THE MPSA WOMEN'S OPERATIVE SERIES

GUARDIAN

BOOK 8

PHASE 3: ENGAGEMENT

MPSA COMPANION WORKBOOK

BOOK 8

GUARDIAN

The Science of Protecting What Matters: Home, Family, and Community

THE MPSA LIBRARY SERIES | BOOK EIGHT

For information about permissions or bulk purchases, contact:
Greylander Press, LLC
MissionPossibleSpyAcademy.com
Pro Bono Non Malo
Greylander Press, LLC
GUARDIAN
The Science of Protecting What Matters: Home, Family, and Community
For the women who stand between danger and everyone they love.
For the mother who hears every sound in the night.
For the officer who clears the scene before she calls it safe.
For every woman who has ever scanned a room
not because she was trained to
but because the world taught her to.
The guardian instinct in you is not fear.
It is intelligence.
This book gives it a name.

COMPANION TO THE GUARDIAN RIBBON

CONTENTS

HOW TO USE THIS BOOK

A Guide for Readers

PROFILER is designed to be read in two ways: straight through, and in conversation with the Profiler Ribbon course it accompanies. You will get something from reading it either way, but you will get something different depending on when and how you read. If you are reading before beginning the course: read it as orientation. Let it give you the scientific and historical foundation for what you are about to train. Pay particular attention to the historical profiles: not for their drama, but for their methodology. Notice what these women actually did. Notice where their capacity came from. Notice that none of them were exceptions. If you are reading alongside the course: read it as context. When the course asks you to practice a specific skill, find the section of this book that covers the science beneath that skill. The course teaches what to do. This book explains why it works: and why it is yours to do. If you are reading after completing the course: read it as integration. You will find, as promised in the introduction, that the second read feels different. By then you will have direct experience with the material, and the historical and scientific context will land differently against that experience. At the end of each chapter, you will find a set of Reflection Questions. These are not assignments. They are invitations: points where the chapter's ideas can be turned inward and made personal. Some of them will be immediately relevant to your experience. Some will not. Take what is useful.

Following the reflection questions, you will find journal pages. Use them or not. Some people find that writing produces a different kind of processing than reading. If you are one of them, use the space. If you are not, leave it blank. Both choices are fine. Finally: this book is free. It is not free because the content is low-quality. It is free because the women who need it most cannot always pay for it. If this book is useful to you, tell someone else about it. That is the only payment requested.

Pro Bono Non Malo: For Good, Not Evil

Introduction: The

INTRODUCTION

Introduction: The

Art and Science of Protection

Introduction: The Art and Science of Protection

Protection is not a military operation or a police function. It is a fundamental human responsibility. From the moment a parent holds their newborn child, humans are engaged in the work of protecting what matters to them. The guardian is the person who stands between danger and those who cannot or should not have to face danger alone. This book explores the science and practice of protection; how to understand threats, how to create secure environments, how to respond to dangers, and how to build a culture of safety in homes and communities. The guardian's work is different from the work of an intelligence officer or a tactical operative. A guardian's primary goal is not to defeat an adversary but to prevent encounters with adversaries. A guardian's goal is to identify threats early and neutralize them before they reach those being protected. A guardian's goal is to create an environment where people can live normal lives without fear while maintaining the security that is necessary to prevent or respond to harm. The guardian faces a different psychological and ethical landscape than other intelligence or security professionals. The guardian has intimate knowledge of the people being protected. The guardian knows their vulnerabilities, their fears, their routines, and their needs. This intimate knowledge is essential for effective protection but also creates powerful emotional connections that complicate decision-making. The guardian must remain professionally detached enough to make clear decisions about security measures, while remaining emotionally connected enough to understand what matters to those being protected.

Throughout history, guardians have protected people at extraordinary cost and with extraordinary commitment. They have identified threats against kings and queens, against political leaders, against activists and refugees, against ordinary families who face extraordinary danger. They have created secure spaces where people could work, live, and raise families. They have trained others in the practices of protection and have built institutions around the principle that safety enables everything else. This book explores protective intelligence from multiple angles. We begin with the fundamentals of protective intelligence assessment; how to understand threats, how to gather information, how to analyze vulnerability. We move through the specific challenges of home and environment security, online threat management, and the psychology of those who threaten. We examine protective detail operations, emergency planning, and building a culture of safety. Each chapter builds on the others, creating a comprehensive framework for thinking about protection. The guardian is not a superhero who prevents all harm. No security system is perfect. No threat assessment is complete. The guardian's responsibility is to reduce risk to the lowest practical level while maintaining an acceptable quality of

life for those being protected. The guardian must understand the difference between paranoia and prudence, between security theater and real protection, between reasonable precautions and restrictions that prevent normal life from occurring. As you move through this book, remember that the ultimate goal of protection is to enable normal life, not to prevent it. The family that is protected but confined to a bunker is not truly safe. The leader who is protected from ordinary human contact is isolated and vulnerable in different ways. The community that tries to prevent all risk becomes sterile and dysfunctional. The guardian's art is balancing protection with the quality of life of those being

protected.

Protective Intelligence Fundamentals

Understanding Threats and Assessing Vulnerability

The threat you understand is a threat you can manage. The unknown threat is the one that destroys you.

CHAPTER ONE

Protective Intelligence Fundamentals

What Is a Threat

A threat is the combination of three factors. Capability, intent, and opportunity

CHAPTER ONE

Protective Intelligence Fundamentals

if they have the skills, weapons, access, or resources necessary to cause harm. A person has intent to harm if they have motivation to harm a particular target. A person has opportunity to harm if they can access the target at a moment when the target is vulnerable. All three factors must be present for a real threat to exist. If any one factor is missing, the threat is reduced or eliminated. Understanding threats requires analysis of all three factors. A person with intent to harm but no capability is not an immediate threat. A person with capability and opportunity but no intent is not a threat. Intelligence about threats requires identifying specific people who have demonstrated intent to harm a particular target, assessing their capability to do so, and analyzing what opportunities they might have to access the target. Without all three factors, risk is reduced.

Threat Assessment and Analysis Threat assessment is the process of gathering information about potential threats, analyzing that information, and determining what level of protection is

necessary. Effective threat assessment requires multiple sources of information. Law enforcement records show who has been arrested or convicted of violence. Court records show who has made threats in legal proceedings. Intelligence from human sources shows who is expressing intention to harm a target. Behavioral analysis shows who is engaging in surveillance or testing security. Financial analysis shows who might be motivated by money to harm someone. The threat assessment process is ongoing. A person who is not a threat today might become a threat tomorrow based on changed circumstances. Someone who was a significant threat might cease to be a threat after being incapacitated or incarcerated. The guardian must continuously monitor threat levels and update security measures as threat levels change. A static threat assessment that was accurate a year ago may be dangerously wrong today.

