CHAPTER 2

A Cyber Taxonomy

As we analyzed the example in the previous chapter, it becomes apparent that there is inherently a problem with the outcomes of research when it is done by people with the wrong context, knowledge experience, or backgrounds. In this chapter, we will explore what sort of people make the right choice when theoretical cybersecurity work, thought, and innovation are necessary. First though, we need to address the taxonomical issue that is plaguing the cybersecurity industry and is at least in part responsible for more widespread issues. If we can understand what the problems are with the way we classify professionals in cybersecurity, we can better find the right people to employ in theoretical exploration of new concepts.

A Case of Identity Crisis

What is cybersecurity? Who is a cybersecurity professional? Those are tough questions; I will cede to a major manifester for some defensible definition.

Officially, in the US federal government, the term was defined on January 8, 2008, in National Security Presidential Directive/NSPD-54 and Homeland Security Presidential Directive/HSPD-23 as

> Cybersecurity means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and

J. G. Oakley et al., *Theoretical Cybersecurity*, https://doi.org/10.1007/978-1-4842-8300-4_2

> electronic communication, including information contained therein, to ensure its availability integrity, authentication, confidentiality, and non-repudiation.

This document and others related to it as well as to cybersecurity rolled out across the United States. This led to a lot of things, such as the formation of U.S. CYBERCOM, it also led to an immense amount of federal funding getting tied to the terms cyber and cybersecurity. Anecdotally, what happened next was that contracts started having such terms in them and so did requests for proposals, proposals themselves, and the products, services, and people associated with such documents. In furtherance of this, the Department of Defense (DoD), in March of 2014, formally changed any use of the term Information Assurance to cybersecurity. I only pick on the DoD specifically because we will use their taxonomy as a point of understanding before working toward our own. So, I guess in the abstract, we can blame the US government and money associated with its budgets and contracts for the diluted and overextended nature of the term cybersecurity.

Let us look at a couple example job titles that are great at illustrating how this has played out, cybersecurity analyst and cybersecurity engineer. If you were to do a job search on these terms on any popular site, you would find they can mean quite different things in different places.

Cybersecurity Analyst

So, what types of jobs might a cybersecurity analyst do? Here is a quick list off the top of my head:

- Intelligence Analysis
- Network Analysis
- Vulnerability Analysis

- Security Operations Center (SOC) Analyst
- Risk Analyst
- Compliance Auditor
- Compliance Manager
- Hunt Team Operator
- Red Team Operator
- Penetration Tester
- Forensics Analyst

Now, if we just used those terms, we would readily understand a good deal about the job functions associated with that given analyst role. Instead, since there is so much money behind the term cybersecurity in government, academia, and industry, we use a singular term that significantly muddies the water.

Cybersecurity Engineer

Now let us look at cybersecurity engineer; this is almost worse to me because it also abuses the term engineer, and usually toward the specific goal of charging more for the person in the billet. The following is my off-the-cuff list of all the different things a cybersecurity engineer might actually be:

- Cloud Administrator
- Network Administrator
- Systems Administrator
- Domain Administrator
- Firewall Administrator

- Security Operations Center (SOC) Analyst
- Compliance Auditor
- Compliance Manager
- Hunt Team Operator
- Red Team Operator
- Penetration Tester

As with the cybersecurity analyst, the term cybersecurity and engineer have both been made so ambiguous as to become almost completely useless in describing something. Yet, the money in the industry has driven the terminology.

Comparison

Now, let's just compare those two, already ultra-ambiguous terms and we can see that they even share many of the same types of job functions. These are not the only job titles that have grown tremendous ambiguity thanks to where cybersecurity terminology has led us, but they are certainly the most illustrative of the problem.

As you can see after reviewing Table 2-1, six of the roles could be either a cybersecurity analyst or engineer. This means that over half of the ones I thought easily associated with either term could be advertised under either job name.

Table 2-1. *Comparison of Roles and Responsibilities*

Roles	Title: Cybersecurity analyst	Title: Cybersecurity engineer
Intelligence analysis	YES	NO
Network Analysis	YES	NO
Vulnerability Analysis	YES	NO
SOC Analyst	**YES**	**YES**
Risk Analyst	YES	NO
Compliance Auditor	**YES**	**YES**
Compliance Manager	**YES**	**YES**
Hunt Team Operator	**YES**	**YES**
Red Team Operator	**YES**	**YES**
Penetration Tester	**YES**	**YES**
Forensics Analyst	YES	NO
Cloud Administrator	NO	YES
Network Administrator	NO	YES
Systems Administrator	NO	YES
Domain Administrator	NO	YES
Firewall Administrator	NO	YES

Taxonomy of the Profession

In Figure 2-1, which is available at https://public.cyber.mil/cw/dcwf/, we can see what the United States DoD thinks a good taxonomy is of various cyber roles. I am including to show a known taxonomy and we will

move past it into our own taxonomy. This is partially due to the military nature of the DoD one, as well as some of the roles not meshing well with the wider cybersecurity industry that we are discussing in this book.

