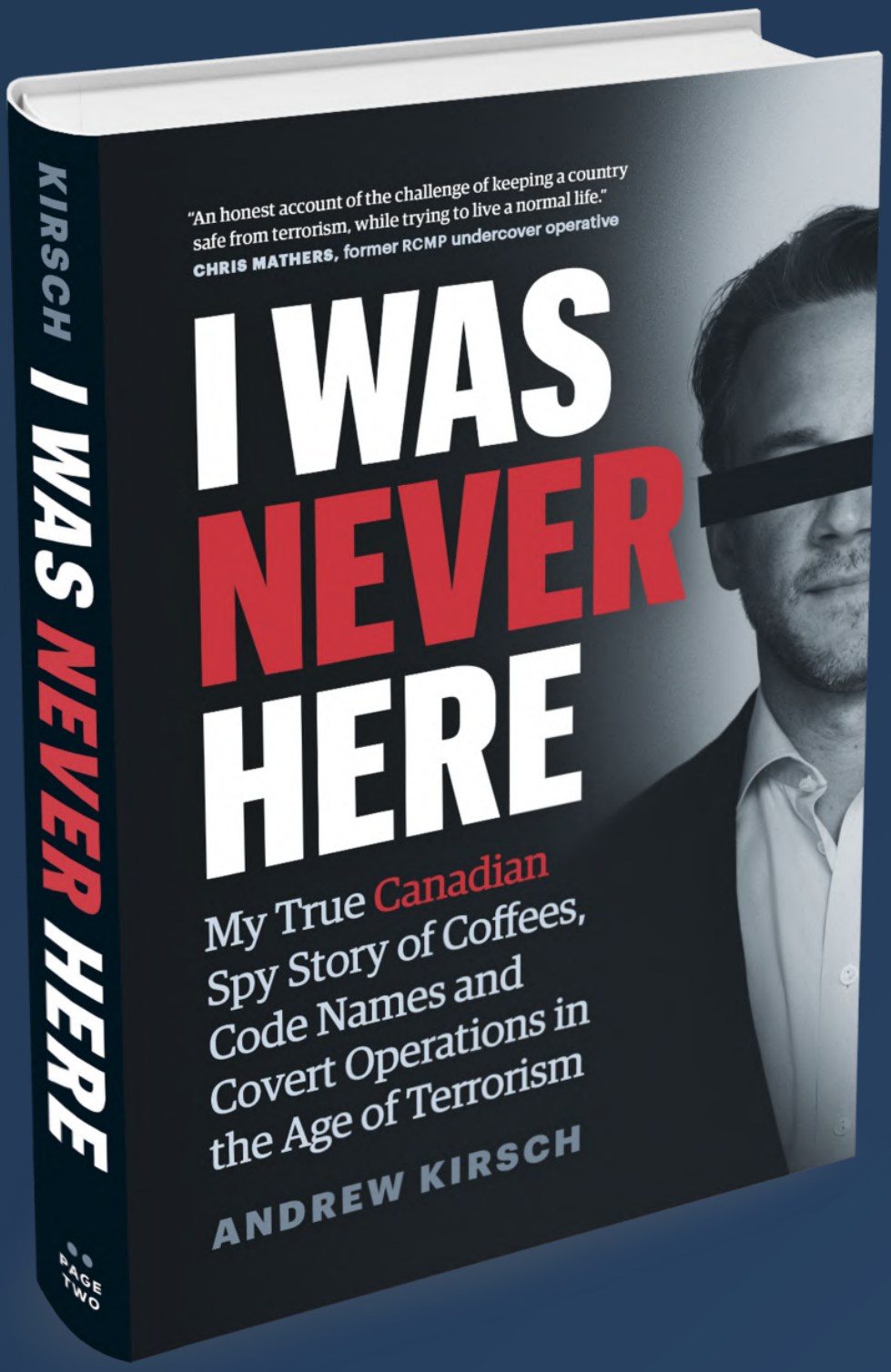
KG | KIRSCH GROUP



In his bestselling memoir, Andrew Kirsch reveals what Canada’s Spy Service does, what it's really like to work there, and why it’s so important you know more about it.

Here's a sneak peek at selected chapters of **"I Was Never Here"** by Andrew Kirsch.



ANDREW KIRSCH

I WAS NEVER HERE

PAGE TWO

Copyright © 2022 by Andrew Kirsch

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, without the prior written consent of the publisher or a licence from The Canadian Copyright Licensing Agency (Access Copyright). For a copyright licence, visit accesscopyright.ca or call toll free to 1-800-893-5777.

The views and opinions expressed in this book are those of the author and do not necessarily reflect the opinions, official policy or position of the Canadian Security Intelligence Service (CSIS), the Government of Canada or any other governmental or nongovernmental organization.

Some names and identifying details have been changed to protect the privacy of individuals.

Cataloguing in publication information is available from Library and Archives Canada.
ISBN 978-1-77458-133-9 (hardcover)
ISBN 978-1-77458-134-6 (ebook)

Page Two
pagetwo.com

Edited by Pam Robertson
Copyedited by Jenny Govier
Proofread by Alison Strobel
Jacket design by Taysia Louie
Jacket photos by Michal García
Interior design by Fiona Lee
Printed and bound in Canada by Friesens
Distributed in Canada by Raincoast Books
Distributed in the US and internationally by Macmillan

22 23 24 25 26 5 4 3 2 1

andrewkirsch.ca

CONTENTS

Introduction *1*

1 **The World's Second-Oldest Profession** *7*
2 **The Long Road of Recruitment** *13*
3 **Spy University** *27*
4 **Analyst Life** *43*
5 **In the Field** *55*
6 **New to the Community** *67*
7 **My Guy** *99*
8 **Back of the Van** *125*
9 **Wait, I'm in Charge?** *145*
10 **The Best Job in the World** *167*
11 **A Delicate Imbalance** *197*
12 **In from the Cold** *213*

Epilogue *223*
Acknowledgements *229*

INTRODUCTION

It was 1:30 a.m. and I was sitting in the passenger seat of a full Dodge Caravan parked on a quiet residential street in the suburbs of Toronto. I was about to lead a covert special operations team to search the inside of the car of a suspected terrorist. The only catch: the car was parked in his driveway and he was sleeping at home with his wife and family.

It would end up being the longest night of my professional career as a spy with the Canadian Security Intelligence Service. That night everything that could go wrong would go wrong, but in the moment I didn't know that. All I knew was that I had a three-hour window to search this car before the sun started coming up and the neighbourhood began to stir. I also had a two-hour window to get home to my wife. She knew I was a spy and never asked where I was going when I left the condo at midnight in a dark hooded sweatshirt. She did like to know when I'd be home. The truth was I never really knew, but I got good at guessing. It was the least I could do. I think it helped her sleep, but if she woke up past the agreed upon time and I wasn't there, she'd really get worried. Operationally, "Don't get caught" was number one. "Don't upset my very understanding wife" wasn't far behind.

From my vantage point in the front seat, it didn't look good. There were a lot of people working that night. There was my team in the van. Surveillants were parked strategically throughout the neighbourhood, and one person back at the office was monitoring communications. The target in the house was an issue, but the more

pressing concern was a neighbour who'd decided to walk his dog and have a smoke at 1 a.m.

I'd surveyed the neighbourhood to prepare for that night. I knew when garbage day was and when the last lights started to go off and the street quieted down. This was new, and it was really annoying. This insomniac dog walker was unknowingly interfering with a high-priority national security operation, and he was costing the government thousands of dollars in overtime pay. We were primed and ready to go. In the meantime, we were taking bets on how long it would take the dog to finish its business.

Stuck in a holding pattern, my mind drifted to the ridiculousness of it all. The pooping dog, our mission that night and the fact that I was responsible for leading it. We were about twenty-five minutes from where I grew up, and what I was about to do would be considered illegal if it hadn't been sanctioned by the government and authorized by a judge. It was a far cry from my previous career as a junior financial analyst at a bank in the UK.

I was part of a post-9/11 wave of civically minded Canadians who had left our day jobs to do our part in the age of terrorism. I had been in CSIS for about seven years and on the special operations team for a year. Even my first post as an analyst at headquarters felt like a lifetime ago. Back then I'd been chained to a desk reading reports and writing memos. It had been slow, but I'd been safe and anonymous behind the organization's walls and my air-gapped computer. My new role in special operations was the tip-of-the-spear stuff. It's what I'd signed up to CSIS to do. As always, sometimes be careful what you wish for.

The man and his dog had gone inside. The lights inside the house were off. The neighbourhood was quiet again. The chatter in the van died down as everyone began to re-focus and mentally prepare for what we were about to do. In the front seat I went back through my pre-operation checklist. Radio check. Phones on silent. Pockets empty of any identifying materials. Surveillance confirmed the perimeter was clear. At the same time everyone in the van checked and then rechecked their gear. They were now sitting quietly waiting for my command.

That was one of my first jobs in charge of an operation. I oversaw all aspects of the mission: plotting our objective, building a plan, procuring the tools we needed, getting the relevant approvals from management and then leading the team to achieve our goals. Most stages are a team effort and involve a lot of time, people and collaboration. However, when you execute a plan, it's not a democracy. The lead calls the shots. Most of the other guys had done hundreds of these operations. It could be intimidating and awkward to tell them what to do. But the reality is that if something happened, there wouldn't be time to have a group chat. A chain of command must be followed so everyone knows where to look for directions and instructions. Now they were looking at me.

I took a deep breath and gathered myself. There would be plenty of time to reflect and laugh at all of it when it was over. It should have been a ten-minute job. It ended up taking over two hours. If I had known, I would have quickly texted my wife and told her I'd be late. Instead, I called over my radio, "All teams, this is One. We're heading out." I turned to the guys sitting in the back of the van. "Let's roll."

I HADN'T always wanted to be a spy. I didn't watch spy movies growing up or dream about being James Bond. I knew about the CIA but never really considered that Canada had an intelligence service or thought about what they did. Prior to 2001, Canada's defining terrorist incident was the 1985 Air India attack. I was six years old. Intelligence wasn't something I'd thought much about until all of a sudden it was.

That was in 2005. I was living in London, England, and a coordinated bomb attack had just blown up a double-decker bus and a Tube station near my office. I was already well into a promising financial services career, but now fighting terrorism started to mean a lot more to me than the markets. That's when I first googled, "How do I become a Canadian spy?" I wasn't recruited; it wasn't an accident and it certainly wasn't a passive act. I moved back to Toronto, applied online and went through a long and arduous process of psychological tests, interviews, role playing, background checks and a polygraph. I didn't exactly know what I was getting myself into, but

I studied and prepped hard for each stage. After fifteen months I got a phone call. It was the middle of the summer and I was living in Toronto. Could I report to Ottawa in September? Absolutely, I told them. What should I tell my family and friends? "Be discreet," was all they advised.

I left the Service in June 2016. This was also a relatively quick decision. I didn't leave angry and there wasn't one moment that pushed me out the door. Just as much as I knew when I wanted to join, I also knew when it was time to leave. The enthusiasm of serving my country gave way over time to the gruelling reality of being a spy. The bureaucracy, the late nights, the white lies and the relentlessness of it all wore me down. On my last day I handed in my badge, various IDs and building passes. I was escorted out of the office with nothing besides a promotional flyer for the next CSIS alumni benevolent society barbeque.

When I decided I wanted to apply to CSIS, I realized pretty quickly that there was little information available about what that actually meant. Since leaving, I've started to be open with people about where I worked and share my perspective on the organization, what it does and what it's like to work there. I realize there is certainly interest, even from people who aren't in the security community or considering it as a profession. This book is my contribution to the conversation. To explain to Canadians what it is their intelligence service does, day in and day out, and to try to describe how that affected my life—from the time I joined, moving from Toronto to Ottawa and back again, to the time I left. I dated women, then got married and started a family, while at the same time trying to conceal from most people where I worked—and even from my closest friends and family, who knew where I worked, what I actually did there. Now I'm able to share what it's like to work there. This book may dispel some of the mystique around spying. While I may not have been an international man of mystery, I am still extremely proud of the work I did and the small part I played in keeping Canadians safe.