Vulnerability Analysis Vulnerability analysis is the assessment of how exposed the person being protected is to potential threats. Where does this person spend their time? What are the patterns of their daily activity? When are they most isolated or most exposed? What are their security habits; do they lock doors, do they vary their movements, do they maintain awareness of their surroundings? What are the physical security features of the places where they spend time? What are their digital security practices? A comprehensive vulnerability analysis identifies all the ways a threat could potentially access the person being protected. Vulnerability analysis must include assessment of the person being protected's willingness to accept security measures. A security system that the person being protected refuses to use is worthless. A vulnerability analysis that recommends measures that are so restrictive that they prevent normal life will

not be accepted or followed. The guardian must understand both the technical vulnerabilities and the human factors that affect acceptance of security measures.

Risk Assessment and Prioritization Risk combines threat and vulnerability. A high threat with low vulnerability results in lower overall risk than a low threat with high vulnerability. Understanding this relationship allows guardians to prioritize security measures. If the threats facing a person are primarily from strangers, then security measures should focus on preventing access by unknown people. If threats are from people with inside knowledge, then security measures should focus on identifying and monitoring those who have access. Different threat profiles require different security approaches. Risk assessment is never perfect. There is always incomplete information. New threats emerge that were not anticipated. Vulnerabilities exist that were not identified. The guardian must manage risk based on the best available information while remaining aware that some threats will slip through defenses. The goal is not perfect security but reasonable security; risk reduced to an acceptable level given the nature of the threats and the quality of life that the person being protected wants to maintain.

Intelligence Sources and Information Gathering Protective intelligence comes from multiple sources. Law enforcement provides information about criminals and criminal organizations. Intelligence agencies

provide information about espionage threats and foreign intelligence activities. Human sources provide information about specific threats; coworkers who make threats, stalkers who are pursuing targets, people with grievances who are expressing intent to harm. Digital sources provide information about online threats; social media monitoring, email monitoring, threat messages online. Physical surveillance can reveal threats that might be conducting surveillance or testing security. Information gathering must be conducted legally and ethically. Eavesdropping on private conversations without legal authorization, hacking into electronic communications, illegally surveilling people; these may be illegal and are always ethically problematic. Effective protective intelligence relies on legal sources; law enforcement reports, intelligence briefings, voluntary human sources, monitoring of public communications, physical observation in public spaces. Intelligence gathered through illegal or unethical means may be unreliable and may create legal liability.

HISTORICAL PROFILE

Harriet Tubman 1820 to 1913

Harriet Tubman is remembered as one of the most important figures in American history for her role in the Underground Railroad, the network that helped enslaved people escape to freedom. Beyond her

famous role as a conductor, Tubman was a sophisticated protective intelligence operative who understood threats, assessed vulnerability, and created secure passage for people in extreme danger. Her later work as a military leader during the Civil War demonstrated her ability to protect vulnerable populations in active conflict zones. Tubman's life exemplifies the guardian at the highest level. She placed themselves at extraordinary personal risk to protect others.

Tubman's protective work on the Underground Railroad required sophisticated threat assessment and planning. She understood the capabilities of those pursuing enslaved people. Slave catchers, local authorities, military forces all pursued those seeking freedom. She understood the vulnerabilities of people fleeing slavery. Exhaustion, fear, vulnerability to recapture all affected those seeking safety. She developed routes that maximized security. She used safe houses that had been vetted. She avoided the most dangerous areas. She understood that her own reputation for bringing people to safety successfully was itself protective. People knew that if they could reach Tubman and follow her guidance, they would reach freedom. Her personal courage and her commitment to protection created a sense of security that encouraged people to attempt escape. Tubman's protective intelligence was based on detailed knowledge of routes, of safe locations, of trustworthy allies, and of the patterns of those pursuing people. She knew which roads were heavily patrolled and which were safer. She knew which communities had people who would provide shelter. She knew the techniques of pursuit and how to evade them. She knew when to travel and when to hide. This detailed knowledge, combined with her willingness to use armed force to protect people under her care, made her an effective guardian against extraordinary threats. During the Civil War, Tubman served the Union Army in various roles, including as a scout and as a leader of military operations. In this role, she continued her protective work. She gathered intelligence about Confederate forces. She guided Union troops through hostile territory. She led operations to free enslaved people held by Confederate forces. Her military effectiveness was based on the same principles that had made her effective on the Underground Railroad. Understanding the enemy, assessing vulnerability, planning secure operations, and protecting those under her care were all critical elements. She demonstrated that protective intelligence and protective operations were not limited to personal protection but could be applied at a military scale.

Harriet Tubman's legacy is as a guardian of extraordinary skill and commitment. She understood that protection sometimes requires risk. Effective guardianship means placing yourself in danger to protect others. The most effective protection is based on detailed intelligence and careful planning. She showed that protection is not the work of elite specialists but can be done by anyone with commitment, intelligence, and courage. Her example continues to influence how protective professionals understand their role. They must be people who are willing to stand between danger and those who need protection, regardless of personal cost.

Protective Intelligence Fundamentals

Protective Intelligence Fundamentals Understanding threats and vulnerability

1. What are the threats that you or your family face? How would you assess capability, intent, and opportunity for each threat? 2. If you were conducting a vulnerability analysis of your home, what would you identify as your vulnerabilities? 3. What sources of information would help you understand threats that might be facing you or people you care about? 4. How would you distinguish between a threat that needs immediate action and a threat that requires only monitoring? 5. If your threat assessment revealed a threat you had not considered, how would you adjust your security measures?

6. How would you communicate threat information to family members or colleagues without creating undue fear or paranoia?

Chapter One: My Reflections

Chapter One: Continued

Home and Environment Security

Creating Secure Spaces for Life

A secure home is a foundation for a secure life.

CHAPTER TWO

Home and Environment Security

Physical Security Fundamentals

Physical security begins with the basics. Doors should be solid and should have

CHAPTER TWO

Home and Environment Security

ideally have coverings that prevent people from looking inside. Exterior lighting should eliminate dark areas where someone could approach without being seen. Entry and exit points should be visible from inside the home so you can see who is approaching. These fundamentals are not glamorous, but they are the foundation of home security. Many burglaries and home invasions are not sophisticated attacks; they are crimes of opportunity against homes that are vulnerable. Physical security is layered. The first layer is the perimeter of the property. Fencing, gates, landscape that prevents easy approach all form the outer barrier. The second layer is the home itself; solid doors and windows, good locks, lighting. The third layer is the interior; room layouts that allow visibility, safe rooms that can be secured from the inside, communication devices for calling for help. Each layer provides a delay and an obstacle to someone attempting to harm people inside. The goal is not to make the home impenetrable; that is impossible. The goal is to make it time-consuming and difficult to break in, so that someone attempting intrusion will move on to easier targets or can be detected and stopped before they reach their goal.

Access Control and Monitoring Access control is the practice of limiting who can access your home and your property. This might involve gates that control vehicular access, locked exterior doors, security cameras that allow you to see who is approaching, or security systems that monitor entry points. Access control should distinguish between people who belong on your property and people who do not. Regular visitors; mail carriers, delivery people, utility workers, friends and family; should be clearly identified and verified. Unknown people approaching your property should be treated as potential threats until their identity and purpose are confirmed. Monitoring of your home and property allows you to detect threats. Security cameras allow you to see who is approaching and to record images if a crime occurs. Alarm systems allow you to detect intrusion. Motion-sensor lights alert you to movement around your property. A neighborhood watch program creates a network of eyes watching the area. These monitoring systems are not perfect and require active monitoring to be effective, but they provide early warning of threats and create a record if a crime occurs.

