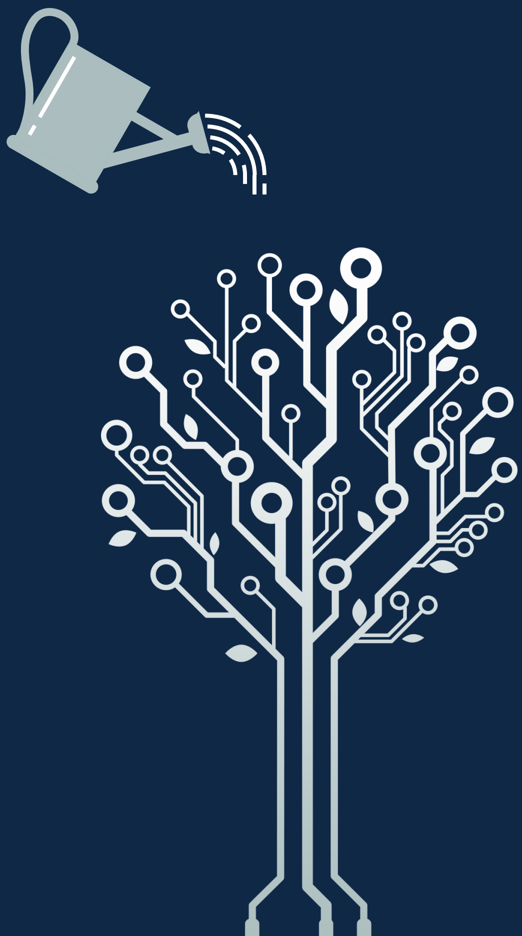
Cybersecurity Startup Founders in Greater Washington, DC

Prior Experience Required

Erran Carmel & Bini Byambasuren,
The Center for Business in the Capital

Jonathan Aberman, TandemNSI



KOGOD
SCHOOL of BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC

EXECUTIVE SUMMARY

The Greater Washington region is one of three leading cybersecurity industry clusters in the world. The proximity of this region to federal agencies, particularly in national security, has created a vibrant ecosystem linking talent and businesses with federal and commercial customers. National security agencies, such as the National Security Agency and the Defense Advanced Projects Research Agency, are a specific driver of cybersecurity research and development. Collectively, these favorable conditions support a broad array of businesses that contract with the federal government and provide cybersecurity innovations to commercial customers around the world.

To better understand the composition of the Greater Washington region's cybersecurity business base, this study differentiates between the more than 850 cybersecurity businesses in the region identified by us in a prior study that did at least some cybersecurity business and focuses more squarely on those that work only in cybersecurity. We describe these businesses as "pure play" cybersecurity firms. Our study examined the roots of pure-play cybersecurity firms by examining the background of their founders. We collected data on 177 pure-play cyber firms – and their founders – in the Greater Washington region (61% of the firms are in Northern Virginia and the rest in suburban Maryland and Washington D.C.). We believe that our dataset represents close to a census of such firms in this region. In these firms, there are 264 founders (48% of the firms have just one founder).

There is clearly a premium placed on prior experience in the national security ecosystem. Almost three quarters (72%) of the pure-play cybersecurity firms had at least one founder with prior experience as either a vendor to the government or as a government employee. And in more than half of these firms (52%) this experience was a direct result of government service. This validates those who have previously argued that there is a close connection between Greater Washington region cybersecurity startups and the national security ecosystem. It also distinguishes the region from competing cybersecurity clusters such as Silicon Valley.

Additionally, the premium on locally gained experience makes the Greater Washington region's pure play cybersecurity startup ecosystem very much a local industry: 78% of founders worked in Greater Washington prior to founding the firm.

