CHAPTER

1

Computer Network Exploitation

A computer once beat me at chess, but it was no match for me at kickboxing.

—Emo Philips

COPYRIGHTED MATERIAL

Since Sun Tzu's *The Art of War,* historians and analysts have searched for guiding theories and principles of conflict. Their purpose was not always to create some academic treatise to be beheld or to provide an endless stream of pithy quotes for marketing presentations. Rather, in exploring the principles of conflict, the goal is to confer an advantage in training, planning, research and development, execution, and defense—in short, to increase the efficiency and effectiveness of a fighting force in all aspects.

Information systems are a new area of conflict; one in which the incursions are virtual and the violations of sovereignty are abstracted. Yet the stakes are tangible. There may be no land involved, but both sides seek to attack and protect a territory and property.

Information systems are integrated into all aspects of the global economy and modern nation-states. Of course, there is e-mail and the Web, but less visible are the inventory, ordering, and payment systems that drive business. You barely notice when the grocery store prints out coupons based on your shopping habits, while simultaneously noting the inventory loss for later restocking. All this data is shared over a network and stored in a data center in…well…you actually have no idea. Yet this unseen database can reveal not only your favorite item from aisle 10, but also whether you are married, have kids, own pets, like to drink, or are out of town right now.

Now the flavor of ice cream you prefer may not be much of a secret worth stealing, but there is a wealth of information that is. Interested in how to log

in to a bank by spoofing someone's supposedly secure login token? Looking to know which of your neighbors are dissidents and are "inciting subversion of the state"? Curious about what an aspiring U.S. vice presidential candidate writes in e-mails? Do you find the source code to the computer systems on the F-35 Joint Strike Fighter appealing? My mint chocolate chip preference is the only untouched thing on this list; though that too is questionable.

Given the huge potential economic and military benefits of acquiring this information, it's no surprise that the act of stealing computer information has become a well-funded profession. And like any profession, it has developed its own set of terminology. So before getting too deep, let's start with the basics.

Computer Network Exploitation (*CNE*) is computer espionage, the stealing of information. It encompasses gaining access to computer systems and retrieving data. An old analogy is that of a cold war spy who picks the lock on a house, sneaks in, takes pictures of documents with his secret camera, and gets out without leaving a trace. A more modern analogy would be a drone that invades a hostile country's airspace to gather intelligence on troop strength.

Computer Network Attack (*CNA*) is akin to a traditional military attack or sabotage. It applies the four D's of "disrupt, deny, degrade, or destroy" to computer networks. Now, the cold war spy smashes a few artifacts as he leaves or maybe *Fight Club*-style, he introduces a gas leak so that the whole place explodes sometime later. Meanwhile, the drone rains hellfire missiles. CNA is the computer equivalent. It describes actions and effects that range from the subtle to the catastrophic.

Non-kinetic Computer Network Attack is a term this book uses to describe the subset of CNA conducted virtually, that is, any disruption, denial, degradation, or destruction initiated and performed via computers or computer networks. Although sending a missile into a data center is a rather effective form of CNA that fits well within the definition, physically initiated acts are outside the scope of this book.

Non-kinetic CNA therefore describes damage with virtual causes; though there very well may be physical effects. To continue with the analogy, instead of breaking anything, the spy remotely shuts off the heat during an extremely cold night causing the water pipes to burst. The cause was virtual, but the effect was not.

Computer Network Defense (*CND*) is protecting your networks from being exploited or attacked. It's the locks, doors, walls, and windows on the house and the police officer that walks by once a day on her beat, or the radar sweeps and antiaircraft missile systems that line the border.

Like CNA, there are both physical and virtual aspects to CND, but the term generally applies only to virtual security and is therefore used that way in this book.

Finally, *Computer Network Operations* (*CNO*) is the umbrella term that is composed of all the previous terms: Computer Network Exploitation (CNE), Computer Network Attack (CNA), and Computer Network Defense (CND).

CNE is the key subject necessary for understanding all aspects of the topic. As shown in Figure 1.1, the effective parts of each discipline are rooted in CNE.