Figure 2-1. *DoD Taxonomy*

As I mentioned, we will not have in out taxonomy that will be leverage for the rest of this book the analyze, collect and operate roles in the same way or at all as they are a foreign intelligence gathering, act of war type of activity that specifically falls under US Code Title 10 and Title 50.

Further, I think this a good point to address one function that will be missing from our taxonomy and that is programmers, coders, or developers. These functions do have security considerations to their own craft such as secure coding in general and DevSecOps specifically. These are activities though that fall under the craft of those individuals and is not in my mind a cybersecurity function. Further, security issues

that are potentially introduced via poor practices of such professionals already have cybersecurity functions associated with the identification and mitigation of such cybersecurity risk.

Our Taxonomy

If in the end you decide that you like the DoD taxonomy or some other taxonomy better or find them more accurate, that is of course fine and well. For the purpose of follow-on discussion though, you will want to refer to the one we will outline in this chapter as further work builds on the foundational point being made and less the specificity of one given category of roles and responsibilities over another.

Types of Cybersecurity

In the following, I will describe the eight types of cybersecurity roles that I will use in our taxonomy and that will be referenced in later chapters. I make no claim that this is perfect or the most accurate specific to a given situation; it is simply the best structure I could come up with to make my point about theoretical cybersecurity and who should really be doing it. If you prefer your own taxonomy of roles or functions, then I suspect you could leverage it in a way similar to how we will at the end of this chapter. Our taxonomy is shown in Figure 2-2 and described in the following section.

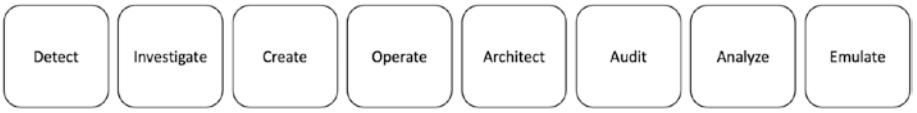

Figure 2-2. *Our Taxanomy*

Detect

By detective roles, we mean any that are involved in the aggregation and analysis of data about a system to perform work in a detect function. The following is a list of examples (not comprehensive) that could fall within this cybersecurity role:

- Net flow and other SOC-related analysis
- Intrusion detection system analysis
- Behavior analytics analysis

Investigate

Investigative roles are those that not only analyze aggregated data provided by other systems, products, and software but also key off of such data and go exploring or hunting to actively collect related data from systems and logs. The main delimiter between detective and investigative at an extremely abstract level is the active nature of investigation in a cybersecurity sense compared to detective. The following are examples of job roles with an investigative function:

- Threat hunting operations
- Forensics analysis
- Blue team type analysis such as nmap scanning

Create

In the create role, we are talking about those individuals involved in the creation of the infrastructure that run a given organization or network. They are responsible for setting up the systems in a secure manner as well as designing them to support operational needs and security requirements. One key attribute of create roles is that they are not directly interfacing with the eventual users of a system. Instead, they are responsible for building

the system or sections of it. It is also important to address here the lack of programmers and developers from our taxonomy. Even with the growing prevalence of secure development operations in the form of things like DevSecOps, there may be utilization by the developers at various stages of their pipeline. This does not mean that they are responsible for cybersecurity considerations. I think it is important to involve security early on in such processes by leveraging things like static and dynamic code analysis tools, but for similar reasons to our moving defense example, relying on people too far from real cybersecurity perspective to have appropriate context can't be dangerous. Therefore, our create role will not include people who interface with systems at the code commit role, as their primary responsibility is that a system perform the actions it was written for and security is traditionally secondary. Example jobs with this role are as follows:

- Router administrator
- Network designer
- Firewall administrator

Operate

The operate role covers those that maintain, repair, and operate the software and settings that run on a system. Unlike the create role, those performing operate actions are often interfacing with the users of the system as well. This brings about a unique cybersecurity challenge to the operate role over the create role in that the most vulnerable part of a system (the people who use it) is the major reason for operate roles to perform their actions. Example jobs that perform the operate role are as follows:

- Helpdesk technician
- Domain administrator
- Website administrator

Architect

The architect role is that which designs cybersecurity systems, policies, and procedures with varying degrees of diversity. A job which I am not indicating falls within this role, and the one which falls more within the journeyman concept, which we will cover later this chapter, is that of cybersecurity architect. A cybersecurity architect is responsible for designing the cybersecurity architecture an organization will use to mitigate risk and enable strategic outcomes. This involves knowledge of and design to every facet of cybersecurity as a body of work. Different than this are role-specific architects who are responsible for designing the implementation of a portion of the larger cybersecurity architecture. Examples of these architect roles, which represent this role of designing specific facets within cybersecurity, are as follows:

- Network architect
- Cloud architect
- Software solution architect

Audit

The audit role is that of compliance, verification, and validation. In this role, individuals are responsible for ensuring that policies, regulations, and standards are being followed and implemented in a system. This can be from the cybersecurity perspective of the organization that owns the system, or it can be by and for a regulatory body that governs the organization actions. In the Department of Defense, this could be system accreditation under NIST RMF, or in the financial industry or healthcare, it could be SEC or HIPAA regulations, respectively. Examples of this role are listed next. In this role, we will also place those that manage the policies and certain auditable assets as the skillsets are nearly identical.

- Compliance engineer/manager
- Compliance auditors
- Independent verification and validation teams

Analyze

Analysis is a term thrown around the entirety of the cybersecurity industry and community, as I indicated in the example where I compared cybersecurity analyst and engineer job titles. In our taxonomy though, we are using it to describe the role of those who make assessments and analysis on data that was not collected or produced purposefully by the hardware and software in a network. That fact is what delimits this role from something like a SOC analyst who is reviewing logs and events and data created by the system's devices. This is more an intelligence creation and analysis role performed by assessing more abstract information about a system and its cybersecurity such as network maps, user behavior, threat data, and so on, and examples are listed as follows:

- Threat intelligence
- Open source intelligence analyst
- Vulnerability analyst
- Exploitation or targeting analyst

Emulate

The last role I will cover is that of emulation. This is where the various levels of adversarial emulation are performed to test, assess, and exercise the cybersecurity apparatus of an organization. This can lead not only to remediation and further mitigation of discovered issues but also to allow defensive mechanisms to be tested and validated through response to the emulation. Job that would perform this role are as follows:

- Web application penetration tester
- Network penetration tester
- Red team operator

Functional Subsets

Next, we will add to our taxonomy by dividing the eight roles we have covered into four functional subsets that tie together somewhat similar experience, knowledge, and skills needed to perform the activities in such job roles. Figure 2-3 shows the four functional areas and the roles they encompass.

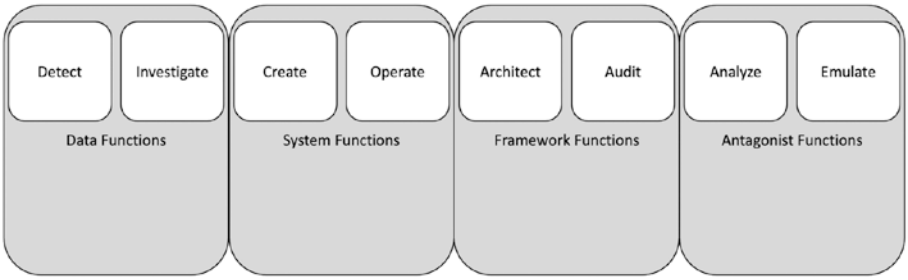

Figure 2-3. *Functional Subsets*

Data Functions

Job roles that have a data function are those that require data about the system, from the system to be performed. Both detective and investigative job roles require a cybersecurity professional to be versed in analyzing information that systems produce. Though the data may be collected somewhat passively in the case of detect roles and active for investigative roles, the perspective that such information is analyzed from is very similar.

System Functions

While there is a difference in job roles that are customer- or user-facing and those that are not, the job roles that perform system functions rely on similar actions by cybersecurity professionals. Diagnosis of issues may differ when users or customers are involved, but configuring, setting up, and fixing systems are done by similarly experienced roles requiring a similar skillset. Job roles in the system's functional domain require understanding of command line syntax, underlying infrastructure, and overall configuration of the devices that make up a system.

Framework Functions

Architecture roles create frameworks, and auditing roles evaluate, verify, and validate them. In either case, there is a need to have an in-depth understanding of what a framework is intended to accomplish, why it has been put in place, and how it is intended to function. As such, both types of cybersecurity job roles can be lumped into a framework function group.