Our research provided some other important insights. More than a quarter (26%) of founders founded at least one firm prior to their current business. Observers of innovation-based economic development often tie the long-term viability of a region as a tech hub to its ability to generate serial entrepreneurs. We also saw less impact from universities than what prevails in competing regions, as only 8% of founders emerged from university work. Demographically, female founders represented 8% of all founders, which underscores the shortfall of women in technology leadership roles since women are more than a fifth (22%) of all cybersecurity workers.

Undoubtedly, understanding how our region's cybersecurity businesses are established and grow is important. Findings from the Greater Washington Partnership contend that cybersecurity contributes $14 billion in annual economic impact to the region and can increase the region's annual GDP growth by 11-18%. There are already about 300,000 cyber related jobs in the region.

In that light, what can we make of our study's findings? The results tell us quite clearly that the source for cyber innovation and entrepreneurship in this region are still very much rooted in U.S. national security ecosystem. It is this breeding ground that should be tapped and accelerated even more to create the dynamism of the cybersecurity industry in the region.

GETTING TO A BETTER UNDERSTANDING OF GREATER WASHINGTON'S CYBERSECURITY INDUSTRY

The density of activity in the Greater Washington's cybersecurity industry places the region squarely as one of dominant cybersecurity clusters in the world.[1] The region has a large concentration of cybersecurity workers.[2]

Prior research that we have undertaken shows that the Greater Washington region had close to 900 cybersecurity related businesses[3]. Our work, as well as recent studies undertaken by the Greater Washington Partnership[4] and employment data available from private sources, show a clear density of cybersecurity employment.

The key insight from this report is that the proximity to the federal government seeds cybersecurity businesses. Observers of this region's businesses knew this anecdotally – and now there are data in this report to support this.

The U.S. federal national security (NS) ecosystem has two main elements: government NS organizations such as those that appear in the sidebar and government-focused services vendors that contract with the U.S. government to address cybersecurity needs. We wanted to find out what impact do entrepreneurial founders' NS roots have on the establishment of cybersecurity firms in the region.

DHS – Department of Homeland Security
NSA - National Security Agency
CIA – Central Intelligence Agency
DIA - Defense Intelligence Agency
FBI – Federal Bureau of Investigation
DOD --Department of Defense
NGA - National Geospatial-Intelligence Agency
DARPA – Defense Advanced Research Project Agency

To evaluate both questions we returned to our data on the Greater Washington region's cybersecurity businesses and narrowed our focus to 177 pure-play cybersecurity businesses.

[11] The Big 3 cybersecurity clusters are Silicon Valley (including the entire San Francisco Bay Area), the Washington D.C. region, and Israel, with clusters in New York city, Boston and London also generated significant density of activities. This ranking is based on vc funding and the CS500.

[2] Greater Washington Partnership, Partnering to Strengthen Tech Talent In The Capital Region, December, 2017, found that the "Capital Region is home for ~15% of cybersecurity jobs in the US, with ~3 times more jobs than second region, NY" and that the "DC metropolitan area also has the highest density of cybersecurity jobs (4 per 1K population)."

[3] Carmel, Erran et al. 2017. From Service to Product: An Assessment of the Washington, DC Metro Region's Cybersecurity Industry.

[4] Greater Washington Partnership, ibid.

NATIONAL SECURITY EXPERIENCE CREATES BUSINESS FOUNDERS

In evaluating the pure play cybersecurity businesses, we were able to identify the composition of the founding teams in 160 of these 177 businesses. We identified 264 business founders among these companies. We identified that many of the founders had a relationship and progression from national security (NS) organizations and the formation of pure-play cybersecurity businesses. This was indicated by a founder's prior experience in cybersecurity through either prior employment in a NS work in the U.S. government or as a member of a cybersecurity business acting as a vendor/contractor to a NS function in the U.S. government.

