EXPERT INSIGHT

Cyber Warfare – Truth, Tactics, and Strategies

Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare

Foreword by:
Gregory J. Touhill
CISSP, CISM (Brigadier General, USAF ret.)

Dr. Chase Cunningham

Packt

10

Survivability in Cyber Warfare and Potential Impacts for Failure

"A good plan violently executed now is better than a perfect plan executed next week."

– General George S Patton

War is just that: war. Be it a "legacy" engagement on the front lines of some foreign chunk of soil, or be it on some digital piece of infrastructure, it is no less daunting and no less ugly. The battleground we find ourselves on today is one that is transitory in nature, ethereal in its definition, and dynamic at its core. Every man, woman, child, device, application, and anything else on the planet that is online and sending or receiving an electron is literally transiting a live fire battlefield. 24 hours a day, 365 days a year, this combat zone never stops, and never takes a moment's rest. The only way to survive in a space that is this fraught with danger is to have a solid strategic approach and to abide by a list of practices that translate equally well between physical combat environments and digital ones.

In this chapter, we will explore the laws of survivability for operations inside this combat arena. Notice we don't say perfection, or dominance, or something like that. Instead, we speak about a pragmatic approach that is focused on using the best technology and approaches to the problem while still being honest about the fact that there is no perfection here. This is about survivability and working to keep moving forward in a never-ending onslaught of attacks.

Focusing on a perfect solution and struggling to have a bullet proof network is part of what has led us collectively to the state we find ourselves in. In battle and in war, the best outcome is to survive long enough and with enough continued gas in the tank to keep moving forward. There is no perfection, and there are no perfect tools, but there are ways to be the "last one standing" when the digital smoke clears.

In this chapter, we will walk through what is and isn't necessary for continual improvement and growth and discuss what tactics, technologies, and approaches to the future state of cyber warfare are most beneficial if adopted now. Buckle up; the ride into battle is always a bit bumpy.

What good are laws in war?

Fair question. After all, war, by its very definition, is what happens when laws have been violated and the structures that surround good order and discipline have fallen into chaos. So why laws? Well we don't necessarily mean "law" in the traditional sense of the word. We aren't thinking about laws in the sense of constraints that hold back our capacity to engage; rather, what we mean in this context is laws for survival and continued operational capability in a space that is dangerous. We mean laws that are solid approaches to the problems that you face in this arena that are based on an analysis and real-world experiences gained while being engaged in actual conflict.

Adoption of these "laws," or guiding principles, or best practices, or whatever you would prefer to call them, is meant to help you stay ahead of the threats that are active in this domain and to help translate the subtle nuances between two domains – cyber and physical. In any conflict zone, there is a seriousness that must be adopted by those that are living and breathing as they transit threatened areas. In war, there are always those that are left behind and must continue to try and live their lives as normally as possible while fire fights and combat rage around them. There are also the ground troops and those that are engaged in the fight that must operate and function without fail, or they will suffer severe causalities. And there is the enemy that is operating with a focus on imposing their will, whatever it may be, on their perceived adversary and targets of opportunity as they continue their chosen campaigns.

Each of those differing groups is always working to simply survive. Everyone in those groups always has the thought in the back of their mind that they want to get on with their lives and be anywhere else but where they are at that dangerous moment. The way an effective combatant does that is to adopt practices and approaches best suited to dominating their enemy to ensure that they are the one that comes out on top. This does not happen by accident. In order to be the last one standing, history has shown us time and time again that those who realize the requirements for the space in which they operate, and abide by well-thought-out strategic approaches to the problems they encounter, are the ones that win and survive.

In cyber warfare, this is no less applicable than in physical warfare. In cyberspace, we operate in a domain with no boundaries, no walls, no clear delineations for rules of engagement, and all of our weapons move at the speed of light. By adhering to, or hopefully at least thinking about, the "laws" provided in this chapter, those of us that are active on the front lines of cyber warfare can have the best chance to "RTB," that is, return to base.

"Law 1" – Default means dead

One of the main issues with technology in the space today is the prevalence of default configurations and accounts. Manufacturers today always set the default configurations of new software and devices to be as open and functional as possible, to enable ease of use and hopefully promote adoption of their particular product. Routers, for example, often will have a predefined password and default username. For other devices, this might mean applications that come preinstalled, again usually having "hardcoded" default login credentials available to the tool or technology.

The reason for this is because it is easier and more convenient to start using new devices or software if it has easy-to-configure default settings. But this does not help the tool or application to be secure. Default settings that are never changed and made safe creates serious security issues and provides adversaries with easy, authorized access to data and networks. Web servers, containers, and application server configurations can also be configured with default accounts that will lead to a variety of security problems.

To demonstrate just how easy this is, during the research for this chapter, I created a custom script containing thousands of Google dorks, simple requests on Google that are crafted to send back specific responses, and ran a few of them to see how many easy targets were available. In a matter of less than 3 minutes, hundreds of vulnerable applications and logins for a wide variety of devices and applications were found. A sample (with all pertinent identifying data removed) is provided here:

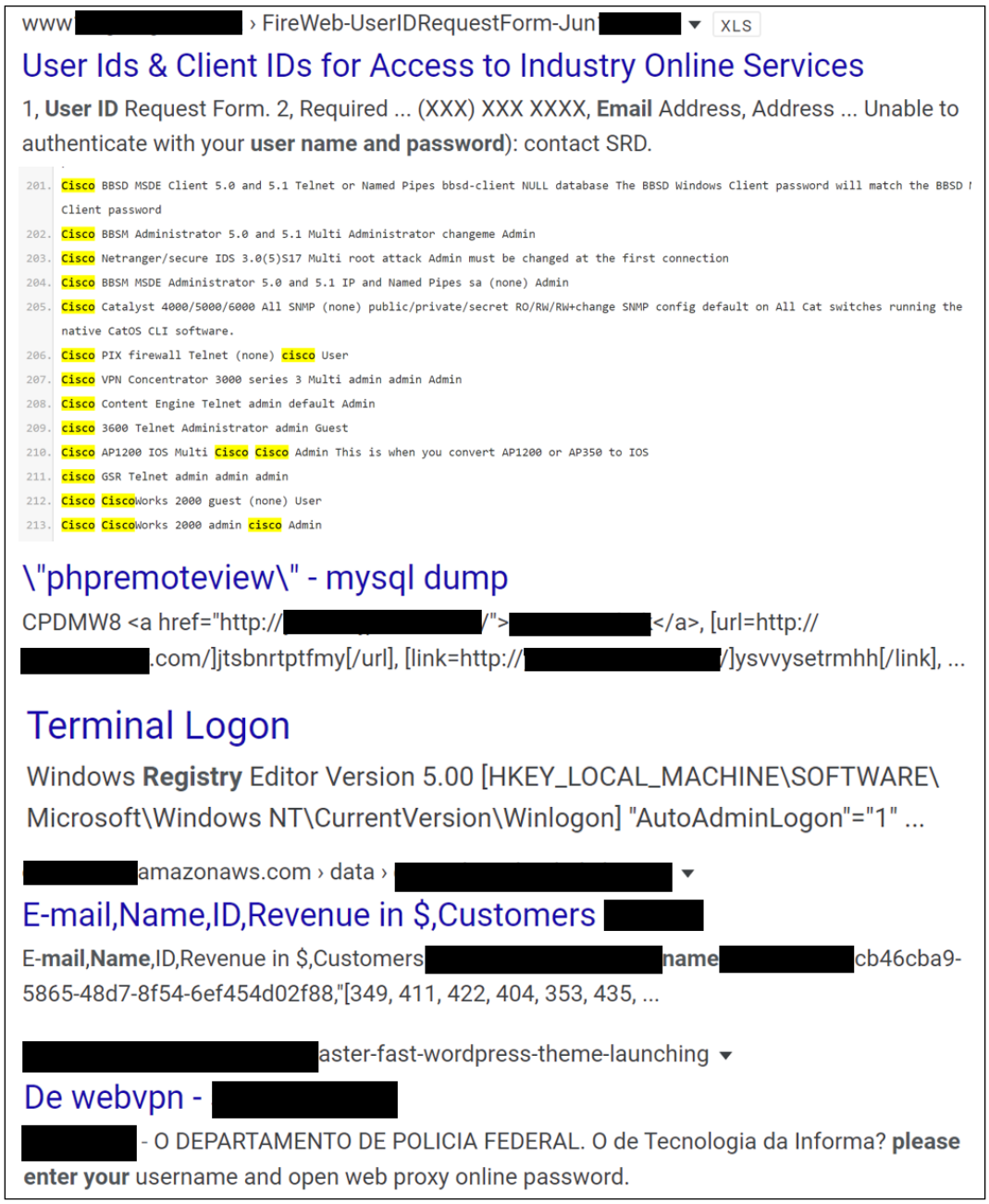

Figure 1: A number of screenshotted samples of exposed vulnerable applications and logins

While the information found might seem somewhat non-threatening at first glance, what should be evident is the fact that with no more than an hours' worth of time, a researcher working from home was able to find large amounts of misconfigured, open, touchable resources and logins with just a script. Odds are that with a bit more time, and some targeted programming, the results could be infinitely better. And because of the interconnected nature of most networks and the usual lack of internal security controls, any one of those potential accesses could have led to further exploitation.

A point of note is that in the sample screenshots that were provided, some of the results had VPN login credentials, email and user IDs, login information, and a variety of other intelligence that could have been used for attack vectors. And all those results were based on the script looking for default configurations and user accounts, nothing spectacular. Were this script to be better programmed and tied into an automated ML backend that could expedite and tailor the commands and parse the responses, the potential for problems increases exponentially.

Looking at GitHub, one popular tool is `changeme.py`:

```
https://github.com/ztgrace/changeme
```

`Changeme.py` focuses on detecting default and backdoor credentials, and not just common account credentials. The tool's default mode is to scan HTTP default credentials, but it can scan for other credentials if the script is modified slightly. `Changeme.py` stores collected credential data in yaml files. `Changeme.py` can gather information or intel from almost every protocol that is used on systems today. Targets can be specified by using a single IP address or host, a subnet, a list of hosts, a network scanner output like an Nmap xml file, or a Shodan (a popular device polling database for hackers and penetration testers) query:

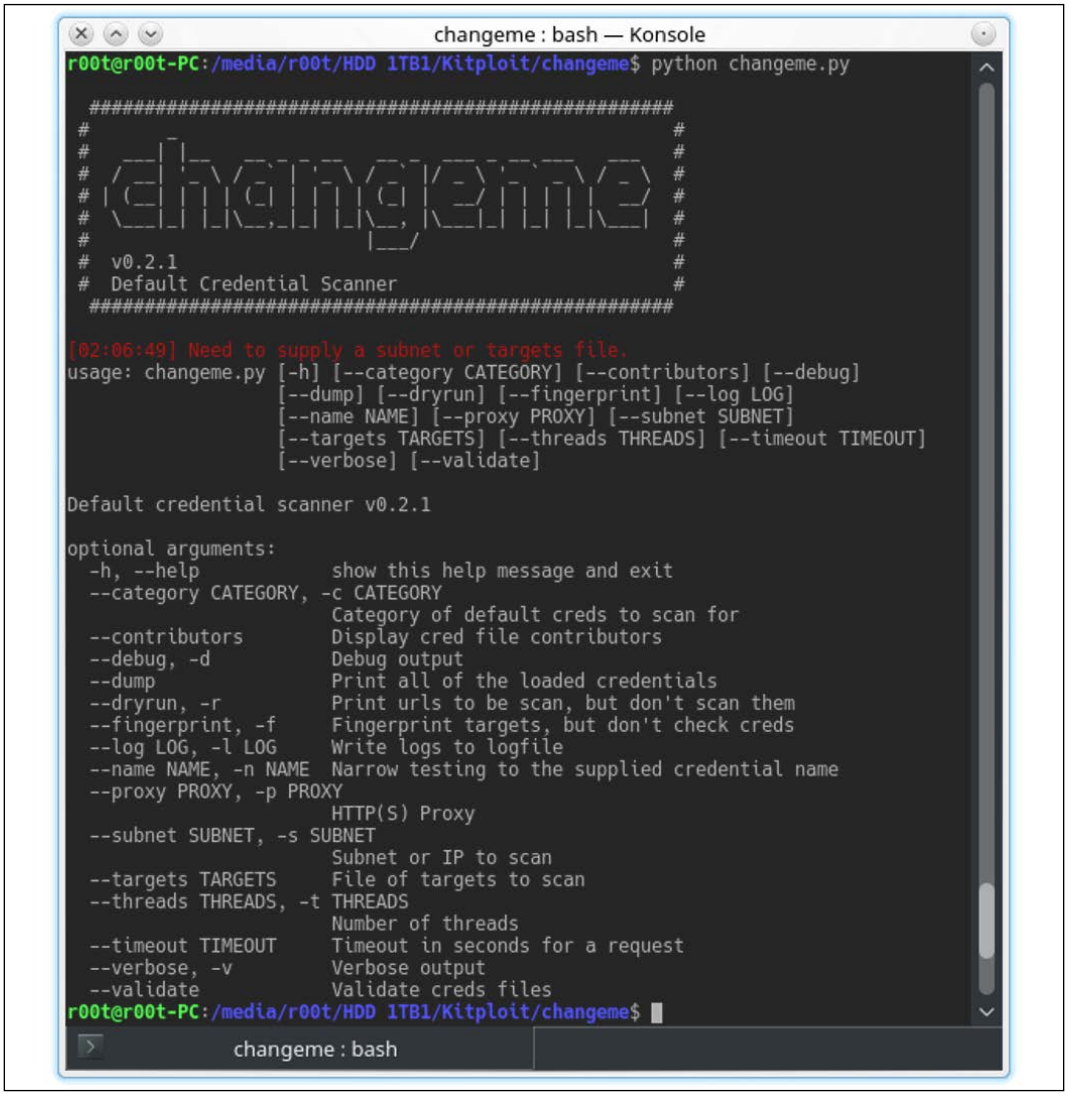

Figure 2: Screen showing options on changeme

Figure 3: Logs on changeme

The following are common scan examples:

- Scan a single host: `./changeme.py 192.168.59.100`
- Scan a subnet for default creds: `./changeme.py 192.168.59.0/24`
- Scan using an Nmap file: `./changeme.py subnet.xml`
- Scan a subnet for Tomcat default creds and set the timeout to 5 seconds: `./changeme.py -n "Apache Tomcat" --timeout 5 192.168.59.0/24`
- Use Shodan to populate a targets list and check them for default credentials: `./changeme.py --shodan_query "Server: SQ-WEBCAM" --shodan_key keygoeshere -c camera`
- Scan for SSH and known SSH keys: `./changeme.py --protocols ssh, ssh_key 192.168.59.0/24`
- Scan a host for SNMP creds using the protocol syntax: `./changeme.py snmp://192.168.1.20`

The point of these examples is that if it is this easy for someone conducting research to find access to such resources, it should be evident to anyone that it should be a matter of the highest priority to remove default configurations. Not doing so threatens the entire network that the default item is connected to, and almost guarantees that a compromise will occur.

Bots and automated AI/ML tools are available to make this intelligence collection even easier and do not require nation state-level capabilities to use.

"Law 2" – Think strategically, move tactically

In warfare, the importance of the need for movement within the battlespace is accepted as critical to survivability. Most of the time, the chaos of the space and the ever changing, and innovating, enemies' actions dominate the thoughts and plans of the defenders. The ways in which actions are being taken by each party result in a constant game of cat and mouse. It is only when one side recognizes that they must more cautiously engage in strategic thinking while enabling tactical movement that the balance of power begins to shift.

This is especially true in cyber warfare. For the last two decades, the major power player nation states on the planet have been engaging with one another in the tactical sense. A constant back and forth of who has the best intelligence and which unit has the newest and most powerful exploitation solution has continually been part of the tactical firefight between nation states. While there could be some argument that the strategy side of these engagements have been part of the equation, in reality the strategic outcomes from those tactical engagements have been tangential to the never-ending game of chess in cyber warfare. No major "wins" have been realized for any nation to date. Yes, there have been some gains and some losses, but, if you look at what has resulted from nation state-level strategic engagement in cyber warfare, no real net gain has been realized.

For any unit or organization to survive – and hopefully thrive – in a warfare environment, there must be an adoption of a strategy at the grandest level. Failure to realize the overarching intricacies and dependencies that are present between actors and their command and control systems and infrastructures is an exercise in failure.