We as a nation have a unique intelligence service with a diverse cadre of officers and support staff that punches above its weight. This

is my story about what CSIS is and what it's like to be a Canadian spy—as much of it as I can share, as authentically as possible—from recruitment, to training, to life behind the desk, to knocking on doors, and then picking the locks and breaking in. I hope you find this book as I did my spy career: mostly fun, at times challenging, but ultimately rewarding.

1

THE WORLD'S SECOND-OLDEST PROFESSION

WE SHOULD probably start before the beginning. You may have some familiarity with the Canadian Security Intelligence Service, but please allow me to provide some background in case you don't, and maybe even dispel some misconceptions that are out there. First things first, the Canadian Security Intelligence Service is also known as CSIS (pronounced see-sis). People who work there often refer to it colloquially as "the Service," which is actually a pretty cool nickname for an intelligence service, in my opinion.

Spying has often been referred to as the second-oldest profession in the world, but CSIS is a relatively new organization. It was founded by an act of Parliament in 1984. Its roots, however, date back to the 1970s and allegations that its predecessor, the Royal Canadian Mounted Police Security Service, used illegal investigative techniques during the Front de libération du Québec (FLQ) crisis. A federal royal commission known as the McDonald Commission was formed in 1977 and issued a final report in 1981. Its main recommendation was to separate intelligence collection from policing and create a civilian intelligence agency. And thus, Canada's domestic security intelligence service was born.

It is important to note that Canada does not have a separate foreign intelligence service. Some countries assume that we do and we're just incredibly covert. But alas, we're not *that* good. And as a result, there is no direct equivalency with the United States, to which we are most often compared. This can be confusing. The Central Intelligence Agency (CIA) works almost exclusively outside of the United States. Its mandate is to collect foreign intelligence relating to the political or economic activities of foreign states. CSIS can only collect foreign intelligence in a limited capacity within Canada (well, there are some exceptions, but they aren't worth getting into here).

Ah, you must be thinking, so CSIS is more like the FBI. Not really. The Federal Bureau of Investigation (FBI) is a domestic security service but also a law enforcement agency that investigates and prosecutes crimes. They more closely align with our Royal Canadian Mounted Police (RCMP). Whenever there is a terrorism or national security arrest, you will see it's the RCMP laying the charges. In many cases, the information that may have started the investigation was uncovered by CSIS. However, as CSIS does not have an enforcement mandate, they will pass that information to the RCMP, in a very limited and controlled manner, so the Mounties can start their own investigation and ultimately prosecute. (And if you are interested in that process, there are many legal and academic papers written about the intelligence-to-evidence challenge of information sharing between CSIS and the RCMP.)

A better understanding of CSIS can be found by looking at our British and Israeli counterparts. The British have two intelligence services. Domestically, the British have the Security Service, otherwise known as MI5. Separately, the British have a foreign intelligence service known as MI6, the Secret Intelligence Service. MI6 is famously James Bond's employer. Bond gets to travel the globe, foiling international terror plots and seducing women in nearly every country he visits. MI5 obviously does very important work too, but I think their equivalent fictional character is Rowan Atkinson's bumbling spy Johnny English. That's got to be tough for recruitment. Do you want to be like Daniel Craig or Mr. Bean? In this analogy Canada is Mr. Bean, which actually does kind of fit.

Israel has this distinction too. The Mossad is responsible for foreign intelligence and covert activities abroad, while the Shin Bet is responsible for internal security in Israel. As much as these organizations may have different geographic areas of interest and responsibility, they must work very closely together. Threats originating abroad may aim to attack closer to home. Any coverage gaps between the two organizations could have disastrous consequences.

In Canada, we have one organization, and it's responsible for covering the globe while operating largely domestically. If that sounds like a tough job, well, it is. We benefit greatly from information sharing with countries around the world and especially close relationships with key allies that are members of the Five Eyes community of countries. In addition to Canada, this group is composed of the United States, the United Kingdom, Australia and New Zealand. We share a broad range of signals, military and human intelligence in what is the world's closest intelligence-sharing network. Canada definitely contributes to this arrangement, but clearly we are one of the smaller players, and our absence of a foreign service does mean in some cases that we rely heavily on our partners for information.

Once again, there are lots of legal and academic papers debating whether we need a separate foreign service or have enough powers under the existing mandate to do what we need to do to keep Canadians safe. I'm sure that in some bureaucrat's bottom drawer in Ottawa there even exists a detailed plan of what it would take to establish our own Canadian MI6 or Mossad. Personally, I think things work fine the way they are, even though it did take me three pages to explain it all.

9/11 and 7/7: My Postgraduate Education

If that quick summary was all new to you, don't worry. There will be no quiz and you don't need to know any of that to understand the rest of my story. Truth be told, I honestly didn't know any of that stuff before I started looking into becoming a spy. And I certainly

didn't back in September 2001. I was twenty-two years old and a few weeks into my senior year at Brown University.

Despite growing up in Toronto, my parents had spent a year at graduate school at Rutgers and fell in love with the US college experience. They encouraged my brothers and me to look at American schools for our undergraduate degrees. Brown is an Ivy League school, famous for its Open Curriculum, and the campus in Providence, Rhode Island, was the exact type of environment they wanted for us. For the purpose of this book, the most interesting thing to note about my experience at Brown is probably that my freshman orientation group leader was John Krasinski, who would go on to a very successful TV and movie career (coincidentally playing fictional spy Jack Ryan). Fans of John might be interested to know that all through university he was putting in his ten thousand hours, performing in improv comedy shows and going for professional auditions. Meanwhile, I was studying public policy and had no idea what I wanted to be when I grew up.

The morning of September 11, 2001, I was at home in the rented house I shared with six of my friends near the main university campus. The television happened to be on CNN as we were getting up and getting ready for our day. I remember the first reports of a plane hitting one of the twin towers. It was confusing more than alarming. Terrorism just wasn't prevalent or even conceivable. I was still a student living in a bubble. The thought of an attack on the United States wasn't something anyone worried about or considered at the time. The moment definitely registered—we just didn't know what it was or what it meant. We kept watching, and were trying to better understand what happened, when the second tower was hit. We were still watching when eventually the two towers crumbled to the ground.

In the following years, terrorism seemed to be everywhere: 2002, the Bali bombing; 2003, bombings of compounds housing Western workers in Saudi Arabia; 2004, the Madrid bombings and the Beslan hostages. War with Iraq was coming. The Canadian Forces began to enter Afghanistan, progressively ramping up operations. Terrorism was always there, and the Great Game of foreign conflicts in Afghanistan certainly wasn't new, but it was all new for me.

During those years, I watched the world change from London, England. As a Canadian in a post-9/11 world, it was hard to stay in the United States without a work visa. However, as a member of the Commonwealth I was able to apply to the United Kingdom for a working holiday visa that would allow me to live and work in the UK for up to two years. I thought it was a better plan than moving back to Toronto and in with my parents. So after graduating in 2002, I moved to London and ended up getting a job as a junior investment advisor with Anglo Irish Bank in a new wealth management division of what was primarily a commercial property lending bank. I had a return ticket to Canada booked for six months out. I stayed with Anglo for three years and took all the exams that were required by the Financial Services Authority to be regulated to give financial advice in the UK. As a side note, Anglo would be nationalized in 2009 (to be clear—after I left and not my fault) at the height of the global financial crisis.

In 2005, Anglo was still the darling of UK and Irish finance, and I had a bright future as a private banker. That was until events conspired to change my path in life. My father passed away suddenly in January. Then, on July 7 of that year, a coordinated bombing attack in the heart of London hit very close to where my brother (who was also in London at the time) and I were working. It was the catalyst I needed to make a change. Four years earlier, 9/11 had happened a few states away from where I was living at that time. Now, on 7/7, the bombs were going off down the street.

I was going through the motions at work. It was a good career and they treated me well. I had put in two years and countless hours studying to earn my investment advisor certification. Deep down I knew it wasn't what I wanted to be. I once told my faculty advisor that I thought I'd go to law school even though I didn't want to be a lawyer. He told me, "People don't go to carpentry school if they don't want to be a carpenter." Now I was studying to be a banker and didn't want to be a banker. Each morning I'd read the news with one eye on the financial pages and the other on the latest developments in the global fight against terrorism. My father's life being cut short made me look around and really consider where I was and

what I was doing with mine. There was something bigger happening in the world. I felt I had something to contribute, and I wanted to do my part. I didn't know anything about the military or spying, but in my mind, those were the two ways to get on the front line of the fight against terrorism. I started researching what little I could find. It sounded good. It felt important, and with my father's death, it started to feel more urgent.

I moved back to Toronto and applied to join CSIS and the Queen's Own Rifles of Canada (QOR), a Canadian Army Reserve infantry unit. I didn't really know what either meant at the time (or that I would be accepted to into both). I was ready to serve my country and do more with my life. I was young, restless in my career and itching to contribute. The army felt like a noble way to serve and a more realistic goal. CSIS seemed more like a pipe dream. They receive thousands of applications a year for only a handful of spots. I knew if I got in I'd have to move to a new city and potentially lie to people about where I worked and keep from those closest to me what I did there. I'd deal with all the life-changing stuff later. The hardest part at that point was just getting in.

2

THE LONG ROAD OF RECRUITMENT

So HOW does one become a spy? That's the question I get asked the most. What is the process like? The short answer is, I applied online. I wish it were a cooler answer; unfortunately, it isn't. I didn't know anyone who worked at CSIS, so I didn't have any better way to approach it than to simply click and submit my CV through the Government of Canada jobs portal. No recruitment by a connected professor in a posh graduate school. I wasn't talent spotted in my business career. That would have been awesome, but no. No one was looking for me. I had to go looking for them.

The requirements to qualify to submit an application are pretty straightforward: Canadian citizenship, a degree of some sort and a valid and permanent Canadian driver's licence. The complete process for applying, however, was much more involved, with a number of stages. After submitting an application online, I had a phone interview, a group information session, psychological tests, a "suitability" interview with role playing, a larger panel interview with more role playing, a security clearance interview, a French language aptitude test, background security checks, a polygraph test and then a final executive interview.

I do remember that for most stages there was a real lack of feedback. I was left wondering each time if I had progressed or not. I would call my designated recruiter and ask for any additional information or feedback she could share. She was a friendly and responsive information black hole. I was up against a seasoned CSIS human resource professional, and she easily swatted away my best efforts to coax some intel out of her about how I was doing in the process. She would tell me calmly and repeatedly that not hearing from them was a good sign. If I did hear from them, it would be to inform me that I was no longer being considered. If I didn't hear from them, it meant that I was. I was hoping I could get some idea of when the next stages would be so I could have a sense of how long the whole process would take. She did not have any interest in providing clarifying information. I did not want to annoy her. In my mind everything was a test, so I sat and waited by the phone.

The first in-person stage in the process was the group information session. I was living in Toronto and was invited to the attend the presentation at the regional office. Without giving too much away, I can say that it's downtown.

My session would be held in a large assembly room on the same reception floor, but outside of CSIS's secure and restricted area.

It was largely an orientation about what was to come and the many stages we should expect to go through. I remember looking around that room and even at that early point in the process feeling a spirit of exclusivity and exceptionalism. It was led by our presenter, the head of recruitment. He was probably in his late thirties, with a full head of shaggy brown hair loosely parted on one side. He wore a dark grey, slightly ill-fitting suit that I'd learn was a bit of a uniform at CSIS. The role was spy, but the dress code was mid-level public service employee.

He made a point to remind us of the thousands of people who apply every year and the reality that of the thirty or forty people who were in that room, only one or maybe two would make it all the way to the end. My competitive side couldn't help but get caught up. The CSIS hiring process is not fun, but it was a gauntlet I was determined to run. It was an exclusive club and I wanted to make it in. The reality

is that when you join CSIS, you realize it's a lot like any organization with a strong HR department. There are many wonderful and talented people; there are also some folks you look at and wonder, How did *you* get in here? And that of course would make you realize, Maybe I'm not so special after all?

The other important note he stressed was that we were interviewing with the Canadian Security Intelligence Service, not the Canadian Security *and* Intelligence Service. We were told if we got this wrong in our interviews, we would automatically fail. Looking back, I wonder if this was actual policy or the presenter freelancing on a personal point of annoyance. At the time it didn't matter. I wasn't going to make that mistake.