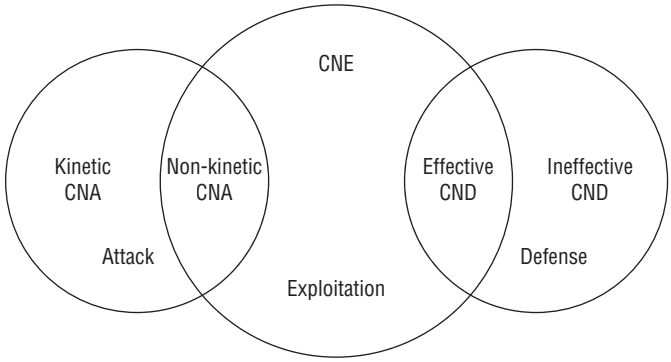

Figure 1.1: CNO disciplines

Effective non-kinetic CNA requires at least a measure of access to the target. Generally, the more access you have, the wider the range of options available. With minimal access, you might temporarily take a website offline. With extensive access, you can erase the data on tens of thousands of computers and take the company down for a week, as was done to the oil company Saudi Aramco, allegedly by Iran.

CND, or defense, does not rely directly on CNE (at least not while it remains illegal to counterattack), but trying to craft a successful network defense without understanding the offense is like trying to design a flak jacket without any knowledge of ballistics. Either way, the exercise is going to end with something full of holes.

CNE is central and therefore worth formally defining. The U.S. Department of Defense defines CNE as

> *Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.*
>
> *—Joint Publication 3-13*

The first thing to note is that CNE is directed. There is a "target or adversary." This is a differentiating factor. Many a computer worm or virus, such as Michelangelo, Code Red, Melissa, or SQL Slammer, has gained access to computer systems. And yet, these infections were not CNE because there was no intended target and no intent to gather information.

An indiscriminate worm is more like the flu. There is no conscious choice of victim, and whether a particular person gets sick is a combination of natural defenses, preparation, and luck. CNE is more like biological warfare, leveraged with a particular target in mind.

This is not to say that a CNE operation is always precision targeted or that it will never compromise a collateral computer. Counterexamples exist. Stuxnet was a wormlike attack that infiltrated Iranian nuclear facilities and then went on to infect other companies. Worms, like those created to exploit the Linux Shellshock vulnerability, can be leveraged to deposit backdoors in preparation for later access. Every action need not be deterministic, but on balance, the bulk of a CNE operation is intended to be focused, targeted, and invisible.

The rest of the Department of Defense's definition provides a good basis for discussion but requires one significant point of emphasis. To understand the missing nuance, you must first understand computer operations.

Operations

A *CNE operation* is a series of coordinated actions directed toward a target computer or network in furtherance of a mission objective. The mission objective may be anything ranging from political intelligence, design plans, company strategies, or plain-old financial information.

Let's parse this definition because several words take on different meanings in a CNE context.

The word *target* has an intentional duality. Whether target systems, target networks, target data, or target employees, "target" simultaneously refers to both the goal and the obstacles to reaching it. Target includes both the data you want to acquire and the forces in place to protect it.

Though the word *attacker* is commonly used to describe the offensive actor, the corresponding *defender* is notably absent from this definition. A target might defend, but it might not. A target may not even know if and when it is attacked.

Now everyone knows what a computer is, right? It's a desktop, laptop, or smartphone. True. But it's also your television, alarm system, building air conditioning system, and increasingly your car. So you must consider a computer in general terms. A *computer* is any device that contains or can be leveraged to access wanted data.

A computer can be a target, an attacker, or both at the same time. The same computer can run a defensive security product and a program designed to circumvent that very product. Computers are not on one side of the attacker/

target relationship any more than a chessboard is on the side of the black or white pieces. Certain squares start out under the control of one side or the other, but as the game progresses, it is not going to stay that way.

A *computer network* is a hierarchy of connected computers controlled by one entity. Computer networks can be simple or complex, ranging from two computers connected by a single cable to millions connected across satellite links and oceans.

Networks are made up of both computers and network devices. A *network device* is any device whose purpose is to facilitate or inhibit communication. Simple network devices are like a house circuit breaker. Electricity, or in this case data, comes in, is potentially transformed, and routed out the appropriate path. Examples include cable modems, DSL converters, and Wi-Fi access points.

More sophisticated network devices not only route data, but also can selectively grant, monitor, or deny access based on the type of data and its destination. Examples include smart switches, routers, and firewalls. These network devices are sophisticated enough that they can be considered just a specialized class of computers.