A classic example of how tactical movements based on a lack of patience and strategic thinking can lead to exceptionally bad outcomes can be found by observing the scenario of Custer's Last Stand. On June 22, 1876 General Terry sent Colonel George A. Custer and his 7th Cavalry in pursuit of the Indian leader, Sitting Bull. That pursuit would lead to Little Bighorn Valley. General Terry's plan was for Colonel Custer to attack the Lakota and Cheyenne Indians from the south. This would splinter the Indian forces into a smaller force that could be dominated by Custer's more mobile cavalry forces. On June 25, Custer's scouts discovered the location of Sitting Bull's forces. Colonel Custer maneuvered to a position that would allow his forces to attack Sitting Bull's forces at dawn the following day. Unfortunately for Custer, Sitting Bull's scouts spotted Custer's forces moving into position and moved to inform Sitting Bull of the coming attack.

Instead of retreating at the realization that he'd been discovered, reorganizing his forces, and strategically planning his next move, Custer attacked. At noon on June 25, a day earlier than his planned attack, Custer split his regiment into three battalions. Custer split his forces and sent three companies straight into the village. He then dispatched three companies to the south to cut off the Indian retreat, and he used five companies to attack the village from the north. Those tactical choices proved to be disastrous. By reacting and splitting his forces, Custer left its three main components unable to provide each other support.

As the Battle of the Little Bighorn unfolded, Custer and the entire 7th Cavalry fell victim to a series of surprises, not the least of which was the number of warriors that they encountered. Custer's intelligence group estimated Sitting Bull's force at fewer than 800 fighting men. The real number was over 2,000 Sioux and Cheyenne warriors. His intelligence also stated that the Indian warriors likely only had hand weapons and bows and arrows for their defenses. This was incorrect intelligence as well. Sitting Bull's soldiers had procured advanced repeating rifles and had a large contingent of cavalry as well.

General George Armstrong Custer made a strategic underestimation of the forces he was about to engage with at the battle of Little Big Horn and was outflanked and overrun by a force of over 10 to 1. The intelligence he had gathered was faulty and led his decision making to be flawed. A tactical judgement based on only partially validated data points and best estimates resulted in a folly that has transcended military history for over a century. His rush to respond to perceived actions of the enemy and to engage them in a tactical pursuit played directly into the hands of his adversaries and cost him and all his men their lives.

In Custer's case, he acted tactically based on partial data about the enemy, and he and his forces never had a true understanding of what they were facing. They did not know how large the enemy force was, they did not know about the technology they were facing, and they had little, if any, actual knowledge of what areas of the battlespace were defensible. They just reacted tactically to the stimuli they had received, and everything went to hell. Avoiding that same engagement model is what should be the focus of those who are engaged in cyber warfare

The key to survival for any group is to adopt the concept of strategy first, and then tactics, not the other way around. Far too often, it is apparent that the organization that is outed as being breached or exploited has focused on implementing tactical controls that are adopted because of vendor marketing, not necessarily the realities of the space. It is rare that the leadership and the defenders can cite a singular statement that details the organizational strategy to secure the infrastructure. In physical warfare, that statement might have been "we will win the war on terror" or "dominate the air, control the battlespace." These statements sound simplistic, but that is the point of a good strategic statement. Clarity of vision and simplicity.

In cyber warfare, this must happen as well. An organizational strategic statement might be as simple as "we secure our users as we secure our infrastructure," or "we defend the edge and entity first." Those are not perfect, but they are simple, concise, and are easy to detail for the defenders who will engage with that strategy.

Once that strategy is shared and understood by the entirety of the defender group, the tactics that align and help to tactically make that strategy employable can be adopted. The strategy should be continually updated and adapted as the space and the tactics and tooling evolves, but there should always be a clear and useful strategy in place. And, contrary to Custer's example, the strategy should be based on a slow and careful response to actual enemy actions based on applied data points from a variety of validated sources. In cyber warfare, functional strategic defense is the correct approach, not half-baked tactical responses.

"Law 3" – Details, details

In warfare, the smallest detail can be the difference between life and death, victory and failure. Throughout history, wars have been won or lost because of details that were ignored. Benjamin Franklin is famously quoted as saying "*For want of a nail, the shoe was lost. For want of a shoe, the horse was lost. For want of a horse, the rider was lost. For want of a rider, the battle was lost. For want of a battle, the kingdom was lost, and all for the want of a horseshoe nail*". He also said, "*A little neglect may breed great mischief,*" in Poor Richard's Almanack in 1758.

There are concrete historical examples of the truth behind that proverb. On the bloodiest day in American history, September 17, 1862, the Civil War Battle of Antietam resulted in nearly 23,000 casualties. After crossing the Potomac River into Maryland on September 9, 1862, Confederate General Robert E. Lee divided the 45,000-man Army of Northern Virginia and spelled out the location for each group on handwritten dispatches for delivery to his commanders. Those dispatches were delivered by couriers on horseback to the commanders, except for one that was accidentally dropped from the courier's pocket when he stopped along the way to relieve himself. That dispatch was found by a Union soldier just a few days later, in an envelope wrapped around three cigars near a fence. This misplaced secret dispatch reached Union Army Commander George B. McClellan, giving him and his 90,000-man army the exact locations of their enemy.

That information led to a strategic Union victory that would ultimately impact the course of the war.

In cyber security and cyber warfare, the focus for most infrastructures has been to focus on the macro. The aim of most of the defenders across systems has been to continue to propagate the failures of the past, namely big perimeters with high "walls." As we described in the section on the failure of the perimeter, this is counter to what needs to happen for security.