What we learned is summarized in the table below:

Key data on 160 cybersecurity firms and their founders in Greater Washington D.C.[5]

	Percent	Number
National security experience in government/ military/ intelligence. There is at least one founder in the firm with this type of experience.	53%	84
National security experience with government vendor. There is at least one founder in this firm with this type of experience.	52%	83
Either kind of national security experience. At least one of the firm's founders has either of the above two elements of NS experience.	72%	115
The founders of the firm have *both* kinds of national security experience represented among them.	33%	52
All the firm's founders have some kind of national security experience	53%	85
Knows cyber. At least one of the firm's founders has cyber experience prior to founding this firm	88%	141
Local roots. At least one of the firm's founders worked in greater Washington D.C. before founding this Washington cyber firm	87%	139
Serial entrepreneur. At least one of the firm's founders has experience starting at least one firm before this	35%	57
University hatching? At least one of the firm's founders has university employment / research experience in cyber	13%	21

National security experience matters. *72% of the firms had at least one founder with some experience in the National Security ecosystem. This is the most powerful result of this study.* The cybersecurity ecosystem is very closely rooted in the Washington cybersecurity ecosystem "boot camp" of national security work.

[5] Of the 177 firms, there was meaningful founder data on 160 firms.

More specifically, 53% of the firms were founded by at least one founder who had NS experience in government – such as US military cyber positions, NSA, U.S. Department of Homeland Security. And 52% of the firms were founded by at least one founder who had experience with vendor organizations – from large defense contractors with major cyber workor smaller, more specialized firms. One third of firms had at least one founder with both types of NS experience. At about one half of the firms (53%), *all* the founders had NS experience.

The NS roots appear even more important to rise to prominence from this region. The Cybersecurity 500 (CS 500) lists the most prominent firms globally. [6] 32 of the 177 Washington firms are in the 2017 CS 500 list. Of these firms 65% have founders with some national security experience (compared to 53% of the entire pool of companies).

The data revealed several more important items:

Business formation comes from within. 87% of these pure-play cybersecurity businesses were founded by people who were already resident of the Greater Washington region. This is not surprising considering the strong relationship between prior national security experience and technical expertise in these business' formation.

The region's cybersecurity innovation ecosystem may be developing a sustainable entrepreneurial culture. One third of the firms (35%) had at least one serial entrepreneur in its ranks as co-founder. Our data also hint anecdotally that many of these serial entrepreneurs had done more than two startup businesses in their career to date.

Universities have to play a bigger role. While the Greater Washington region's universities and community colleges represent the largest national source of accredited national security talent, they are not yet seeding many cybersecurity businesses. Only 13% of all these businesses had any apparent connection to a university, through any founder, either through commercialized research or direct business incubation by a founder (and as we noted above, only 8% of all 264 founders).

[6] Cybersecurity 500.

Key data on the entire pool of 264 **founders** of Greater Washington D.C. cybersecurity companies

The founder has….:

	Percent	Number
national security experience in government/ military/ intelligence	43%	112
national security experience with a government vendor	43%	112
either kind of national security experience	63%	166
both kinds of national security experience	21%	55
cyber experience prior to founding this cyber firm	78%	205
local roots, by having worked locally, in Greater Washington D.C., before founding of local cyber firm	77%	203
become a serial entrepreneur, by having experience starting at least one firm before this firm.	26%	67
Cyber-related university employment / research experience	8%	22

We also looked at the entire pool of founders – there were 264 founders and co-founders. 63% of these individuals had some kind of national security experience. More specifically, 43% of all founders had worked for government national security (DHS, NSA, etc.) And 43% of all founders had worked for vendors. 21% of the founders had worked for *both* the government and the contractors – in a progression that many see as classic Washington – government to contactor to startup – but is not as common as we think.