One final definition needed, though not explicitly included in operations, is the Internet. The *Internet* is a large system of networks linked together, but with no common entity controlling access. It is a series of contradictions: simultaneously concentrated and dispersed, interconnected and segmented, and established but under constant change. It is conceptually simple yet enormously complex in architecture, design, and regulation.

Within a CNE operation, an attacker is not concerned about the entirety of the Internet, but only the attacker's own network, the target network, and any intermediary devices, networks, or services connecting the two. Thus, you can view the Internet as a means of communication for carrying out a mission's objective.

Operational Objectives

All CNE operations have an operational objective, or put simply, a goal. The specific objectives vary widely with the actors and their capabilities, but the types of objectives are common. Operational objectives can be broadly divided into the five categories shown in Figure 1.2.

An operation falls into one or more of these categories at any given point in time. Operations, though, are not static. An operation may begin as firmly fixed in one category, but change over time or with a change of circumstances. The arrows in Figure 1.2 denote how this form of mission creep typically proceeds.

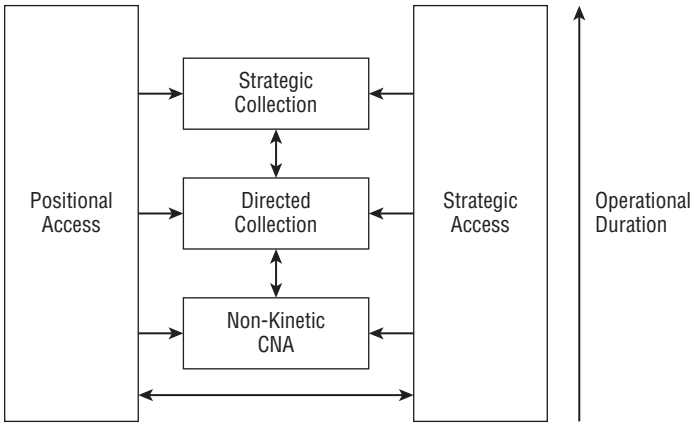

Figure 1.2: Operational categories

Strategic Collection

Strategic collection operations target the collection of economic, political, financial, military, or other information for strategic reasons. The aim of strategic collection is not one particular piece of data, but rather the collection of data *over time* that you can analyze to determine power shifts, plans, trends, adversarial capabilities, and so on.

For example, according to WikiLeaks, the NSA has been recording nearly all phone conversations in Afghanistan.[1] This is a perfect illustration of strategic collection. This collection may reveal the strength and plans of various warlords, the low-level leadership structure of any remaining Al-Qaeda, or perhaps any shifts in government corruption. Each of these is a strategic intelligence requirement for the U.S. government.

Strategic collection may also lead to tactical information. In this example, monitoring the communications of a particular warlord to understand regional stability is a strategic objective, but doing so may provide actionable tactical information that can be used to intercept a weapons shipment coming in from Pakistan. This information could tip off analysts to other targets of interest, giving birth to a directed collection operation.

Strategic collection requires substantial analytic capabilities for success because there may be an enormous amount of information to sort through, and the exact nature of what is useful may be unknown. There are somewhere in the neighborhood of 20 million mobile phone subscribers in Afghanistan.[2] If we assume each subscriber makes only a single 1-minute phone call each day to another subscriber, then recording every call requires processing and storing 10 million minutes of audio, or about 19 years' worth, every day. This much data is worthless unless analysis can be automated.

Due to the cost and sheer technical magnitude of strategic collection, this objective is limited to nation-states or well-funded criminal organizations.

Directed Collection

Directed collection operations target the collection of information to meet an immediate objective. The nature of the wanted information, or at a minimum the general class of it, is known from the beginning.

For example, China is alleged to have stolen the plans to the next-generation Patriot Missile system, a so-called aerial interceptor, or system that knocks incoming missiles out of the sky. Imagine that someone shoots a bullet at you. Now imagine trying to hit that bullet with another bullet, and you can get some sense of the amount of advanced engineering and technology that must go into these types of systems. This is a worthy target of interest.

Of course, there is no way to know whether the Chinese specifically sought out these plans or just happened upon them, but it seems more likely than not that it was a directed effort. China's military would be keenly interested in both building its own versions and studying ways to defeat them.