Emergency Planning and Response No matter how good your security, emergencies can happen. Home invasions, violent intruders, fires, natural disasters; these are rare but they do occur. Preparing for these emergencies reduces casualties when they do occur. This involves creating emergency plans. What will you do if someone breaks into your home? What is your first action? Where will you go? How will you communicate? These plans should be practiced so that family members know exactly what to do without having to think about it in the moment of crisis.

Emergency response also includes communication. A charged phone kept near you in case of emergency allows you to call for help. A panic button or emergency alert system allows you to notify

security personnel if something dangerous is occurring. Teaching family members how to describe an emergency to a 911 dispatcher ensures that police and emergency services know what they are responding to. Emergency supplies; water, first aid, shelter, food; allow you to survive if access to normal services is disrupted.

Operational Security in Daily Life Home security is not just about the physical structure. It is also about the daily practices and habits of the people living there. Do you establish routines that make you predictable and vulnerable? Do you leave windows or doors unlocked? Do you leave your home unoccupied and dark for long periods, signaling that nobody is home? Do you advertise valuable possessions? Do you discuss your travel plans on social media? These operational security practices affect your vulnerability. Varying your daily routines reduces your predictability. Securing all entry points makes forced entry more difficult. Making your home appear occupied when you are away deters burglars. Maintaining privacy about your movements and your possessions reduces motivation for crimes. Operational security also includes awareness of your surroundings. Do you notice when the same person or vehicle appears repeatedly in your neighborhood? Do you notice if someone is watching your home? Do you notice unusual activity that might indicate criminal planning? Awareness is not paranoia; it is the basic observation that allows you to detect threats before they become dangerous. People who have been successfully burglarized often report that they noticed unusual activity but did not take it seriously. Trusting your

instincts when something seems wrong is part of good security practice.

Secure Locations and Safe Rooms For people facing significant threats, a secure location within the home; a safe room that can be locked from the inside and that has communication with the outside; provides a place to go if someone forces entry. A safe room should have secure locks on the door, should not have windows that can be broken to allow entry, should have phone or alarm capability to call for help, and should have supplies sufficient for a person to survive there for an extended period if necessary. A safe room is a last resort; the goal is to prevent people from forcing entry. But if prevention fails, a safe room provides a location where vulnerable people can be secure until help arrives. Safe rooms are particularly important for families with children or elderly family members who may not be able to run or defend themselves. Adults might evacuate the home, but young children might not be able to run. Elderly people might not be able to move quickly. For these vulnerable people, a safe room that they can access provides security. Safe rooms are also important for people facing specific threats; activists facing violence, people in domestic abuse situations, immigrants facing persecution; safe locations provide protection while authorities respond or while longer-term solutions are arranged.

Irena Sendler 1910 to 2008

Irena Sendler was a Polish social worker and nurse who became one of the most successful protectors of Jewish children during the Holocaust. Using a combination of threat assessment, secure location planning, access control, and operational security, Sendler and her network protected over 2,500 Jewish children from Nazi persecution. Her work demonstrates the protective intelligence principles applied at a massive scale in conditions of extreme threat. Sendler's success came not from military force but from careful planning, secure locations, and networks of trustworthy people who understood the risks they were taking. Sendler understood the threats facing Jewish people in occupied Warsaw during the Nazi occupation. She assessed the capabilities of the Nazis. She understood their ability to search homes, to interrogate people, to enforce deportation. She understood their intent; the genocidal goal of murdering Jewish people. She understood the vulnerabilities of Jewish children and families. They were isolated, had limited resources, had limited ability to flee or hide. Based on this threat assessment, she developed an extensive system for protecting children by hiding them in safe locations and providing them with false identity documents. Sendler's protective operations required secure locations. She identified families, orphanages, and convents willing to hide Jewish children. She assessed each location for security. Would they be discovered? Would the people hiding the children remain committed if German forces discovered them? She created systems to track which children were in which locations, though she kept records hidden so that if she was captured, the locations would not be revealed. She provided false identity papers that would pass scrutiny. She

personally

facilitated

communication with them.

placement

of

children

and

maintained

Sendler's operational security was sophisticated. She worked with a trusted network of collaborators, but compartmentalized information so that if one person was captured, they could not reveal the entire network. She created elaborate systems for smuggling children out of the Warsaw Ghetto; hidden in boxes, buried in dirt carts, through sewer systems. Each child had a false identity, false papers, a cover story. She used her position as a nurse to have legitimate access to places where she could move around and make contact with people. What made Sendler's protective work successful was not force or violence; it was intelligence, planning, courage, and a network of people who understood that protecting children was more important than their own safety. She assessed threats accurately. She identified secure locations. She planned operations carefully. She trained and coordinated her network of protectors. When captured by the Nazis, she was tortured but did not reveal the locations where children were hidden. Her legacy is of a guardian who protected the most vulnerable people against one of history's greatest evils, and who did so not through military force but through careful protective intelligence operations.

Home And Environment Security

Home and Environment Security Creating secure spaces

1. What are the physical security features of your current home? What improvements would increase security? 2. How would you design an emergency plan for your household? What scenarios would you prepare for? 3. What is your current level of awareness about who is approaching your home and your property?

4. How would you balance security measures with maintaining a home that is welcoming and comfortable? 5. If you needed to create a safe room in your home, what would be the most practical location and what supplies would it need? 6. How would you teach family members to follow security procedures without making them feel paranoid or restricted?

Chapter Two: My Reflections

Chapter Two: Continued

Online Threat Management

Protecting Yourself and Your Family in the Digital World

The digital threat is invisible but not less dangerous. Protect your information as you protect your home.

CHAPTER THREE

Online Threat Management

Threat Landscape in Digital Environments

Digital threats are distinct from physical threats but equally important.

CHAPTER THREE

Online Threat Management

information that can be used to extort or harass people. Malware can compromise computers and devices. Data breaches can expose sensitive information. Social engineering can trick people into revealing passwords or sensitive information. Stalkers and harassers can use digital means to locate, monitor, and threaten people. Online predators can manipulate children. Understanding these digital threats is the foundation for protecting against them. Digital threats are often more difficult to detect than physical threats because they leave fewer traces. Someone could be monitoring your email and you might never know. Someone could be tracking your location through your phone and you might not realize it. Someone could be gathering information about your family from social media and you might not see the threat until they appear in person. Digital threat assessment requires understanding what information is publicly available about you, what information you are voluntarily sharing, what vulnerabilities your devices have, and what digital behaviors might attract predators.