Antagonist Functions

Antagonist functions are those that require an antagonistic or adversarial perspective and understanding to best perform the cybersecurity role. This is obviously the case with emulation roles such as red teaming or penetration testing. It is also required when performing intelligence analysis of an organization or system. This is because instead of making analysis of system-created or system-collected data, the assessment and analysis focus on information related to the scoping and targeting of an organization with the specific fact that motivation is antagonistic in nature.

Actional Subsets

It is also worth showing the roles in our taxonomy based on the split between roles involving reactive and proactive cybersecurity. Figure 2-4 shows this delineation.

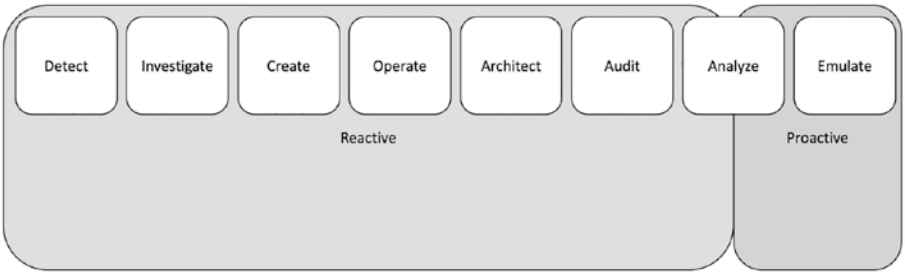

Figure 2-4.

Reactive

The majority of cybersecurity roles are reactive in that they require information from existing attacks to inform security functions. Even threat hunting, which is often referred to as generally proactive, requires knowledge of actors, associations, or other attributions to inform hunt activity.

Proactive

Emulate job roles are mostly proactive as they rely on individuals to attack a system as a malicious actor would. This attempt to discover misconfigurations and new exploitation efforts make it proactive. In the same way that threat hunting is not truly proactive, there are times when unsophisticated penetration testing can also be viewed this way. When performed by less skilled individuals or with certain motivations in respect

to time and scope, scanning and exploitation of only known capabilities is also arguably not proactive. The reason the proactive domain extends partially into the analyze role is that there are times where intelligence assessments made about threats or systems can provide truly proactive information to guide cybersecurity efforts.

Analogy

Now that we have covered our taxonomy that will be leveraged for this chapter and others, we will show an analogy of similar roles in a different industry. This should aid to illustrate the point we are making at the end of this chapter regarding the professionals most appropriate for theoretical cybersecurity endeavors. We will call this industry in our analogy the shopping mall industry. The goal of the shopping mall industry is for its malls to stay open and operational as long as possible. Figure 2-5 shows the taxonomy of job roles for our mall operations and what follows is a quick list of these roles with descriptions.

Figure 2-5.

Detective

Our shopping mall industry detective work, where data is gathered from systems in the shopping mall, could include many types of detective data analytics that support shopping mall operations. These analytics could be based on detecting data from things like security cameras, HVAC systems, power usage, and others that can allow shopping mall operators to tailor the usage of these systems to optimize longevity of business operations.

Investigative

For an investigative analogy in the shopping mall business, we will put pest control professionals in this role as they go through and look for things like termites and other pests that might impact the structural integrity of the mall or impact business operations.

Create

For the create role, we will refer to those that built the shopping malls including carpenters, plumbers, electricians, and others.

Operate

For the operate role, we will have those professionals in the shopping mall industry that interface with the customers and users of the mall. This could be repairmen, retail staff of shops in the mall, cleaning crews, and others that keep the mall operational.

Architects

Here architects will be those structural architects who designed the mall. We don't have the same need to separate these architects from broader architects as shopping mall operations architecture is not a thing.

Auditors

Shopping mall operations also have auditors who ensure that mall policies are kept up as well as other regulations and standards are followed. This could include things like workplace safety standards auditing by an organization like OSHA or a fire marshal making sure that stores are not over capacity.

Intelligence Creators

Just as intelligencer assessments can inform cybersecurity activities, shopping malls can have business-related intelligence. Business intelligence can be about where to place what types of stores in the mall based on purchasing habits for instance.

Adversary Emulation

Adversary emulation for a shopping mall is a little less likely than this job role is in cybersecurity; however, a shopping mall operator could certainly hire physical penetration testers to see how easy it is to do things like shoplift or break into the mall given its security system and cameras.

So, What's the Point?

The thesis of this chapter is that we need to identify the right type of people to perform theoretical cybersecurity efforts for the betterment of the industry and to improve the body of work. The reason for this shopping mall taxonomy is to illustrate the importance and relevance of our suggested theoretical cybersecurity professionals. In shopping mall operations, individuals would need varied and lengthy experience across several job roles to realistically provide contextual and defensible theoretical improvements to shopping malls.