Micro-focusing also requires a switch from defending those high walls on the perimeter to one where the focus and the "optics" are aimed into the core of the infrastructure and then maneuvered outward. Host-based isolation, ringfencing for data stores and databases, granular access controls, and vectored analytics that are based on behavioral anomalies are necessary to bolster defenses from the inside out. Those small details that are indicative of potentially threatening activity should be part of the response and remediation protocols that enhance the defender's ability to remediate potential threats. Without the details and a focus on using powerful, specific analytics that enable a fix to the problem, the best "big firewall" in technology won't help better secure the system. As we'll see in the next section, the strongest and tallest wall is worthless if an enemy can simply go around it.

"Law 4" – Kill the password

> *"The weakest link in any chain of security is not the technology itself, but the person operating it; iron gates have no compassion to appeal to, nor fears to exploit, nor insecurities to use to one's advantage. They are, however, operated by us – by beings of unlimited vulnerability and limited energy. Why waste time brute forcing what can easily be circumvented by a clever façade and a crimson tongue?"*
>
> *– A.J. Darkholme, Rise of the Morningstar*

One of the biggest obstacles any organization will face is their own staff. In studies on cyber security, nearly 84% of leaders noted employee negligence as their biggest security risk. Many were also found to believe the risk of a data breach is higher when employees work remotely. Data collated from a variety of studies indicates that almost 3 out of 4 data breaches reported by leaders stated that users were at least partly responsible for a breach of the infrastructure due to their negligence in relation to basic cyber security practices. As hackers and nation states move "downstream" to continue their attack activities, as discussed earlier in this book, this will impact small businesses more and more. Those small businesses and contractors will face a bigger challenge, as they often operate with limited budgets and restricted security tooling.

Users and their devices now represent the furthest edges of an infrastructure's security apparatus. They are the "front line" in the war that is raging in cyberspace and they are the first place that an attacker can reach into an infrastructure for an exploitation. Consider that in the chapter on this topic, we pointed out the reality of how exploitations have happened and provided specific data that shows that in nearly every instance in history, it has been a user that at some point was the activator of the exploitation life cycle. Data from those same references also shows that training and education do not "fix" users. Even a 1% click rate on an enterprise with a hundred thousand users is too large a likelihood that something will be compromised.

With the reality being that most users are reliant on their password to act as their primary means of security, the issues for user security become even more evident. Users are beholden to the paradigm of passwords and, as stated in the chapter on this topic, relying on the password is not only a management nightmare but it is also a practice that will lead to a failure at some point.

To help better secure this front line, there are a few methods and technologies that might be employed.

- **Biometrics as part of an authentication program –** While a password is nothing more than a string of numbers and letters and, in some cases, special characters, biometric data can be much more specific and useful. There are a variety of biometric authentication protocols and tools that might be applied to help eliminate the password. Some of the more innovative types are new to the market and are primarily in a research phase, but soon they might be available as part of an identity and access management tool set.
- **Brain wave-based authentication –** By using sensors to capture electroencephalograms (EEGs), or the measurement of brain waves, computers can authenticate identity. Scientists at Binghamton University in New York recruited 45 volunteers and measured how each person's brain responded to certain words. The researchers recorded each brain's reaction, which were all different. That information was then used by a computer system to identify each person with 94% accuracy. That system was then applied to a login mechanism and users were asked to log in with nothing more than a thought about a specific word. Obviously, this method is far fetched at the current time, but with the reduction in costs and the size of the sensors required ever decreasing, this approach may be viable in the near future:

Figure 4: A brain wave authentication device in use by researchers

- **Heartbeat-based authentication –** Users have a smart watch, or similar device, and the band or sensor features an ECG sensor or sensors, one on the interior of the band touching the wrist, and another on the outside of the band. A user's ECG, echocardiogram, also known as heartbeat, data is captured. That user would then activate the sensor on the band or smartwatch. After a user sets up their login profile, they then would use the band or device to verify their identity. That unique heartbeat acts as their biometric authentication mechanism to unlock certain devices while the users are wearing it:

Figure 5: The Nymi heartbeat authentication tool

- **Voice and ambient noise authentication –** Another form of biometric data is using sound to enhance security for authentication. Users can use their voice print to log into their bank accounts, make transfers, and check balances using the app, which is powered by voice-recognition technology by the company Nuance. Other sounds can also be used to help secure traditional login systems and can be combined with voice printing solutions to bolster this approach. A team of researchers at the Swiss Federal Institute of Technology in Zürich, Switzerland, revealed a tool they had created called Sound-Proof, which uses ambient noise to enhance the security of multi-factor authentication.

In this approach, access to a site that has Sound-Proof employed requires an app on the user's phone to start recording. Then the microphone on the computer also begins recording a few seconds of ambient noise in the room near the computer requesting access. The software creates a digital signature for the recording from each device and then instantly compares them. If they match, or are within very narrow tolerances, the system grants the user access to the site without them having to enter a second pin because the system assumes that the user's smartphone is in the same room:

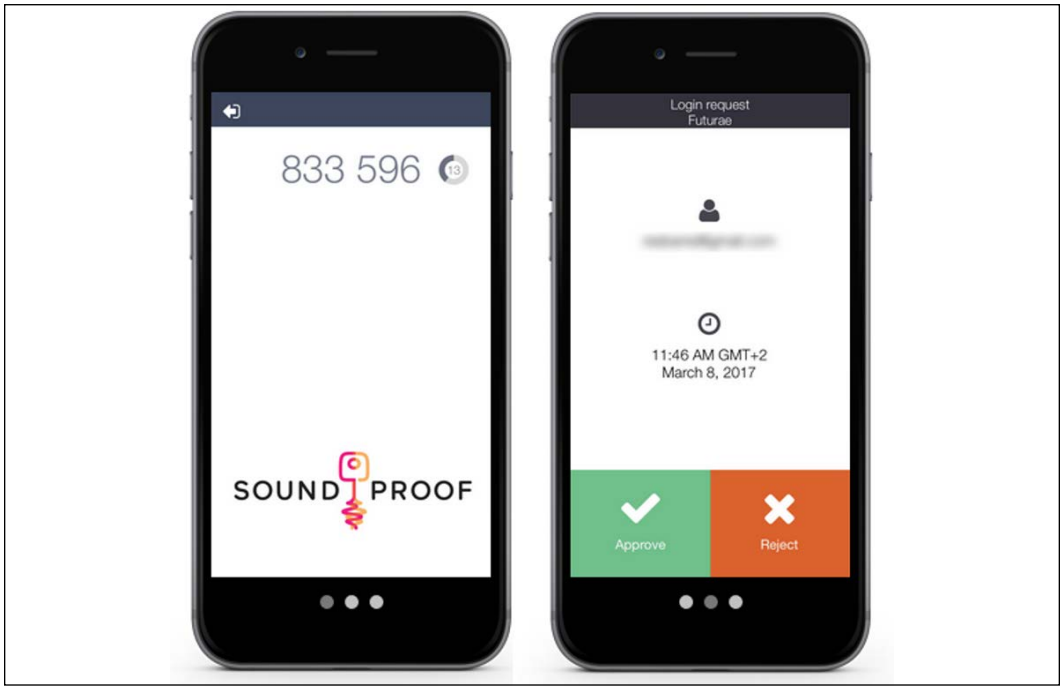

Figure 6: The ambient/voice authentication app, Sound-Proof

There are certainly ways that a well-focused and capable nation state actor or threat group could attack and possibly circumvent these approaches, but to do that would require concerted efforts and is not nearly as failure prone as simply relying on the password. The takeaway for the defenders here is to employ the simplest technologies that offer the biggest "bang for your buck."

If users are where the enemy will first operate and represent the further extension of the edge of the secure infrastructure, then logically, this is a primary point of focus. Employing technologies and tooling that eliminate the issues that a user has regarding them having to be responsible for their own security management and that eliminates the obvious issues that a password-based authentication protocol puts in place should be a key piece of any defense efforts.

"Law 5" – Limit the blast radius

If we accept the points – facts really – that have been presented throughout this book that speak to the reality of cyber warfare, then it is pivotal that we also adopt a position that states that at some time, we will get "hit." Transiting a warfare environment is an inherently dangerous proposition. At any time, a random chunk of metal can come flying across the space and forever impact your survival in that space. When everything we do, all of the time, is situated on that battlefield and is constantly transiting that environment, the chances of that negative outcome increase by the second. The digital space is fraught with danger, and it is the only space that humanity has ever seen that in some way touches everything, and where every power that exists can actively engage one another on a relatively level playing field. To be blunt, in war you can expect things to inevitably hit the fan.

It is not the actual attack, infection, or exploit that is what is so negatively impactful in this battle space. In reality, if those infections and exploits were contained and limited in their ability to propagate, they would be not much more than an inconvenience for the IT teams to reimage and "fix" the exploited machines. It is when that nuisance infection becomes a global pandemic that things go from bad to worse. That is when a digital flesh wound becomes a binary arterial bleed. It is that metamorphosis that must be stopped at all costs. The blast radius of the exploit must be contained in order to have a hope of survivability.

If there was an "explosion" in the infrastructure, how far would that damage go before it could be stopped? How much "blood" would be spilled before the gushing could be assuaged? A secure infrastructure that is correctly segmented should be able to limit that explosion, and it should be strong enough to do so without harming that infrastructure's ability to function. To reach this position of being "armored up," as tank operators in the Army say, there are a few principles that should be part of the infrastructure and strategy:

- **The hackers are already here –** The enemy is already inside the gates. The perimeter model of security has fundamentally and epically failed to secure infrastructure and has allowed nation states and hackers to gain access to infrastructure across the globe for decades. Assuming this position and recognizing that the enemy is already inside is a key strategic point that can help leaders and technicians better address infrastructure security. Just as in physical warfare, the approach to addressing the issue must be based on the truth of the space, and the truth of this space is that everything is probably already compromised and keeping the enemy beyond the wire is an exercise in futility.
- **Eliminate keys to the kingdom –** Nation states and hackers attack the traditional administrators because of the power of that role for an organization. They do this to get those valuable "keys to the kingdom." One administrator login or account is worth 1,000 users who have no real authority across infrastructure components. That elevated set of permissions allows an administrator to do almost anything. Those accounts and those users must be defended and their access closely monitored and tracked at all costs. One compromised admin is akin to a potential tactical nuclear warhead detonating inside a network. The best approach here is to limit and control administrator accounts and accesses as if they were radioactive material. Nothing short of total caution and care should be afforded those volatile assets.

- **Segmentation at a grand scale –** If an intrusion occurs, the exploitation or compromising of one component must not result in the entire system getting taken over. Multiple layers of defense should be applied to "up-armor" the infrastructure from the inside out to eliminate movement; controls regarding role-based access control applied at multiple levels, strict limits on account privileges, monitoring, granular asset segmentation on servers and hosts, and anti-malware and updated patches for all assets. Whitelisted software is the only software that should be allowed to execute, and native tools like PowerShell should be strictly controlled or limited.
- **Use hardened assets –** To date, hardening systems have generically relied on the **Security Technical Implementation Guide** (**STIG**), which dictates what should be done to harden an asset and reduce vulnerabilities. The US DoD has released 461 STIGs and continues to release more on a semi-regular basis. STIGs are published and are available for a variety of software packages, including operating systems, database applications, open source software, network devices, wireless devices, virtual software, and mobile operating systems. Using these tried-and-tested guides from an organization such as the DoD that has been fighting the good fight in cyber warfare longer than any other organization can help to secure infrastructure quicker and with a more formulaic approach. A full listing of STIG-suggested configurations can be found at `https://stigviewer.com/`.