Information Control and Digital Hygiene

Digital protection begins with controlling what information is publicly available about you. Social media posts reveal where you live, where you work, what time you are away from home, where your children go to school. Photos reveal what your home looks like, what valuables you have, where you are located. Digital footprints; the trail of information left behind by your online activity; can be assembled into a detailed picture of your life. Controlling what information you share is the foundation of digital protection. This does not mean you cannot use social media or the internet; it means being intentional about what information you share and with whom. Digital hygiene includes protecting your devices from malware and unauthorized access. Strong passwords that are difficult to guess, changed regularly, and unique for each account prevent unauthorized access. Two-factor authentication makes it harder for someone to access your accounts even if they have your password. Keeping software updated patches security vulnerabilities. Avoiding suspicious emails, links, and downloads prevents malware. Careful management of permissions that applications request prevents malware from accessing sensitive information. These practices are not glamorous but they are essential for digital security.

Online Harassment and Cyberstalking Online harassment and cyberstalking are increasingly common threats, particularly against women, activists, public figures, and minorities. Harassers use anonymous accounts to send threatening messages, to post false information, to attempt to intimidate people into silence or into leaving online spaces. Cyberstalkers use information available online to locate, monitor, and threaten their targets. These threats can escalate to physical violence. Protecting against online harassment requires documentation of the harassment, limiting

engagement with harassers, reporting to platform administrators or law enforcement, and in severe cases, obtaining legal protections such as restraining orders. Protection against cyberstalking includes limiting information available online, using privacy controls on social media, being cautious about sharing location information, and monitoring who is following or contacting you online. If you are being threatened or harassed, documentation is important; saving messages, taking screenshots, recording threats. This documentation can be provided to law enforcement or used in legal proceedings. Law enforcement increasingly has the capability to investigate online harassment and to identify and prosecute perpetrators.

Children and Digital Protection Children face unique digital threats because they are less experienced in identifying dangers and because they trust more easily. Online predators groom children through social media and messaging apps, building relationships and trust before attempting to sexually exploit them. Cyberbullying can drive children to self-harm or suicide. Exposure to inappropriate content can affect children's development. Identity theft using a child's information can have long-term consequences. Protecting children in digital environments requires a combination of technical protections; parental controls on devices, limiting access to age-appropriate sites; and educational protections; teaching children about online dangers, encouraging them to report threats, maintaining open communication about their online activities. Parents should know what their children are doing online. This is not about invading privacy or preventing independence; it is about ensuring that children

are safe from predators and harmful content. Knowing their children's passwords, knowing who they are in contact with online, understanding what apps they are using; allows parents to detect threats early. Teaching children that if someone online asks them to keep communication secret, or asks them to send photos, or makes them uncomfortable, they should tell a trusted adult; provides a safety net if predators attempt to exploit them.

Responding to Digital Breaches and Compromises If your digital security is compromised; your account is hacked, your device is infected with malware, your information is exposed in a breach; immediate action is necessary. Change your passwords for that account and for other accounts using the same password. Run malware scans on your devices. Monitor financial accounts for unauthorized activity. Place fraud alerts with credit bureaus if financial information may have been compromised. Report the compromise to law enforcement if it involves criminal activity. Review what information was exposed and take steps to protect against the exposed information being misused. Long-term recovery from a digital compromise involves vigilance. Continue monitoring for signs of misuse of your information. Be alert for identity theft attempts. Be cautious about suspicious emails or communications that might be targeting you based on the compromised information. If your personal information was exposed and sold to criminals, expect ongoing attempts to exploit it. Remaining

vigilant and responding quickly to signs of exploitation minimizes the damage caused by the initial compromise.

HISTORICAL PROFILE

Miep Gies 1909 to 2010

Miep Gies was a Dutch rescuer who, along with others, hid Anne Frank and her family in a secret room behind a bookcase in occupied Amsterdam during the Holocaust. Gies' role was to procure supplies, maintain the safety of the hiding place, and manage the operational details necessary to keep the family hidden. Her work demonstrates protective intelligence applied to the extraordinary challenge of keeping people hidden from occupying forces conducting active search operations. Gies succeeded in keeping eight people hidden and alive for twenty-five months in an incredibly challenging environment. Gies understood the threats facing the Frank family. The Nazis were actively searching for Jewish people in hiding. Neighbors could report a hiding place. German authorities could search buildings. Employees of the company could discover the hidden room. The threat of discovery was constant. Gies assessed these threats and, along with others, created a secure location; the hidden room that was completely concealed from view and that could be accessed only by people who knew it existed. The security of the location was maintained through compartmentalization; most employees of the company did not know the hiding place existed. Miep Gies' protective work involved constant attention to operational security. She procured supplies without drawing attention, knowing that purchasing large quantities of food could raise suspicion. She arrived at the office at regular times, not exhibiting any change in routine that might indicate unusual activity. She paid rent on the office to keep it legitimate. She maintained relationships with people in the neighborhood without revealing anything about the hiding place. Every interaction with the outside world potentially threatened the safety of the people in hiding, so every interaction had to be carefully managed.

Gies was also the primary human contact for the people in hiding. She provided supplies, news from the outside world, emotional support. She understood that people who were confined to a small space for months would develop psychological strain and would need support. She treated the people she was protecting with dignity and respect. She maintained detailed security discipline while also maintaining the humanity and emotional connection necessary to keep people alive and stable in impossible circumstances. After the war and the discovery of Anne Frank's diary, Gies became famous as one of those who had protected the Frank family. She spent the rest of her life speaking and writing about her experiences. What she emphasized was that protecting the Franks was not extraordinary; it was what ordinary people did when faced with evil. She understood that she had been fortunate to succeed, and she was aware that many others trying to hide people had not succeeded. Her legacy is as a guardian who created a secure location, maintained its security through careful operational security, and protected vulnerable people against extraordinary threats.

Online Threat Management

Online Threat Management Digital security and privacy

1. What information about yourself and your family is publicly available online? How would you reduce your digital footprint? 2. What are your weak points in terms of digital security? Weak passwords, predictable patterns, oversharing on social media? 3. If you discovered that someone had hacked into one of your accounts, how would you respond?

4. How would you protect children in your care from online predators and cyberstalking? 5. What digital monitoring and security tools would you implement for your household? 6. How would you balance digital security with the benefits of being connected online?

Chapter Three: My Reflections

Chapter Three: Continued

Stalker and Predator Psychology

Understanding Dangerous People

Understanding how dangerous people think is essential to protecting against them.

CHAPTER FOUR

Stalker and Predator Psychology

Stalking Behavior and Patterns

Stalking is persistent, unwanted contact or pursuit that creates fear. Stalkers fall

CHAPTER FOUR

Stalker and Predator Psychology

end of a relationship and pursue their former partner with unwanted contact, gifts, or surveillance. Some are acquaintance stalkers who misinterpret normal friendliness as romantic interest and persist in pursuing contact. Some are erotomaniac stalkers who believe that their target is in love with them despite no evidence of reciprocal feeling. Some are territorial stalkers who are angry at someone and pursue them to express that anger. Different types of stalkers have different risk profiles and require different protective strategies. Stalking often follows predictable patterns. Initial contact that is rejected. Persistence despite the rejection. Escalation of contact attempts. Surveillance to gather information. Testing of security to assess vulnerability. In some cases, escalation to violence or to attempted abduction. Understanding these patterns allows protective operatives to intervene early and to assess the risk that a particular stalker presents. A stalker in early stages of the pattern is less dangerous than a stalker who is testing security or planning violent action.