This is the essence of directed collection. The target was known: the U.S. Defense contractor Raytheon or any of its suppliers and partners. And the general class of information was known: weapons system data. It was likely just the specifics of which network to go after, the type of data to search for, and so forth that were learned after the operation commenced.

A weapons system is just one example. Financial and credit card data is a common goal of criminal directed collection. Customer lists and e-mail addresses are another. A specific person's skype communications may be yet another. The common thread is a priori knowledge of the end goal.

But as noted previously, strategic collection can result in this type of information. So what's the difference between strategic and directed collection? The only differences between the two are the initial intent of the operation and the duration.

Because directed collection operations seek specific information, the operation may end after that information is obtained. Does this sound likely though? Does anyone believe that the Chinese are going to walk away from whatever systems they compromised containing weapons design plans? Of course not.

In practice, directed collecting is extended. If useful information is gathered once from a target, that target is likely to contain useful information again. For another example, why would a criminal steal one batch of credit cards, say from eBay, and then stop if he could remain undetected and harvest more credit cards later? Answer: he wouldn't.

Directed collection operations may begin with a short life expectancy, but successful operations will be extended over time.

Non-Kinetic Computer Network Attack (CNA)

Non-kinetic CNA operations are meant to disrupt, deny, degrade, or destroy the operational capability of a computer network. The extreme examples are

often portrayed in the media: the vulnerability of the power grid, the air traffic control system, river dam controls, and such. The fear is that some nefarious actor can cause devastating physical consequences. There is an element of truth in this, enough to make it a real security issue, but the reality of non-kinetic CNA operations to date has been much less spectacular. More often than not a website is just knocked offline for a day or two.

The methods of non-kinetic CNA can be divided into two general categories: attacks conducted from outside the target network without access and those conducted from inside with access.

Attacking from the outside of a network without access is relatively common. Amazon.com, Yahoo, eBay, Microsoft, and pretty much every major company with an e-commerce website have had their networks degraded by attackers leveraging thousands of computers in Distributed Denial of Service (DDOS) attacks.

DDOS attacks have been used against nations as well. In 2007, an attack disrupted much of Estonia's government, finance, and news outlets. And in 2008, another attack took down services in Georgia, ever so coincidentally timed a few weeks before Russia invaded part of it. The attacks may have been perpetrated by Russia or by cyber-rioters as the Russians claimed—an interesting question itself—but the fact that a nation-state's electronic governmental and commercial infrastructure was attacked and degraded is not in dispute.

DDOS attacks require a substantial number of computers to launch. If attackers owned or leased thousands of computers, they could do it themselves, but realistically, DDOS attacks are launched from *botnets*, a network of often thousands of third-party computers where attackers have *durable* access and control.

Outside attacks, though often effective, suffer from several disadvantages. They are easily detected. The disruption lasts only as long as the attack is active. They have no impact on the sensitive core of a network. There is little if any lasting damage, and recovery is almost immediate as soon as the attack subsides. Finally, the attack may steam roll innocent third parties that just happen to be in the way.

Non-kinetic CNA launched from inside the network provides a much wider range of options. Attacks can be subtle and difficult to detect. They have the potential to reach more sensitive or critical systems or data. Damage can be severe and last well beyond the duration of the attack. Recovery can be expensive and time-consuming. Finally, an inside attack can be tailored and highly targeted to reduce collateral damage and the impact to untargeted systems.

The fist reported large-scale example of this kind of attack had all these qualities. In 2010, the world was introduced to Stuxnet, a tailored attack against Iran. The attack software spread via 0-days, unknown and unpatched vulnerabilities, to reach its ultimate target: the programmable logic controllers that control Iranian centrifuges. When installed, the program subtly modified the controllers in a way that caused the centrifuges to break. This first-of-its-kind attack

reportedly damaged 20 percent of Iranian centrifuges before it was detected. At that point, it had been in progress for at least 1 year, with components of the software under development for at least 5 years.

A couple of years later the Wiper malware struck in two separate incidents. The first incident was against the oil company Saudi Aramco in 2012. The second was against various South Korean financial and media companies in 2013. The Wiper program spread by stealing and using credentials, and then, depending on the variant, either immediately or at the appointed time wiping critical sections of the infected computers to make them unbootable. Subtle it was not.

