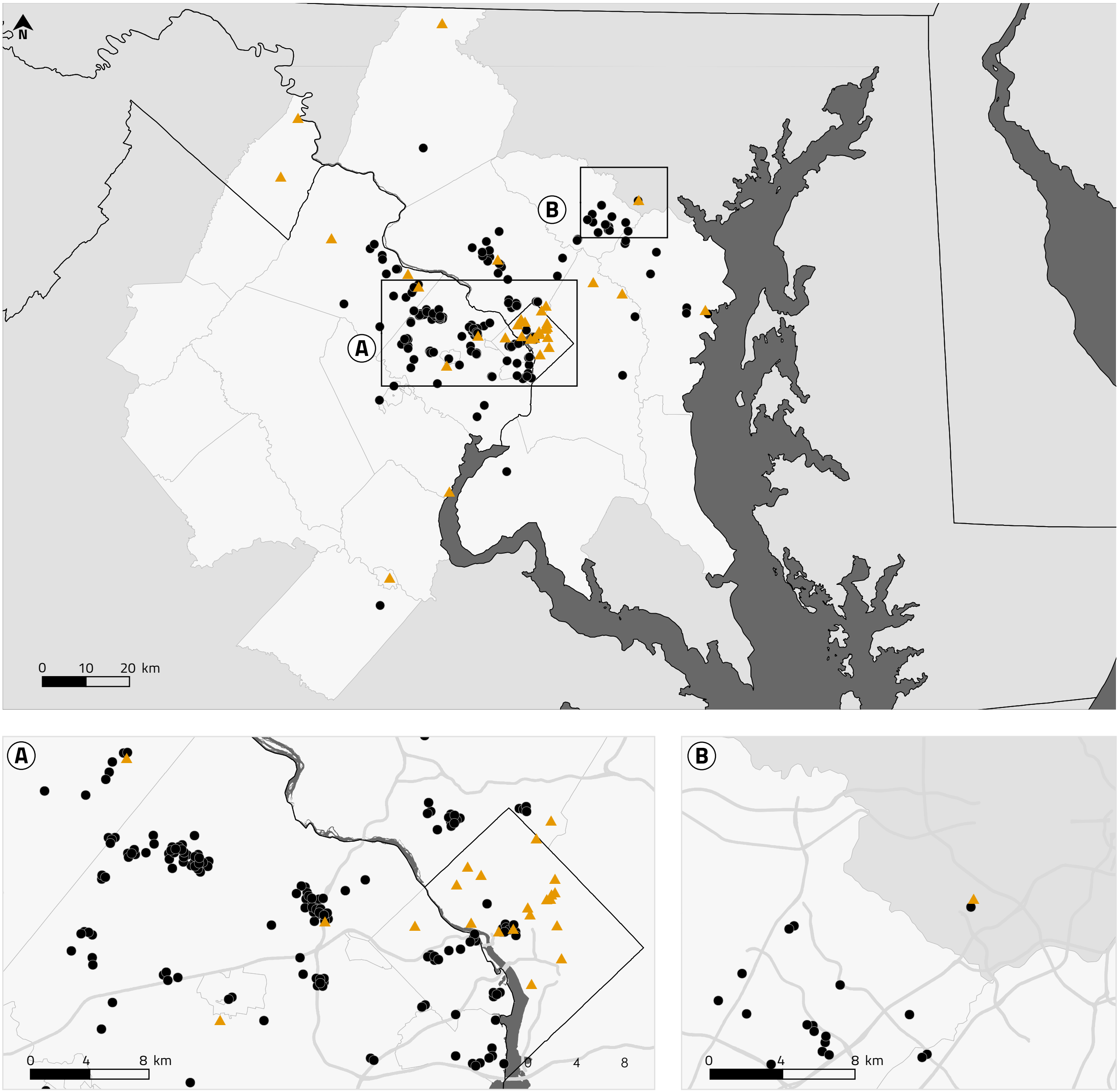


Map 3.9 Washington-headquartered pure-play cybersecurity firms & socioeconomic status

Household Median Income ($/year)

🟨	Below 50,000	●	Cybersecurity Company
🟧	50,001 - 100,000	—	Highway/Primary Road
🟧	100,001 - 150,000	-+-+-	Railway
🟥	150,001 - 200,000	—	State Boundary
🟥	Above 200,001	□	County Limit
▨	NA		

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



Map 3.10 Washington-headquartered pure-play cybersecurity firms & post-secondary institutions

● Cybersecurity Company

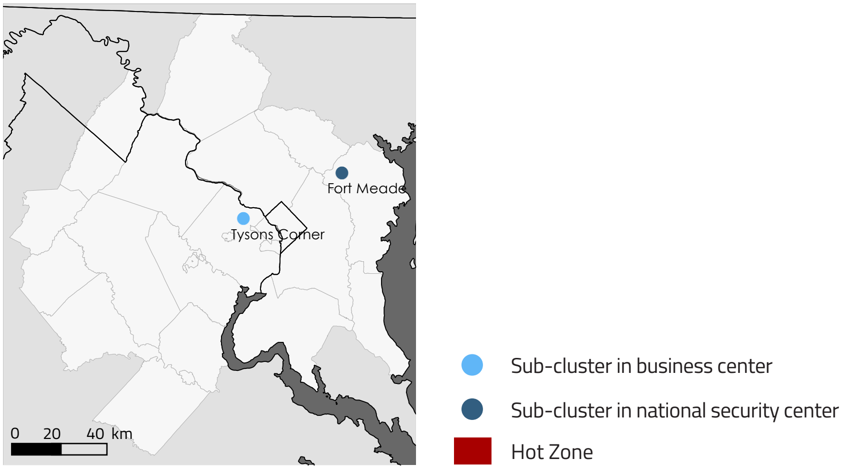
▲ Postsecondary Institutions

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)

Table 3.2 summarizes key features of the Washington cluster. Significant and consistent government and military expenditure provides stability for existing tech firms and reduces entrepreneurial risk when forming new ventures. Military and government-trained personnel enter the local labor force and/or form new companies, further supporting growth of existing industry and attracting major cyber firms to the area. Government and military presence and investment played a crucial role the cluster's strength. While the private sector and other factors contribute to the growth of the cybersecurity cluster in Washington, it is primarily a product of government and military influence.

WASHINGTON D.C.

The Washington D.C. cybersecurity cluster stretches from Dulles International Airport in Virginia, through the District of Columbia to Maryland suburbs approaching Baltimore. In Washington DC there is no distinct "hot zone", rather there are sub-clusters situated in neighborhoods throughout the region. The most important sub-clusters are located in Reston, Tysons Corner, and Ballston running east-west along Interstate 66 and Route 267 which connects Washington D.C. with Dulles International Airport. There is another sub-cluster outside of Baltimore, in close proximity to the NSA offices.


Fort Meade
Tysons Corner
0 20 40 km
● Sub-cluster in business center
● Sub-cluster in national security center
🟥 Hot Zone

INFRASTRUCTURE

Key Cities & Transportation

- Washington D.C. – Maryland – Virgina metro region contains several sub-clusters.
- Complex network of highways, railways, public transportation, shipping and several international airports.

Industries & Services

- High percentage of current or past government employment.
- Hub for professional business services
- 5th largest metro economy in the US.

SOCIAL CAPITAL

Socioeconomic

- Young, highly-educated workforce
- High ratio of workers and founders with military backgrounds.
- Highest ratio of tech workers in the country.
- Stark division of income and education levels.

INSTITUTIONS

Government & Military

- Unrivalled government and military presence.
- Highest government spending on tech of any region.
- Crossover of labor between public and private sectors.

Research & Education

- Government-funded training and military re-integration programs.
- Several top-tier universities with degree specializations.
- Collaborative efforts between academic institutions and other sectors in research, training and investment.

Table 3.2 Features of Washington D.C. cybersecurity ecosystem

c. Israel: a top-down cluster

A case of intentional government intervention in cluster development

The Israeli cybersecurity cluster includes the center of Israel (metropolitan Tel Aviv) and sub-clusters in the south and in the north. Israel's population is heavily concentrated in the west along the Mediterranean coastline and in the central section of the northern half of the country. The City of Tel Aviv-Jaffa (hereafter, "Tel Aviv"), its high-tech and cybersecurity epicenter, lies at the heart of an urban agglomeration home to approximately 3.7 million people. Israel has a total population of approximately 8.3 million. The Israeli mega-cluster does not exhibit an even geographic distribution of firms. Rather it displays one distinct hot zone in central Tel Aviv, along the rail corridor close to the Ayalon Highway. This hot zone contains 120 firms and is about 8 sq. km (3 sq. miles). In addition to this hot zone, several sub-clusters are visible in the Tel Aviv periphery (Herzliya, Petah Tikvah) and outside Tel Aviv (in Israel's other major cities: Jerusalem, Haifa and Be'er Sheva). This distribution pattern also reflects national population distribution, with no firms in the southern half of the country, south of Be'er Sheva, a desert region known as the Negev. Map 3.11 shows clustering of cybersecurity firms in Israel based on size, as measured by number of employees. All firms with more than 100 employees are located in metropolitan Tel Aviv (3.11A). The three largest firms, each with more than 1,000 employees, are located within close proximity of a train station. Note in magnification A, two of the largest firms are outside the Tel Aviv hot zone (along the border of Tel Aviv and Petah Tikvah). Magnification 3.11B shows the small firms in Be'er Sheva sub-cluster.

Viewing this cybersecurity industry growth in wider set of variables, including infrastructure, social capital and institutions, the following points emerged.

Infrastructure. Map 3.12 also displays major transportation infrastructure, highways and primary roads, rail corridors, and airports. The regional map shows a clear agglomeration of firms in the greater metropolitan region around Tel Aviv. Magnification 3.12A is an expanded map of Tel Aviv where a significant concentration of firms is evident within very close proximity to the Ayalon Highway, Road 2, and the rail corridor. This location provides a high level of physical connectivity within the city region and the country, as well as access to Ben-Gurion International Airport, Israel's main airport. Significant sub-clusters are also visible in Tel Aviv suburbs: in Herzliya, close to the Ayalon Highway, Road 2 and the train; as well as in Ra'anana, proximate to Highway 4. Magnification 3.12B shows an expanded map of Be'er Sheva, where all cybersecurity firms are located in a very tight cluster close to the train station.

In terms of policy, Israel's governments – both at the local and national level – are proactively supportive of and involved in development of the country's national cybersecurity strategy. This includes coordination of public national security efforts as well as supporting growth of private industry. Israel's National Cyber Initiative taskforce was created in 2011 by Prime Minister Benjamin Netanyahu "to pursue a comprehensive approach to cyber security, exploring potential macroeconomic and strategic benefits for Israel."[135] The National Cyber Initiative is an independent agency tasked with developing a holistic, multi-pronged approach to cybersecurity, including through "education, R&D, security, economic development, and international cooperation." The Israel National Cyber Directorate expands Israel's cyber capacity and strengthens its position as a global leader in cybersecurity by developing human capital starting as early as high school and investing heavily in public and private R&D.[136] Israel identifies and trains high school students with exceptional computer skills in order to recruit them for cyber-intelligence programs in the military. The Israel Defense Forces (IDF) then directly develops cyber-specialists through Intelligence Unit 8200, and the C4I Corps (the command and communications division), which

[135] Dmitry (Dima) Adamsky, "The Israeli Odyssey toward Its National Cybersecurity Strategy," *The Washington Quarterly* 40, no. 2 (April 3, 2017): 113–27, p. 115 https://doi.org/10.1080/0163660X.2017.1328928.