The suitability interview was the first big individual test I faced. It would be with my steel-trap HR rep and a more genial intelligence officer (what we call an IO) in the Toronto regional office. Unlike the information session, this would be held *inside* the restricted area. It was my first literal small step into CSIS—and it was almost my last.

I had prepared *a lot* for this interview. As I mentioned, prior to my UK revelation that I wanted to fight terrorism, I didn't know a lot about CSIS. We were instructed in the information interview that we would be quizzed on the CSIS Act, so I read the Act cover to cover. I made flash cards about every chapter. I wasn't a lawyer, so I found the whole thing a bit dry, but I did it. I covered warrant powers, cooperating with foreign governments, security screening responsibilities, everything. I ended up with a huge stack of flash cards covering all the minutiae of the Act. In my mind this was a test of information collection and retention. I was determined not to miss anything. I think I even had some cards with French translations.

I got so caught up in memorizing every little thing, I couldn't see the forest for the trees, and my overpreparation ended up being to my detriment, almost devastatingly so. The first question my HR rep asked me was, "What are the threats that CSIS is mandated to investigate?" This was an easy question. I mean, if you're interviewing with any organization, you should probably know what it is you will be expected to do. The threats are the core of the CSIS mandate. It is

the fundamental purpose of the organization. Its raison d'être. And I drew a complete blank.

I sat there for a second in silence. I saw a look of concern cross my HR interviewer's face. It was the first trace of genuine emotion I had seen or heard her express, and it made things so much worse. I looked at my cue cards stacked in front of me. What were the odds that the card with threats to the security of Canada was on top? It wasn't. My heart sank. I started to think about how nice it was to have made it this far, slowly considering that my dream of being a spy was about to die with question number one of my very first interview. I thought about what I would do next with my life.

Mercifully the intelligence officer, my future co-worker and in that moment best friend in the world, decided to take pity on me. Whether it was because she could feel my anxiety and was trying to save herself from the growing awkward tension or because she felt some sympathy as she knew what it was like to sit in my chair, it didn't really matter. She threw me a lifeline.

"Terrorism . . .?" she softly hinted, her voice rising at the end of the word as if she were asking me the question.

"*Yes!* Terrorism!" I exclaimed. "Of course, terrorism!"

My blood started to circulate again, and the terrorism flash card popped back into my mind. "Terrorism, espionage and sabotage, foreign-influenced activities and subversion!"

I wanted to give her a high-five. Like we were a team. I was back in the game!

Amazingly they let me continue to the next phase of that interview, and the biggest hurdle in the whole process, the role-playing exercise. I'd be playing out a scenario with the intelligence officer. I was handed a piece of paper with the instructions and given a few minutes to quietly prepare. I was told they would start whenever I was ready and not to break character until the end of the exercise.

I'd known this part was coming, but there really isn't a way to prepare for a role-playing exercise when you aren't given the scenario in advance. All I knew was that I was not going to say Canadian Security *and* Intelligence Service. That's all I had practised. I'd learned my lesson from the earlier interview: get the basics right. "Hello, my

name is Andrew, and I'm here from the Canadian Security Intelligence Service." I nailed it!

It was so silly, but once I got that out, I really relaxed. I think the other thing that helped was not having expectations about what I was supposed to achieve. Build rapport and trust, listen and gather information, ask clarifying questions, and make sure to leave the door open for future conversations, because there will inevitably be things that you wish you'd asked in the interview and you are going to want to follow up on. That was my "strategy" for my suitability interview role-playing exercise, and it didn't change much throughout my career.

I was cruising right along when suddenly the fire alarm rang out in the entire building. My first thought was, Don't break character. My second thought was, Gosh, this sure is an elaborate way to get me to break character, setting off the fire alarm in the whole building. Though it became clear pretty quickly that it wasn't. I looked at my counterpart and she looked mildly annoyed. I guess she was in a role-playing groove too and didn't want to be disrupted. In character, I turned to her and said, "I realize we may need to depart shortly; however, I would like to continue our conversation. Would you mind if I contacted you again?" She gave the game away when she paused briefly, looked out the door to see what other people were doing and then came back to sit down. "Nah, I think we'll be okay, let's keep going." The alarm stopped and we continued. The fire alarm wasn't a test, but I passed anyway.

After nearly disqualifying myself on the very first question of the recruitment process, I started to hit my stride. The next big obstacle was the National Assessment Panel (NAP). This was a panel interview including the head of recruitment, the head of HR and a couple of senior managers. I was once again in the Toronto regional office, but now I was on a higher floor and farther down the hall in an executive boardroom. With each successful stage I was making my way deeper into the office, and now I would be facing even more daunting opposition. I was seated at one end of the table with the head of recruitment, who had done the information interview group presentation, at the other. While he had a youthful appearance, the

executives seated on either side of me looked more seasoned, hardened and even a little sour at being forced to participate. They gave the impression that this activity was ruining their day and they were holding it against me that they had to be there. It was certainly intimidating, but it actually could have been a worse arrangement. I could have been seated on one side and had five people across from me. This was only slightly less hostile a configuration than that. It nevertheless left me alone feeling surrounded rather than in front of a firing squad.

They peppered me with tough questions that I wasn't provided with in advance. I tried to talk through my thought process. I explained my answer and rationalization. If I got it "wrong" I was hoping for part marks for consideration and thoughtfulness. In most interviews or even conversations I typically look to the other individual for feedback or cues to see if I am on the right track or if they agree with me or not: a subtle confused tilt of the head, a nod, a smirk, leaning forward, leaning back. In this interview I didn't get much. I wouldn't say they were intentionally trying to rattle me but they certainly weren't revealing anything, which in itself was unnerving and definitely not comforting. I think some of them took pleasure in seeing someone in the hot seat and putting me through my paces.

I did my best to keep calm and answer their questions seriously, but I also started to let myself have fun with it. I even got a laugh. It was a question about what I would do in a particularly confrontational theoretical situation with a human source (this is what CSIS calls informants, as they are people who regularly provide information to our officers). Basically, it was someone I was expected to have a close existing relationship with, but in that moment we were having a difficult conversation. I ended my answer with, "I would then say to him, 'Let's hug it out . . .'" It was a reference to a recent (at the time) episode of a TV show, either *The Office* or *Entourage*. The full quote is, "Let's hug it out, bitch." Now I don't think I said the full quote, but I think the head of recruitment thought I had, and despite his best attempts to hold it in, I did see him chuckle a bit to himself. I considered it a small victory and a demonstration of how I could be cool under pressure. I quickly put a lie to that notion.

They had given me a glass of water at the start of the session. After our little bonding giggle over my clever pop culture reference, I thought I might like to have a quick sip. I had done my best to give an air of confidence throughout the interview. I don't think my voice had cracked or crumbled, my feet were flat on the floor and I thought my responses were reasonably thoughtful and concise. But when I went to raise the glass of water and bring it to my lips, my hand and arm started shaking fiercely. It was like all of my anxiety and nerves just started shooting down my arm, causing my hand to tremble and the glass of water to shake. I felt it immediately and looked down at my hand to see if I could pull myself together. The glass was about two or three inches off the table. It was now shaking violently. That's as far as it ever went.

It hung there long enough that I'm sure everyone saw it. I put the glass down as gently as I could; it was like landing a plane in turbulence. I watched it intently the whole way down—I had zero confidence in my ability to land that glass of water. I got it down without any spilling, which at that point I considered a success. I pulled my hands back together on the table in front of me and just continued on as if nothing had happened. I never mentioned it, and neither did they.

I didn't hear from them for weeks this time, maybe even a couple of months. I remembered that no news was good news, but I was definitely getting a little impatient. I had taken a job as a consultant and was living with my younger brother and his girlfriend in an apartment we rented on the ground floor of a Midtown Toronto townhouse. My job and living situation were fine, but in my mind, they were both placeholders. On the one hand, I knew that the recruitment process could take a long time, so I couldn't just sit around and wait. On the other hand, if I were offered the job, I would have to move to Ottawa for the intelligence officer training course. It didn't make sense to find a permanent place of my own in Toronto or a better job until I knew if I was going to make it or not.

Finally, I got a call. I'd passed the NAP. It was time for a security interview and a deep dive into my past.

Jaywalking and Other Dark Secrets from My Past

Up to that point, as much as I was preparing for every stage and advancing through the recruitment process, in the back of my mind I don't know if I ever really thought it would happen. I knew the stats. Thousands of people apply. Some years only a few dozen make it. The odds were always bad, and by no means did I ever feel confident that the one to make it would be me. I was enjoying the process, though. I was certainly trying my best, but ultimately it felt very outside the realm of possibility that I would actually be offered the job.

I had so little confidence that I hadn't told anyone I was even applying. Not my mother, my three brothers or my new girlfriend of a few months. I just assumed at one point I'd get a letter in the mail that said, "Thanks but no thanks," and that would be that. Why tell everyone if it wasn't going to work out anyway? In my thinking, years later I would have a rejection letter as a souvenir to prove that at one point I'd applied. It would be a keepsake from the experience. With each phone call I got closer to making it, but it still didn't feel real until the next paperwork I received. It wasn't a letter; it was a form.

The security clearance and background check application required the names, birth dates and hometowns of everyone in my family, as well as non-related character references who would be interviewed to speak on my behalf. Now it was no longer just some fun thing that I could keep secret. Shit was getting real. I was going to have to have some awkward conversations with some of the people closest to me.

So as we were sitting around the table of an extended Sunday night family dinner I announced to everyone that I was in the process of applying to CSIS. I told them that I'd started to apply months ago, and I had advanced to a significant enough stage that I thought it was a real possibility I could make it.

In the vetting process CSIS was conducting on me, my family would now be checked out too—whether they liked it or not. I wanted to give them an opportunity to say whether they were in the "or not" category. I think I phrased it very matter-of-factly: "I am applying for top secret security clearance and I need to give the government all of your information. If there is any reason why you would like me *not* to do that, please speak now or forever hold your peace."

Fortunately, there were no confessions that night. A little confusion and lots of questions about what CSIS was and where I was in the process, but that was it. Everyone was supportive. Truth be told, we probably should have had a more open discussion. As much as this was my decision, their lives would be affected too. When I became a spy, I would ask them to lie to everyone they knew about where I worked and what I was doing. It was more to ask than I knew at the time. At that family dinner, though, that reality still seemed very far away.

CSIS didn't interview any of my family but they did check my references. I had given them a list of people who had known me most of my life. One was a childhood friend who had just started his career as a junior researcher at a financial services firm in Toronto. I had told him CSIS would be reaching out for a security clearance application I had submitted related to my army reserve career, which was already well under way, so he wasn't totally surprised when they asked to meet. I do think his employer was, though. The CSIS security screeners showed up at his office and announced their presence at reception. As he told me later, their receptionist came to the open-plan office where all the analysts sat together and announced quite loudly, "Mike [not his real name], CSIS is here to see you." He said it was a like a scene in a movie where the whole office suddenly got quiet and everyone turned their chairs to get a look at this new guy. One senior analyst blurted out loudly, "Who the fuck did we just hire?" I'm not sure if he ever lived that down, and I can't believe he didn't totally tank my reference check as payback.

The security checks ran in the background as my own process continued. Each stage was a stressful and unique experience; probably none more of both and none more distinct to CSIS than the polygraph test. There just aren't many other jobs that require it. To make matters worse, I'm what you would call a pleaser. I want people to like me. I want to be helpful to others, and it stresses me out when someone else is upset or uncomfortable. If a situation gets tense, I'm the first person to tell a joke to try to lighten the mood. It's a great reflex at dinner parties but not so helpful during a polygraph test.

They used a small vacant room in the Toronto regional office. It was the size of a large walk-in closet. It was furnished but lacked any

personal charm that might have been a distraction for the test. I sat down in a chair and got hooked up to the machine.

For all the issues I have with movie depictions of spies, I have to admit they actually get the polygraph pretty accurate. Just call me Greg Focker from *Meet the Parents*. My polygraphist was definitely straight out of central casting. He was in his late fifties, a little dishevelled in a slightly oversized brown blazer, with a permanent scowl that would force him to only play the bad cop in any interrogation scene. He asked me if I was comfortable. I considered making a joke about "the circle of trust" but thought better of it.

I can't remember the exact wording of the first question, but what I heard was, "Have you ever done anything bad in your entire life?" And this is when the pleaser in me kicked in: Where do I start!