This type of non-kinetic CNA done with access exhibited by Stuxnet and Wiper is far more effective than an outside attack, but also far more difficult and expensive. It first requires gaining access to the target network. This makes the first part of the operation effectively identical to strategic or directed collection. Access must be gained for all of them. The only difference is that the access is leveraged to cause damage rather than gather information.

Strategic Access

Strategic access operations are executed for the purpose of future flexibility. Unlike strategic collection, it is unknown but hoped that the access will become useful at some point later. The access may lead to strategic or directed collection, non-kinetic CNA opportunities—or nothing at all. The attacker simply does not know at the onset.

In 2013, it was reported that GCHQ, Britain's signals intelligence service, hacked Belgium telecom provider Belgacom. This seems like a logical strategic access operation. Gaining access to this company might enable collection against European governmental organizations or diplomats within Brussels. Or it might open up opportunities to eavesdrop on or manipulate communications that traverse Belgacom's International Carrier Services, which, as the name implies, provides wholesale carrier services to countries around the world. This is, of course, complete speculation, but it fits the pattern of a useful strategic access operation.

Other examples of this operational objective are harder to come by, as their nature is to lie in wait and take minimal action. Still, it is plain to see that a strategic access operation is most useful if the access is *extended* if and until that access proves useful.

Positional Access

Positional access operations target computers and networks that are not themselves of interest but are useful in furthering a different objective.

An example of positional access is gaining access to the home computer of an employee of a target company. The computer itself may be of no interest, but perhaps the employee connects into the target company from home. This is exactly how Microsoft was hacked some 15 years ago. Positional access via the employee's computer provided an avenue for an attacker to circumvent Microsoft's perimeter security.

This method was also used to compromise the department store Target in late 2013. As shown in Figure 1.3, the intruders first compromised one of Target's suppliers, an HVAC vendor. They then used that vendor's credentials to compromise Target itself and make off with some 40 million credit card numbers.

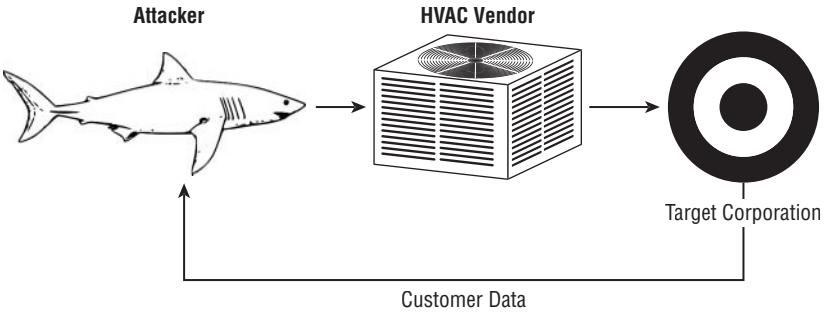

Figure 1.3: Positional access

Another example of positional access is compromising a university network to launch an attack. Again, the university network itself is of no interest, but it provides a layer of anonymity to an attacker. Some organizations, notably GCHQ according to the Snowden documents, allegedly proactively scan for vulnerable hosts they can add to their real estate portfolio for later use.

By attacking through these intermediaries, it will be more difficult for the target to trace the origin of the attack. This explains why China allegedly hacked a mental health clinic in California. It makes a suitable intra-U.S. launching point. It also explains why the Chinese offensive organization PLA 61398, a.k.a. APT1, purchased or leased hundreds of servers spread throughout 13 countries. Why bother compromising an intermediary when you can just buy one?

Positional access operations, like directed collection, may begin with a specific intent and a short life expectancy. However, just like directed collection, these operations may be extended. The employee's home computer may be needed if an attacker ever loses access to the target organization's network. Access to the mental clinic or a leased server could be used to launch several operations.

That said, out of all the operational objectives, extending positional access carries the most risk. The access may prove useful, but it may link together different operations if one is discovered. This is a calculated risk each attacker must weigh.

CNE Revisited

In each of the five operational objectives—strategic collection, directed collection, non-kinetic CNA, strategic access, and positional access—the likely success of the operation is linked to its duration. Extended access yields greater potential for gathering useful data in strategic collection, a potentially constant stream of updating information for directed collection, and a larger window of opportunity and a wider range of options for performing non-kinetic CNA. Extended access increases the likelihood that the systems compromised for strategic access or for positional access become or remain useful.