[136] Adamsky, 2017.

ensures security capabilities are fully coordinated. The IDF, national government and private sector coordinate and collaborate on projects, as cybersecurity is recognized as a shared and vital priority. Projects such as the Advanced Technology Park in Be'er Sheva create physical space in which government personnel, universities, private firms, and the military can share information and innovations, and work together on joint projects in close physical proximity.[137]

Although not specifically directed towards cyber industry, local policies play a major role in emergence of the cluster. Thus for example, the Tel Aviv Municipality supports early stage startups which have the potential to improve the quality of life for residents and/or promote Tel Aviv as a Smart City. Support includes meeting with a municipal expert, using the city as a beta site, property tax reductions for startups, and public relations.[138]

Social Capital. Israel has more high-tech start-ups per capita than anywhere other country.[139] Another commonly-cited metric is the number of companies listed on the high-tech heavy NASDAQ exchange. By this measure, Israel consistently ranks in the top tier of countries worldwide.[140] Israel's tense sociopolitical dynamics and restrictive geographic conditions force it to consistently rely on technological advancement, knowledge, and innovation for its defenses.[141] This is reflected not only in proactive action taken by the government and military, but by academic institutions, the general public, and the private sector. At the core of Israel's culture of innovation is a "dense start-up ecosystem composed of an array of meetups, hackathons, lectures, training sessions, mixers, social media sites, conferences, co-working spaces, venture capitalists, angels, and accelerators."[142] As is the case in SFBA and Washington clusters, Israel, too, exhibits a culture of collaboration between and amongst citizens, private firms, government and non-government agencies, military, and academic institutions.[143]

Mandatory military conscription in Israel also shapes the work ethic of its populace and, further, trains a large percentage of the labor force in marketable skills; such as goal-oriented strategic thinking. Military service provides network connections and social capital which aid in entrepreneurial success after military service is completed.[144] The people of Israel place a high value on "entrepreneurialism, science, technology, and innovation" and believe they are critical elements of "national security, prosperity, and quality of life."[145] Israel exhibits a relatively flat social hierarchical structure, a culture of individualism, and high levels of nationalism, attributes that promote and foster innovation and entrepreneurialism at the national level.[146]

Map 3.13 illustrates general distribution of population by academic achievement in relation to cybersecurity sub-clusters in Israel. A high concentration of those with at least a Bachelor's degree is clearly evident in the central region, which includes Tel Aviv and the area immediately surrounding it. There is another concentration of highly

[137] Matthew S. Cohen, Charles D. Freilich, and Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response," *International Studies Perspectives* 17, no. 3 (August 1, 2016): 307–21, https://doi.org/10.1093/isp/ekv023.

[138] For further information see the municipality website https://www.tel-aviv.gov.il/en/WorkAndStudy/Pages/Supporting-Local-Startups.aspx

[139] Steven Fraiberg, "Start-Up Nation: Studying Transnational Entrepreneurial Practices in Israel's Start-Up Ecosystem," *Journal of Business and Technical Communication* 31, no. 3 (July 1, 2017): 350–88, https://doi.org/10.1177/1050651917695541.

[140] Catherine De Fontenay, and Erran Carmel, 2004. Israel's Silicon Wadi: the forces behind cluster formation. In Timothy F. Bresnahan, Alfonso Gambardella, and AnnaLee Saxenian. (eds.) Building High Tech Clusters, Cambridge University Press.

[141] Fabio Kon et al., "A Panorama of the Israeli Software Startup Ecosystem," *SSRN Electronic Journal*, 2014, https://doi.org/10.2139/ssrn.2441157.

[142] Fraiberg, "Start-Up Nation," p. 352.

[143] Gil Baram and Isaac Ben-Israel, "The Academic Reserve: Israel's Fast Track to High-Tech Success," *Israel Studies Review* 34, no. 2 (September 1, 2019): 75–91, https://doi.org/10.3167/isr.2019.340205.

[144] Baram and Ben-Israel.

[145] Professor Gili S. Drori and Avida Netivi, "STEM in Israel: The Educational Foundation of 'Start-up Nation,'" Consultant Report (The Hebrew University of Jerusalem), accessed July 26, 2020, https://www.voced.edu.au/content/ngv:56958.

[146] Kon et al., "Panorama."

educated people in and around the City of Haifa. Magnifications 3.13A and 3.13B show the Tel Aviv and Be'er Sheva respectively. Though much of the government's policy is applicable nationwide, in Map 3.14 there appears to be correlation between higher income level and location of cybersecurity companies. Higher income levels are concentrated in the large cities: in Tel Aviv, and in smaller, yet notable, concentrations around Herzliya (part of metropolitan Tel Aviv), Be'er Sheva, Jerusalem and Haifa. The location of high-income individuals close to high-paying tech-sector employment likely reinforces their mutual geographic clustering.

Institutions. Israel developed national, government-sponsored programs aimed at finding promising youth, and providing them with specialized training before and during their military service. Universities and research facilities in Israel collaborate with the national government and the private sector to train and develop a highly-skilled workforce. Development of high-quality research and development institutions has been a central priority since the state was established. Science, technology and innovation are key strengths of its major universities: the Technion, Hebrew University, The Weizmann Institute, and Tel Aviv University.[147] Ben-Gurion University in Be'er Sheva has been playing an active role in developing the adjacent tech park as part of a bid to secure the city's position as a hub in the tech sector. At Tel Aviv University, students in almost *any* discipline can specialize in cybersecurity, and the university plays host to a major international cybersecurity conference every year. Technology and innovation education, particularly in cybersecurity, begins as early as middle and high school[148] and 46% of Israeli adults hold a post-secondary academic degree, the 3rd highest ratio in the OECD.[149]

Private firms and non-profit agencies work closely with academic institutions to "cultivate science and technology education." Different actors consolidate "knowledge in entrepreneurial and innovation management fields" making it accessible and available to a global market. Technology and innovation education initiatives include accelerator programs, dedicated entrepreneurial education, and R&D.[150] These initiatives are further supported by agencies, professional networking organizations, industry boards, and conference, among other initiatives. Israel "Advanced Technology Industries" is an umbrella organization supporting the general tech sector, representing and bringing together not only private industry but academia, municipalities, hospitals, research centers and the national government.[151] The Israel Cyber Alliance is a joint venture between the Israel Export Institute, the Ministry of the Economy and Industry, and the National Cyber Directorate, representing and supporting over 350 cyber companies in Israel.[152] The Israeli Ministry of Foreign Affairs directly supports industry events such as the Cybertech Conference which took place, most recently, in January 2020 in Tel Aviv.[153]

Map 3.15 shows the locations of major post-secondary institutions overlaid on the location of cyber firms. In the regional map (left), the location of universities generally appears correlated to the clustering and sub-clustering of cybersecurity firms, with at least one institution in each sub-cluster. Yet at a smaller scale, magnifications 3.15A and 3.15B show less acute correlation between locations of universities and cyber firms in the city of Tel Aviv. The spatial relationship is more relevant in Be'er Sheva and the Tel Aviv suburb of Ra'anana. This suggests that the presence of a large university compensates for lack of other physical, social and economic factors in small cities, but is not a driving factor in highly developed and connected urban environments. It further suggests that activities of firms and universities are not necessarily related on a day-to-day basis. However, they likely have some mutual relative proximity benefits as well as some shared favorable ecosystem characteristics.

[147] Kon, "Panorama."

[148] Donaldson, Stow, and Hobson, "UK Cybersecurity Sectoral Analysis and Deep-Dive Review."

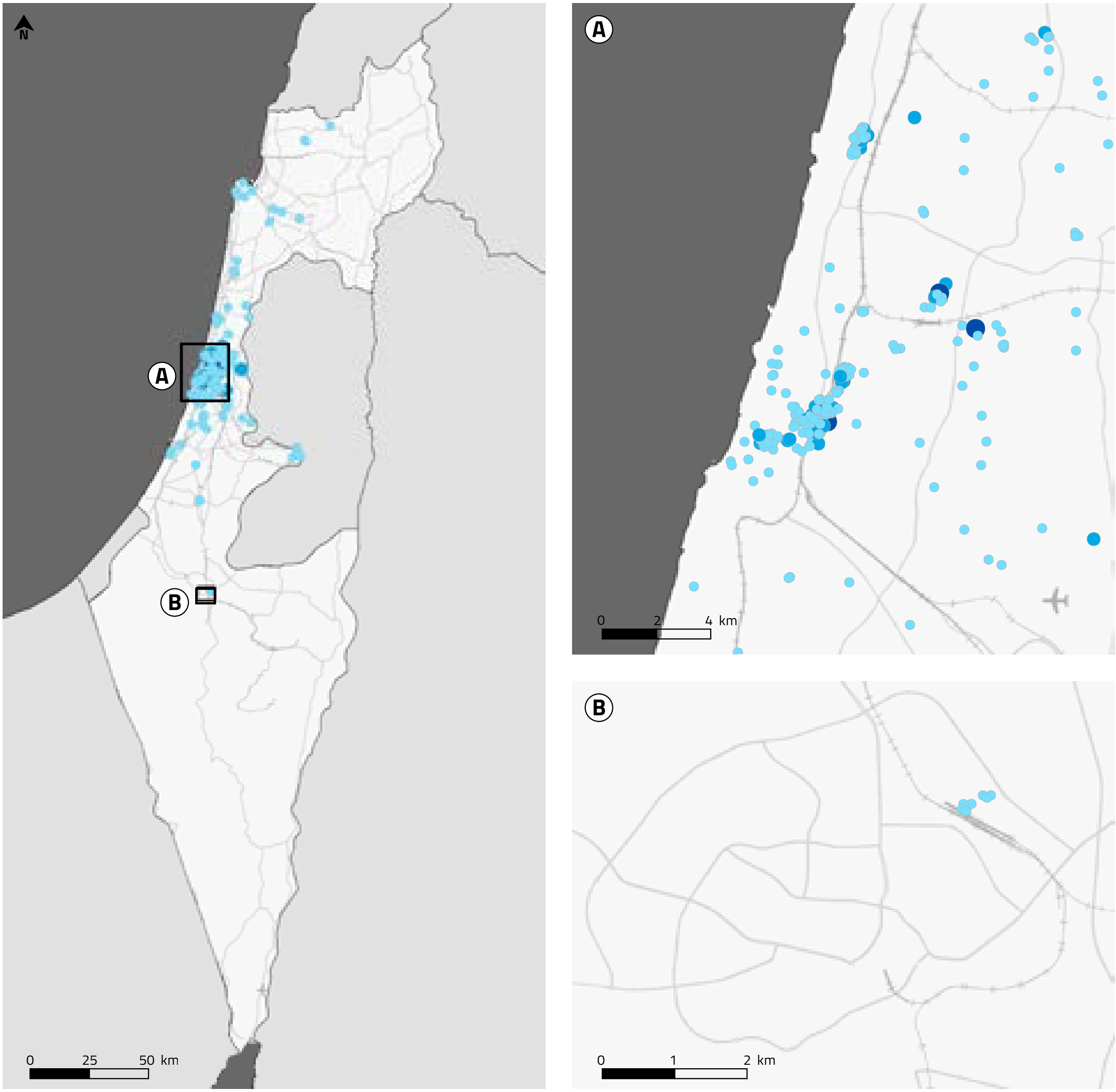
[149] Drori and Netivi, "STEM in Israel: The Educational Foundation of 'Start-up Nation.'"