I've lived a pretty upright existence—there are definitely things I wish I had done differently or better, but nothing that I'm overly ashamed of. That said, everything I've ever done wrong I feel absolutely terrible about. I started the confessional, "One time when I was ten or eleven years old, I was with a group of kids and we ripped off the hood ornament of a Mercedes-Benz for no particular reason. I felt sick about it at the time and still feel bad today."

I could see the polygraphist take a deep breath. "Any more recent examples?" He only wanted to hear about things he thought were relevant and clearly didn't want to be there all day. I wanted to make sure I didn't leave anything out. It wasn't a good mix.

Next I told him about how I'd plagiarized sections of a grade seven book report for French class, and how I felt bad about not calling some girls back after first dates. The polygraphist seemed frustrated, which only made me more anxious. To calm down I tried to remind myself what I thought CSIS was looking for. Can I be blackmailed for something I've done that would make me compromise my loyalty to Canada? I'm certainly embarrassed about many things in my life, but nothing I'm so ashamed of that I would give up secrets to keep from being exposed.

I couldn't see most of what I was hooked up to. I assumed from the movies that somewhere in the room there was a needle moving over a piece of paper, measuring my responses. I imagined my

needle slowing down as more questions came and the reflection on the boringness of my life washed over me.

Just as I started to feel a little better, the polygraphist said to me, "What about criminality?" Then he added, "I mean, we get guys in the chair and we think everything is fine and then we find out they have illegally downloaded music from the internet." Oh no! The needle started flying around again.

This predates streaming; in the early days there were sites like Napster and LimeWire where you could download movies and music for free. I certainly did do that. I said, "Downloading music is illegal, isn't it?"

"Of course it is," he said.

"Well I've done that," I sheepishly admitted.

"Well, a few songs shouldn't be too bad," he turned the knife.

"I've got thousands!" I replied, concerned.

My mind was racing to anything else that I hadn't realized was illegal. I felt like my needle might break off the machine. Jaywalking and times when I hadn't paid for parking were all that came to mind.

I wanted to be honest because I didn't want it to look like I was hiding anything, but I couldn't remember anything. I could tell my polygraphist wasn't satisfied with my answers, which was only adding to my stress. If he wanted to rattle me, mission accomplished.

I never got to see the results of my polygraph, but I guess I passed. I got the job. And I never downloaded anything illegal ever again knowing I would be having that fun again in another five years, when my refresh was due. Something to look forward to.

The Inner Sanctum

I started my recruitment milling about the ground-floor lobby of the CSIS office building in Toronto. By the time I made it to the final stage, the executive interview, I was at the highest and innermost office of the building. I believe at this point it was a foregone conclusion I was going to be hired. It certainly felt that way. It was much more collegial than the previous stages. The interviewer was the

person in charge of the Toronto regional office. He would go on to rise to director of operations (second in command) for the entire organization. He could not have been nicer. It was like a boss getting to know a new employee. Tell me about yourself: Do you have a family? What would you like to get out of your CSIS career?

He made it a point to stress and return again to the issue of mobility. I was given this speech at every stage, by everyone I spoke to at CSIS in the hiring process. The Service reserves the right to move you where they need you. The wrinkle at this moment was the pending reality of it all. If I were hired, I would move to Ottawa for training. There was no knowing how long it would take me to get back to Toronto.

It was a positive conversation. He didn't ask me any hard questions and I didn't give him any reason to. I was excited to be there, and I don't think I hid it well. I was eager, earnest, excited and deferential. I almost couldn't believe it. This crazy idea I'd had of becoming a spy felt very real. This was the final stage of a fifteen-month battle of attrition, and for the first time I allowed myself to believe that I had won.

I honestly can't remember if I got an email or received a welcome package in the mail. I do remember speaking with my recruiter on the phone and her asking me when I could start. I think it was August and she had a French language class spot ready for me in September. After the cold shoulder I'd got in response to every inquiry, I desperately wanted to say in that moment, "You take fifteen months to move me through this process and then ask me to move my life in a couple weeks?" Of course, what I said was, "Absolutely, whatever you need."

I told my family. They were excited. Their next question was, What do they tell people? I didn't have any more information yet. I said, "Don't tell anyone anything. Say that I'm moving to Ottawa to work for the government doing policy work." That was my degree from university, so it made sense. I told them, "I'll let you know more as soon as I do." I was positive there would be more instructions now that I was officially an employee. (Spoiler alert: There weren't.)

My girlfriend and I had a more involved conversation. We had only been together for about six months at that point. It would have been easy to call it quits. Ottawa was a long way away, and I don't

think either of us was particularly excited about a long-distance relationship. Ottawa wasn't a permanent post, though. There was a chance I could get back. I had to complete French training and then intelligence officer training. That would be about a year and a half. After that I could get a posting in the Toronto office. There was a light at the end of the tunnel. Everyone stressed throughout the recruitment process that mobility was tricky and just because you wanted Toronto didn't mean you would get it. On the flip side, Toronto was the largest regional office, so there were better than zero odds. It was a gamble, and we rolled the dice that it would all work out. (Another spoiler alert: It didn't.)

10

THE BEST JOB IN THE WORLD

My time in special operations did not revolve around a single case, plot or large group that monopolized all of the Service resources the way larger files like the Toronto 18 or the Via Rail guys had in the past. Rather, at times different individuals in the region rose and fell on the priority list based on the most recent reporting and opportunities that would arise. There wasn't an investigation that we didn't touch in some small way. We were mercenaries brought in on a file to help fill specific intelligence gaps that human sources were not able to report on. For the next two years I was everywhere—and of course never there.

I loved working in the unit. It was an adrenaline rush and a feeling of accomplishment that I may never experience again. The high-stakes covert recruitments, the nighttime missions. I grew extremely close with the members of my security team. We'd have lunch together almost every day and hang out outside of work. I will always owe a debt of gratitude to them for their support in both doing the work and helping me deal with the surrealness of where we worked and what we were asked to do. Even the techs who would

occasionally drive me crazy will always be my brothers and sisters for the times we shared and the things we accomplished together. But like any job, special ops had its ups and downs, and like in any family, there were also tough moments with my teammates and siblings. The bureaucracy, the technology and even the weather would at times take some of the joy and fun out of what was an otherwise amazing job.

It's Frickin' Freezing

If I were to point to a single adversary I faced that caused me the most stress, frustration and pain, I'd have to point my finger at the weather. It just so happened that the Toronto winter in 2015 was one of the coldest of all time. It was a polar vortex unlike anything I had ever experienced. Every day was minus twenty. It just wreaked havoc on our missions, equipment and morale.

Weather was always a big consideration when planning an operation. On a nice warm summer night, you are far more likely to get people up late, hanging outside, or worse, sleeping with their windows open. Conversely, rain really can be your best friend. It's not great to work in if you are going somewhere and don't want to get things wet, but it certainly is useful in keeping people indoors and providing some noise cover for any activity outside. Plus, it has a way of washing away traces showing you were there. The worst of the worst weather is cold and snow. That winter we had plenty of both.

It's very hard to not leave any tracks in snow. One night we were planning an entry into the office of a target. It was an industrial park in the suburbs. We knew it would be quiet in the evening. As we headed to our McDonald's pre-operation bathroom break, it started to lightly snow. It didn't look like there was going to be much or that it would stay on the ground, so we continued on. It didn't stop.

At the complex, a pathway that had been cleared earlier that day was now covered with a light dusting of snow. It was enough to leave footprints. Nobody was supposed to be there, and the sight of many footprints leading in and out of the building from the parking lot

would be suspicious. If we thought that the snow would be heavier or continue throughout the night, we wouldn't have been as concerned, but the weather wasn't guaranteed to cooperate. It wasn't snowing enough to cover our tracks and it wasn't warm enough for us to be confident the snow would melt and remove the evidence.

There was an option to wait. There is almost always an option to wait. It's tough, though, because when everyone is mobilized and the overtime clock is running, we all would prefer to find a solution than admit that things couldn't be done. These operations were by their nature risky. We built up trust and credibility with our management by conducting successful operations. In the back of our minds, we were always concerned that by admitting something couldn't be done, we would erode that confidence. The next time we proposed a job in winter, they might hold a missed opportunity against us. It wasn't an antagonistic relationship; it was a delicate one.

We did the job as smoothly as we could and got back to our car to survey the damage. It was clear someone had been there. Would it be less noticeable in four hours? We didn't know, and we couldn't take the risk. We had a shovel in the trunk. I didn't want to shovel the entire area if I could avoid it. It might make too much noise and take some time. I didn't want to be in the neighbourhood any longer than I had to. The snow that had been previously cleared was in a large pile beside the path. I tried to see if I could spread some of it from the pile back evenly over the path and around our vehicle. If anyone had been looking it would have appeared quite bizarre. Why is this guy taking snow that has been shovelled and placing it back on the ground? Regardless of the optics, the bigger problem was it wasn't working so well. The snow on the pile had hardened. The snow on the ground was loose. I was putting chunks on the path rather than a dusting that would blend in. The same went for the parking lot and the area around our car. It clearly looked like a uniquely disturbed area compared to the uniform snow cover in the rest of the lot.

I put the shovel back in the trunk and took out a blanket. I thought we could simply smooth over the area to make it look more uniform. We would quietly wipe away our tracks or at least blend them in so you couldn't see a large number of footprints. Once again, if

someone was watching they would be curious why someone was now dragging a blanket across the path and parking lot. It looked weird but it worked. It erased the footprints. Any snow that would fall on top of that would be even and mask our presence further.

We were confident, but a few of us went back in the morning just to double check. If it had looked really bad, we'd have needed to try something else. It didn't end up mattering. Enough snow had fallen that our tracks were well covered over. There was no trace except for the wet blanket we still had in the trunk of the car.

Everyone Back in the Van

That office job was a nice respite from the outdoors, especially given the issues we had with the snow. In the middle of that same winter, during the coldest snap, we got a request for another car job. It would be parked in an above-ground residential parking lot in front of the owner's building and some surrounding high rises. This wasn't a particularly nice part of town, and during our survey of the neighbourhood we had seen some vehicle content theft—kids checking car door handles to see if any were open so they could take what was inside. We had also seen some low-level drug dealing happening in the lot and on neighbouring streets.

We briefed the surveillants in advance. Given the layout of the lot and surrounding buildings, a few of them would need to be outside and on foot to establish a good perimeter. They were all extremely professional, and although I'm sure there was some squabbling between them about who would get the assignments to hang outside in the freezing temperatures for an extended period of time, they never raised an objection with us.

That night was worse than we expected. It was bitterly cold. We all had our bulkiest snow jackets and toques on. It would be tough to use the radios with thick gloves, so we went with thin ones or kept our hands buried in our pockets. I felt for the techs. They would have the real challenge. They had to manipulate their equipment in the cold, and I knew they were very concerned the temperatures would

affect the gear. The techs liked to build in excuses in case things didn't work. It wasn't unusual for them to say they would have liked more time to test their gear or they didn't have enough advanced knowledge of the target area so they couldn't predict if it would be compatible. I took most of these complaints as a cover-your-ass exercise; I probably had more faith in them than they had in themselves. This night, however, I shared their concern.

As was normal practice, the surveillants would take up their positions first. They are experts at blending in and getting a sense of the area. I didn't want to leave them out there too long because once the area is secure it may not stay that way. Also, it was really fucking cold, and they would look out of place. Nobody would just be hanging around outside on a night like that.

The bulk of our team was waiting nearby for the all clear. It came and we moved into position. We were in a van and drove into the parking lot. We sat for a moment to get a sense of our immediate area. It was clear, so we started to disembark. As team lead, I was riding shotgun. I got out first to provide watch as the techs left the van. With all the extra layers, it took a few moments for everyone to gather themselves.

I was looking to the rear of the van when I heard the driver come over our radio: "Someone's coming." I turned to look to the front and could make out one of our surveillants walking towards us. He gave me a wave and was fidgeting with his earpiece. It looked like he was having technical problems but wanted to tell us something. I told everyone to freeze. This wasn't a good sign and we'd need to see what the issue was before we could continue. He was coming from a good distance and he was all bundled up. He was walking straight towards us, but nothing was coming in over the radio. Maybe everyone's radios were out?