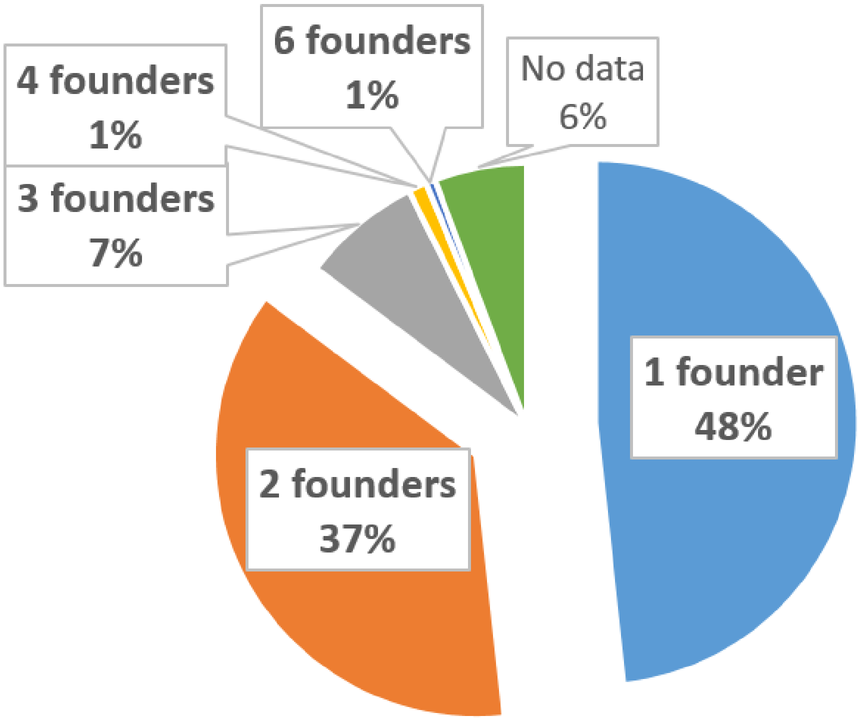
Although cybersecurity is a highly technical area in which to start a business, close to a quarter (22%)of the founders had no cybersecurity experience. This somewhat surprising percentage is mitigated by two factors. Some of these founders were paired with co-founders with cybersecurity experience. In other cases, the firms are older firms (often from more than 10 years ago) that launched as network and I.T. firms and evolved, over time, into cyber firms.

Also, of all founders and co-founders in the pool: 77% of founders were local (15% came from outside; 8% incomplete data). 26% of were serial entrepreneurs[7], and only 8% of entrepreneurs had some cybersecurity employment or research roots in universities.

[7] Even more serial entrepreneurs: Interestingly, we also noticed quite a few entrepreneurs who became serial entrepreneurs once they founded this cybersecurity firm in question. That is, they got the itch to do this again, though we do not have data on their actions after the original founding.

Additional Insights: Number Of Founders

It is often remarked that entrepreneurship is a lonely activity, and that founders should not start businesses without at least one partner. The business formation history of the pure-play cybersecurity businesses suggests that its founders heed this advice. About half of these firms were founded by two or more founders; and in one unusual case (IronNet) there were six founders.



Number of founders per firm
in greater Washington cyber companies

Additional Insights: Venture Capital and Mergers & Acquisitions

Participants in the Greater Washington region will often state that there is insufficient venture capital available to grow cybersecurity businesses.[8] Our data cannot address whether this anecdotal statement is correct. Seemingly, the data suggest that vc has only a light touch here: only 28 out of these 177 cybersecurity businesses – approximately 16% -- have at least some venture capital funding. Rephrased, a substantial majority of the region's cybersecurity business emerged without venture capital. But this shouldn't be surprising, since many of these regional firms are in services and solutions that service the federal government and are able to achieve cash flow positive and profitable operations without external capital.

Interestingly, the composition of businesses that obtained venture capital were not materially different from the ones that didn't. Of the vc-backed cyber firms, 78% have founders with some national security experience and 22% of the total had founders with both kinds of national security experience among the founders. Thus, in most cases, national security experience matters for both vc-backed and non vc-backed. We suspect that is because unlike some other technology areas, the cybersecurity industry requires client expertise to attract customers and develop tangible offerings.