[150] Kon et al., "A Panorama of the Israeli Software Startup Ecosystem."

[151] "IATI - Israel Advanced Technology Industries," accessed July 28, 2020, https://www.iati.co.il/.

[152] "Israel Cyber Alliance," Israel Cyber Alliance, July 28, 2020, https://israelcyberalliance.com/.

[153] "CyberTech 2020," accessed July 28, 2020, https://mfa.gov.il/MFA/InnovativeIsrael/Conferences/Pages/CyberTech-2020.aspx.



Map 3.11 Israel-headquartered pure-play cybersecurity firms by number of employees

Number of Employees

● 1-100

● 101-1,000

● 1,001+

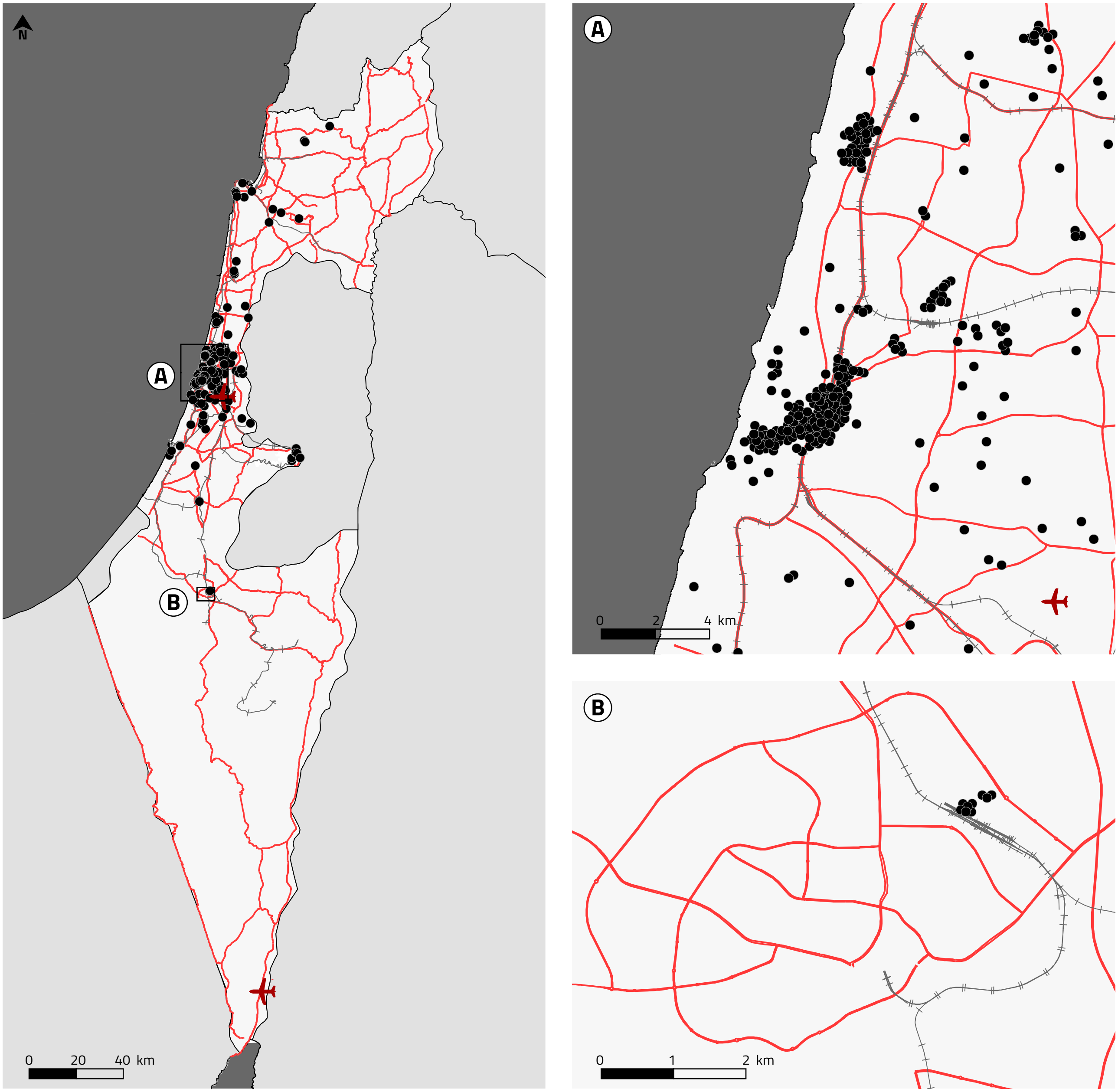
— Highway / Primary Road

┼ Railway

✈ Major Airport

— International Border

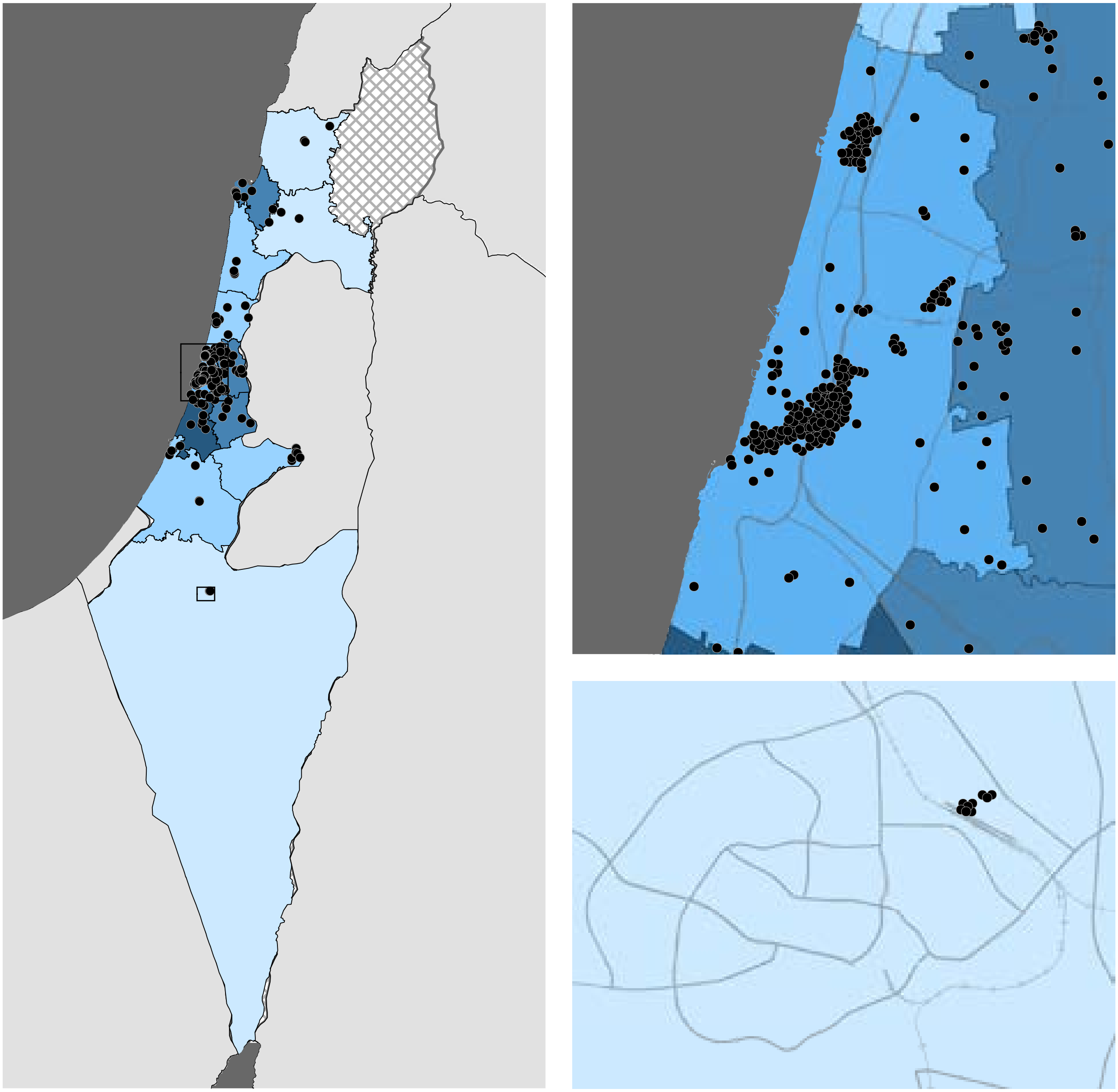
Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



Map 3.12 Israel-headquartered pure-play cybersecurity firms & transportation infrastructure

●	Cybersecurity Company
—	Highway / Primary Road
┼	Railway
✈	Major Airport
—	International Border