Predator Selection and Grooming

Predators, particularly sexual predators, select targets based on vulnerability. They look for people who are isolated, who lack strong social connections, who are in institutional settings where abuse is less likely to be reported. They look for people who are emotionally vulnerable or who have low self-esteem. They observe potential victims over time to assess vulnerability. Once they have selected a target, they begin grooming; building a relationship of trust, testing boundaries gradually, moving toward inappropriate contact. The grooming process can last weeks or months, and victims often do not recognize it as manipulation until they are already in an abusive situation. Protection against predatory behavior requires awareness of grooming patterns. Adults should be alert to people who take unusual interest in children, who attempt to create situations to be alone with children, who give inappropriate gifts or attention. Children should be taught about boundaries and should know that certain types of contact from adults are inappropriate. Creating an environment where children know they can report uncomfortable behavior to trusted adults is essential. Teaching children that if someone tells them to keep something secret from parents, that is a warning sign, provides important protection.

Risk Assessment for Dangerous Individuals Some individuals present a significantly higher risk of violence than others. Risk factors include prior history of violence, substance abuse, access to weapons, lack of impulse control, lack of remorse for past violence, and specific threats against particular people. Someone who has made explicit threats against your life, who has shown planning for how they would harm you, who has attempted to acquire weapons or explosives; presents a much higher risk than someone who is simply hostile or angry. Risk assessment by professionals

trained in this area is valuable when you are facing a potentially dangerous individual, because they can distinguish between genuine danger and behaviors that seem threatening but are less likely to result in violence. Risk assessment must also consider whether a dangerous individual has a particular focus on a particular target or whether they are generally aggressive toward many people. Someone who is focused on a particular target and is engaged in planning against that target is higher risk than someone who is generally aggressive but without a specific target. This distinction affects the type of protective measures that are necessary.

Protective Measures Against Dangerous Individuals Protection against stalkers and dangerous individuals involves multiple layers. Documentation of all contact from the individual; threats, messages, surveillance observations; creates evidence that can be provided to law enforcement. Minimizing visible patterns and routines reduces the ability of a stalker to predict where you will be and to conduct surveillance. Maintaining awareness of your surroundings allows you to detect surveillance or approach by a dangerous person. Communication protocols with family members or colleagues allow you to raise an alarm if you are threatened. In some cases, legal measures such as restraining orders or protective orders can be obtained. In extreme cases where a dangerous individual has demonstrated specific intent and capability to harm, protective detail or secure location may be necessary. This is not an overreaction; it is appropriate response to a legitimate threat. Someone who is being pursued by an individual with prior violence and specific threats is right to take extraordinary protective measures.

Reporting and Law Enforcement Response If you are being stalked or threatened, reporting to law enforcement is important. Law enforcement can investigate the stalker, can warn them that contact is illegal, can arrest them if they violate laws against stalking or threat. In some jurisdictions, law enforcement has specialized units that investigate stalking and that understand the patterns and risks. Providing law enforcement with all the information you have; threats, surveillance observations, prior context; helps them understand the threat and respond appropriately. If law enforcement is not responsive to reports of stalking or threat, obtaining a restraining order or protective order through the civil legal system provides legal recourse. A restraining order prohibits the person from contacting or coming near you and provides legal consequences if they violate the order. In cases where stalking or threats escalate to violence or attempted violence, criminal prosecution provides longer-term protection through incarceration of the dangerous person.

Stalker And Predator Psychology

Stalker and Predator Psychology Understanding dangerous people

1. Have you ever experienced concerning behavior from someone that resembled stalking? How did you respond?

2. What early warning signs would indicate that someone's behavior toward you or someone you care about might be dangerous? 3. How would you document threatening behavior to provide to law enforcement? 4. If someone you knew was being stalked or threatened, what advice would you give them? 5. How would you help a child in your care understand dangerous behavior and know to report it? 6. What would you do if someone was threatening you online or in person?

Chapter Four: My Reflections

Chapter Four: Continued

Protective Detail Operations Providing Security for High-Risk Individuals

Effective protection is invisible. The principal never thinks about security until something goes wrong.

CHAPTER FIVE

Protective Detail Operations

Protective Detail Structure and Organization

A protective detail is a team of trained security personnel who maintain the

CHAPTER FIVE

Protective Detail Operations

responsible for overall security, advance personnel who scout locations and assess threats in advance, close protection officers who remain in immediate proximity to the person being protected, support personnel who handle communications and logistics, and canine units or other specialized personnel if appropriate. Different detail structures are used depending on the level of threat and the type of protection required. A high-profile political figure facing extreme threat might have a detail of dozens of people. A businessperson facing moderate threat might have a small protective detail of two or three people. The protective detail operates as a coordinated team. Each person has a specific responsibility and a specific area they are responsible for. The close protection officers watch people approaching the protected person. The advance team assesses the location for threats. Support personnel coordinate movement and communication. The detail leader maintains overall awareness and makes decisions about security. Coordination is critical because a gap in coverage; a moment where no one is watching a particular area; creates vulnerability.

Threat Assessment and Movement Planning

Protective operations begin with detailed threat assessment. What are the specific threats facing this person? What is their capability to harm? What is their likely method of attack? Based on this assessment, protective measures are designed. A person facing threat from long-range shooters requires different security measures than a person facing threat from close-range violence. A person facing threat from a specific group requires different measures than a person facing threat from multiple uncoordinated individuals. Understanding the threat drives the protective strategy. Movement planning is critical. Protective details do not use the same routes repeatedly. They vary timing of movements. They assess each location in advance for security vulnerabilities, for entry and exit routes, for potential hiding places for threats. They establish counter-assault teams positioned to respond if an attack occurs. They maintain communication with law enforcement so that police can be present when the protected person is in public areas. All of this advance planning is intended to prevent attacks or to respond rapidly if an attack occurs.

Venue Security and Environment Assessment When a protected person will be at a particular venue, advance teams conduct detailed assessment. They inspect the venue for security vulnerabilities. They identify who will have access to the venue and conduct background checks on facility staff. They plan entry and exit routes. They identify positions where protection officers can be stationed. They assess roof lines for sniper threats. They identify areas where hostile people could gather. They test communication systems to ensure they will work in the venue. All of this assessment occurs in advance so that when the protected person arrives, the venue is as secure as possible.

Venue security also involves restricting access. People attending a function where a protected person will be present must be screened, credentials must be verified, prohibited items must be prevented from being brought in. Metal detectors can screen for weapons. Bag searches can prevent explosives or weapons from being brought in. These security measures are not popular with attendees, but they significantly reduce the risk of violence.