Someone with time spent as a retail professional and as a builder of malls or as a business intelligence professional would have a wealth of perspective and experience to draw from. The importance of this context, as discussed in Chapter 1, is that it allows for theoretical ideas to be framed by reality, in this case the reality of operating a shopping mall. The opposite is also true that experience in only one facet of shopping mall operations would not make someone reasonably capable of coming up with theoretical shopping mall ideas.

The Tradecraft Concepts

The same concepts are true of cybersecurity as well, that variance and depth of experience across the body of work is necessary to produce professionals with the appropriate context to explore theoretical cybersecurity. Our shopping mall analogy is useful to make at least two points regarding cybersecurity professionals. First, to further my point about developers not being cybersecurity professionals. In the same way that the developers of a point-of-sale machine do not need to have in-depth knowledge of shopping mall operations, neither do developers of code need in-depth knowledge of cybersecurity. Second, our scientists from Chapter 1, who came up with the moving target idea without good cybersecurity context, are a lot like the scientists who design better nails through metallurgy or plastic flooring through chemistry but would not be expected to conduct experiments toward shopping mall operations.

This isn't to say that things like better nails and better flooring through scientific experimentation aren't necessary and beneficial because they are. The point is that they do not perform experiments on their areas of expertise in chemistry or metallurgy and call it a shopping mall experiment. This is essentially what happened with our Chapter 1 example. Scientists who are experienced in something such as computer science performed a computer science experiment and billed it as a result that proved a cybersecurity concept.

So how do we avoid this? How do we insure that the people carrying out theoretical exploration in the field of cybersecurity are doing so with the right context and experience behind their efforts to result in true cybersecurity innovation?

What we propose is a sort of tradecraft structure where individuals in the functional areas we outlined in our earlier taxonomy represent four domains of cybersecurity apprenticeship. In a specific functional area, we

could say that two years make an apprentice, six years make a journeyman, and ten years make a master. Years of experience could also count as years in completing a relevant bachelor's or master's degree. These timelines are similar to other trades such as electricians and plumbers. We can then levy this system to create apprentices, journeymen, and masters within the broader body of cybersecurity.

We could say that once a person has six years of experience in a functional domain (becoming a journeyman in that domain) they are an apprentice of cybersecurity at the broader stage. To become a journeyman of cybersecurity though, we should require someone to be a journeyman in one domain and at least an apprentice in another. Further, we could say a master cybersecurity practitioner must be a master of a domain and at least an apprentice in another or be a journeyman of two different functional domains. Figure 2-6 shows this example structure.

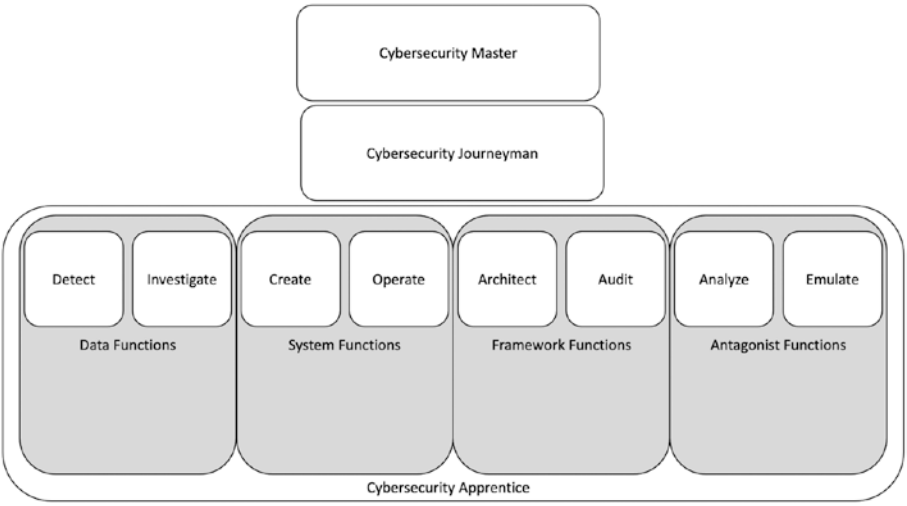

Figure 2-6. *Cybersecurity Trade Levels*

Summary

To wrap up, we have established a trade structure for the cybersecurity tradecraft. The semantics of our system bear hashing out at scale and the years of experience and other requirements could certainly be put up for debate. The takeaway is that we should establish some structure that produces a minimum qualification for professionals in cybersecurity to be considered journeymen or masters of the trade and not of specific functional domains. If we can do that as a field, we will have a pool of professionals who could be entrusted to take the lead and provide direction for further theoretical cybersecurity.