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



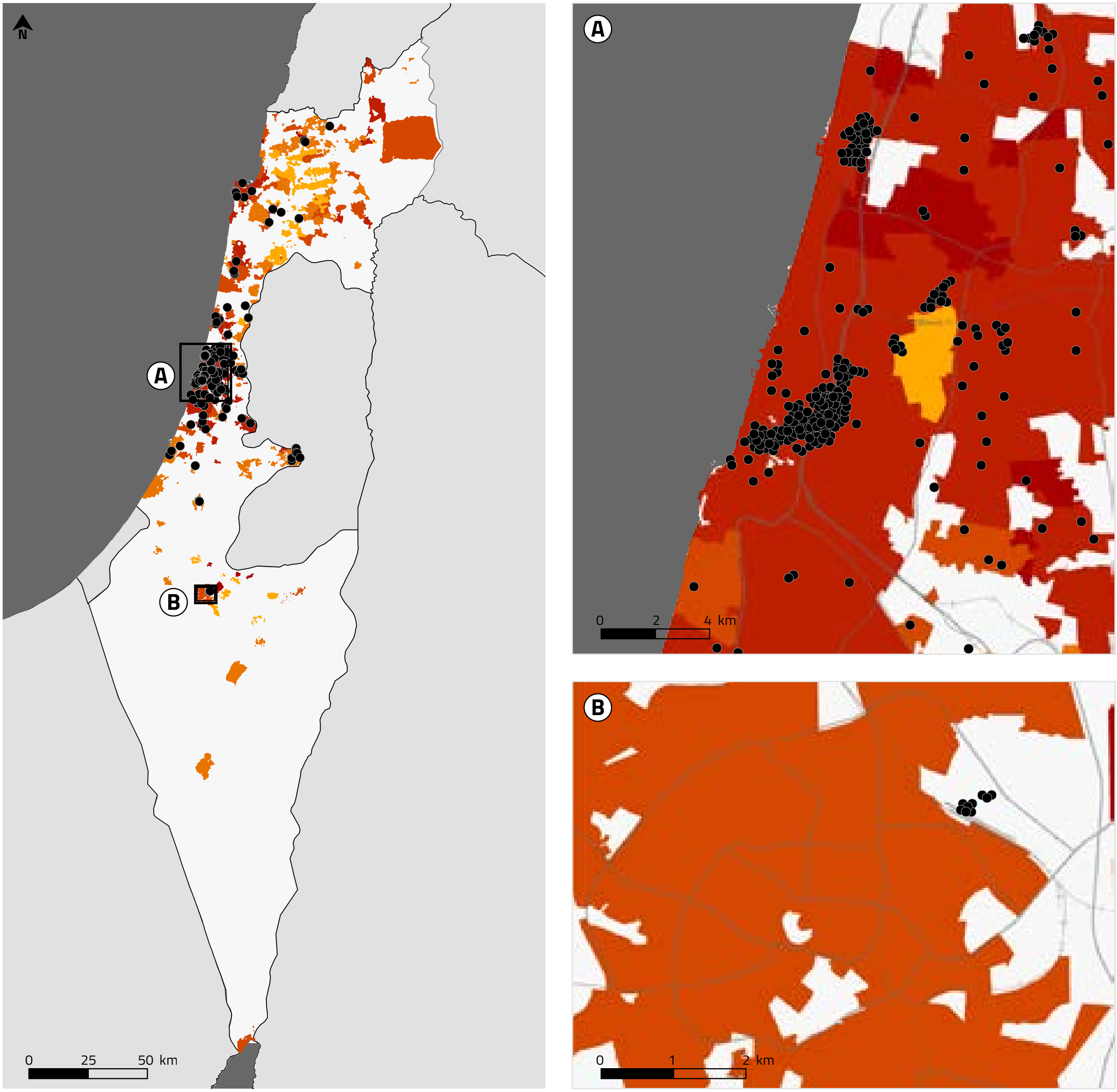
Map 3.13 Israel-headquartered pure-play cybersecurity firms & academic achievement

Pop. with Bachelor's Degree or Higher

🟦	0% - 20%
🟦	21% - 40%
🟦	41% - 60%
🟦	61% - 80%
🟦	81% - 100%
▨	NA

●	Cybersecurity Company
—	Highway / Primary Road
┼	Railway
—	International border

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



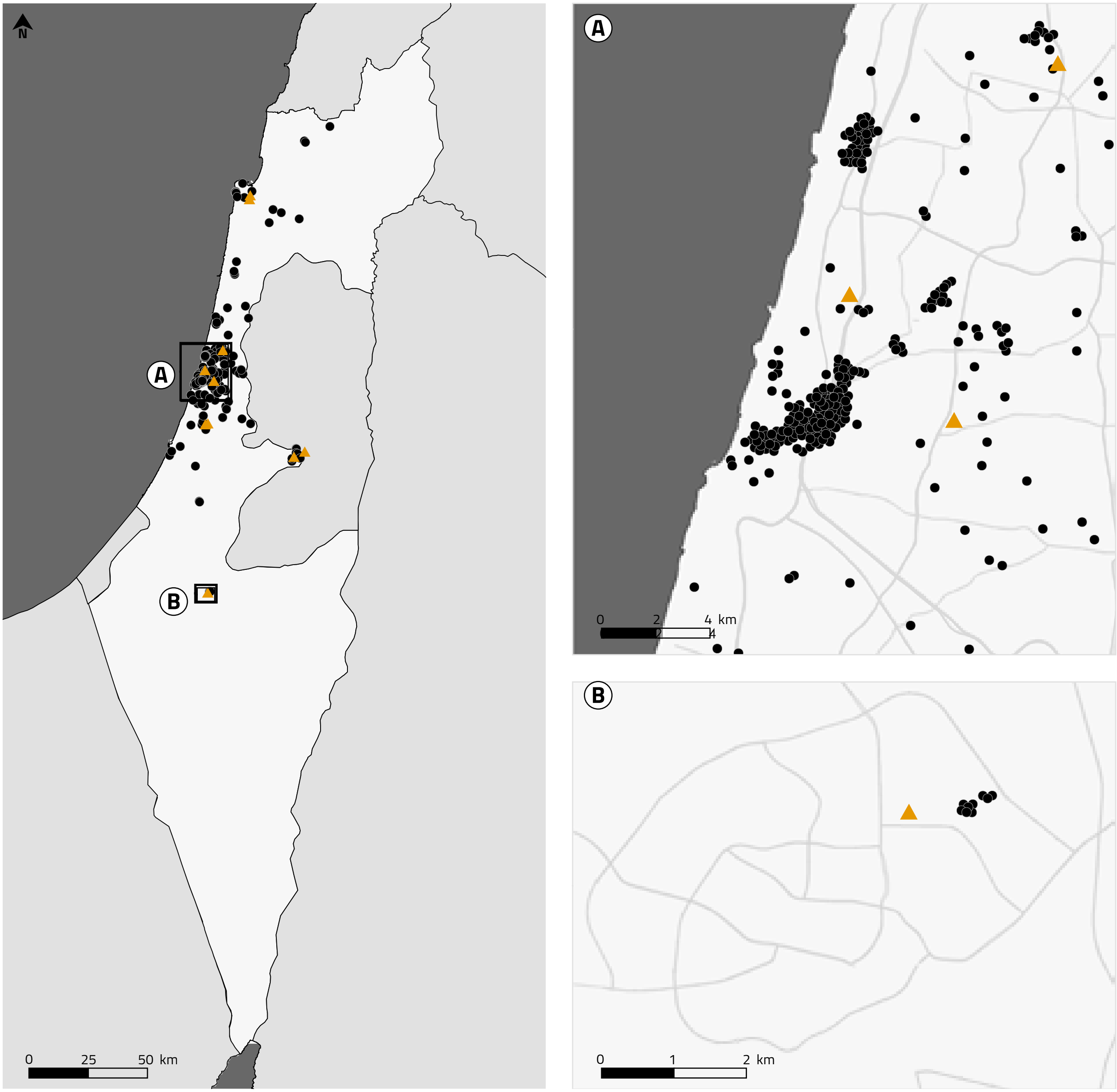
Map 3.14 Israel-headquartered pure-play cybersecurity firms & socioeconomic status

Socioeconomic Index (10=highest)

🟨	1 - 2
🟧	3 - 4
🟧	5 - 6
🟥	7 - 8
🟥	9 - 10

●	Cybersecurity Company
—	Highway/Primary Road
-+-+-	Railway
—	International Border

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)



Map 3.15 Israel-headquartered pure-play cybersecurity firms & post-secondary institutions

● Cybersecurity Company

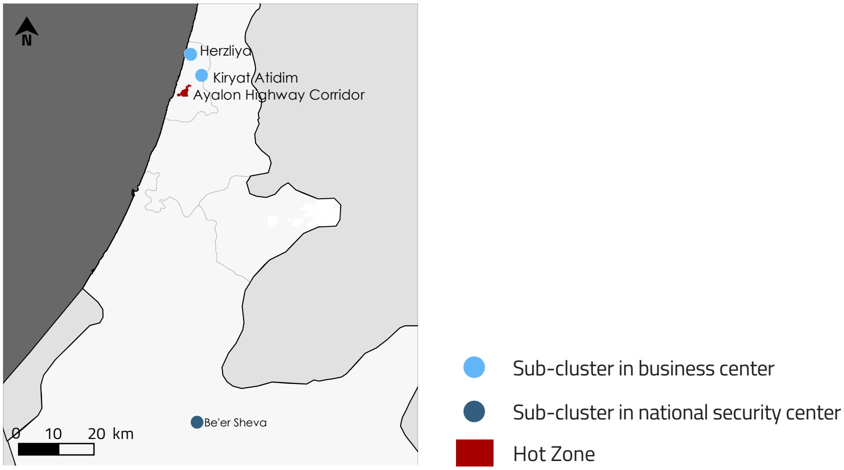
▲ Postsecondary Institutions

Created by Tali Hatuka and Antonio Mendoza, Laboratory for Contemporary Urban Design, Tel Aviv University
(Sources: Cyber companies database, Erran Carmel, Business In the Capital, American University; US Census Bureau, OpenStreetMap, Crunchbase, Owler, PrivCo)

Table 3.3 summarizes key features of the Israel cybersecurity cluster. Proactive and intentional government intervention enabled establishment and subsequent growth of the cybersecurity cluster in the Israel. Holistic government and military support of the sector includes labor force training and education, specialized university programs, direct investment, favorable public policy, and a large military presence. Israel has a large and diverse technology sector which contributes to the ongoing success of the cyber industry. Nevertheless, the cybersecurity cluster in the Israel is predominantly the result of specific actions taken by local governments as well as the presence and influence of the military.

ISRAEL

The Israeli cybersecurity cluster includes the entire country. In the Israeli Mega Cluster, there is one distinct hot zone in central Tel Aviv-Jaffa, along the rail corridor close to the Ayalon Highway. In addition, several sub-clusters are visible in the periphery, most notably in Herzliya, and Be'er Sheva. This distribution pattern reflects population distribution in the state, with no firms in the southern half of the country south of Be'er Sheva in a region known as the Negev.



INFRASTRUCTURE

Key Cities & Transportation

- Highly concentrated in metropolitan Tel Aviv-Jaffa
- After 2010 a micro-cluster begins to develop in Be'er Sheva
- Development of large tech park and military base in Be'er Sheva.

Industries & Services

- Tel Aviv is a cultural and economic hub for other creative industries and specialized services

SOCIAL CAPITAL

Socioeconomic

- Culture of innovation and entrepreneurialism
- High public and private sector funding
- Cross-sector collaboration

INSTITUTIONS

Government & Military

- Israel has more high-tech start-ups per capita than anywhere else in the world
- Large military presence with significant dedication to cybersecurity
- Mandatory conscription with conjunctive technology degrees
- Proactive support at all levels of government

Research & Education

- Government-sponsored education programs as early as high school and at every university in the country
- Development of cybersecurity research centers at several universities

Table 3.3 Features of Israeli cybersecurity ecosystem

3.3 Cyber security clusters as ecosystems: strategies and lessons

While all three mega-cluster cases are large by global standards (Table 3.4) the analysis highlights the hegemony of the SFBA cybersecurity industry over that of the other two clusters. Nevertheless, although they differ in many ways, three key points arise regarding the cybersecurity clusters.