In short, almost all operations, independent of objective, are more likely to enjoy greater degrees of success if access can be sustained. Therefore, when thinking about strategy, a more useful definition of CNE than the one presented earlier in the chapter is

> ***Sustained*** *enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.*

This small addition of one word makes a large difference in fashioning a framework. Sustaining an operation is not easy. It adds an order of magnitude of complexity over simply gaining access. Yet sustained access is the key to both strategic and tactical success. It is the true art of CNE.

Construing CNE to emphasize duration also has the welcome side effect of marginalizing the attention-seeking behavior such as that shown by various "hacker" groups or self-appointed electronic armies. There's no real strategy behind defacing a few websites. Media coverage is anathema to sustained access and thus to CNE.

Though as duration is stressed, some operations will be intentionally short-lived. Perhaps there is only one useful piece of data to gain from a network. Maybe circumstances change and the political risk of exposure suddenly outweighs the benefits of the information. There are always exceptions. However, frameworks must be developed around the expected case. With such structure in hand, it becomes clearer why the special cases are indeed special.

And for CNE, as with anything that yields political, military, or economic advantages, the expected case is that operations are rarely willfully abandoned.

A Framework for Computer Network Exploitation

The tactics of CNE ebb and flow, but certain aspects of the discipline remain constant. These tenets can structure your thinking and help provide direction to both offensive and defensive actors. The tenets of CNE can be divided into

three categories based on their respective expected durability: first principles, principles, and themes.

First Principles

First principles are immutable and fundamental. They transcend the constantly shifting technology they seek to describe. For CNE, there are three such foundational supports, which are the principles of access, humanity, and economy.

- **Humanity**—CNE is grounded in human nature.[3] Although it is a highly technical domain, the technology is designed, built, used, and monitored by humans. The most sophisticated technology in the world is envisioned, brought to life, and in CNE, torn apart by people. As Carl von Clausewitz (Prussian general) noted for war, "[Theory] must also take the human factor into account, and find room for courage, boldness, and even foolhardiness."
- **Access**—There is always someone with legitimate access and a means to use it.[4] Whether it's the president of the United States and nuclear launch codes, the bank manager and the vault, or me and my collection of decorative soaps, there is someone with access to everything that is secured. Data is no different. It does not exist in a vacuum. It is generated and stored for the express purpose of being accessed later by someone with legitimate access.
- **Economy**—Ambitions always exceed available resources.[3] Whether it's a nation's foreign policy goals, an educational board's budget outline, the charity one supports, or just the kind of car one wants to buy, there are more goals than people, expertise, time, money, or technology can support. The same is true for both computer offense and defense. There is a priority, cost, and benefit to every action and to every outcome.

Principles

Principles shed light on various aspects of a subject. They are not universal truths, but as Clausewitz stated, "intended to provide a thinking man with a frame of reference." They are tools to "stimulate and serve as a guide for reflection."[5]

Principles may change, albeit slowly, as circumstances or perspectives change. For example, the U.S. Army used to expound the war principle of *cooperation,* but in 1949, it replaced it with *unity of command.* This change of principles and doctrine reflected changing circumstances, mainly the advances in communication that allowed real-time information to flow between physically separated units and commanders. Cooperation bacame less important if a well-informed hierarchy was in place to see the big picture.

Principles may also be redefined. The war principle of *mass* was derived from ancient times, and the idea of massing forces, that is, people, at the critical point of a battle. If the general could bring more soldiers than his enemy to bear in the right place and time, he was likely to prevail. However, with the increasing power and range of weapons over the centuries, concentrating forces at a single point was a recipe for annihilation. Rather than abandoning it outright, the Army reinterpreted the principle to mean the massing of combat power instead, that is, the focusing of ground, sea, and air capabilities at the decisive point.

Still, principles are more than just passing fads. A good principle will withstand evolutionary changes in technology. There are currently six principles of CNE, shown supported by the three first principles (access, humanity, economy) in Figure 1.4.