Crowd Management and Public Interaction Many protected individuals need to interact with the public; politicians need to campaign, activists need to speak to supporters, business leaders need to appear at public events. Protective details must enable these public interactions while reducing security risks. This involves careful planning of how the crowd will be controlled, how people will be allowed to approach the protected person, how threats within the crowd will be identified. Close protection officers watch the crowd for signs of threat; people reaching toward pockets, people moving toward the protected person rapidly, people with glazed or agitated expressions that might indicate intent to harm. Working protection at public events requires balancing security with the public role of the protected person. The most secure option is to prevent all public contact; keep the protected person behind barriers, allow no one to approach, control all movement. But this security posture prevents the protected person from doing their job. A detailed team that enables public interaction while maintaining close observation and rapid response capability is more difficult to manage but allows the protected person to remain effective in their role.

Emergency Response and Crisis Management Despite all protective measures, attacks can occur. When an attack or emergency happens, the protective detail must respond. This requires rapid threat assessment; is this a genuine emergency or a false alarm? Rapid movement of the protected person to safety. Engagement with any threat. Communication with law enforcement and emergency services. Protection officers are trained to respond to active shooter situations, explosions, medical emergencies, and other crises. The goal is to move the protected person to safety as quickly as possible and to neutralize any threat. After an emergency, investigation and debriefing are important. What happened during the emergency? Did your response plan work? What would you do differently if a similar emergency occurred? What did you learn? Conducting a thorough review allows you to improve your emergency response plan and increases the likelihood that the next time an emergency occurs, your response will be more effective. Communities and organizations that learn from emergencies are better prepared for future emergencies.

Protective Detail Operations

Protective Detail Operations Professional protection services

1. If you were responsible for protecting someone at high risk, how would you design their protective security?

2. What are the trade-offs between security and normal functioning that a protected person must consider? 3. How would you coordinate a protective detail to ensure no gaps in coverage? 4. If a threat occurred while a protected person was in public, how would you respond? 5. What kind of training and preparation would protective detail officers need? 6. How would you balance enabling normal life for a protected person with maintaining their security?

Chapter Five: My Reflections

Chapter Five: Continued

Emergency Planning and Response

Preparing for Crisis

The emergency you have planned for is the emergency you survive.

CHAPTER SIX

Emergency Planning and Response

Identifying Risks and Scenarios

Emergency planning begins with identifying what emergencies are possible. For

CHAPTER SIX

Emergency Planning and Response

For a business, this might include workplace violence, active shooter, terrorism, equipment failure. For a community, this might include natural disaster, mass casualty event, infrastructure failure. Different scenarios require different response plans. An emergency plan that is effective for fire response might be ineffective for active shooter response. Planning requires identifying the scenarios most likely to occur in your particular situation. Once you have identified potential emergencies, you assess your vulnerability. How likely is each emergency? What would be the consequences if it occurred? What is the warning time; do you have hours to prepare, or seconds? How severe would the impact be? Based on this assessment, you prioritize. You plan for the emergencies that are most likely and most severe first. You might not be able to plan for every possible emergency, but you can plan for the most important ones.

Response Planning and Decision-Making

For each emergency scenario, you develop a response plan. What will you do immediately when you become aware of the emergency? Where will you go? Who will you contact? What supplies will you need? These response plans should be simple enough to be executed even under the stress of an actual emergency. Complex plans that require lots of thinking and decision-making will fail when you are in shock or panic. Simple plans that you can follow automatically are more likely to succeed. Response planning also includes designated roles and responsibilities. If a fire occurs, who is responsible for getting people out? Who is responsible for calling emergency services? Who knows where the fire extinguisher is? Assigning specific responsibilities in advance means that people will know what to do without having to figure it out in the moment. Family members or team members should practice the plan so they understand it. A plan that exists only on paper and has never been practiced will be much harder to execute in a real emergency.

Communication and Coordination in Emergency During an emergency, communication is critical. If a building is being evacuated because of fire, people need to know where to go. If there is an active shooter, people need to know whether to evacuate or shelter in place. If a medical emergency occurs, 911 needs to be called. Communication systems that work normally might fail during an emergency; electricity might be down, phone lines might be overwhelmed, radio systems might be congested. Planning alternative communication methods is important. A plan to meet at a specific location if communication systems fail allows people who are separated to reunite.

Coordination in an emergency involves knowing who is in charge of making decisions. If there are multiple authority figures present, confusion about who is making decisions can be dangerous. Establishing a command structure in advance; this person is in charge, they will make decisions about what everyone does; allows rapid, coordinated response. This is particularly important in organizations and communities where multiple people have authority.

Recovery and After-Action Review After an emergency, recovery is necessary. If a fire has damaged a home, you need to find temporary shelter and eventually rebuild. If a business has suffered a major incident, you need to restore operations. Recovery can take weeks, months, or years. Planning how you will recover and having resources available for recovery reduces the long-term impact of the emergency. Insurance, emergency savings, backup systems; all of these help you recover faster from emergencies. After-action review is also important. What happened during the emergency? Did your response plan work? What would you do differently if a similar emergency occurred? What did you learn? Conducting a thorough review allows you to improve your emergency response plan and increases the likelihood that the next time an emergency occurs, your response will be more effective. Communities and organizations that learn from emergencies are better prepared for future emergencies.

Psychological Resilience After Emergency Experiencing an emergency can be traumatic. People who survive emergencies often experience stress responses; fear, difficulty sleeping, anxiety, intrusive thoughts about the emergency. These responses are normal reactions to abnormal situations. Acknowledging that the emergency was difficult, allowing time to process the experience, talking with others who experienced the same emergency; all of these help people recover from the psychological impact of emergencies. In some cases, professional mental health support is necessary to recover from the psychological trauma of experiencing an emergency. Families and communities that have experienced emergencies together often find that the experience strengthens their bonds. Knowing that you and the people you care about survived an emergency together, that you worked together to overcome it, can create a sense of unity and resilience. This collective recovery can be as important as individual recovery in moving past an emergency.

Emergency Planning And Response

Emergency Planning and Response Preparing for crisis

1. What emergencies are most likely to affect you and your family? What would be the impact of each? 2. What would your response plan look like for your most likely emergency scenarios?

3. How would you practice emergency plans so that people could execute them without confusion? 4. How would you communicate during an emergency if normal communication systems were

unavailable? 5. What supplies and resources would you need for emergency response and recovery? 6. How would you support people psychologically after they had experienced an emergency?

Chapter Six: My Reflections

Chapter Six: Continued

Building a Culture of Safety Creating Communities Where Safety Enables Flourishing

A culture of safety is built on the foundation that everyone has a responsibility to notice threats and to act.

CHAPTER SEVEN

Building a Culture of Safety

Leadership and Safety Commitment

A culture of safety begins with leadership commitment. If leaders view safety as

CHAPTER SEVEN

Building a Culture of Safety

resource allocation, others will follow. If leaders view safety as bureaucratic inconvenience, others will treat it the same way. Leaders who acknowledge when safety procedures prevented harm, who support people who report threats, who allocate resources for training and improvement; create an environment where safety matters. Leaders who ignore safety concerns or who punish people for reporting threats create an environment where safety is not valued. Leadership in a safety culture also includes holding people accountable for safety violations. If someone bypasses security procedures, if someone ignores safety warnings, if someone fails to report threats; addressing these behaviors is important. Accountability is not about punishment. It is about reinforcing that safety matters and that violations have consequences. This accountability must be consistent; applied to everyone, including senior leaders.