	San Francisco Bay Area	Washington D.C.	Israel
Cluster emergence model →	Hybrid	Top-Down	Top-Down
Percent of Cyber TOP 150 Firms →	32%	9%	12%
Venture Capital →	US$13.1 Billion	1.9	4.0
Total Firm Revenue →	US$26 Billion	3.6	3.2

Table 3.4 High-level quantitative comparison of Big3 clusters

Cluster Emergence Model. It is unlikely that there is a truly "organic" form of cybersecurity cluster. In each of the Big3 clusters, there is notable government and national security influence acting as a development catalyst. While national security influence is more apparent in the Washington and Israel clusters than in SFBA, it is well-known that U.S. national security played an antecedent role in spawning the Silicon Valley miracle in the post-war era, thus serving, indirectly, as the foundation of the SFBA cyber industry. Each of these cases represent a different model: SFBA is a case of private sector entrepreneurialism and public support strategy, Washington is a case of cluster formation as a direct result of major government and military presence, and Israel is a case of intentional government intervention in cluster development.

Scale and intensity. Scale is a direct result of the central government scope of interventions, funding, and the concentration of social capital in a place, with the latter being a crucial component. Yet, it is the scope of these three components that defines the scale of the cluster as a whole. Clusters are not homogeneous and characterized by varied types of aggregation intensities. In the SFBA cybersecurity there are two distinct hot zones; in Washington, there are sub-clusters; and in Israel, there are both hot zones and sub-clusters. Hot zones are found in cities that either cultivate or are characterized by the culture of tech companies. In that sense, the hot zone cannot be viewed as autonomous entity but rather as part of a larger agglomeration of the tech industry. Local policies are crucial in the cultivation of hot zones. Sub-clusters are a manifestation of a decentralized approach to clustering. In the case of Israel, decentralization is a deliberate approach led by the government (as in the Be'er Sheva sub-cluster), while the Tel Aviv municipality is fighting to maintain the hot zone within its juridical boundaries. In that sense, the varied intensities in the cluster are not organic but rather manifestations of polices or their lack, on the part of the local and central governments.

Industrial Ecosystems. The cyber industry is part of a larger ecosystem and cannot be view in isolation. In examining the urban dimensions of the Big3 cybersecurity clusters the following points emerge:

Infrastructure. The epicenter of each cluster is based in a large, diverse urban environment with a sophisticated transportation network. The SFBA cluster is distinctly bi-modal, with large agglomerations of firms in both Silicon Valley and in downtown San Francisco. The Washington cluster is more dispersed than the other two, with sub-clusters in the Virginia and Maryland suburbs. In Israel, on the other hand, the sub-cluster in the City of Tel Aviv is clearly dominant, with significantly smaller clusters in the suburbs as well as in smaller cities such as Be'er Sheva. Policy, both national and local, plays a key role in the development of the cluster. National policy tends to be more specifically directed towards cyber, and local policy tends to support tech industry in general, and is highly influential for local culture. Indeed, the Israeli government's strategic policy toward the development of the cybersecurity industry is more intentional than the other two clusters. However, there are multiple examples of practical measures taken by government authorities in SFBA and Washington toward the same goal. Thus, although local and national economic policy manifests in different ways dependent on locale, holistically supportive regulations and multi-pronged, proactive strategies are critical for nurturing cybersecurity clusters.

		San Francisco Bay Area	Washington D.C.	Israel
Key Cities	Similarities	Distinctly bi-modal cluster, with hot zones formed across **large urban agglomeration** in downtown SF and in Silicon Valley; complex, **multi-modal transportation networks** including rail & transit, highways, international airports;	Multi-modal micro-cluster spread across **large urban agglomeration** within DC, Mayland and Virgina; complex, **multi-modal transportation networks** including highways, rail & transit, & international airports;	Primary hot-zone in **large urban agglomeration** in and around Tel Aviv-Jaffa with multiple smaller sub-clusters in other cities; complex, **multi-modal transportation networks** including rail & transit, highways, and international airports;
	Differences		No distinct hot zone, rather sub-clusters throughout urban region	Transportation infrastructure, particularly mass transit, seems to be less developed than other clusters;
Complementary Industries	Similarities	Plethora of professional, highly-**specialized service** firms directly serving innovation & tech sectors; **major industrial hub** for banking, manufacturing, food-processing and tourism	Many **specialized service** firms directly serving pivate sector cyber firms, as well as related government & military agencies; **major industrial hub** for service sector, health & education, trade, & tourism	Many highly-**specialized service** firms directly serving innovation & tech sectors, as well as government and military agencies; **major industrial hub** for banking, biotechnology, medicine, & media
	Differences		Government presence is so significant in Washington that it seems to influence all sectors	

Table 3.5 Comparative analysis (infrastructure) of Big3 clusters

Social Capital. It is abundantly clear that access to a large pool of skilled labor is critical for firms of all sizes and stages, and that a labor shortage in the cyber industry is being felt globally. Large and consistent capital flows are also vital, as are a culture of innovation and a diverse urban environment. Although each of these elements exists in all three clusters, their scope of impact differs greatly. For instance, venture capital makes up a much larger percentage of capital flows in both San Francisco and Israel than it does in Washington.

		San Francisco Bay Area	Washington D.C.	Israel
Socioeconomics, politics and culture	Similarities	Large, **highly-skilled labor pool** mostly with private sector experience; cross-pollination and **knowledge spillover** as workers move between firms; steady massive volume of **capital flow** mostly through VC & other private investment, as well as government contratcs; **innovation & collaboration** are part of the culture; most patent filings in US; huge number of Fortune 500 companies; large number of start-ups worth over US$ 1B; culture of entrepreneurship and risk-taking; **diverse urban population** with distinctly liberal culture & identity, unique entrepreneurial history beginning with gold-mining era.	Large, **highly-skilled labor pool** with a huge ratio from defense or military background; Highest ratio of tech workers of any region in the US; steady high volume of **capital flow** mostly through government and military spending/ contracts; lower cost of living than other comparable U.S. cities; **innovation** through low private transaction cost and massive government spending reducing risk for investors; **diverse urban population** with unique history as US capital influenced heavily by government and military presence.	Large, **highly-skilled labor pool** with private sector and military background; steady high volume of **capital flow** both through direct government investment & private sector VC; Mandatory conscription means most people have defense background and it has a major influence on culture; **collaboration, innovation,** research and improvisation are part of work and social culture; cross pollination and **knowledge spillover** between industries is common; **diverse urban population**, particularly in Tel Aviv, physical and sociocultural development heavily influenced by young, militaristic history.
	Differences	Firms have fewer direct relationships with government/military relative to other clusters (lower ratio of personnel with military/ govt background); more than double the VC/private funding of other two clusters combined.	Least known specifically for collaboration/knowledge sharing relative to other clusters; Share of capital flow is heavily in favour of institutions vs VC funding relative to other cluster; socioeconomic divide manifests geographically more than other clusters.	Mandatory conscription brings defense to forefront of public discourse/culture more broadly than in other two clusters.

Table 3.6 Comparative analysis (social capital) of Big3 clusters

Institutions. Though many of the characteristics are broadly shared, such as military influence and supportive government policy, there are important contextual differences in terms of how each characteristic manifested historically and its developmental impact on the given cluster. For example, government and defense agencies are more pervasive in both Washington and Israel than in SFBA. Nevertheless, historical contextualization elucidates the role of military spending in the development of the SFBA cluster just as it does in the other two. As another example, the locations of academic institutions are correlated with those of cyber firms, but the correlation appears weak in all three clusters. The part each organization, agency or type of institution played in the growth and maintenance of each cluster differs greatly and is beyond the scope of this study. What is clear, however, is that it is no one organization or type thereof is critical for cluster development, but rather the active presence of a network of complimentary institutions and organizations.

INSTITUTIONS & ORGANIZATIONS

		San Francisco Bay Area	Washington D.C.	Israel
Government & Military	Similarities	Significant **government investment** during formative years, early pillar companies formed through **military contracts** during WWII and Cold war; **collaboration** between government, military, academics & private sectors through joint projects; **supportive government policy** allowing institutional & private sector ownership of government research increased capital flow.	Significant and quickly increasing **government spending** through local defense agencies & private contractors; huge **military presence** & influence creates massive trained workforce & immediate market for new firms; intersector **collaboration** on defense technology development; **supportive government policy** enables veteran re-training & allows for direct investment in private firms.	Significant direct **government investment** in new firms & R&D; large **military presence** provides labor force & market, military influence through mandatory conscription & threat of conflict; **collaboration** between government, military, academics and private sector in R&D, training, & product development; **supportive government policy** for cyber investment, training, & promotion.
	Differences	Less physical government presence than other clusters; Less intentional government intervention in cluster creation; little physical military presence relative to other clusters.	Largest workforce with military/defense background in US.	Most calculated, intentional and publicly stated government intervention in cyber cluster; Mandatory conscription; most direct government investment in private sector ventures per capita.
Institutions - Research & Education	Similarities	Top-tier universities long **dedicated to research** in cyber and other technology innovation provide fresh talent; open **collaboration** between academic institutions as well as with the private sector through direct investment, joint R&D projects; **public and private investment** in education, training and R&D through shared labs, private and publicly-funded research centers.	**Dedicated research** in cyber through federal and state-funded education programs, increasing trained workforce; significant **collaboration** between academic institutions through dedicated local cyber initiatives; home to many post-secondary institutions, 16 of which have been recognized for academic exellence by the NSA and Department of Homeland Security (DHS); D.C. and Virginia have amongst the largest pools of doctoral science and engineering graduates in the US;	**Dedicated research** labs at several universities; **collaboration** between academic institutions and public & private sector through shared labs, tech parks & joint projects; direct **public and private investment** in education, training and R&D, specifically through military training programs & private education centers; dedicated scouting and training programs start as early as high school; many universities offer degree programs specializing in cybersecurity;
	Differences		Less notable private sector investment & collaboration with academic institutions than other two clusters.	