Venture capitalists are a bit more selective in demanding cybersecurity content experience: 24 of these 28 vc-backed cyber firms had at least one founder with prior cyber experience (for one firm there is no data). Put differently, 7% of vc-backed cyber firms have founders with no cyber background.

Because vc investors see M&A exits as essential to achieving their financial objectives, we looked at the exit activity of the pure-play businesses. We identified 16 exits among the pure-play 177 businesses – 9% or all businesses.

[8] In 2017 venture capitalists invested $1.55 billion into D.C. area, representing a six-year high for technology investing (Source: Washington Post, 2018).

Additional Insights: Product, Service, Solution

We parsed the firms by product, solution, service – as we did in prior studies.

Our prior study of the region’s cybersecurity industry showed that only 5% of all businesses were solely engaged in delivering cybersecurity products to customers. When we looked at just pure-play businesses in this report, this percentage increased to 11% of companies, with the remainder engaged in solutions (56%) and services (33%). While the percentage of product-based businesses is higher (11% versus 5%), when compared with other leading cybersecurity regions Washington D.C.’s pure-play businesses have a very different profile and lean towards solution and services. In particular, the services firms represent the stereotypical government contracting businesses in the Washington area -- that are less frequent in other large cybersecurity clusters.

The key ecosystem indicators stay roughly aligned in these three types—products, solutions, services.   For example, there are at least one founder with NS experience in government in 50% of the product firms and 63% of the solutions firms.

Finally, we expected that service firms would have larger proportions of firms with founders with no cyber background. This wasn't the case. While 3 of the *product* firms had no cyber/founder experience -- only 8 of the companies in the larger *services* sector has inexperienced founders. Thus, lack of cyber experience seems to be roughly evenly distributed across a number of sub-segments and seems to be un-illuminating.

ADDITIONAL INSIGHTS: GEOGRAPHICAL DISTRIBUTION

The roots of the regional industry are in the government contracting firms that began to do cybersecurity work as part of their larger national security portfolio – the likes of Booz Allen and SRA. The U.S. Federal cybersecurity market is estimated to reach $22 billion by 2022, growing at 12% CAGR. Most of these dollars stay in the Washington region.

Given that the defense-oriented industries have traditionally been concentrated in the Northern Virginia suburbs -especially along the Tysons to Dulles axis-- it is not surprising that most, 61%, of the pure-play companies are in Northern Virginia.

Geographical distribution in the region

	All companies engaging in cyber[9]	Pure-play companies
Northern Virginia	535	108
Maryland suburbs	278	56
Washington, D.C.	45	13

[9] Carmel, Erran et al. 2017. From Service to Product: An Assessment of the Washington, DC Metro Region's Cybersecurity Industry, ibid.

ADDITIONAL INSIGHTS: WOMEN FOUNDERS OF CYBERSECURITY FIRMS

While women are estimated to make up about 20% of the cybersecurity workforce[10] their representation as regional company founders is lower. 22 of the entrepreneurial founders are women founders, representing 8% of all founders.

10 firms were founded solely by women—and all such cases had one founder (rephrased—there were no firms co-founded, for example, by two women). 11 firms were founded by mixed gender teams: all were one woman with one man, except for one unusual case, Mindpoint, founded by two men and two women. Two of the mixed-gender founder teams were founded by husband-and-wife teams.

Importantly, women had much higher likelihood then men to have had work experience in the Washington NS ecosystem. Only one of the women did not come out of that ecosystem.

7 of the 22 women are women of color (with 2 instances for which we do not have data) . 7 of the 22 women were serial entrepreneurs. And 6 of the 22 women majored in STEM (but for 5 we have no data). Finally, 11 of the women are in women-certified firms (for purposes of government contracting).

[10] Women in Cybersecurity, Q1 2018, published by Cybersecurity ventures.

Capsules of a cross-section of regional firms focusing on their founders' pedigrees.