He'd got to about ten metres away when we realized it wasn't a surveillant. It was a drug dealer. He wasn't threatening or in a particular hurry. We had seen this before on an evening survey. Someone pulled up in the proximity of where we'd pulled up and someone else came out to meet them. We'd assumed that you would call to make an appointment and that this activity wouldn't be happening

this late or on a night this cold. We were wrong. This guy was a real professional, still vigilantly looking out for potential customers and willing to brave the freezing temperatures to serve them. We didn't stick around long enough to hear what was on offer.

"Everyone back in the van!" I called out.

We piled back in and left the parking lot before he got close enough to negotiate a deal.

Technology Can Break Your Heart

That winter was particularly hard on our equipment, which only added to the existing stress of planning and executing successful operations. There were things I could control as the security team lead—how we staged the operation, what we did, when we did it—ultimately, though, we relied heavily on technological tools and equipment, and that was something I couldn't control. Dealing with management and the techs could be challenging. Yet nothing was as frustrating as dealing with technology that just never seemed to want to cooperate. We were constantly at its mercy. I cannot get into the types of tools we used or what we did with them. I do however want to explain how soul destroying they could be.

Every operation required a choice of what type of device we might use, and each choice involved a trade-off. A lot of the time it felt like there were no good options. My tech guys showed me a device when I first started on the job. It was a little half-inch box of a thing, and they said, "Here's your implant." That's fantastic, I thought. We could hide that anywhere. Then they showed me a brick of what must have been thirty-four D batteries and said, "And here's your power. That should get you a few months." Their message was clear. If you don't find us a power source, we will use batteries. And here's the thing about batteries: small batteries are great for hiding; big batteries last longer. All batteries die.

A number of things can kill a battery. A lot of use obviously is one; so is the cold weather. And did I mention that 2015 was one of the coldest winters in Toronto history? I still shiver thinking about

it. We were constantly working because our batteries were dying all over the place. In one rushed case we used a tracking device for a car thinking it would last for months, and a couple weeks later our techs sheepishly came into my office to say that the device was running low. "You said it'd last for six months," I questioned them. "Yes, but it was cold, and they were driving a lot." I was told since we hadn't had the tracking device before, they could only guess on what the usage would be. Apparently with the bad weather the target was walking less so the device was collecting and transmitting much more information than we'd originally thought. It was a double-whammy battery drain. What could I say?

Other devices or software implants would occasionally seize up too, like all technology does from time to time. Think about any time you've had something happen with a phone, modem or computer that can be solved by simply turning it off and starting it back up again. Sometimes our devices would also freeze and need to be restarted. Maybe there was a power surge and they needed to be rebooted or reset. It could be maddening when we'd taken the time and effort to put a device somewhere we didn't have access to, and then it stopped working. The whole point of close-access operations is to hide the device so the target can't find it. That also makes it pretty difficult to get easy access to power it off and back on. Most of the time it just isn't possible.

Submitting an operational plan required a lot of work and approvals. Management would sign off on our recommendations. It hurt our credibility when stuff didn't work the way we said it would. And it was embarrassing to submit a plan for approvals that said, "Breaking into house to hit reset on the device," or, "Changing the batteries on a device we've already placed there." I've definitely written one or two of those.

A dying battery wasn't the worst technology fix operational plan I had to write. I lost one device a day after we implanted it. We had managed to get our hands on a target's computer. It took months of work, some good luck and a few bucks. It was a big coup and I was psyched. The technical guys were able to load it up with lots of great software that would give us all the access we could have ever wanted.

It was then returned to the target (not directly), and I gave myself a pat on the back for a successful operation.

The very next day I was in the bullpen with the techs and I excitedly asked how it was going.

"We lost it," they told me flatly.

"What? No, the computer was returned." I assumed they thought they'd lost the computer since it was no longer in their office.

"We lost the implant," they clarified.

"What do you mean? We just put it in yesterday." What I was really asking was, Who screwed up? I'd literally handed them a computer and gave them unlimited time to make sure everything worked. It was the best they could hope for. Had they not tested it properly? Had they not installed it properly? They understood my disappointment but were unmoved by my pleas.

"There was an operating system patch and we lost it." Nobody was to blame, they shrugged. "That just happens sometimes."

I wasn't a tech, so there wasn't much I could say. I didn't question them often. That doesn't mean I wasn't suspicious at times that they weren't giving me the whole story. I knew we were on the same team, but they also looked out for each other. There was definitely a code among the techs. I knew something was wrong on a job when I could see them huddling together and whispering. They would inevitably emerge from this formation with the explanation to the mission lead about a problem that was nobody's fault but had to be dealt with nonetheless. The tech team's collusion and message control was a standing joke we'd tease them about. They'd laugh it off, in no way denying that was exactly what was happening.

In a way we were at their mercy. I didn't have the technical knowledge to challenge them on their solutions. I was also much less experienced. If they made a request or suggested doing something that I didn't think would work, they'd always come back with some precedent that predated me and claim, "We do this all the time." It was my job to push back, and it was my nature to do so gently. On one freezing cold winter's day spent changing batteries, I lost it.

We were doing a repair job on some gear we had in a friendly location outside. Once again, the batteries had run out due to the weather and an underestimation of their usage requirement. It was a

secure area. We took our usual place beside the techs while they did their work, switching out our teams back and forth to give everyone some time to heat up in a car we kept running nearby. I had dressed for my day. I had fur-lined boots, long underwear, heavy gloves—it was still miserable. The conditions, the reason we were there and the fact that it was taking longer that it should have really started to get to me.

Finally, I was informed that everything was fixed and would definitely now last much longer than before. It was a sweet relief. All that was left to do was test the equipment with the gear at the office to make sure everything was relaying well on their side. The techs would test things when they were working on them in place, and it was good to do another test back at the office if we had the chance. It would ensure things were still working and connecting like we needed them to. That way if they weren't, we still had an opportunity to go back to make any tweaks.

I was standing by the equipment waiting for the word to come over the radio. Nothing came. I was all alone at this point. The techs who were with me had now taken shelter to coordinate the live test from the comfort of the car.

"What's going on, guys?" I asked over the radio.

"One second," came the response from the on-site tech.

I waited a few minutes.

"We all done here, guys?" I asked again. "Do you need to come back out to fix anything?"

"No, no, we're good. Should just be a minute. Waiting on the office."

I continued to wait alone for a final confirmation call that never came. I was getting colder and more irate. If something needed to be fixed, they should have been out there working on it with me.

"What's up, guys? What's HQ saying? We need to get back on this?"

There was a long pause. Finally a tech came back to me over the radio.

"HQ's gone to grab a coffee. We're waiting for him to come back. Should be any minute now. Then we can run the test."

"Are you fucking kidding me?" The tech in the office had been sitting on his ass all day waiting for us to be done to run this test. None

of our techs on the job had bothered to tell him we were getting close, to get ready for the two minutes we'd need him? The guy hadn't checked in to see if we were close before taking his afternoon coffee break, either. Meanwhile everyone was trying to keep this from me as I was twisting in the frozen wind waiting for an "all clear" call they knew wasn't coming. I was pissed and I let them know it. That was serious tech huddle cover-your-ass bullshit, and I didn't need to be an engineer to know that was one hundred percent their fault. It was cathartic to be so clearly in the right.

The test was ultimately successful and the device was fixed. I rushed back into the heated car to join the rest of the team. My body and mood started to warm up again. That's when the ribbing started in on me. People weren't used to seeing me worked up and they got a kick out of it. We were a close group that worked together a lot. In the moment frustrations were usually either forgotten or brought up to tease each other over coffees or beers. The techs had their quirks and we intelligence officers had ours too. That could lead to some standoffs. But we were still a team, and ultimately nothing was more unifying than a working device.

A Place to Call Home

We weren't always borrowing other people's homes. Sometimes we needed a place of our own, and the special operations security team was responsible for making it happen. We'd refer to these as safe houses; really, that's a catch-all term for any place where meetings or conversations could happen discreetly, with no connection to CSIS. These were unique circumstances. As you can tell from my career, most meetings happen in coffee shops and hotel rooms, but a safe house could be required in the exceptional case where extra security was needed to debrief a human source, or where a fully private and unassociated venue was required to accommodate a particularly sensitive operation.

My job would be to rent or procure an apartment and make sure it looked lived in so as not to draw attention to it. We wouldn't want

a property manager or maintenance person to walk in and find a completely empty space. I would need to furnish and regularly visit the place. The furnishings were generally moved around from safe house to safe house. It was a real mishmash of stuff. A lot of it was donated by previous members of the special operations teams, and I contributed items to the collection too. Rather than take things down to the garbage room in my building when I moved condos, I donated them to the safe houses. It was the same for clothes. I think if anyone actually went through the closet in a safe house, they would be surprised to see the range of clothing sizes and styles. These closet props had been accumulating and moving around buildings probably since the 1990s.

Ideally, when setting up a safe house, it would be like a cover story. You'd try to paint a picture of who lived there and decorate and furnish the place accordingly. Over the years that didn't quite stay consistent, though. There'd be lots of men's items, a few women's and this random bag of baby clothes, with no accompanying baby furniture or accessories. There would be minimal food in the fridge (because we didn't want food going bad) and typically a few cans of beer. It actually painted quite a sad picture—which wasn't necessarily bad since it might ward off questions from any inquiring property managers.

Covert procurement was responsible for all aspects of the space. I'd check the mail, clean and generally keep the place looking lived in. For some places, in the wintertime, I'd make sure to stop by more frequently to run the water and flush toilets to keep the pipes from freezing. It didn't require a lot of maintenance, but there was some. We didn't even use the places. They were for source handlers and their sources. We never got any complaints—except for once.

We were closing down a safe house and moving the contents to another location. It was the day before the last meeting was scheduled to occur with the human source. Ideally, we would do this afterwards, but the timing didn't work out. We moved everything out of the place and left two chairs facing each other in the living room so the source and the investigator wouldn't have to sit on the floor for their last conversation. We thought we were being helpful.

Apparently, the source opened the door and saw the apartment empty with only two chairs and thought they were going to get seriously interrogated, or worse. It looked like something straight out of a gangster movie—there may as well have been newspaper or plastic wrap lining the floor. It took a while for the handler to calm the source down.

One Man's Trash

Special operations wasn't all fun and games, though. It also had a dark and smelly side. The least glamorous aspect was obtaining garbage. That old expression "one man's trash is another man's treasure" cannot be talking about literal trash. If there is anything worse than your own garbage, it's going through someone else's.

For a while it seemed like everyone we were investigating had small children and I was just constantly wading through piles of dirty diapers. It was revolting. I joked with my wife that we should start throwing out all of our paper phone and banking statements in our kid's dirty diapers. My feeling was, if I'm going to get spied on or be a victim of fraud, I want that person to have to earn it!

Garbage collection was also the most regulated and administrative of our special operations. CSIS is still a government organization, and health and safety rules applied. There were full hazmat suits, washing stations and procedures we were expected to follow. In typical government fashion, we would have to watch a video about handling garbage safely before we were allowed to go through the trash. This was a requirement. If I were smarter, I would have gotten out of watching that video so I'd never actually have had to do it.

Handling garbage safely was one thing. We also had to consider storing it. In 2008, CSIS got "scolded" by the Supreme Court of Canada for destroying operational notes. In short, a ruling now meant we had to retain every scrap of paper that supported an operational report. Once again, being government, we received training on how to file notes. We were all trained on the proper file folder to use, how to cite the case file, where to take it, what should be included, how long it should be retained for, et cetera.

The requirement to preserve the official record proved a very special challenge for garbage. How were we expected to handle garbage? Should we put it in the file folder? Should we leave it in a freezer? Should there be a special freezer file folder for all garbage collected? Mercifully we never had to go that far in my time there. We found a few receipts and notes that we were able to file regularly. I always thought it would be some kind of justice, though, if a bad guy did put a critical piece of intelligence in a diaper, we found it, then years later, when they made a request to see all evidence held against them, we were able to produce it, let it thaw out and mail it to them.

Not Moving Fast Enough to Catch IP Ghosts

The cleanest and least dangerous part of covert procurement was serving warrants to telecommunications providers to track down subscriber information for phone and internet users. It could also be the most frustrating. In Canada we have a few major telecom companies, but as I learned there are also many small resellers of phone numbers and website hosting services. Tracking down these smaller providers could be incredibly time consuming, and we were already dealing with information that got stale very quickly.