A sample of STIG hardening for a Windows 10 machine is presented. Note that for conciseness the information is not presented in full; if you'd like to see the full details, you're encouraged to check out the stigviewer website previously cited. The sample follows:

Finding ID	Severity	Title	Description
V-63797	**High**	The system must be configured to prevent the storage of the LAN Manager hash of passwords.	The LAN Manager hash uses a weak encryption algorithm and there are several tools available that use this hash to retrieve account passwords. This setting controls whether or not a LAN Manager ...
V-63651	**High**	Solicited remote assistance must not be allowed.	Remote assistance allows another user to view or take control of the local session of a user. Solicited assistance is help that is specifically requested by the local user. This may allow ...
V-63869	**High**	The Debug programs user right must only be assigned to the Administrators group.	Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the "Debug Programs" user right can attach a debugger to any process or ...
V-63325	**High**	The Windows Installer Always install with elevated privileges, must be disabled.	Standard user accounts must not be granted elevated privileges. Enabling Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain ...

V-63353	**High**	Local volumes must be formatted using NTFS.	The ability to set access permissions and auditing is critical to maintaining the security and proper access controls of a system. To support this, volumes must be formatted using the NTFS file ...
V-63667	**High**	Autoplay must be turned off for non-volume devices.	Allowing autoplay to execute may introduce malicious code to a system. Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs or ...

While there are always other techniques, strategies, or tactics that can be part of your "laws" for surviving in combat space, the preceding basic laws are meant to help provide a basic few points to always think on. As with anything in survival situations, it will always be the simple things that matter most first. If you ignore the basics, surely the advanced issues will be even more problematic.

Impact from failure

Apart from causing substantial economic loss to businesses and monetary systems, cyber warfare can harm critical national infrastructure in a variety of ways. In one way, cyber warfare can affect the delivery of essential services to the populace. This has been shown with cyber attacks against electrical grids and the healthcare sector over the past decade. Second, there is the potential to cause physical damage. This was demonstrated by the Stuxnet attack against Iran a decade ago. Cyber warfare tactics may affect the delivery of healthcare as well.

Compromising healthcare

As healthcare sectors continue to move toward increased digitization and interconnectivity, the likelihood of this type of action becomes more real on an almost daily basis. New medical devices are now almost categorically connected to a hospital's information technology system to enable automatic actions and help with healthcare insurance filing, and to enhance patient care. That increased digital dependency, combined with the ever expanding "attack surface," has not corresponded with vast improvement in more secure infrastructure, or better cyber security practices. That infrastructure is particularly vulnerable and has potentially life and death consequences for patients and those who are connected to those devices.

The WannaCry ransomware attacks in 2017 affected a hospital in Hollywood, California, as well as a hospital in Singapore, and another large hospital in the UK. The resulting post-attack investigation into the Singapore attack revealed that the exploit on that hospital's network was in place for more than 10 months. Using their specialized malicious software, attackers were able to query databases for specific patients, including the prime minister. Over time, there was also the potential for attackers to tamper with prescriptions and shut off connected systems. In the cases of the WannaCry Hollywood and UK hospitals, the attacks stopped the medical facilities from operating normally by stopping uptime and impacting data availability.

Patients were literally turned away and denied care because of these exploits. As more digital dependencies are ingrained into healthcare and hospital systems, the more difficult it will become for those critical facilities to operate when those dependencies stop functioning. Other healthcare facilities may soon be under attack as well. Pharmaceutical companies may be targeted for intellectual property theft or may be infiltrated and have their formulas or cures tampered with or possibly rendered unreadable. While it is possible that those operations may not always be destructive in nature, they might still cause damage beyond property theft.

If medication supply lines or vaccines are impacted, the entire medical industry, and the faith that consumers have in those providers, might be called into question. The potential also exists for attacks on research facilities that store dangerous materials, like viruses or diseases.

Bringing down ICS (Industrial Control Systems)

Cyber attacks against industrial control systems have typically been less frequent than other types of cyber operations. However, the frequency of those actions is reportedly increasing, and the severity of the potential impact in this sector is plainly evident. A few days without light and power, and the civilized world will tumble into the dark ages; chaos will follow. Because of the growth of connected capabilities and the potential benefit for humanity with internet-enabled ICS systems, this area is particularly ripe for an attack. Because of the interconnected nature of infrastructure, and the increasingly refined capability of nation state actors and their weapons' capabilities, it is extremely possible that there are already several undetected actors present in ICS systems across the globe.

Nation state threat groups will work to cause large-scale harm to industrial control systems via firmware and supply chain vectors. It is also possible that malware used on industrial control systems could cause unintended collateral damage to other unprotected industrial control systems. There is also the risk that nation states have already installed self-propagating malware that is lying in wait for the command to "go loud" and exploit the system. When considering the impact that an ICS or SCADA system exploit might have, it is important to focus on the reality that even a small-scale attack could have cascading consequences on such systems.

Threatening the fates of nations

When it comes to the added issues of **artificial intelligence** (**AI**), cyber warfare, and the impacts those issues might have on national security, there are more uncertainties than answers. One of the primary issues that should be part of that line of questions is how does cyber warfare, AI, and cyber security affect nuclear security and even the fabric of democracy?