Founders with NS experience:

- **IronNet** was co-founded by former NSA Director Keith Alexander. Appropriately, the HQ is a new office park not far from the NSA.
- An alumnus of both the NSA and government contractor (**Northrop Grumman**) Len Moodispaw founded **KeyW** (2008) as a government contractor. The company had a $91 million initial public offering in 2010 and had 1000 employees by 2014.
- **Dragos'** founders have deep NS roots -- and founded the firm in a specialized local incubator, **Datatribe**, which focuses on firms that come out of national security/ cybersecurity. Dragos focuses on SCADA: industrial systems that are used by Siemens, Honeywell, and ABB with operating systems that last for many years, usually unpatched.
- **Centroid** has about 15 employees, which are focused on writing cyber software. It is veteran-owned, with its key co-founder having worked in several government contractors prior to starting his own firm.
- **American Cyber** was co-founded by a husband-and-wife team with one of them having NS experience. The firm is focused on government contracts in cyber.
- **Dependable Global Solutions**, with several dozen employees, made it into the 2017 Inc 5000 fastest growing private firms. Both co-founders have NS experience as government contractors prior to founding the firm in 2005
- **Looking Glass**, a cyber services company, was founded in 2006 by two founders-- only one has NS experience -- as a contractor. The company has grown via acquisitions. It provides a service that protects government agencies and businesses from cyberattack, raising $50 million in a series-C round in 2015, augmented with a smaller round in 2017.

Firms with *no* founder NS experience:

- Two founders founded **Phishme** in 2011 with no NS experience but extensive cyber experience. The firm received successive vc rounds including Series C at $42 million. It was acquired in early 2018 and changed its name to **Cofense**.
- All three founders of **Distill Networks** have no NS experience. The firm now has a dual-HQ model with HQ in DC and also San Francisco. The firm raised $65 million in venture capital. Its products protect websites from harmful "bot" traffic and has 400+ customers.
- **Thycotic**'s founder had no NS experience and now has 7500 organizational customers worldwide.
- Only one of three founders at **Tenable Network Security** (founded in 2002) had NS background. But, recently the firm brought in a CEO with deep Washington NS chops, Amit Yoran, who served as Founding Director of the United States Computer Emergency Readiness Team (US-CERT) program in the U.S. Department of Homeland Security.
- Other well-known regional firms with no national security roots are **Threat Connect** and **Paraben**.

APPENDIX A: METHODOLOGY

The dataset consists of 177 *pure* cyber firms from the Washington metropolitan region. We believe that our dataset represents close to a census of such firms in this region through 2017.

The original dataset included 858 cyber security businesses identified by Carmel et al. (2017). This was narrowed down to 177 pure-play (or mostly cyber) firms.[11] Firms of two employees or less were eliminated.

Founder biographical data came predominantly from LinkedIn and the firms' own websites, and in less frequent cases, from news sources.

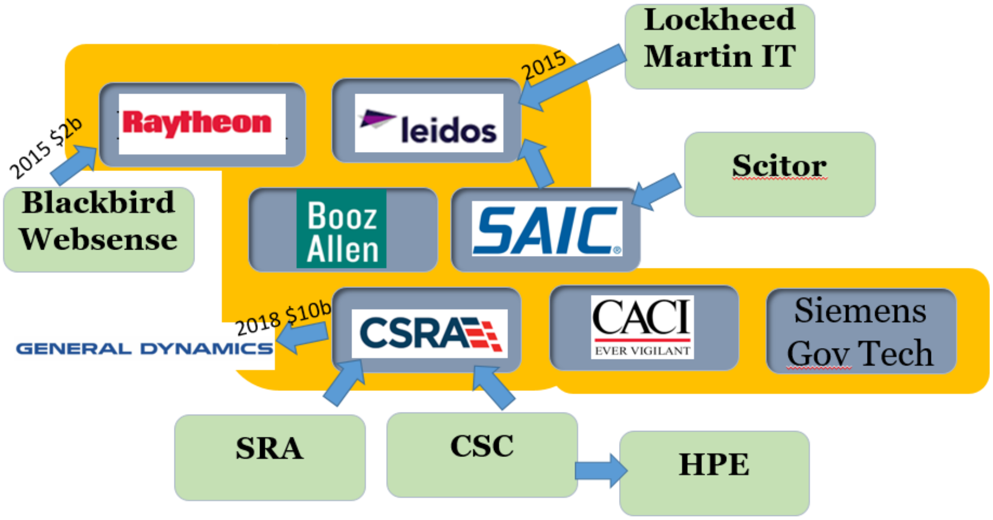
Government certification came from Company website, Fedspending.org, Federal Procurement Data System (https://www.fpds.gov), and Govtribe.com; venture capital data came from company website.