Table 3.7 Comparative analysis (institutions and organizations) of Big3 clusters

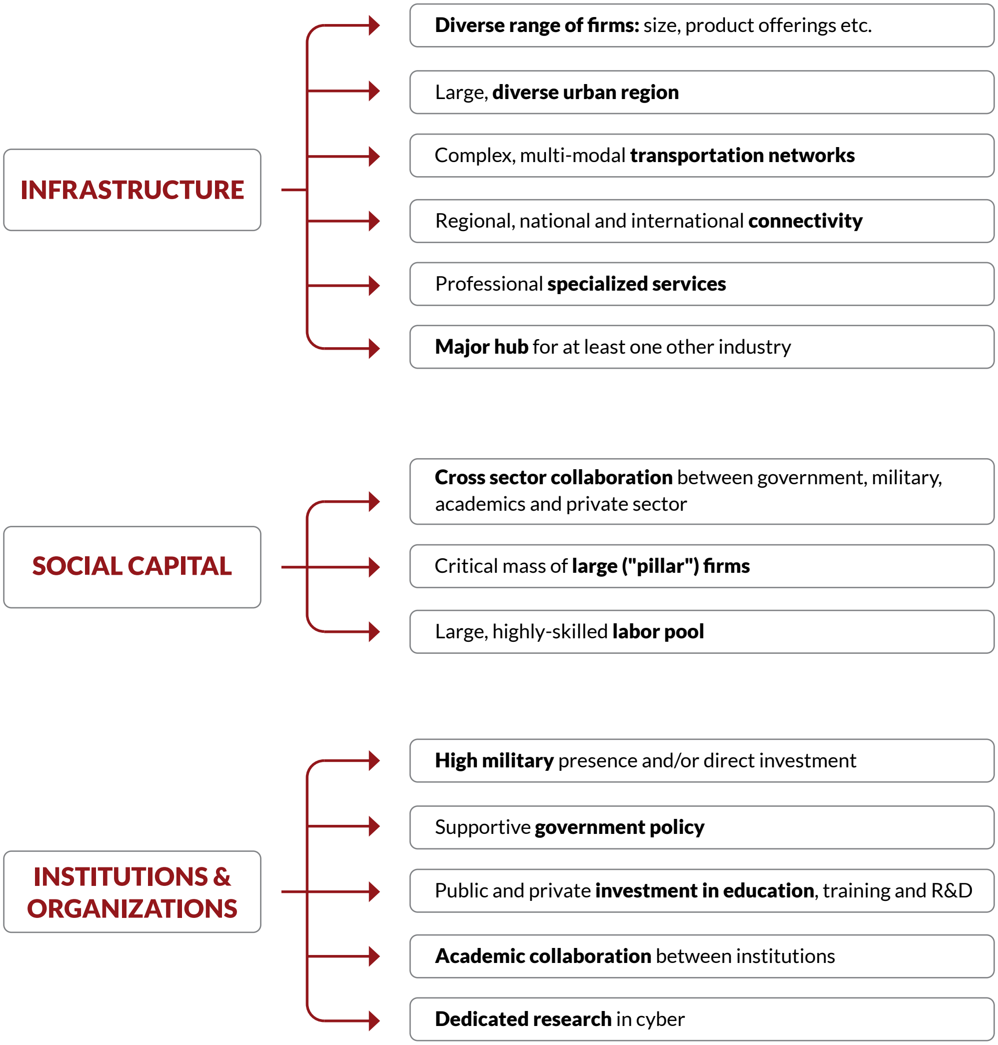

INFRASTRUCTURE
Diverse range of firms: size, product offerings etc.
Large, diverse urban region
Complex, multi-modal transportation networks
Regional, national and international connectivity
Professional specialized services
Major hub for at least one other industry
SOCIAL CAPITAL
Cross sector collaboration between government, military, academics and private sector
Critical mass of large ("pillar") firms
Large, highly-skilled labor pool
INSTITUTIONS & ORGANIZATIONS
High military presence and/or direct investment
Supportive government policy
Public and private investment in education, training and R&D
Academic collaboration between institutions
Dedicated research in cyber

Figure 3.2 Key components of cybersecurity ecosystems

The key question is what are the key components of a cybersecurity ecosystem, and can the ecosystem be viewed as a distinct prototype? Based the Big3 clusters framework of analysis, cybersecurity clusters emerge in large, diverse urban region, with complex, multi-modal transportation networks connected to regional, national, and international infrastructure. These places are often hubs for specialized professional services, and tend to be a major hub for at least one other industry. In terms of social capital, cybersecurity clusters are characterized by cross sector collaboration between government, military, academics and private sector. Clusters include a critical mass of large ("pillar") firms but also a diverse range of other firms. Finally, institutions play a major role in the cluster's development, and they often include high military presence and/or direct investment by military. Clusters often enjoy supportive government policy, and from public and private investment in education, from training and R&D, from academic collaboration between institutions and from dedicated research in cyber. This dynamic contributes to high volume of public and/or private capital flow.

CHAPTER 4

Developing Cybersecurity Clusters, an Urban-Economic Perspective

Chapter 4

DEVELOPING CYBERSECURITY CLUSTERS, AN URBAN-ECONOMIC PERSPECTIVE

Tali Hatuka and Erran Carmel

Conceptualizing the **cybersecurity industry as an ecosystem**, this report focuses on three distinct cases of mega clusters: the San Francisco Bay Area (SFBA), the Washington D.C. region, and Israel. The key conclusion of this report is that the cyber industry cannot be understood in isolation, but only as part of a larger context. Although this industry has some unique features, cybersecurity clusters are not autonomous, and their emergence is connected to a wider technological infrastructure, and to a particular urban and regional context.

4.1 Between cybersecurity industry and place of production

Genesis and Continuation. As our world became networked in the 1990s, cybersecurity emerged as a universal necessity. Even in its very early years, before the industry became distinguishable, the Big3 clusters were catalyzed. All three cybersecurity clusters emerged as specialized clusters embedded within a larger high-tech ecosystem. That is, they began inside the hegemonic innovation ecosystem of SFBA, inside the defense and high-tech ecosystem of Washington, and inside the "start-up nation" ecosystem in Israel. While each of the Big3 cybersecurity clusters have their own unique genesis story (see Chapter 2), none of them were set up deliberately by the government as clusters, and thus their founding cannot be perceived as a "top down" process. At the same time, government was a key actor in facilitating the high-tech and defense ecosystems in each of these three regions, the ecosystems that were the nest from which the clusters emerged. Silicon Valley (SFBA), was germinated by the early Cold War contracts given to Stanford; Washington, by the proximity to the Pentagon and NSA contractors; and Israel, by military veterans and quasi-governmental defense firms.

The cluster data show respectable, uninterrupted, long-term levels of firm formation (startup) supported by venture capital (see Chapter 2). For example, all three clusters raise large amounts of capital, by global standards; SFBA alone has raised U.S.$13 billion in venture capital. Most importantly, firms continue to be established up in the Big3 clusters; from 2010 to 2018, 634 new firms were added in the clusters. This is the ultimate validation of their success and markers of healthy innovation ecosystems.

Moving beyond its genesis, the cybersecurity industry can be viewed as a manifestation of two far-reaching interplays of the relationships between the cybersecurity industry, clustering processes and the place of production, that is, the socio-spatial context where the industry is located. These interplays are described below.

First, the interplay between the cybersecurity industry and clustering is evident in questions of density: **cluster concentration and industry consolidation**. To understand the scale of **cluster concentration**, note that the Big3 mega-clusters together serve as headquarters for 53% of the largest and most influential global cybersecurity firms (see Figure 1.3). This is a high degree of concentration: by comparison, when economists look at company concentration levels, a similar figure is considered oligopolistic. Additionally, the Big3 clusters have remained hegemonic for many years— ever since the industry's birth. Further to the oligopolistic framing: Are the Big3 cyber clusters too powerful? Would it be in the interest of governments to reduce their influence? Such a move would go against the very essence of clusters and the benefits they provide. Density is positive and leads to increased returns to the firms and to the region. There is no evidence of the U.S. government being concerned with the geography of cluster concentration. In Israel, geography plays a crucial role in the evolution of the cluster, and over the last decade the government has invested in seeding a cybersecurity sub-cluster in Be'er Sheva, with the aim of developing the southern area of the country.

Regarding the scale of **industry consolidation**, the global cybersecurity industry — especially in the Big3 clusters — is consolidating at a rapid pace. For example, 393 firms worldwide have been acquired by larger and more established firms that are headquartered in the Big3 cybersecurity clusters. However, the industry still remains quite fragmented because of the continued entry of new players, and is only at Stage 2 (of 4) of the consolidation curve (see Figure 2.3). In today's technology industry, there is always a concern of oligopolistic firms emerging (as currently apparent in firms like Google) yet there is no evidence of market dominating cybersecurity mega-firms that behave as an oligopoly. The market is still reorganizing firms, as evidenced by the recent breakup of the giant cybersecurity firm Symantec.

The second interplay, between the cybersecurity industry and its cluster, is closely related to questions of place and more specifically to **social context, human capital and institutions** (see Chapter 3). As exemplified by the analysis of the Big3, cyber clusters are located in established, high-income places. The epicenter of each cluster is a large, diverse urban environment with a developed transportation network. Policy, both national and local, plays a key role in the development of the cluster. National policies tend to be more specifically directed towards cyber industry itself, and local policy, emanating from municipal government, tends to support innovative industry in general, by initiating programs, projects and incentives that influence the environment and local culture.

In addition, the choice of firm location in the cybersecurity industry is linked to human capital. Access to a large pool of skilled labor is critical for firms of all sizes and stages, and a labor shortage is being felt in the cyber industry around the world. Large, consistent flows of capital are also vital, as are a culture of innovation and diverse urban environment. Furthermore, clusters benefit from institutional support. Generally, clusters share military influence and supportive government policy. The active presence of a network of complimentary institutions and organizations is critical for the development of a cluster.

In conclusion, cybersecurity clusters emerge in large, diverse urban regions, with complex, multi-modal transportation networks connected to regional, national, and international infrastructure. Clusters often enjoy supportive government policy, public and private investment in education, training and R&D, academic collaboration between institutions and dedicated research in cybersecurity technology. This dynamic contributes to a high volume of public and/or private capital flow.

Taxonomy and dimensions of analysis. Categorization plays a key role in the way we conceptualize industry, the way we understand its dynamic, and the way it affects policy. In terms of taxonomy, our research suggests that we ought to understand cybersecurity clusters using a spectrum of intensities (i.e., mega-, mesa-, micro-clusters, sub-clusters, and hot zone). In addition, our research suggests that industry economics be linked to the social dimensions and the built environment configuration. This, in turn, offers a new way of assessing fast-developing industries.

4.2 Facing forward: future challenges

What are the key challenges that the cybersecurity industry faces? We identify three: workforce shortage, resiliency, and durability.

Workforce shortage. The workforce for cybersecurity is tiered. The top layer consists of highly-paid, innovative workers, such as those employed in the Big3 cyber clusters, mostly by pure-play firms. At lower levels, there are many technicians who perform day-to-day operational activities (primarily on the Operate and Maintain (OM) level, as defined by the NICE[154] Cybersecurity Workforce Framework).

To date, the cybersecurity skills shortage is dramatic: in the U.S. it is estimated at half a million workers.[155] In Israel, with a population 40 times smaller, the shortage is ten thousand.[156] Given this gap, global information systems face concerns for the future. Universities are not producing enough trained workers in cyber professions,[157] in the U.S., Israel, or elsewhere. A State of California study found, "only 3,200 awards were conferred by programs that focused directly on cybersecurity or clearly included aspects of cybersecurity in their curriculum" concluding, unsurprisingly, that California's educational institutions are not supplying enough candidates to fill the thousands of cybersecurity job openings that exist.[158]

Thus, to make up for lack of formal, university preparation, cyber workers are being trained by industry and national security organizations, and in some specialized non-university settings. Evidence of this gap can be seen in the urban landscape of sub-clusters and hot spots, which emerged with universities having little influence on location decisions. Rather, the motivators of cybersecurity location choices are workplaces such as the NSA. In Washington, a regional initiative, the Greater Washington Partnership,[159] has attempted to address this educational gap by catalyzing new training programs but can only cover a small part of the large labor gap. Driven in part by the labor shortage, the CSIS study found that more than half of organizations outsource their cyber work.[160] In the spirit of previous outsourcing dynamics, this funnels cyber work to mid-wage or low-wage geographic regions. But unlike the large offshoring wave of the early 2000s, that cyber work stays within national borders.