Education and Training A safety culture requires education about safety. Everyone should understand what the threats are, what the security procedures are, why the procedures

matter. This is not one-time training; it is ongoing education. People need reminders about security procedures. New employees need to be trained. Procedures change and people need to understand what changed and why. Training should be practical and should help people understand how to apply security principles in their daily work. Training that is abstract or disconnected from daily life is not effective. Training should also include empowerment. People should feel that they are able to report threats and that reporting is supported. People should feel that they can ask questions about security without being punished. People should understand that a security concern, even if it turns out to be a false alarm, is valuable because it might prevent a real threat. A culture where people feel empowered to speak up about safety concerns is a culture where threats are more likely to be detected early.

Threat Reporting and Response A safety culture requires mechanisms for reporting threats and for responding quickly to reported threats. People should know how to report a threat; who to contact, how to document it, what will happen to the report. Reports should be investigated promptly. The person who reported the threat should be informed of what action was taken, to the extent that security allows. People who report threats should not face retaliation. When people report threats and see that their report is taken seriously and acted upon, they are more likely to continue reporting threats. Response to reported threats should be proportionate and should address the actual threat. Overreacting to a minor concern can create cynicism about the safety reporting system. Underreacting to serious threats creates danger.

Balancing appropriate response with proportionate response is the responsibility of security professionals and leaders.

Continuous Monitoring and Improvement A safety culture requires continuous monitoring of whether safety procedures are working. Are threats being detected? Are incidents occurring? If incidents occur, are they being prevented or just responded to after the fact? Metrics about safety provide information about whether the safety culture is effective. These metrics should be tracked over time so you can see if safety is improving or deteriorating. If safety is degrading, investigation into why and implementation of improvements is necessary. Continuous improvement means regularly reviewing procedures and updating them based on new threats or based on changing circumstances. A procedure that was effective five years ago might not be effective today if the threat environment has changed. Regular review of procedures and testing of procedures (through drills and simulations) ensures that procedures remain current and effective.

Integration of Safety into Daily Life In a mature safety culture, safety is integrated into daily operations, not bolted on as an afterthought. Safety considerations are built into how decisions are made. When planning an event, security is considered at the beginning of the planning, not added at the end. When designing a space, security features are built in, not added later. When hiring people, background checks are routine.

Security is part of how things are done, not something that gets in the way of doing things. Integration of safety into daily life also means that safety becomes automatic. People lock doors without thinking about it. People maintain awareness of their surroundings without having to consciously think about it. People follow safety procedures without viewing them as restrictions on their freedom. When safety is fully integrated, it enables normal life; people can focus on their work, their families, their communities, while safety operates in the background protecting them.

Building A Culture Of Safety

Building a Culture of Safety Creating communities where safety matters

1. In your organization or community, what is the current approach to safety? How would you improve it? 2. What barriers exist to people reporting threats or safety concerns? How would you address those barriers? 3. How would you train people in your organization about safety without making them feel fearful or paranoid? 4. What metrics would indicate whether your safety culture is effective?

5. How would you integrate safety into daily operations so that it is automatic rather than burdensome? 6. What is the leader's role in building a safety culture, and what would you do differently if you were in a leadership position?

Chapter Seven: My Reflections

Chapter Seven: Continued

Conclusion: Living

INTRODUCTION

Conclusion: Living

Safely and Fully

Conclusion: Living Safely and Fully

CONCLUSION

Conclusion: Living Safely and Fully

Protection is not about living in fear or about retreating from life to hide in a bunker. Protection is about understanding risks, taking reasonable precautions, and then moving forward confidently knowing that you have done what you can to protect yourself and those you care about. The guardian's goal is to enable normal life, not to prevent it. Security measures that prevent normal life are ultimately counterproductive because they diminish the quality of life you are trying to protect. Good protection is often invisible. The security system that prevents a break-in without anyone ever knowing it was attempted is the best kind of security. The threat that is detected and neutralized before it reaches you is the best kind of threat management. The goal is not to live constantly aware of threats but to have systems and awareness in place such that threats are managed quietly in the background while you go about your life. Building a culture of safety in your family or organization requires leadership commitment, ongoing education, clear procedures, and psychological trust. People are more likely to follow safety procedures and to report threats if they trust that leadership cares about their wellbeing. People are more likely to maintain safety awareness if they see examples of safety being valued. People are more likely to report emerging threats if they have confidence that reports will be taken seriously. Remember that protection is a shared responsibility. In a community, when everyone understands threats and everyone is watching for threats, threats are

more likely to be detected early. In a family, when everyone understands security procedures and everyone follows them, security is stronger. In an organization, when everyone sees themselves as responsible for safety, safety culture is stronger. The most effective protection is not protection by specialists but protection by a community that values safety. As you apply the principles in this book, start with the most basic steps. Assess the threats facing you or the people you are protecting. Make sure your home is physically secure. Develop an emergency plan for your household. Build relationships with people you trust and with whom you could ask for help if needed. Once these basics are in place, you can continue to deepen your protective knowledge and practices. Protection is a journey, not a destination. You will always have more to learn and more ways to improve your security posture. Finally, remember that living under threat for extended periods takes a psychological toll. Guardians need to maintain their own psychological wellbeing and resilience. Protect yourself as you protect others. Build support networks. Access professional help if needed. Recognize that your commitment to protecting others comes at a cost, and be willing to invest in your own wellbeing so that you can sustain that commitment over time.

Mission Possible Spy Academy

Conclusion: My Reflections

Conclusion: My Reflections

Tools

Operational Self-Assessment

Use this assessment at the beginning of your Profiler Ribbon work, and again when you complete the course. It is not a test. There are no correct answers. It is a calibration tool: a way of taking a precise inventory of your starting point so that change, when it happens, is visible.

Rate each statement on a scale of 1 to 5: 1 = Not at all like me. 3 = Sometimes like me. 5 = Consistently like me.