[11] Pure players are those that offer products or services specialized in the field of cyber security as opposed to that of information, computer and technology. We define mostly cyber firms as those that perform roughly ½ (or more) of their products and/ or services in cybersecurity. In this way, we hope to exclude IT companies with cybersecurity being a small fraction of what they do.

APPENDIX B: THE GREATER WASHINGTON D.C. CYBER INDUSTRY BACKGROUND AND ECOSYSTEM

The roots of the regional industry are in the government contracting firms that began to do cybersecurity work – the likes of Booz Allen and SRA. The U.S. Federal cybersecurity market is estimated to reach $22 billion by 2022, growing at 12% CAGR. Most of these dollars stay in the Washington region.[12]

A stylized illustration of key large national security focused cyber firms appears below. However, note that most of these firms are not pure cyber firms. Rather they engage in a wide range of national security / defense activities, including building jets, rockets, or managing troop deployments in dangerous locations.



These big government contractors have gone through a pendulum swing on cybersecurity: first acquiring cyber assets after 2010, then shedding them, and now acquiring them once again.

The original government-focused cyber firms have re-aligned in recent years. Today, key firms include Leidos, Booz Allen, General Dynamics/CSRA, SAIC, and CACI International. Raytheon's cyber division is called Forcepoint and is made in part from assets of the acquired firms Blackbird and Websense. Leidos cyber business came from blending Lockhead Martin and SAIC assets. CSRA cyber came from CSC and SRA. Boeing has reduced its cyber activities selling off much of its Narus division. General Dynamics spun off its Fidelis division, but then acquired CSRA with its cyber assets in 2018. And Northrup Grumman spun-off its cyber as Blue Vector. Two European firms, Siemens and BAE, are also important cyber government contractors. Somewhat smaller defense contractors that do cyber are ManTech International Corporation, Engility Corporation, L-3 Communications. The government/defense contractors that spin off cyber divisions tend to stay in the DC area: Blue Vector, Fidelis, and Forcepoint – all with large defense "mothers" – all remain in the region.

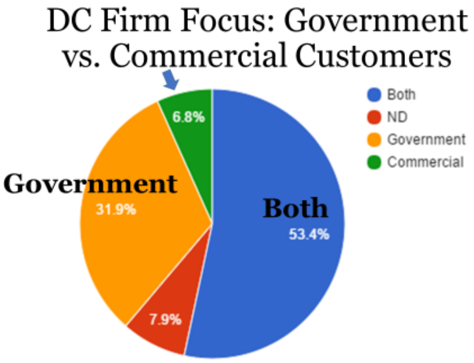
[12] Market Research Media, U.S. Federal Cybersecurity Market Forecast 2017-2022, February 2018

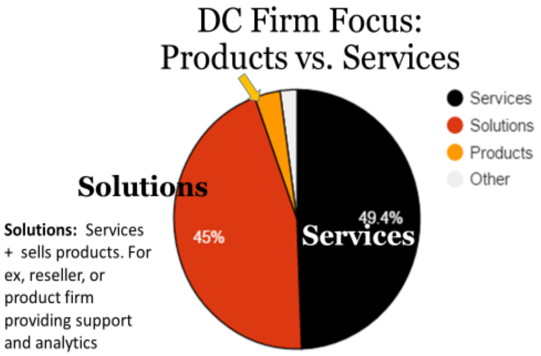
In parallel to the larger national security activity, cybersecurity firms emerged which are focused on the commercial sector or sell products – or both.   These firms tend to be more like the cyber firms that have been successful out of Silicon Valley and Israel.

