INTERVIEW

Interview of Brian Murphy, Former Chief of Intelligence, Department of Homeland Security*

Laura Fraedrich**

Background: Brian Murphy has just wrapped up a decorated twenty-five-year career in the government, which included five years in the Marine Corps, followed by twenty years in the FBI. Brian's career in the government recently concluded with a stint at the Department of Homeland Security, where he was the Chief Intelligence Officer, Chief Information Sharing Officer, and Chief Counterintelligence Officer for the department. M. Murphy also became the highest-ranking whistleblower in US government history in 2020 when he said he was told to stop discussing the threat of Russian interference in the 2016 Presidential election and to highlight the role of left-wing groups in anti-racism protests. All of these experiences provide him with a unique view about the intersection of national security and international trade issues.

1 Tell us about your career path

I graduated from the College of William and Mary with a government degree in 1994 and began working for the federal government as an officer in the Marine Corps. I then served as a special agent in the Federal Bureau of Investigation (FBI) from 1998–2018. My first assignment was at the New York FBI field office. I served in six additional offices and one embassy (in Algiers) during my twenty-year career at the FBI, having started as a street agent and concluding as a Senior Executive Service officer. While in the FBI, I was responsible for both criminal and national security threats. I took military leave while in the FBI and rejoined the U.S. Marine Corps for a tour in Iraq in 2004.

In 2006, I earned an Master of Arts in Islamic studies from Columbia University to add an academic perspective to my national security work. From 2018 until September 2021, I worked as the principal deputy and acting under secretary for intelligence at the Department of Homeland Security. I served as the Chief Intelligence Officer, Chief Information Sharing Officer, and Chief Counterintelligence Officer for the department. I am a Certified Intelligence Community Intelligence Officer and am Joint Duty Certified by the Director of National Intelligence.

In 2003 and 2007, I received the Attorney General's Award for Excellence in Investigations. I also am currently an adjunct professor and a Doctoral Candidate at Georgetown University.

2 How does this align with what you thought you might do when studying government at William and Mary and what advice do you have for students who might want to work in the national security field?

While at William and Mary I can't say I had a clear plan on where I wanted to go with my career. I knew I was interested in public service and national security. Looking back, a degree in government makes sense. My advice to students interested in the field is not to wait for the 'perfect' job in the government, but instead find a good one. Once you are in, it is much easier to move around.

Notes

* Interviewed by Laura Fraedrich, Lowenstein Sandler, Washington, DC, GTCJ Editorial Board Member. For more information, *see* https://abcnews.go.com/Politics/dhs-whistleblower-testifies-house-intelligence-committee/story?id=74675983.

** Email: LFraedrich@lowenstein.com.

3 What is the most interesting work that you have done in your career?

I am not sure I could point to just one aspect and claim it as the most interesting. But ranking near the top has been working with Congress. Observing our representatives up close and personal has been both enlightening and frightening. My respect for Congress has grown and diminished at the same time. I tell people there are two sets of congresses. The first is the public one we all see in open hearings and the second one is operating behind the scenes and in closed hearings out of the public eye. I still can't figure out which one is better.

4 How have global security threats changed over the last Twenty years?

We no longer live in a world where we have a homeland security and a national security mission. They are merged. Threats transcend boundaries. Our connectedness has brought both the exceptionally positive and the exceptionally negative to the fore. Existential threats to the United States revolve around information. This includes the protection of intellectual property, data, and supply chains.

We are living in a post-cyber threat environment. And yes, I mean post-cyber. Cyber is not a threat vector. For a long time cyber was the threat. But it is simply the latest tool for threat actors to use against their victims. Continuing to label cyber as something to be on guard against makes virtually no sense. It only serves to muddy any real debate on the substance of the issues we face. Determining the goal of our adversaries is the better approach; what are they trying to steal or manipulate? Some within the federal government recognize this reality, but most either do not, or choose to remain ignorant, resting in the familiar. Thus far, progress has been slow. We are guilty of re-fighting several of the last wars.

5 What do you see as the biggest current national security risk?

Externally, it is China. Post 9/11, it took a number of years for me and many in government to put terrorism in its proper context. The threat from terrorism is important, but it is less likely to impact the United States in the long run. China, on the other hand, seeks to replace the United States in every way. This includes replacing democracy. China doesn't play by the same rules as the United States. The separation between business and the government does not exist in China. They are one and are fairly in sync.

Internally, our greatest national security risk is societal polarization. I'm not picking a political side. All sides are responsible. There is a multitude of reasons that this polarization is morphing into a national security threat. It would fill several volumes to explain it. So, instead of dissecting the causes, I'll focus on the outcome: we are starting to look at our fellow citizens as the 'other'. And more and more citizens don't want to associate with citizens who are not like themselves. Instead, we often want to destroy those in the other group. In the past, we had several identities in the United States, but shared common ideals. Unfortunately, we are focusing more and more narrowly on fewer and fewer identities. Collaboration and compromise are decreasing. The good news is that this is entirely fixable. As a nation we don't have to rely on exogenous factors or events. We own the problem and the solution.

6 How do you predict the polarization you describe will be solved, based on your government experience?

The solution starts with understanding the full spectrum of the problem. I'm not sure government can innovate quickly enough to provide a solution. Instead, I see the government's role as providing resources and being supportive. Advanced technology is needed to fully understand the threat and to mitigate it. In the end, resiliency building, civics education, and credible messengers on the topic will serve to counter the problem.