[154] William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," August 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[155] ICS2, "Cybersecurity Workforce Study," 2019. https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study#

[156] Maayan Manala, "There is a shortage of 10000 cyber workers," Calcalist, December 10, 2018. In Hebrew https://www.calcalist.co.il/local/articles/0,7340,L-3751688,00.html?ref=ynet

[157] Center for Strategic and International Studies (CSIS), "Hacking the skills shortage," 2017. https://www.isc2.org/News-and-Events/Press-Room/Posts/2019/11/06/ISC2-Finds-the-Cybersecurity-Workforce-Needs-to-Grow--145. "In the U.S. market, the current cybersecurity workforce estimate is 804,700 and the shortage of skilled professionals is 498,480, requiring an increase of just 62% to better defend U.S. organizations."

[158] Centers of Excellence for Labor Market Research, Economic and Workforce Development Program, California Community Colleges, Cybersecurity: Labor Market Analysis And Statewide Survey Results From California Employers And Postsecondary Institutions 2017, p. 5. https://static.business.ca.gov/wp-content/uploads/2019/10/cybersecurity-labor-market-analysis.pdf

[159] Drew Hansen, "Major local employers, including JPMorgan and Amazon, endorse regional tech education framework," *Washington Business Journal*, Dec 12, 2019. https://www.bizjournals.com/washington/news/2019/12/12/major-local-employers-including-jpmorgan-and.html

[160] CSIS, ibid.

In conclusion, regional and national policy makers who wish to help their cyber industries grow might choose to invest in enlarging local cyber education programs, and then encourage alumni to remain in their locale.

Resiliency. The second challenge is the resiliency of clusters in cities. Over the last decade, with the communication revolution, there have been changes in work and consumption routines. The Covid-19 crisis accelerated the trend of remote work, which is weakening high-tech clusters, along with their surrounding supportive environment, e.g., restaurants, services. If this trend continues, the hegemony of global cities is expected to diminish, with the workforce possibly migrating out of expensive and unhealthy cities. This dynamic also leads companies to think "outside the box" about their locations and office infrastructures. Thus, for example, during the pandemic, a major Israeli cyber firm Check Point announced an architectural competition with a focus on new models of work, aimed at shrinking its footprint in cities.[161] Such actions could initiate a sea change in the conceptualization of clusters, which will affect the firms' footprints and perhaps the economy of cities and culture.

Durability. The third challenge is the durability of the cybersecurity industry itself. Are there too many cybersecurity firms? Will a new generation of powerful AI cyber tools reduce the need for so many complicated cyber firms? While these two arguments have some validity (the first one is discussed in Chapter 2), their short-term impact is likely exaggerated.

4.3 Lessons from the Big3 clusters

What lessons for policy makers can be derived from our examination of the Big3 clusters? In responding to this question, three vectors are addressed: lessons from the Big3 mega-clusters; lessons from the sub-clusters within the Big3, and finally, lessons for other clusters outside of the Big3.

Lessons from the Big3 clusters. Deliberate, top-down policy has been a minor factor in the continued growth of the mega-cluster ecosystems of cybersecurity. It continues to be driven mostly by organic forces, such as presence of highly-skilled labor, as well as anchor organizations. Generally, governments tend to intervene when there is a "market failure," such as an absence of agglomeration effects. The Big3 mega-clusters have not suffered from market failure, and all three are still vibrant clusters. However, both the U.S. and Israeli national governments have been an active force in fostering more robust cyber innovation markets in the Big3 clusters. Thus, for example, the U.S. government acquires many services from Washington-based cyber firms, and created a venture capital arm, In-Q-Tel, with offices in both Washington and SFBA, to further national security related innovation. In Israel, cyber firms are nurtured in many ways by the Israel Innovation Authority, a national body that acts as facilitator and government venture arm, with a track record of growing and supporting Israel's high-tech sector. Briefly, in the U.S. there is no particular concern about the need to advocate for the agglomeration of cyber mega-clusters in Washington or SFBA. In Israel, however, the national government actively supports its mega-cluster via executive-branch policy.

Another future potential market failure is cyber-Balkanization. At the national level, this refers to cumulative national security prerogatives, situations in which where national security priorities cause discrimination against foreign IT products. These security prerogatives will likely intensify as countries become increasingly suspicious of foreign software products. Such actions advantage local/domestic players. Export controls, already present in the U.S., may increase; import controls, already present in the U.S. and elsewhere, are likely to increase as well; cross border investment constraints will continue. Furthermore, in spite of close collaboration between Israel and the

[161] Ruti Levi, "Check Point's Challenge returns: A prize for those who solve it, at least NIS 14,000 per month," *The Marker*, August 8, 2020 (In Hebrew)." https://www.themarker.com/technation/1.9083389

U.S. on many cybersecurity dimensions, in 2005, Israel-based Check Point was blocked by the U.S. government from acquiring U.S.-based intrusion prevention company Sourcefire.

In sum, national governments will continue to make national security decisions with little concern for the cluster's development and growth.

Lessons from the (localized) sub-clusters within the Big3. The sub-clusters in Washington and Israel are distinct within the mega-cluster. In Washington, sub-clusters have grown within politically bounded areas, such as Fairfax County (Virginia) or the State of Maryland. The catalysts for these sub-clusters were largely organic, and once the sub-cluster began to grow, the role of local government policy has been to nudge further growth and cement the firms, labor, and capital within the local geography. In Israel, some sub-clusters developed organically as in the case of the city Herzliya (adjacent to Tel Aviv) in proximity to the vibrant high-tech environment. However, Israel has simultaneously initiated a "top-down" cybersecurity sub-cluster in the city of Be'er Sheva (as described in Chapter 2). In this project, the government played an unusual role as sub-cluster catalyst, with modest results so far, but it is too early to judge its future development and growth.

Lessons that can be inferred from the Big3 to other smaller clusters globally (see Map 1.1). The spread of mesa-clusters and micro-clusters around the globe is ongoing. At the outset, the Big3 clusters, as mega-clusters, are fundamentally different due to large size/depth; therefore, policy recommendations have to be offered cautiously. Furthermore, as noted, the environment plays a major role and thus all policies are contextually bounded.

Yet a few overarching lessons can be deduced from this study. Cybersecurity hot zones and sub-clusters grow where one of two conditions exists: an anchor organization (as with the NSA outside Washington) and/or where there is already a strong high-tech culture. Thus, if these conditions are met, the locale is likely to attract cyber firms within the cluster. Nurturing a new cybersecurity cluster is a long-term strategy, one that requires many years of patience, as in the case of the Be'er Sheva sub-cluster. The Be'er Sheva sub-cluster is located in proximity to a major university and military bases, but the evolving ecosystem that can support the sub-cluster is still in its infancy.

Another lesson is the role that regional and local municipalities play in the growth of the clusters. Municipalities initiate direct and indirect policies for industrial growth. Direct policies often include financial support to firms through tax concessions and grants. Other direct policies include the local advocacy initiatives (usually an office run by the local government) whose mission it is to advocate for the growth of the cluster. In the Washington area – at the state and local levels – there are several full-time, cyber-focused officials competing and collaborating with each other to bring cybersecurity businesses to their domain. Furthermore, regional governments can facilitate cyber-focused startup *accelerators*, such as Mach37 near Washington D.C. (and, outside the Big3 clusters, the 12F cyber accelerator in New York City). The indirect, yet important, policies support the built environment development through housing projects, infrastructure and other initiatives as a means of enhancing the area's image and attractiveness. Yet, these direct and indirect policies do not take place in a vacuum; rather they are part of the ongoing competition between regions and cities. Regional competition over the firms and human capital is a key factor that influences the growth of a cluster, even in small country like Israel. Thus, cluster growth requires more than a bundle of policies; it needs a cohesive strategic plan that will structure a set of direct and indirect policies for nurturing the industrial ecosystem in a place. Only with a holistic vision, which takes into account the social, economic and spatial context, can a cybersecurity cluster evolve and grow.

FURTHER READING

FURTHER READING

Cybersecurity Industry

1. Donaldson, Sam, Christian Stow, and Jonathan Hobson. "**UK Cyber Security Sectoral Analysis and Deep-Dive Review.**" Department for Digital, Culture, Media and Sport, June 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751406/UK_Cyber_Sector_Report_-__June_2018.pdf. This report offers an overview of the current state of affairs and overall economic contribution of the cybersecurity industry in the U.K. It suggests a framework for terminology and data collection, as well as potential policy recommendations and areas for further research.

2. Samtani, Sagar, Maggie Abate, Victor Benjamin, and Weifeng Li "**Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective.**" *Palgrave Handbook of International Cybercrime and Cyberdeviance*, Springer, 2019. This report provides a systematic review of existing CTI platforms within the cybersecurity industry today. It offers a perspective on a rapidly changing industry and possible areas of major growth going forward.

3. Cohen, Natasha, Rachel Hulvey, Jittip Mongkolnchaiarunya, Anne Novak, Robert Morgus, and Adam Segal. "**Cybersecurity as an Engine for Growth**." *New America*, September 2017. newamerica.org. A report on three case studies, U.K., Israel, and U.S., in an effort to understand what drives clustering of cybersecurity firms and growth of regional cybersecurity industries. The data is used to advance the discourse on cyber clusters in terms of policy intervention, culture, and other advantageous ecosystem characteristics which contribute to the initial development, growth and maintenance of cyber clusters.

4. Kelly, Douglas, "**The Economics of Cybersecurity**," in International Conference on Cyber Warfare and Security; Reading (Reading, United Kingdom: Academic Conferences International Limited, 2017), 522–529, https://search.proquest.com/docview/1897683119/abstract/6AB9E2E6226A434APQ/1. This paper discusses the economic impact of cybersecurity threats and the complexity of calculating appropriate public and private sector investment. It examines the "incentive dilemma" and other microeconomic dynamics unique to the cybersecurity industry in order to assess socially optimal levels of spending.

Economic Clustering

1. Porter, Michael E. "**Clusters and the New Economics of Competition**." *Harvard Business Review* 76, no. 6 (December 11, 1998): 77–90. This paper examines the seeming paradox of competitive advantages of geographic proximity and a global economy. Porter emphasizes the importance of location as a driver for innovation, efficiency and access to specialized inputs – advantages afforded to adjacent firms that cannot be matched by distant competitors.

2. Vinod K. Aggarwal and Andrew W. Reddie, 2018a. "**Comparative Industrial Policy and Cybersecurity: A Framework for Analysis.**" *Journal Of Cyber Policy*. vol. 3, no. 3, 291–305; and Aggarwal V. and Reddie, A.W.

2018b. "**Comparative Industrial Policy and Cybersecurity: The US Case,**" *Journal Of Cyber Policy*. vol. 3, no. 3, 445–46. These reports analyze the role of private sector firms, government institutions and other industry actors with regard to industrial policy in the most important nations in the world of cybersecurity. The report reviews on a number of countries, providing specific, distinct insights into each case.