In addition, the region has some specialized cybersecurity resources:

- Strategic Cyber Ventures (SCV), a DC-based venture capital firm focused on the cybersecurity industry. Has 4 firms in its portfolio
- Mach 37 is a cyber accelerator founded in 2015 that has funded about 50 firms through its pipeline.
- DataTribe (mentioned above) is a specialty incubator and for cyber firms founded in 2016.

A broader perspective on the region's cybersecurity industry can be found in our 2017 study, which is summarized in the pie charts below. The overwhelming majority of companies are in services and solutions and correspondingly, few of the firms are focused on the commercial market while 31% of the companies are solely focused on government contracts. See exhibits with pie charts below.





Solutions: Services + sells products. For ex, reseller, or product firm providing support and analytics

REFERENCES

- Erran Carmel, Jonathan Aberman, Michael Hoffman, Jeffrey Blair, Drew Bailey, Sam Woods, Rhys Leahy, From Service to Product: An Assessment of the Washington, DC Metro Region's Cybersecurity Industry April 6, 2017, American University, Kogod School of Business. https://www.american.edu/kogod/research/publications/upload/Kogod-Cybersecurity-Report-2017.pdf1
- Cybersecurity ventures; Women In Cybersecurity, Q1 2018, https://cybersecurityventures.com/women-in-cybersecurity/
- Cybersecurity ventures; Cybersecurity 500. https://cybersecurityventures.com/cybersecurity-500/
- Greater Washington Partnership, Partnering to Strengthen Tech Talent In The Capital Region, December, 2017, found that the "Capital Region is home for ~15% of cybersecurity jobs in the US, with ~3 times more jobs than second region, NY" and that the "DC metropolitan area also has the highest density of cybersecurity jobs (4 per 1K population)." http://www.greaterwashingtonpartnership.com/wp-content/uploads/2017/09/GWP_tech_report_final_12_124.pdf
- Market Research Media, U.S. Federal Cybersecurity Market Forecast 2017-2022, February 2018, https://www.marketresearchmedia.com/?p=206
- Washington Post, January 2018, Capital Business, D.C.-area technology investment soared in 2017, but early-stage firms still struggle. https://www.washingtonpost.com/business/capitalbusiness/dc-area-technology-investment-soared-in-2017-but-early-stage-firms-still-struggle/2018/01/14/6dc4e5ae-f730-11e7-a9e3-ab18ce41436a_story.html?utm_term=.c72f487021f1

About the Center for the Study of Business in the Capital

The Kogod School of Business established its "Business in the Capital" center to provide insight on key regional issues and start productive conversations about improving the Greater Washington business climate. Kogod is committed to sharing its research and expertise with policy makers and business leaders to build the economy of the Greater Washington region.

The Center also benefits the future business leaders we are training in our classrooms. As the DC area's oldest business school, Kogod has been educating students for over 75 years, many of whom stay and contribute to the regional economy. The Business in the Capital Programs – research papers, industry discussions, speakers and events – create even stronger bonds between our school and local businesses to better prepare our students to work in Washington and the world.

About TandemNSI

Tandem National Security Innovations helps government agencies discover breakthrough innovations to solve national security challenges. It is based in Arlington, Virginia.

Acknowledgements

We thank our Research Assistants at American University for helping to gather the data: Omer Kaufman, Hannah Farley.

<end>

AMERICAN UNIVERSITY
WASHINGTON, DC