AI-augmented cyber capabilities are already in play. There are potential military risks associated with emerging technologies and especially inadvertent or accidental escalation within those circles. Consider the increasing potential vulnerabilities thanks to the interconnected nature of global networks and the focused nation state efforts to impact nuclear systems.

AI has the very real potential to make existing cyber warfare weapons exponentially more powerful. Faster advances in AI technologies and increasing capabilities in autonomous systems could amplify future attacks. To avoid hype and provide clarity to the understanding that is needed, here are a few specific, but possible, ways that AI and cyber warfare might combine in these areas.

Advances in autonomous systems and machine learning means that more networked and physical systems are vulnerable to cyber warfare. As nation states and their associated threat actor groups leverage more AI, capable systems and tools can offer attackers access to cyber attacks to be executed on an infinitely grander scale. The speeds at which those attacks will proliferate also will accelerate across disparate civilian and military domains. The speed and breadth of the next generation of AI cyber tools could have destabilizing effects on entire countries.

Outside of simply attacking via cyber weaponry, a nation state or threat actor could also use AI or machine learning techniques to target the systems that backend common data-specific applications. Those attacks could work to spoof critical data points or inject incorrect data at scale into those critical systems. An attack like that could cause unpredictable and undetectable errors, system malfunctions, or behavioral manipulation to a system's controls. Those civilian systems that use AI or machine learning as part of their decision engine rely on high-quality data to enable their algorithms to function properly. By attacking those backend data repositories and injecting bogus data into those datasets, those unsecured systems would continue to operate "normally" but would, in reality, be making decisions based on faulty data, which could be cataclysmic for systems such as nuclear control actions or hospital patient tooling.

Were that to happen in a nuclear system, or a nuclear-related weapons system, the perceived ability of the state to defend itself from a physical attack could be compromised. Additionally, the faith in the system and the reliance by other nations that those systems are safe to operate would be called into question. The entire nuclear gambit could be called into question with an invalid data action.

The previous section focused on what the larger issues are regarding cyber warfare and ICS, healthcare, and other critical systems. In the following section, we will detail a few potential attack scenarios to try and provide some clarity on what is more realistic in future cyber warfare engagements.

Threat scenario – DeepFakes

Nation state 1 uses outside agents and hackers to send DeepFake video or audio to nation state 2's rival leadership. Those videos indicate that senior military commanders of state 3 are conspiring to attack nation state 2. In short order, those DeepFakes are leaked onto the internet with specific Twitter and Instagram influencers targeted for reposting. This causes civilian panic in the area and escalation of defensive positioning.

Nation state 2 reacts to the perceived threat with actual physical or kinetic actions, which lead to war. AI and ML tooling could be injected into this scenario to either escalate the tensions or to speed the delivery of social media, which would fuel discourse.

Threat scenario – Data manipulation

Nation state 1 uses an ML-based cyber attack to spoof data for nation state 2's civilian air control and tracking system. The fake data injected causes air traffic control to interpret a valid track as a potential threat. Military action is taken to prevent casualties and the valid track (airplane or jetliner) is kinetically eliminated. The security and veracity of the systems and the components that power it is called into question. An entire industry is impacted, and the global economic impact is felt. Civil unrest and discord are also likely to follow as the population reacts to the outcomes of the attacks. Social unrest is potentially widespread.

Threat scenario – Attacking democratic processes

Thanks to the poor state of security of voter registration databases and local, state, and national election systems, and the increased circulation of voter information available in the underground community, nation state 1 attacks the voting process. By using voter registration records, nation state 1 builds out a targeted, localized disinformation campaign. In that campaign, vectored tweets and postings are put online that show elected officials touting inflammatory campaign slogans. At the same time, a campaign is launched with narratives that indicate that voting systems have been compromised and all votes will be calculated for opposition parties regardless of the voters' input.

Those are simply a few examples of what might be possible if these sorts of actions are taken in cyber warfare engagements. While it should be noted in this regard that in no instance did the attacking nation engage in what would be considered a kinetic cyber attack, the results would still be felt by the target nation. By using "softer" tactics powered by targeted cyber activities and coordinated by malicious command and control entities, the attackers can still impact the adversary.

The nature of warfare and the realities surrounding cyber impacts are ever changing and will be a difficult beast to manage if ever unleashed in a coordinated manner.

Conclusion

Providing true cyber warfare survivability requires a fully committed leadership, technical team, and partner alignment. Surviving these types of conflicts is a technically, politically, financially, and procedurally complex issue. In combat, the ability to move and maneuver and the adoption of basic concepts and solid practices is what will help an entity survive. Survival is the goal; anything better than that is simply icing on the cake. Those that survive the longest win.

The goal of cyber defense is to minimize the magnitude of the attacker's effect, increase costs to the attacker, increase the uncertainty that the attack was successful, and increase the chance of detection and remediation. Survivability is the ability of a system, subsystem, equipment, process, or procedure to function continually during and after a disturbance. This must be the focus of our attention as the digital battlespace continues to be transited. As long as the critical functions of the entity can continue, and the entirety of the infrastructure is not rendered useless, the ability to "fight through it" remains.

The aim of this book was to try and provide some real insight into the true history of what cyber warfare looked like in the past and what it will resemble in the future. In doing that, and providing a real-world look into the strategies, tactics, and tools that are active in this space, the author hopes that you have found some nuggets of knowledge that can be used to better defend your organization.

If any one thing should be taken away from this book, it should be that the battlespace in cyber warfare is ever changing, and those that stagnate and focus on what is the current threat are missing the coming onslaught. In digital combat, everything can be a weapon, and everything can be a shield. It all depends on how that item is used and how skillfully the strategy for the use of that shield or spear is applied by those who wield them.