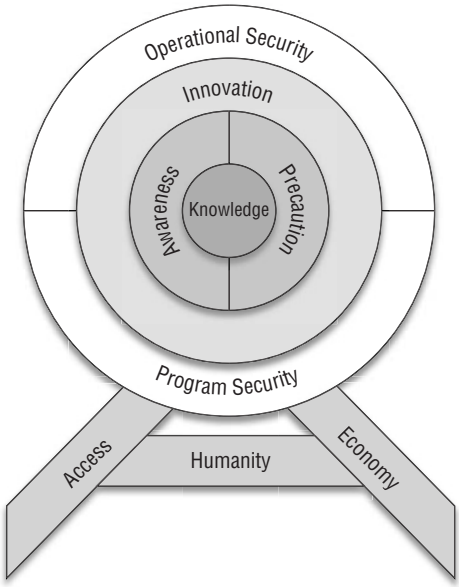

Figure 1.4: Principles of CNE

In brief, the principles are

- **Knowledge**—The broad and deep understanding of computers and computer networks, as well as the behavioral and psychological characteristics of people and organizations.
- **Awareness**—The mapping of the operational domain, including the active detection and monitoring of events in near real time.
- **Innovation**—The ability to create new technology, leverage existing technologies, or develop and adapt operational methods to new circumstances.
- **Precaution**—The minimization of the impact of unwitting actions on an operation.

- **Operational Security**—The minimization of defender exposure, recognition, and reaction to the existence of an operation.
- **Program Security**—The containment of damage caused by the compromise of an operation.

Together these principles form an ideal offensive goal, a target as it were. They are all interrelated. Some offer synergy. The first principles support everything, with humanity as the crucial connector. Knowledge is central to all of the other rings. Increased innovation improves every principle it touches.

Other principles trade off against each other. Operational security and program security are often at odds. The greater awareness one has, the less need for precaution and vice versa.

The principles will be explored in depth in Chapter 7, "Offensive Strategy," but for now, it is enough to understand that sometimes principles are in concert and other times they are in conflict. That is why principles must not be considered goals in and of themselves. They are a guide to planning and execution. Each operation is unique, and the equities involved must be individually weighed and continually balanced throughout the operation's lifetime.

Themes

Themes are reoccurring ideas that often underlie the means of an operation. They are like the theme song to a movie, found in different forms over and over again throughout the picture. Themes are useful to help quickly determine a suitable course of action in consideration of a strategic principle.

In an ideal world, you could catalog and reference a list of all possible tactics and quickly choose among them as the need arises. This works for a static and finite problem, such as tic-tac-toe or Connect Four, but the number of tactics and the speed and variability of technological change make such an approach impossible. You must therefore resort to using themes, a form of distilled operational experience.

Themes have more staying power than a specific tactic. Common themes include:

- **Diversity**—Leveraging a wide range of tools, technologies, development methods, network signatures, infrastructure, and operational methods
- **Stealth**—Leveraging tools, technologies, and methods that are largely hidden from view, or if in view, unlikely to attract attention
- **Redundancy**—Reasonable fail-safes, backups, and contingency plans for foreseeable setbacks and obstacles

Themes make poor stand-alone goals without principles and context. Stealth, for example, has no meaning unless one defines from what and for what purpose.

To make everything redundant without the context of what is at risk is to make everything prohibitively expensive.

Themes must always be considered within the broader strategic context. For example, developing a CNE capability against Blackberry devices may improve an attacker's technical diversity. The collection method may be stealthy. And it may offer redundancy into accessing someone's e-mail. But developing such a capability is a poor strategic move because as Blackberry's market share continues to plummet compared to iPhone and Android devices, the number of interesting targets using Blackberry devices will diminish. (That said, if a high-priority target shows no sign of abandoning them, then perhaps it is worth the investment.)

There are other themes as well that one may discover better suit a given organization, such as speed of execution or automation of tasks. Regardless, a diverse, stealthy, and redundant collection of tactics provides an incredibly powerful weapon for any attacker. With the right strategy, few defenses can withstand it.

Summary

Computer Network Exploitation is but the latest reincarnation of espionage. As an increasing part of the world's political, economic, and military information is stored on networks, a framework for organizing and analyzing CNE becomes necessary to national security.

Though CNE motivations and objectives are essentially infinite, operations can be grouped into one of five general categories: strategic collection, directed collection, non-kinetic CNA, strategic access, and positional access. Regardless of category, sustaining an operation likely leads to greater success.

CNE may be a fast-moving technological field, but some aspects are enduring. These are worth identifying, as they can help you derive strategies for building, planning, and executing operations or for defending against those that are.

The next chapter explores how the offense is guided by these principles.