1. Threat Assessment Can I accurately identify and assess threats facing me or my family? [ ] 1. Not at all [ ] 2. Somewhat [ ] 3. Moderately well [ ] 4. Excellent

2. Security Awareness Am I maintaining awareness of my environment and my security situation?

[ ] 1. Not at all [ ] 2. Somewhat [ ] 3. Moderately well [ ] 4. Excellent

3. Emergency Preparedness Have I planned for likely emergencies and do I have supplies and knowledge to respond? [ ] 1. Not at all [ ] 2. Somewhat [ ] 3. Moderately well [ ] 4. Excellent

4. Digital Security Am I protecting my personal and family information in digital environments? [ ] 1. Not at all [ ] 2. Somewhat [ ] 3. Moderately well [ ] 4. Excellent

5. Physical Security

Are my home and the places where I spend time physically secure? [ ] 1. Not at all [ ] 2. Somewhat [ ] 3. Moderately well [ ] 4. Excellent

6. Support Network Do I have trustworthy people who would support me if I faced a threat or emergency? [ ] 1. Not at all [ ] 2. Somewhat [ ] 3. Moderately well [ ] 4. Excellent

Score Interpretation Level 1 (mostly first options) You are beginning this work with real room to grow. That is the correct starting condition. The Profiler Ribbon is calibrated exactly for this starting point. Level 2 (mostly second options)

You have developed real situational awareness but have not yet systematized it. The Ribbon will give you the vocabulary and the protocol that makes what you already do more consistent and reliable. Level 3 (mostly third options) You are already reading people with substantial accuracy. The Profiler Ribbon will sharpen the precision of the read and extend it into high-pressure situations where your current skill degrades. Level 4 (mostly fourth options) You are operating at an advanced baseline. The Capstone Mission will be your growth edge: not acquiring the skills but integrating them under sustained operational conditions.

Take this assessment again after completing the Profiler Ribbon. The changes will be specific and measurable.

Assessment: Notes & Observations

Assessment: Notes & Observations

ASSESSMENT: INITIAL SCORES (DATE: _____)

Assessment: Initial Scores (Date: _____)

Reference

Key Terms Definitions of terms and concepts used throughout this book, organized alphabetically for reference.

Access Control Limiting who can access particular areas or information

Baseline Normal patterns of behavior and activity in an environment

Capability The ability to cause harm, including weapons, skills, and resources

Contingency Planning Preparation for alternative courses of action if the primary plan fails

Counter-Intelligence Operations against enemy intelligence activities and personnel

Crisis Management Response to urgent, high-impact situations

Digital Footprint Trail of information left behind by online activities

Emergency Response

Immediate actions taken in response to a crisis or disaster

Erotomaniac Person with delusion that another person is in love with them

Grooming Process of building trust with potential victim before exploitation

Intent Motivation and determination to cause harm

Malware Software designed to damage or compromise computer systems

Opportunity Moment when threat can access target without being prevented

Protective Detail Team of security personnel protecting a high-risk person

Risk Assessment Analysis of likelihood and severity of potential harms

Threat Assessment Evaluation of specific threats and their nature

Threat Reporting Communication of identified threats to appropriate authorities

Vulnerability Weakness or exposure that can be exploited by threat

Venue Security

Assessment and control of security at a specific location

Perimeter Security Protection of the outer boundaries of a location or property

Back Matter

Further Reading The following works were foundational to the ideas in this book and are recommended for readers who wish to explore these subjects in greater depth.

The Gift of Fear (1997) by Gavin de Becker

Analysis of intuition and threat detection in situations of danger.

The One-Minute Prepper (2014) by Christopher Dunn

Practical emergency preparedness and family safety planning.

Cutting the Fuse (2010) by Robert Pape and James Feldman

Analysis of terrorism and threat assessment.

Generation Z (2017) by Jean M. Twenge

Parenting and youth protection in digital age.

Blink (2005) by Malcolm Gladwell

Psychology of rapid assessment and intuitive threat detection.

Everyday Survival (2008) by Laurence Gonzales

Psychology of decision-making in crisis situations.

Dare to Lead (2018) by Brene Brown

Leadership and building cultures of trust and safety.

Presence (2015) by Amy Cuddy

Psychology of confidence and assertiveness in threatening situations.

Influence (1984) by Robert Cialdini

Understanding manipulation and predatory tactics.

The Deepest Well (2018) by Nadine Burke Harris

Trauma recovery and building community resilience.

The Series

The MPSA Library Series

GUARDIAN is Book Eight of the MPSA Library Series: a collection of ten free reference books, one for each ribbon in the Mission Possible Spy Academy program. Each book provides the historical, scientific, and conceptual foundation for its corresponding ribbon course. They are companion volumes, not curriculum replacements. The courses teach tradecraft. The books explain why that tradecraft works: and how women have been using versions of it for centuries.

Book One: ANALYST Analyst Ribbon

Environmental awareness, the evolutionary origins of female perceptual intelligence, historical operatives, and the architecture of learned helplessness.

Book Two: PROFILER Profiler Ribbon

The science of behavioral reading: micro-expressions, baseline deviation, deception detection, and the history of women who read people for survival.

Book Three: SENTINEL Sentinel Ribbon

Personal security and threat assessment: stalking patterns, target selection, pre-incident indicators, and the women who understood threat before it materialized.

Book Four: STRATEGIST

Strategist Ribbon

Strategic thinking, planning under uncertainty, decision science, and the women commanders and strategic thinkers history tried to forget.

Book Five: DIPLOMAT Diplomat Ribbon

Influence, persuasion, social engineering, and negotiation: the intelligence of soft power and the women who wielded it.

Book Six: HANDLER Handler Ribbon

Human intelligence, source development, trust and betrayal, and the women who ran networks of people in impossible conditions.

Book Seven: TACTICIAN Tactician Ribbon

Operational planning, counter-surveillance, cover and concealment, and the tactical thinking that kept women alive in hostile environments.

Book Eight: GUARDIAN Guardian Ribbon

Protective intelligence, close protection, emergency response, and the women who kept others safe when no one was keeping them safe.

Book Nine: GHOST Ghost Ribbon

Deep cover, identity management, the psychology of invisibility, and the women who lived double lives and brought both home.

Book Ten: FIELD COMMANDER Field Commander Ribbon

Leadership under fire, operational command, organizational intelligence, and the women who led when they were told they could not.

All ten books are free. All ten are available at MissionPossibleSpyAcademy.com.

My Notes

My Notes

My Notes: Continued

My Notes: Continued

My Notes: Continued

My Notes: Continued

My Notes: Continued

My Notes: Continued

About the Author

Dr. Terry Oroszi is the founder and director of Mission Possible Spy Academy, based in Dayton, Ohio. A U.S. Army veteran and behavioral intelligence educator, her career spans academia, federal consulting, and national security. She has worked with women across the United States and internationally, including women surviving under conditions of extreme threat, to develop practical skills in awareness, self-protection, and resilience.

She began writing the MPSA curriculum in 2013, long before AI-assisted content generation existed, driven by one conviction: that the skills of intelligence professionals: honed by decades of field experience and research: belong to every woman who needs them. The MPSA Library Series makes these foundations freely available to every MPSA student, everywhere.

"I started writing in 2013: not because it was easy, but because it needed to be done. These women needed this. They still do." Dr. Terry Oroszi

About Mission Possible Spy Academy Mission Possible Spy Academy (MPSA) is an intelligence-training program founded by Dr. Terry Oroszi. MPSA teaches women: and men: the foundational skills of situational awareness, behavioral analysis, deception detection, strategic communication, and operational discipline. The curriculum draws from intelligence tradecraft, behavioral science, and applied psychology. Courses are delivered online and accessible globally. The MPSA Library Series provides free companion reading for all MPSA ribbon courses.

MissionPossibleSpyAcademy.com Pro Bono Non Malo