Some legal background: In 2007 Matthew David Spencer was charged with downloading child pornography using peer-to-peer file-sharing software. The police approached the service provider without a search warrant and asked for the information behind Spencer's IP address. The company voluntarily obliged, and that information led to the police getting a search warrant and ultimately finding his computer, resulting in an arrest. However, the Supreme Court found that the police needed a warrant to even get the information from the provider. This was a victory, I suppose, for privacy advocates, but it was a pain in the ass for us (and, I'm assuming, for law enforcement).

The challenge was the amount of paperwork and the time it took for those requests to make it to my briefcase for delivery. In the case of a suspected malicious IP address, it had to be detected and

then, after analysis, determined to be malicious. That determination would be documented and approved at senior levels. A warrant or court order would then need to be drafted and sent to a judge for a ruling. Upon approval by a judge, someone would have to draft a memo or request to get the subscriber information for that user. That request would have to be approved at appropriate levels. Then it would be sent to a regional investigator like me to track it down. The regional investigator would conduct their own due diligence to determine who to approach for the underlying information. Many people use the large providers but, as I mentioned, there are a number of small resellers who buy and resell bandwidth and server space to clients. These resellers often do not have offices, only rented cage space in large co-located data centres.

I did my best. I learned quickly not to bother going to the registered office of the hosting business. Instead I'd track down the ultimate owner of the company at home. I made sure to go in the afternoon; even then, there was a seventy-five percent likelihood they were in their pyjamas. I saw a surprisingly large number of people in their pyjamas over the years.

These smaller players were always willing to help and were often more frustrated than I was about the whole situation. Largely for cost reasons they typically didn't keep the information for more than a few days. Depending on how long it took for the request to be approved and get to me and for me to track down the reseller, that underlying subscriber information might be gone. At the very least it would be pretty dated and therefore not as useful or actionable.

It turned into an odd exchange. I'd knock on the door, explain who I was and what I wanted and then get lectured on how bad it was that it took me so long to get there. Didn't I realize how perishable the information was? Did I not understand how these things worked? In my community interviews I often got to pretend that I was all-knowing; with these service providers I had to convince them that I wasn't completely out to lunch.

I know there is a lot of talk about what subscriber information should be available without a warrant and even rules for preserving that underlying information. All I can tell you as the guy on the ground trying to track these things down is that we need to make this

process smoother and more efficient. We are chasing things that are moving much faster than we can keep up with. I am not a lawyer. As a practitioner, it was extremely frustrating trying to carry out this function of my duties. I would get the request for assistance and see the date of the call or click that I was trying to track down and realize right away how little chance there was that I would be able to get the relevant information—and even if I could, that it would be useful by the time I did. There simply has to be a better way.

Who's in Charge: When the Plan Changes

At CSIS, there wasn't much we could do about court rulings and occupational health and safety requirements. Sometimes, however, our internal bureaucracy and personality conflicts could make us our own worst enemy. Before we conducted any operation, the plan for the job would go through a very long approval process. Management had to sign off, and they would only do so with input from all stakeholders as well as support from our headquarters counterparts. These were some of the most complicated and risky operations. Employee safety, the secrecy of the investigation and the CSIS reputation could be compromised if any number of things went wrong on a job. Therefore, there were a lot of people and groups within the organization that needed to be on board and have their concerns mitigated.

That is why the approval process for any operation could be contentious. There's a lot of inside baseball that doesn't make for interesting reading. What is important to note is that even after all the horse-trading and compromises, it was generally acknowledged at all levels that things would happen in the course of the operation that we didn't or couldn't account for. Many real-time decisions would have to be made on the ground. When that happened, protocols and procedures existed for the people conducting the operation to make a change. And for the most part, the teams in the field were trusted to make that call. For the most part.

We had a plan in place for a car job in the Windsor area. It was about a four-hour drive from the office in downtown Toronto. We were going to target the vehicle when it would be parked near the

individual's home overnight. It was a classic evening job that everyone was happy with. It would turn into anything but. We were already in Windsor when we got some reports that the target was going to be working late that evening and then heading over to his girlfriend's house. If this had been in Toronto, we would have simply aborted the job for that night. Presumably we would have been able to do it another night when the target and car were at home. At that point, however, we were already in Windsor with a large team. It was a big commitment of resources to be wasting and it might have been tough to justify and coordinate getting everyone back out again. We were already there. This was our window. We were staying overnight anyway. We needed a new plan.

We scoped out the target's workplace to see where the car was parked and where he would be for his shift. Let's just say it was a "food outlet" and he was working the counter. He did not have a direct line of sight to his vehicle, but it wasn't very far away. We thought maybe it would be a minute max. That wasn't a great buffer, especially when the person was working and not asleep at home.

We took a few minutes, as a team, to put a new plan together. We were huddling around our car in a suburban parking lot. We got out some pens, paperclips and other items from our bags to make a map on the ground to orient ourselves and make sure we were all on the same page. It was like kids designing plays in the dirt with sticks and pebbles in the middle of a neighbourhood football game.

We would have a member of our team go into the target's workplace to engage him and keep him occupied. Not only would this keep him there but, worst-case scenario, we would also have some sort of warning if he was on the move. We also put precautions in place to secure the area from witnesses or passersby.

I thought it was a reasonable plan that had a better-than-good chance of success. It was the same car. We had the same technical tools; all that had changed was our perimeter security. As the operational team lead, that was my call. I was comfortable with it. I ran it by my boss; she was not.

My boss was back in Toronto. She was aware of the target plan change as I had been in regular contact with her throughout the day

to let her know what was happening. I gave her a call and provided the most recent update. We had a suitable alternative that I felt was secure and, given the circumstances—we were out of town, the clock was running, overtime was accumulating—we were going to go for it. I tried to make it sound as though I was briefing, not asking; then my boss started asking questions and I knew I was in trouble. She wanted to see the photo of the paperclips. She asked me about the lighting. This was a cold call gone bad. We were negotiating, and I was losing.

I'd made this phone call in front of the team expecting a quick word of support. I realized right away this was not going to be a conversation either my boss or I wanted to have in front of them. I tucked my head and phone down low into my chest and turned around to give myself some privacy. The act itself revealed to the team that something was wrong. The conversation I was having was worse. There's a reason they say it's sometimes better to ask for forgiveness rather than permission.

I was blunt: "Do you expect me to type this all up on my phone and email you a new plan from the parking lot? It's 10:30 p.m. Are you going to wake up senior management? We don't have that time." She told me to stand down. She needed to get my new plan approved. She wanted to go through the whole process again. I was stunned.

The policy and standard operating procedures state that the team lead has latitude to make adjustments on the fly. We simply couldn't clear every hurdle we encountered with our superiors. If we'd been in Toronto, she may have even known the area and been more comfortable with the variation. We were in Windsor and she was hundreds of kilometres away.

"Give me the big bullets," she said. "I want to look at it."

It wouldn't surprise my boss to read that she had a well-earned reputation as a micromanager. My own personality tends towards deferential. Like with the polygraph: I'm a pleaser. It was a bad mix. She was also a new supervisor on our team. We didn't have a long history working together at that point. A different boss with more familiarity with me and the team may have trusted us to do the job. A more direct intelligence officer with established credibility with

his manager might have just done it without asking. That's not who or where we were.

As for the mission at hand, we were running out of time. We thought the target might work until 11:00 or 11:30 and then head over to his girlfriend's house. We didn't know for sure. We did not have a plan for the girlfriend's house. This was our best and likely only chance.

I was in a very uncomfortable position. I had an entire team of people waiting to do this job. I remember it very clearly. About ten of us were in a parking lot a few blocks away from the target's workplace. There were more waiting in cars nearby. The more experienced special operations officers were pleading with me to make the call. They were adamant it was within my authority and they swore they would all stand behind the plan. We needed to go now, they confidently asserted, and I didn't need permission.

On the other end of the phone was my direct supervisor. She was telling me she was going to call management to advise them of the change in plans. I felt I had two options. I could tell my supervisor I was making the call under the powers given to the operational team lead. I could have stated it in a way that implied it was a done deal and I was just advising. I knew that while just going ahead might have solved a short-term problem, it would cause me a lot of headaches going forward. The unit had lots of jobs in the works, and I wanted to be a part of them. I took door number two and asked for permission. I said, "We have a good plan. We are running out of time. Can I go ahead?" My boss said no.

At that point there wasn't much I could do. It's one thing to assert the authority I had; however, I'd effectively conceded that authority when I'd asked if it was okay. After that, I would be disobeying an order.

I looked over at the team and could see how disappointed they were in me. There is a strong bond, a camaraderie in special ops, forged during previous missions and in the trust we all put into each other when we have a job. We do our best for each other whether we are Number One or Five. Up to that moment it had been another bonding moment for our team. We had an obstacle and we'd worked together to come up with a solution. We were proud of that solution

and wanted to get it done. The boss was saying no, and in the movies the renegades say "fuck the authorities" and get the job done anyway. That's not what I did. I sided with management. My team took it as a betrayal. It was a lonely feeling in that parking lot.

I tried to explain that we would hear back shortly. They didn't do a great job of hiding their frustration. Mercifully, I did get a call back quickly, but my boss just had more questions. She had been talking to management, and they had their own questions. We couldn't go on like this.

The dejection I saw on my team's face stiffened my spine. I reminded my boss that I didn't need permission; I was simply briefing up to advise. I said we needed to do the job now. I wasn't threatening—if anything, I wanted to give her confidence in me. Asking permission had put the ball back in her court, and since she was not on site it wasn't necessarily a fair thing to ask, especially of a detail-oriented micromanager. I needed to take back some control.

I think her conversation with her own supervisors had probably been as frustrating as mine and that helped get her back on board. She said, "I'm going to tell management that this is happening, and I'll call you back in two minutes with a go." To her credit, she did.

The team rallied. At the end of the day we did want to do the job, and now we were doing it. We got our game faces back on quickly. I was technically the team lead on this job, and typically the lead would be escorting the techs to the target vehicle. However, there were some experienced members on this job and I had to assign myself a different, less glamorous but crucial role for this operation—I would be holding the door.

There wasn't much room between the target and his vehicle. If he decided for whatever reason to go and check his car, it would only be a few seconds before he was on top of us. All that stood between us was his attention span and a building exit door that for fire code reasons could not be locked. We had planned to send someone inside to engage the target in conversation and keep him occupied; if that didn't work, we would need to delay him from stumbling upon us. We tried to back a car up to wedge the other side of the door but there wasn't enough space, and the longer we were back there driving around and making noise, the more likely he was to hear us,

which increased the possibility he would come and see what was going on. So, I volunteered myself to stand on the other side of that door and act as a human barricade to keep him or anyone else inside that building. My job was to keep that door closed with him on the other side until the team could complete the mission or get out of the area securely.

It was a pretty simple plan. The target was roughly my size. I thought there was a better than good chance I could hold him off. Looking back, there may have been some unanswered questions that senior management could have grilled us about, given the chance. Even I hadn't really considered what I would actually do if he managed to break through. What I did know was that it was a role I wasn't comfortable delegating to someone else, and given the makeup of my team that night, I was probably physically the best candidate.

I deployed from the van and took my position at the door. I didn't even look back to see what was happening at the car. I had effectively ceded control and oversight of the job to my Number Two. I couldn't run things from where I was, and the nature of the operation meant that if things did go wrong, Two would be responsible for getting everyone out of there. I had gone from the team lead to a literal doorstop. There are no egos on a job. We all had our roles, and for things to work everyone needed to do their part.

I dug my feet into the ground like a sprinter at the start of a race. At first, I put both of my arms straight in front of me. I quickly realized that if someone did try to bust through, they would probably break both my arms and my face. I turned sideways and leaned my whole body into the door—trying to get as much of my shoulder, forearm and opposite hand pressed firmly against it. I didn't wait to brace myself. The minute I got into position I pushed on that closed door as hard as I could. My shoulder hurt; my hands were white from the pressure. I didn't know if or when he might come, so all my energy went into pushing my whole body against that closed door, assuming he could come at any moment. Mercifully he never did.

I heard over the radio the job was going smoothly. The target was still engaged when they started to pack up. Then I was the last one left outside the van. I was still pushing with everything I had until I

got the call from Two that everyone was packed up. I peeled off the door quietly and started walking down the laneway to meet the rest of the team.