7 Where do you see the United States/China relationship going?

In the short run it will be status quo. We need them and they need us. Both economies are integrated and interdependent. There are a few apex moments on the horizon which will define how the relationship unfolds. First, China is in transition from an industrial to a service economy. A major element of their transformation involves information. They will stop at nothing to obtain it. Being clear-eyed about their tactics is something we all need to agree upon. As the Chinese technology advances, if China overtakes the United States in quantum computing this could be a break-through moment. China's transition will accelerate. The end-game for the Chinese is to become the most powerful economy in the world and the plan relies on becoming the world leader in technology.

Second, how the United States innovates to check the threat is going to matter more and more. For the question, *What do you see as the biggest current national security risk?*, I initially wrote, 'a lack of imagination'. Those in government continue to forget the adversary has a say. The post-cyber world is one in which there are no borders and no boundaries. Yet, organizations continue to operate as if the water's edge is some sort of buffer, or better yet a naturally occurring *Maginot Line*, we are able to hide behind. Our laws and authorities must be updated to take into account the complete cross-border penetration of our adversaries. The 'post cyber' seismic shift has elevated the existential threat other nation states present to the United States. And, this danger thrives with in the contiguous border of America. It is not something of the future, it is here

and now. It has also opened us up to all manners of fraud and manipulation.

8 What are the new concerns for supply chain security?

White labelling of critical components. Nation states and criminal organizations operate to find a back door into systems to steal information. As the cyber shield gets better, our foes look for the path of least resistance. Why keep trying to hack if you don't need to? Instead, they will build malicious code into the software and hardware.

9 How has supply chain security changed from the days of C-TPAT until now?

I think the most fundamental change is what security threat we are looking for. Under Customs-Trade Partnership Against Terrorism we worried about Weapons of Mass Destruction entering the United States. Now we are just as worried about product origination. What has not changed is the critical importance of public-private relationships. The threat changes, but relationships remain one of our best defences.

10 Can you explain how we can leverage our relationships to help with supply chain security?

The constant exchange of intelligence between business and government is paramount. Government's job was articulated in the Constitution and has not really changed. Its role is to protect its citizens from adversaries. The social contract between the governed and the government is founded on this notion. This clearly includes the protection of commerce. If the government has derogatory intelligence on a widget it needs to warn business. The free market is not actually free if a nation state is covertly manipulating the environment.

11 How is disinformation affecting the global marketplace and what should companies do to prepare themselves for possible issues?

Covert disinformation is the weapon of choice by both hostile nations and rival corporations. By laundering false information through the social media landscape, it becomes believable. And it gets picked up by credible, and incredible news sources. A consistent campaign was unleashed by a nation state during Covid to undermine one of the vaccine makers. The adversary set about their campaign for two reasons. First, they wanted to undermine trust in American institutions. Second, the hostile nation wanted the market share for its company.

Disinformation is intimately tied to information control. Remember, we live in the post-cyber world where information control is the objective. Illicit competitors and hostile nations look at undermining American business as a low cost, quasi-legal, technique to control the market.

Companies should invest in technology that enables finding the source of the disinformation early and before it becomes a crisis. They need to work to de-platform those accounts, expose the covert disinformation effort, and immediately counter the narrative. Time is not on companies' side. If they don't invest now, when (not if) it happens, it will be too late. The phrase, 'A lie can travel halfway around the world while the truth is still putting on its shoes', is certainly not new. But what is different is how quickly and easily the lie leaves the realm of rumours and becomes fact.

12 News reports indicate that you filed a whistleblower complaint against DHS and testified before Congress. What can you tell us about that experience?

Where to begin? First, I filed three complaints against corrupt and unethical behaviour. I used the process to both protect classified information and to point out wrongdoing. The first complaint I filed was in 2018, just a few months after I arrived at DHS. I filed the next one in early 2019 and the last one in 2020. First, I felt that there was a pattern from certain officials in the most senior ranks who put politics and themselves above the country. Prior to arriving at DHS, I had never filed any complaints. I also believe that the more responsibility you have as a leader, the more you owe to the public. While the road was challenging, I'm not a victim in this scenario. I have won many awards in government but the title of whistleblower is the one I am most proud of. Although, to be clear, I never saw myself becoming a whistleblower. Yet somehow, I became the highest-ranking whistleblower in US history. I will forever be in debt to several lawyers who guided me through the complex process.

13 From your perspective, what are the top two issues that global traders should focus on from a regulatory perspective?

First, the recent set of regulations on supply chain issues are just the start. It all comes down to getting into the weeds on who your supplier is and who your supplier's supplier is. Foreign products emanating from hostile nations will increasingly be the subject of scrutiny. Supply chain risks are now seen through a prism of intervention by hostile countries. Regulation will continue to get more granular with respects to components and parts.

The second is partnerships. By this, I mean who are your investors and partners? I'll keep beating the drum on hostile nation states. Should your partner or investor be located in a country where the government is an adversary to the United States, US regulations will soon require more and more disclosure from your business. New regulations will centre on the gathering of information.

14 So, what's next for you professionally?

I am lucky to be at the right place at the right time in history. My next stop is working as the Vice President of Global Operations at a tech company called Logically. I feel my new role has enabled me to combine my experience in government, with my academic studies, to produce an outcome helping to improve our way of life. The company tackles the harmful impact of mis- and dis-information at scale using the best of innovation to combat a complex and evolving threat. It has been lots of fun and I can see the impact we are making. My former government colleagues ask, 'how is the transition going?' I tell them the biggest challenge so far is not showing up at meetings in my typical government suit; I'm still reminding myself I'm in the private sector and it's ok to dress down.