3. Malmberg, Anders. "**Agglomeration,**" In *International Encyclopedia of Human Geography*, edited by Rob Kitchin and Nigel Thrift, 48–53. Oxford: Elsevier, 2009. http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-110510. This paper focuses on the notion of localization economies and the advantages gained by spatial clustering of similar or related firms. It reviews the mechanisms held to comprise the concept of agglomeration economies and discusses their full lifecycle evolution.

4. Wood, Stephen, and Kim Dovey. "**Creative Multiplicities: Urban Morphologies of Creative Clustering.**" *Journal of Urban Design* 20, no. 1 (January 1, 2015): 52–74. https://doi.org/10.1080/13574809.2014.972346. This paper studies the urban morphology of creative clusters by mapping particular creative industry components in Australian case studies. It discusses the necessary synergies created by a "mix of mixes" and further discusses the cluster effect produced by co-location of a multiplicity of functions, people, industries, and built-form.

5. Feldman, Maryann, Johanna Francis, and Janet Bercovitz, (2005), "**Creating a Cluster While Building a Firm: Entrepreneurs and the Formation of Innovative Clusters.**" *Regional Studies*, 39: 129–142. This paper aims to outline a theoretical model of cluster development based on case study analysis with a focus on the critical, foundational role of entrepreneurs. It sheds light on external factors that help spark early development of innovation clusters.

6. Scott, Allen. "**The Mainsprings of Urban Economic Performance,**" in *The Cultural Economy of Cities: Essays on the Geography of Image-Producing Industries*, 16–29. London: SAGE Publications Ltd, 2000. https://doi.org/10.4135/9781446217481. A discussion of co-location's competitive advantage in creative industries. The paper highlights the linkages between creative industries and their urban-industrial clustering and illustrated why global cities are centers for contemporary creative economies.

7. Temouri, Yama, "**The Cluster Scoreboard: Measuring the Performance of Local Business Clusters in the Knowledge Economy**," OECD iLibrary, accessed May 27, 2020, https://read.oecd-ilibrary.org/industry-and-services/the-cluster-scoreboard_5k94ghq8p5kd-en. This study assesses and compares the performance of key high-tech and knowledge-based clusters before and during the global economic recession of 2008. It notes that clusters commonly had significant shifts in their performance from pre-recession to recession periods, indicating there are different characteristics for success during economic booms and busts.

8. Hatuka, Tali, "**Facing Forward: Trends and Challenges in the Development of Industry in Cities**." *Built Environment* vol. 43 (March 6, 2017): 145–55, https://doi.org/10.2148/benv.63.3.145. The paper outlines some of the developments and trends associated with the "Fourth Industrial Revolution" with a focus on three main themes: technology, manufacturing, and cities. Three interlinked dimensions are viewed as crucial to the development of industrial areas in cities: geographic proximity, localism, and planning regulations.

San Francisco Bay Area Cluster

1. McNeill, Donald, "**Governing a City of Unicorns: Technology Capital and the Urban Politics of San Francisco**," *Urban Geography* 37, no. 4 (May 18, 2016): 494–513. This report empirically explores municipal governance in San Francisco, specifically the direct involvement of tech investors in recent municipal elections. It also examines and discusses the growing influence of technology firms and the industry overall on management and planning at the city level.

2. Casper, Steven, "**New-Technology Clusters and Public Policy: Three Perspectives**," *Social Science Information* 52, no. 4 (December 1, 2013): 628–52. This article analyses three potential catalysts for development of innovation clusters: universities and academic institutions, social networks, and institutions. The discussion that follows explores the individual roles of each element, as well as their relation to each other, as well as potential policy perspectives.

3. Engel, Jerome S., "**Global Clusters of Innovation: Lessons from Silicon Valley**," *California Management Review* 57, no. 2 (February 1, 2015): 36–65. This article examines the role of innovation and entrepreneurialism in the growth of technology clusters, offers an in-depth analysis of the networks created by government, academic institutions, NGOs, and major corporations, and concludes with a discussion on potential government policy to support growth of tech clusters.

4. Florida, Richard, "**Why San Francisco May Be the New Silicon Valley**" *CityLab*, August 5, 2013 https://www.citylab.com/life/2013/08/why-san-francisco-may-be-new-silicon-valley/6295/. This article brings to light the shift from a single-nucleus cluster in Silicon Valley to a bi-modal pattern, with sub-clusters in Silicon Valley and downtown San Francisco. It highlights a suburban to urban shift of innovation, creative industries and the creative class associated with them.

Washington D.C. Area Cluster

1. Aberman, Jonathan, Erran Carmel, Michael Hoffman, Jeffrey Blair, Drew Bailey, Sam Woods, and Rhys Leahy. "**From Service to Product: An Assessment of the Washington, DC Metro Region's Cybersecurity Industry.**" April, 2017, Center for Business in the Capital, American University. This report identified 858 Washington cybersecurity businesses, finding that a very high ratio of service and solution-based business models. Only 5% of the firms were focused solely on developing cybersecurity products.

2. Carmel, Erran, Bini Byambasuren, and Jonathan Aberman. *Cybersecurity Startup Founders in the Greater Washington Region: Prior Experience Required.* April 2018. Center for Business in the Capital, American University. This study examines the entrepreneurial founders of Washington D.C.'s pure-play cyber firms, of whom almost three quarters (72%) had at least one founder with prior experience as either a vendor to the government or as a government employee.

3. Mayer, Heike, "**What Is the Role of Universities in High-Tech Economic Development? The Case of Portland, Oregon, and Washington, DC**," *Local Economy* 21, no. 3 (August 1, 2006): 292–315. Through analysis of two case studies – Portland, Oregon and Washington, D.C. – this paper examines the growth of regional technology sectors in the absence of a major research university. The author confirms the strength of the triple-helix model but questions the degree to which universities play an essential role in cluster development.

Israel Cluster

1. De Fontenay, Catherine and Erran Carmel, 2004. "**Israel's Silicon Wadi: the forces behind cluster formation**," in T. Bresnahan, A. Gambardella, and A. Saxenian, (eds.) *Building High Tech Clusters*, Cambridge University Press. This paper highlights Israel's competitive advantages leading to the development of the local high-tech innovation cluster. It discusses both long-existing and recently developed advantages related to the private sector, government, military and institutions.

2. Engel, Jerome S., and Itxaso Del-Palacio, 2011. "**Global Clusters of Innovation: The Case Of Israel And Silicon Valley.**" *California Management Review* 53.2 (2011). Through an examination of case studies in Israel and Silicon Valley, this paper aims to build on a previous work which analyzed clusters of innovation and their global connectivity. It focuses on key characteristics of these two regions and how they use global connectedness to enhance their competitive advantage and bolster local industry.

3. Adamsky, Dmitry (Dima), "**The Israeli Odyssey toward Its National Cyber Security Strategy**," The *Washington Quarterly* 40, no. 2 (April 3, 2017): 113–27. This paper explores the underlying holistic political strategy behind Israel's rise as a cybersecurity leader. Through analysis of the Israeli case, this article aims to provide policy and strategy insights that are more broadly applicable to other nations and regions.

4. Fraiberg, Steven, "**Start-Up Nation: Studying Transnational Entrepreneurial Practices in Israel's Start-Up Ecosystem**," *Journal of Business and Technical Communication* 31, no. 3 (July 1, 2017): 350–88. This paper focuses on high-tech entrepreneurs in the Israeli technology and innovation sector. It examines the culture of innovation and the network elements set up by and supportive of entrepreneurs as critical to development of the Start-up Nation.

5. Kon, Fabio et al., "**A Panorama of the Israeli Software Startup Ecosystem**," *SSRN Electronic Journal*, 2014. This paper uses Israel as a tech and innovation case study to explore vital elements of successful innovation ecosystems. The research and discussion provide answers and insights on "questions related to sociocultural, institutional, technological, methodological, and educational aspects of entrepreneurship, startups, and their ecosystem."

BIBLIOGRAPHY

Aberman, Jonathan, Erran Carmel, Michael Hoffman, Jeffrey Blair, Drew Bailey, Sam Woods, and Rhys Leahy. “From Service to Product: An Assessment of the Washington, DC Metro Region’s Cybersecurity Industry.” April, 2017, Center for Business in the Capital, American University.

Carmel, Erran, Bini Byambasuren, and Jonathan Aberman. Cybersecurity Startup Founders in the Greater Washington Region: Prior Experience Required. April 2018. Center for Business in the Capital, American University.

Cohen, Natasha, Rachel Hulvey, Jittip Mongkolnchaiarunya, Anne Novak, Robert Morgus, and Adam Segal. “Cybersecurity as an Engine for Growth.” New America, September 2017. newamerica.org.

Donaldson, Sam, Christian Stow, and Jonathan Hobson. “UK Cyber Security Sectoral Analysis and Deep-Dive Review.” Department for Digital, Culture, Media and Sport, June 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751406/UK_Cyber_Sector_Report_-__June_2018.pdf.

Engel, Jerome S., and Itxaso del-Palacio. “Global Clusters of Innovation: The Case of Israel and Silicon Valley.” *California Management Review* 53, no. 2 (February 2011): 27–49. https://doi.org/10.1525/cmr.2011.53.2.27.

Florida, Richard, and Karen M. King. “Rise of the Urban Startup Neighborhood: Mapping Micro-Clusters of Venture Capital-Based Startups | Martin Prosperity Institute.” Accessed July 28, 2020. http://martinprosperity.org/content/rise-of-the-urban-startup-neighborhood/.

Katz, Michael L., and Carl Shapiro. “Network Externalities, Competition, and Compatibility.” *American Economic Review* 75, no. 3 (June 1985): 424.

Malmberg, A. “Agglomeration.” In *International Encyclopedia of Human Geography*, edited by Rob Kitchin and Nigel Thrift, 48–53. Oxford: Elsevier, 2009. https://doi.org/10.1016/B978-008044910-4.00131-0.

Marcus, Alan, Derek O’Halloran, Elena Kvochko, and Roshan Vora. “Risk and Responsibility in a Hyperconnected World.” World Economic Forum in collaboration with McKinsey & Company, January 2014. http://reports.weforum.org/hyperconnected-world-2014/wp-content/blogs.dir/37/mp/files/pages/files/final-15-01-risk-and-responsibility-in-a-hyperconnected-world-report.pdf.

Porter, Michael E. “Clusters and the New Economics of Competition.” *Harvard Business Review* 76, no. 6 (December 11, 1998): 77–90.

Temouri, Yama. “The Cluster Scoreboard: Measuring the Performance of Local Business Clusters in the Knowledge Economy,” August 1, 2012. https://doi.org/10.1787/5k94ghq8p5kd-en.

West, Tobi, and Aeron Zentner. “Managing Security Risks: An Assessment of U.S. Critical Cyber Infrastructure Protection,” November 10, 2019. https://doi.org/10.2139/ssrn.3484552.