I rejoined everyone and got the full rundown. The job had gone off without any issues. The person we'd sent inside had kept the individual occupied, and we'd been able to get access to the vehicle without incident or anyone walking up on us. Everything had gone as smoothly as it could. I called my boss to let her know.

We got back to our hotel rooms that night and debriefed over a beer. This was typical, especially when we were on the road. We were staying overnight anyway, and it was always good to have a little time to wind down. We addressed what had happened. The armchair quarterbacks said their piece, and a little venting all around helped get unity restored.

I got back to the office the next day and my boss and I had our own closed-door meeting to hash out what we needed to do differently next time. It was a tough night and there were lessons learned for both of us. We were able to move past it, but some souring was starting to set in.

I didn't become a spy for the glory because I knew there wouldn't be any. Even my closest friends and family would never know what I did, and public acknowledgement wasn't on offer. I imagine if I tried to explain to my wife that we'd had a successful operation and that my critical role had been to hold a door that nobody came through, she would have given me a slightly bemused, "That's nice." My colleagues were the only ones who were there to witness my contribution and give me feedback on the meaning of it all. The minor spats and disagreements didn't linger interpersonally, but over time they definitely added up. The job was stressful and involved sacrifice. I was happy to do that to fight terrorists, but the constant little battles got to me.

To finish this story on a lighter note—and also give a quick example of how bureaucratic being a special operations operator could be—weeks later the team member who had gone into the restaurant to engage the target came sheepishly into the bullpen to ask for a favour. In order to keep the target occupied he had bought a bunch

of food. Unfortunately, I can't be more specific on what that was—I can say it was a lot. And it was a pretty random grab bag of stuff. The accounting team didn't like the fact that we hadn't gotten appropriate prior approvals for the expense. They also questioned why he needed so many things and whether he was trying to get the government to subsidize his late-night snack.

This led to a debate with the finance team about whether this food purchase should be expensed as a travel food stipend and count against his eligible per diem. They asked if he'd shared his bounty and who else should be on the hook for the expense and potential per diem clawback. It was silly. His job had been to keep the target busy, so getting him to make or ring up a bunch of food was a totally reasonable solution. I ended up having to write a memo, which was signed off by my management team, stating that the items ordered were an operational requirement and an eligible expense.

Unsecure and Insecure

If I'm totally honest, I have to admit the big and little battles had an effect on my performance at work. I was doing very cool stuff, but it was still a job, one that came with highs and lows of challenge, fulfillment and doubt. The highs were unbelievable. The lows and the minor annoyances stuck with me just as much, if not more. I was serving my country, but my day-to-day accountability was to my supervisor and most of all my team. My original reason for joining CSIS was to make a difference in the world. It was easy to lose sight of that years later when the realities of the job were more front of mind than the purpose behind why I was there. After a while, my motivation came from the expectations and performance of those around me, and in some cases led to decisions I look back on with regret.

We had just completed a nighttime operation planting a listening device. I was not the team lead. I was, however, the most senior member of our special ops team and was mentoring a junior member of our unit who was getting some of his first lead experience. It was a bit messy as to who was responsible and accountable. It wasn't my

name on the plan; I was there to look after things and make sure it all went well. In my mind, it had.

We left the building and gathered back at our rendezvous point to make sure everything was working properly. It was late, and we were all tired but still wired from the adrenaline of the job. There was a rush that came from completing an operation. It was in those moments directly afterwards, still together as a group, that we really got to revel in it all. That night not everyone was feeling so good.

The team lead and I checked in with our lead tech. He was hunched over his computer in the back seat of the car showing the screen to a member of his own team. He gave me the thumbs up that the gear was still working and transmitting. I could see, though, that neither of them was totally happy with what they were seeing. I asked again, "Everything okay?"

"Uh, yeah," he replied, in a not very convincing fashion.

I made a good-natured but half-serious joke about the battery already dying and how I looked forward to going back to fix it tomorrow. He looked at me straight, like he was looking for the words to say, and then said, "Nah, I think we're okay."

That really didn't sit well with me. It didn't sit well with the team lead, either. He also picked up the apprehension in the tech's voice. We looked at each other and realized we were going to need to have a conversation. It was time for a team huddle.

The team lead and I climbed into the front seats, turning our bodies to lean over the middle arm rest to engage the techs directly.

"What's wrong?" I asked. "Is it working?"

"Yes, it's working," the lead tech confirmed. He was adamant it was working. "As I was leaving, I thought I felt it wiggle a bit."

"Wiggle?" I asked.

The team lead got right to the point. "What does that mean?"

"I think it might be a little loose," the tech mumbled.

"What?" I snapped back at him. It came out harsher than it should have been.

"No, look, I'm sure it's fine."

I looked at the team lead and he looked at me. This was not a good spot to be in. Our job as security was to check the gear to make sure it

was fine. This meant we looked at it. I would have never thought to touch or move the device to test its structural soundness. The techs would have lost their minds, and they would have blamed me forever if it didn't work. If I had, if someone had, we'd now be able to give the tech a second opinion and the reassurance he seemed desperately to need.

That's what would have happened if that conversation had occurred during the operation. It wouldn't have been a problem. We would have taken a few minutes and fixed it. Now we were in the parking lot sitting in our car.

The surveillants were still in the area, though. They were always the last to leave an operational zone. They were covering us as we got out and also kept some eyes on the area to make sure nothing weird happened after we left. They were exposed and waiting on us to give them the all clear that they could leave. It was late and they wanted to go home. When the call didn't come as soon as usual, they decided to check in.

We were all sitting in quiet contemplation when the surveillance team lead called over the radio. "We all good here, guys? Can we get out of here?"

"Hang tight. Just testing the gear," the team lead shot back.

We looked at the tech, who looked back at us. In my mind it all hinged on the lead tech and his recollection of whether the device had wiggled or not. Although it was an option, he knew we didn't want to go back. He didn't want to go back either. I'm sure he was hoping we would spare him from having to make that decision. Though he was brave to mention it, he wasn't willing to commit. And if he wanted us to make the decision for him, we weren't going to. This was the constant balance between the security team and the techs. They were the experts and often had more experience. We were expected to make the final call on things. We relied on them for the information to make informed decisions. In that moment, that's where we were. If he said it was loose, we'd go back. If he said it was fine, we'd let it go.

It was tense in that car. The excitement of a job well done had turned into a standoff. We were annoyed at the tech's indecision, and

I'm sure he was annoyed at us for being annoyed. The team lead looked at me and I looked at the tech and the tech stared back down at his computer screen to make sure the device was still working. He was probably quietly hoping it would fail, to give them an excuse. It was working fine.

At that point we should have gone back. We had the surveillance team in place, and it would have given everyone peace of mind. As the security team, we should have mandated it. We didn't. We accepted his semi-confident reassurance and decided to call it a night. The joy was sucked out of the occasion. At least we were done. We were all on the same page. It didn't wiggle. Everything was fine. Or so we thought.

I didn't sleep great, and clearly the lead tech had a bad night too. I showed up in the office the next morning and got an earful. He had confided up the chain that the device wasn't secure. He was more certain now than he had been in the car that there was a problem, or at least could be one. This was now a huge issue. The equipment is the most important, most top secret, most sensitive part of operations. And in the eyes of management, we had loose gear that could be discovered at any moment by the target.

We got chewed out by the highest levels of regional management and told we would all be working that night to fix the problem. The same team would be assembled. I was initially pissed, and this time I was on the other side, feeling betrayed by a colleague. In my mind the time to make that decision had been in the car, as a team. We totally would have gone back. We had given him the opportunity to speak his mind and he'd made his decision to let it go. What was even worse was he had told management before us. He could have come back the next morning and advised us of his growing concern. Then we all could have huddled again and come up with a plan together. Instead, I felt ambushed.

We went back that night. We'd had all day to calm down and it wasn't as tense as you might think. Ultimately, I respected that the tech was so concerned he'd felt he had to speak up, and I took responsibility for the fact that we should have just fixed it on the spot and not let it go. There was plenty of blame and shame to go

around. We had a job to do and we were all professional. Of course, this job did have a new wrinkle, and when we did get back into the operational zone, we all went and stood around that device when he tested it. I watched him put his hand on the equipment and do his best to give it a little jiggle.

"Well?" I asked.

"It's good!" he said, relieved. "I mean, I knew it was good. Just going to put a little more stuff on here to make sure, though."

"Good idea," I said as I let out a bit of a sigh under my breath.

Friends from Out of Town

Any tough talks and stressful stare downs on the job were far outweighed by the good times. I truly did like and enjoy the company of everyone I worked with. The tense and contentious moments are better stories, but the majority of my time was spent hanging out in the office, writing plans and joking around. There was also a lot of time out of the office sitting in a van surveying an area or waiting for an operation to start just shooting the shit. There was so much "hurry up and wait" time we filled with ribbing, practical jokes and a high esprit de corps.

I remember one night we were going to do a car job in a driveway and the neighbour's front room TV was on. The whole neighbourhood was dark except for this flashing blue light coming from next door. We assumed someone was there and from that window they had a direct view of where we planned to be working. We couldn't start the job until they were gone. So we waited. And we kept waiting. It was getting late and it was a weeknight. We started to think maybe the person had fallen asleep on the couch.

A surveillant did a walk-by to get a closer look. We called out questions over the radio to help us try to understand the situation. Was the TV channel changing? Were there commercials? What were they watching? Who was in it? The surveillant was relaying whatever information they could as we were trying to look up the TV schedule on our phones to figure out when this person might finally go to sleep.

The initial questions were serious: What was he watching and how long might be left? But the whole exercise degenerated into farce. Was this movie any good? What else was on that he was missing? What kind of cinephile were we dealing with who was staying up until 2 a.m. on a weeknight to finish this movie? It was this funny little moment, though I'm sure you had to be there to fully appreciate it. My point is that we shared many silly moments like this, in the back of the van killing time, enjoying each other's company, while we waited to go to work.

When we needed to move from a casual to an operational state, we'd flip the switch. But there were also times where we got to work in a controlled environment with almost unlimited time. In those operations we could allow ourselves to relax a bit and continue the joking, while doing the jobs that we all greatly enjoyed.

And nothing was more fun and brought the team together like an out-of-town visitor. It didn't happen often, but every once in a while we'd get some advance warning of a target passing through Toronto who didn't live in the city. We would have all the warranted powers and they were going to be on our turf. Much like in sports, the home team always has the advantage.

Visitors took a lot of the guesswork and surveying out of the operational plans. Often we'd have a hotel reservation well in advance. We'd know when they were coming, where they were staying and when they were leaving. Plus, it wasn't the target's house or another location that would be a challenge to access. Hotels were very open public spaces. It was easy to get in, out and around them in large groups, with lots of equipment in bags, without arousing suspicion.

It might be a good moment to quickly make clear that targets were not exclusively young wannabe jihadists, or any specific demographic. Targets of investigation—whether ideologically motivated violent extremists of all stripes, "non-traditional collectors" such as local researchers passing on sensitive or proprietary information to foreign states, or agents from hostile intelligence services conducting local influence operations in support of their own foreign policy objectives—had very diverse backgrounds and profiles. It was largely due to the nature of the time I worked at CSIS and

the desks I was assigned to that my investigations mostly revolved around terrorism.

In all target milieus, there could be entrepreneurs, labourers, students, trades, executives and other professionals of all ages and backgrounds. Toronto is a large city with financial service, technology and research hubs, so we had them all. Plus, with many international conventions and gatherings that attract a large number of participants from out of town, we occasionally got targets from other regions passing through, either in their normal course of business or specifically to conduct their threat-related activities here, such as foreign influence campaigns or recruiting. And no matter whether you are a local businessman conducting economic espionage activities on behalf of a foreign intelligence service or a young high school ISIS supporter with dreams of setting off bombs in downtown Toronto, everyone wants to visit Niagara Falls.

Getting Burned in the Departure Lounge

The airport, like hotels, was also a great place to conduct operations because it was a somewhat controlled environment and easy to blend in. The one complicating factor was the high approval and deconfliction required due to the number of agencies with jurisdiction there. Once all the coordination was done, the people on the ground from the many different departments were excellent to work with.

I'll never forget one time when I grabbed a target's suitcase and was carrying it for a search when the handle broke off. It was an old bag and looked beaten up; regardless, I thought the target would notice his handle missing and it would arouse some suspicion. We were being assisted by an agency, and our liaison could see that I was concerned about the situation. He came up to me and said, "You know how many bags we break around here? Don't even worry about it." It was funny and made me feel a little better—but not enough.

Thankfully our techs came to my rescue. They got out the needle and thread and fixed the handle so nobody would ever know there had been anything wrong. Putting things back to their natural state was their specialty and they were good at it. I was happy for their help.

Getting discovered by the target, a neighbour or even a hotel cleaner was always a risk to an operation; thankfully it never happened to me. Getting caught on a job by a friend was a close second, and it took eight years into my career until I was finally busted. Amazingly it would happen in an airport, which had typically been an operational refuge due to its transient patrons and general chaos.

I was at my sister-in-law's wedding brunch. She had just gotten married and some of the couple's closest friends and family were gathered for a midday celebration. The attendees were some of our closest friends and family too, yet only a handful knew where I worked or what I did. I had been to many events like this before and always managed to bluff my way through. And at that point, besides the just-trying-to-be-polite "How's work?" inquiry, nobody really asked me anymore.

I was lucky that the event was a brunch and not a dinner. I was scheduled to work that evening. It would be an unusual 8 p.m. operation. As was typical, my wife had no idea where I was going or what I would be doing, only that I would be out.

All was going fine until I overheard a family friend mention that she would be heading to the airport that night. She lived in Toronto, so this caught me a little off guard. Toronto Pearson is a huge airport. What are the odds? Really good, as it turns out.

I gently inquired, "Where are you going? What time?" It was the same flight I was interested in.

At that point I considered my options. What was the likelihood I'd be seen that night? I was sure the airport would be busy. I could wear a baseball cap or hooded sweatshirt. Maybe she wouldn't notice me. What if she did? Getting caught at the airport would make for a challenging cover story. It's one thing to wander into the same coffee shop. Being at the airport is not very random. Even if I could think of a good excuse, I'd have to deliver it to my friend, and that would take time, focus and energy away from the operation. Also, if she did see me and we'd just had this conversation about her trip, surely she'd be confused as to why I hadn't mentioned I'd be there too.

It was all a little too risky. It's hard enough to track one person in a crowded space. I didn't want to also have to be looking over my shoulder for my friend to make sure I was avoiding her. It would

be an obstacle to a successful mission, and I couldn't let her be a distraction.

I decided to confront the issue head-on and deal with it in advance. I pulled my friend and her husband aside at the brunch. I told them, "Look, I work for CSIS. We can have a longer conversation about this, but I need to tell you because you may run into me tonight at the airport and I need for you not to say hi." My friend is Jewish and immediately told me she had a friend who was in the Mossad, so she totally understood. I responded, "Thank you. And we should probably talk about your Mossad friend at some point."

Of course, the next question my friend asked me was, "Is there anything wrong with my plane?"

"No, no, no," I said. "It's okay. I promise."

Despite my best efforts not to let her presence distract me, it certainly did. I wasn't worried about her sneaking up on me; I was conscious of not getting close. She still wasn't supposed to know what I was doing or who I was with. I had now alerted her to my presence and the fact that something was going on. I was trained in the art of blending in and living my cover; she wasn't. It would be natural for her to look around and be inquisitive. I didn't want her to look strange or attract any attention and I thought that would be more likely if our paths crossed. I tried my best to keep my distance.

Everything worked out. We successfully did what we needed to do. When my friend got back from her trip she said she had seen me at the airport but had kept her distance as instructed. She still teases me a bit for getting caught and not being some invisible super spy. To this day I believe she only saw me because I'd told her I'd be there and she was looking. Nevertheless, it seemed like I'd made the right call.

I did feel bad because I sort of ruined her flight. I couldn't tell her anything about what I was doing, so she assumed the worst. Anytime anyone got up from their seat to go to the bathroom she kind of freaked out a little. I'd said there was nothing to be worried about. Of course, in her mind the fact I was there at all meant there must have been something to worry about. I apologized for causing a stressful flight and said I'd make it up to her over beers—while we talked about that Mossad friend of hers.

EPILOGUE

I HOPE I HAVE done a reasonable job of explaining the challenges we faced during my time at CSIS. While violent extremism remains a significant security threat, I'd now like to take a moment to look forward and talk about cyber security, explain why it's a unique challenge and make a final plea for everyone to stay vigilant and do their part to keep each other safe.

It's a big part of what I do now in the risk advisory practice I started when I left the Ontario Public Service. We conduct physical security threat risk assessments and recommend protective controls where we find gaps that can be exploited. I joke that I used to break into places, so I know how to help organizations defend themselves. We also do online exposure risk assessments to determine if an individual's digital footprint and internet activities are creating vulnerabilities in their physical lives. The origins of this cyber security risk relate back to trends that started when I was still doing covert operations.

Breaking Into Phones, Not Homes

The stories that the older techs and special operations IOs told about how much tougher the job was in their day were largely true. They operated in a different era. The close-access team used to have to get near the targets to physically place any listening or tracking

equipment in proximity to where we wanted to collect information. Now, everyone carries a microphone, camera and location tracker on them at all times in the form of their phone. All we have to do is get access to the devices to gather the information they are collecting for us.

The transition from close to remote access accelerated throughout my time in the special operations unit. The remote techs were increasingly able to get their hands on the same information as the close-access teams, from behind their computers. It changed the financial cost and risk profile of the operations completely. No more overtime for large teams. Even if we got caught hacking a phone, there was much more plausible deniability than being discovered in someone's house physically holding it.

The unfortunate truth is that for all the reasons that remote access has become a more attractive option for CSIS (and remember, these are the good people), the criminals and malicious foreign states took notice too. I actually witnessed this first-hand. We were sitting in the special operations bullpen one day trying to figure out how to get access to the computer of a target who we were told was very paranoid and technologically sophisticated. We were gaming out expensive and labour-intensive scenarios to break into his home when we were alerted urgently by one of our communications analysts who was listening to his calls. Apparently, the target had just been speaking to someone claiming to be Microsoft tech support, and for the fee of five hundred dollars they would "fix" an issue with his computer. The target agreed. It was amazing. We were listening over the phone as not only did the scammer break into the computer, but also the target actually paid him to do it.

This is the rapidly growing cyber threat we all face today. Online, bad guys aren't restricted to attacking people in their geographic location. They now have access to billions of people all over the world from the comfort of their own keyboard. The cost-benefit analysis of a cyberattack is also much different from that of a common criminal. The amount of time it takes to send a phishing email, and the likelihood of getting caught versus the potential award of having someone click the link, has made hacking an extremely attractive, lucrative and comfortable occupation.

Online Chum to the Cyber Sharks

So how do they get you? Well, in the early days phishing scams were almost quaint in their simplicity. I remember one attack another intelligence service used that included four text messages. They were, in order: naked picture, naked picture, malicious link, "oops that wasn't for you." There was a one hundred percent success rate. Sounds easy, right? Their joke was, "Do you know how many hours were spent selecting those naked pictures to make sure they were the right ones?!"

While we have definitely collectively raised our game from the naked picture texts, Britney Spears computer viruses and Nigerian prince email scams, I'm sorry to report that as our own digital security awareness improves, so does the sophistication of our attackers. We are now up against advanced social-engineering techniques to get us to click links and give up our credentials and sensitive information.

The attackers are aided by another trend that started while I was at CSIS: the explosion of data that is now publicly available about any individual. This can be the information we voluntarily place online about ourselves, but also data that is being collected about us from the apps we use or the internet-connected devices and other technology tools we have in our homes.

Think about all the social media and networking sites that are out there. Facebook launched after I graduated from university and it's already considered the site for boomers. I met my wife online (twice) and even that was before the current crop of sites like Tinder and Bumble. There are probably new ones that have come up in the time I've spent writing this epilogue. I'm not trying to make myself sound old but to highlight these numerous and growing large repositories of information that we continue to populate with details about our business interests, social network, family life and hobbies.

The sheer volume of this personal data available online has also had a dramatic effect on the spy game. It has become essential for recruiting human sources and covert procurement assistance. Back at CSIS, I'd never rely exclusively on my skills on the phone or at the door. In the early days, I would crudely try to profile people from

their profession, civic engagement or maybe old newspaper clippings, if I could find any. Now we can see who they are following on Instagram, what they like or retweet and who they are friends with on Facebook or connected to through LinkedIn. All of this helps paint a much better picture when trying to decide who to approach and how. This information is also available to those who wish to do harm. They can find vulnerable individuals with the access they want and then use publicly available information to target and exploit them.

As a quick side note to any future spies out there, this trend will affect how we monitor and assess our subjects of investigation. In addition to human source reporting and technical sources, we will have access to more and more of the target's publicly available information. The challenge will change from trying to get access to it to making sure that we are processing that raw information into good intelligence through sound analysis when assessing a target's threat-related activities.

Spying will always include recruiting and targeting individuals. Both of these pursuits will be increasingly aided and tested by the ever-expanding pervasiveness of the internet in our lives. The next generation of spies will need to have the ability to understand and use technical tools to process, synthesize, analyze and interpret this information for its relevance. My advice to the intelligence officers of the future is to get comfortable navigating this digital space.

Now back to my original point. My advice and plea to everyone else is this: Be careful out there. Because once again, the bad guys are getting better at all of this too.

Stay Vigilant—For Yourself and for All of Us!

At this point, you may be wondering why a former spy is worried about you being phished or scammed online. You also may be thinking you don't have anything of value for anyone to take. And some of you may even think, If they get me, they get me, so why should anyone else care? Well, for one, I don't want to see anyone get cyberstalked or lose money, their identity or worse. Additionally, you

absolutely do have valuable information, and more importantly you provide access to your friends, business and wider network online. For some, this could mean access to government secrets and sensitive information. I am writing this in my spy book because even if you aren't interested in taking steps to protect yourself, please do it for your friends, your co-workers and your country.

Don't just take it from me. This is something CSIS has been waving their arms about for the past few years. In the spirit of helping CSIS spread their message (you're welcome!), let me highlight the sentiments expressed in both the CSIS public reports and a 2021 speech given by the current CSIS director: economic espionage activities in Canada by hostile foreign states are having a devastating impact on our prosperity and sovereignty. Our adversaries are intent on stealing our intellectual property and advanced research, whether it be from the Canadian government, large corporations, small start-ups or universities. They are doing this the old-fashioned way by recruiting, coercing and partnering with local witting or unwitting accomplices to gather intelligence that would provide an economic, military or political advantage. They are also increasingly using cyber methods to target and exploit Canada and Canadians.

The ultimate public example of the devastation a state-sponsored remote attack can have on Canadian industry is Nortel, whose market capitalization fell from $398 billion in 2000 to less than $5 billion in 2002. The fall of Nortel has largely been attributed to a large-scale systematic hacking of the company by the Chinese military that was facilitated by them stealing some executive passwords. Reporting in 2020 from Global News and others suggests that Nortel was aware of the risks but dismissed them as "exaggerated spy novel plots." The cold reality is that by taking advantage of a few key individuals with the right access, the hackers were effectively able to destroy a one-time Canadian telecom industry giant.

Organizations need robust physical security controls to protect their people, assets and information. There is a collective need for increased cyber security awareness and vigilance as well. The Nortel case study demonstrates what makes this challenge so difficult to defend. The breaches of large organizations or small start-ups

with cutting-edge technology often originate with an individual who has allowed their personal access credentials to be compromised. People can be their company's or government's greatest asset, but they are also its biggest vulnerability. I can recommend high-security locks on a front door. We all have usernames, passwords and logins that can serve as their own keys to our wider and extremely valuable IT networks. Every single day the bad guys are trying to steal all of our keys.

I may no longer work for CSIS, but I still have a role to play in keeping Canada safe and prosperous. We all do—because we are only as strong as our weakest link. We all need to do our part. Bad things may unfortunately still happen. Like millions of people, I was a victim in the Yahoo! hacks. (To the hackers: If you wanted to know my fantasy football roster, you could have just asked.) The key is not to get discouraged. It's an ongoing battle. And while the threats may change, whatever we face, we are stronger and safer when we work together.

I know Canadians are always willing to help if asked. So consider this my knock on your door.