The twelve principles of cybersecurity warfare

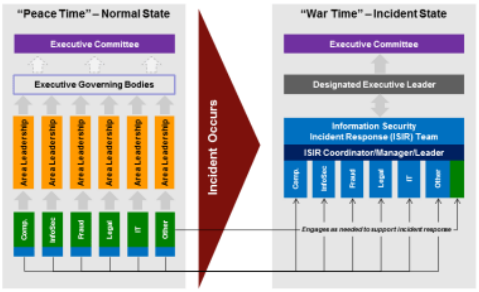
The following is a collaborative article with Brian Kelly.

Introduction by Brian Kelly

Several years ago, Justin and I had a conversation regarding the influence of information technology on modern warfare and tried to draw parallels to the challenges we face today on the battlefield of cyber warfare. We acknowledged that military history has taught us the value of embracing new technology. Just as gunpowder and mechanization rendered familiar forms of warfare obsolete, today's dramatic improvements in the ability to "sense" the battlefield from almost any point pressured military strategists to reevaluate basic concepts and practices of employing military force. While technology is often the "engine of change" it is only one of the constituent elements. Achieving transformational change in the way we do things – such as engage in war or fight cyber criminals – requires complementary changes in organization structures, operational strategy and culture.

What can we learn from military history that we can apply to cyber warfare? The constant flow of new "security tools" provides the illusion that technology will ultimately solve all our problems. The same

problem plagued military commanders who introduced new technology into military operations yet failed to achieve a strategic return on their technology dollars. The reality is that while technology is intended to increase efficiency and effectiveness of decision-making, it can actually cause confusion and consume more resources than it returns. That's a dangerous proposition for functions like cybersecurity where fast and effective decision-making can mean the difference between a major catastrophe and a minor inconvenience. The best hope for exploiting the potential of emerging technology solutions lies in understanding the fundamental principles that cut through the confusion that often exists on the business battlefield.



Justin and I have worked on building information security organizations and programs for large global clients in the past. Information security departments are unique in that they are perhaps some of the most combat-ready battalions in a company. Building effective incident management programs, for instance, we've long described as a "war time/peace time" model of the military to maintain a shifting state of command and control.

During times of peace, the General assumes command of the day-to-day operations of the military with the mission of organizing, training and equipping our forces. But during times of war and conflict, command and control shifts to the Joint Chiefs of Staff and designated war fighting commanders. Information security is not that dissimilar. During times of peace(1), a CISO/CSO will preside over the department running the day-to-day responsibilities and projects. Yet, during an attack (e.g. breach, hack, incident, etc.), your incident response leader takes control and leads the team through the steps necessary to counter the attack or respond to the incident. Effective command and control during these times of crisis is critical. Decision-making, not information flow, is at the core of the command and control process.

So, if information security by its very nature, is analogous to "going to war" then are there lessons we can

learn from the military to make this war an easier-fought battle? Are there tried and true principles that guide us in winning the war on cybersecurity? Brian's military training turned our attention to the **US Army's Field Manual 3-0 (FM 3-0)** which outlines the nine principles of warfare. These nine principles are also supplemented by an additional three principles in **Joint Publication (JP 3-0)** which discusses the guidance for joint operations (between military branches and multinational military engagements).

FM 3-0 describes itself as "the Army's capstone operations manual. Its lineage goes back to the first doctrine written for the new American Army, Baron von Steuben's 1779 Regulations for the Order and Discipline of the Troops of the United States." The guide has stood the test of time and has been updated and adapted to suit the changing conditions of modern warfare.

Surely we can find some good principles here!

The manual goes on to explain that "its contents are not truly capstone doctrine until Army forces internalize it. This requires education and individual study by all Army leaders. And it requires more: Army leaders must examine and debate the doctrine, measuring it against their experience and strategic, operational, and tactical realities. They must also recognize that while FM 3-0 can inform them of how to think about operations, it cannot provide a recipe for what to do on the battlefield."

We loved this. The lessons in the manual must be internalized, practiced and adapted to the terrain of the battle. So, we set out to do just that: adapt the [combined FM 3-0 and JP 3-0] principles of warfare to the terrain of cyber security and information security organizations to see what we could learn from the tested and proven methods for winning military battles. From the hand-to-hand combat of new advanced threat actors to the politics of fighting for precious budget; how can we learn from these military principles to run an efficient and effective organization? And just as the military warns that these ideals are not to be used as a "recipe," we believe these principles provide guideposts that anyone can follow to improve the way information security organizations are run.

1. Objective

> *Direct every military operation toward a clearly defined, decisive, and attainable objective.*

Call it a mission statement, call it a charter, call it strategic statement of intent…whatever you call it, a well run organization must define its objective. "What are its goals?" and "what is it trying to achieve?" Some security departments just focus on monitoring network activity. Some only focus on provisioning identities and managing access. Others expand their scope and manage the holistic physical and logical security of the organization. Some organizations have not yet defined what types of information they care about, what assets they protect and how they will protect them. That is a dangerous place to be. Imagine being dropped into the middle of a battle, rifle in hand, surrounded by the swirling chaos of the battle and turning to your fellow soldier and asking "now, which way do we run?" You likely wouldn't last very long. Operating an information security department without a defined objective is near suicide.

One suggestion we have found effective is to remove the word "prevent" from your cybersecurity framework. The threat surface of any organization is large and complex. Believing we can prevent a cyber attack sets a false expectation (for the board, your customers and the organization). Rather, we should be focused on deterring attacks – making it as difficult as possible for an adversary. This means then that our priority must shift to being the absolute best we can be in detecting and responding to attacks. Bad things happen to the best of companies. Expect it…and be ready for it.

2. Offensive

> *Seize, retain, and exploit the initiative. The purpose of specifying the objective is to direct every military operation toward a clearly defined, decisive, and achievable goal.*

Once the mission is defined, it's time to execute on it. This often involves building new capabilities, implementing advanced technologies and assembling processes to support the objective. These initiatives will not launch themselves and it takes a true leader to proactively obtain the necessary

resources and direct those resources. How many people do you know who are excellent strategists and visionaries but fall down when it comes to execution? Plenty. The principle of “offensive” tells us we must be proactive and pursue our mission and exploit every opportunity for success.

Just as combat is not a scripted process, decisions in cyber warfare will be made under conditions of stress, fatigue and confusion and in response to seemingly random events. Given enough time, most uncertainty could theoretically be eliminated; but battle rarely affords commanders the luxury of time to do so. Instead, we must reduce uncertainty to an acceptable level and in a time appropriate to the situation. History demonstrates seizing the initiative, despite some degree of uncertainty, usually provided a military advantage that outweighs the option of waiting until perfect information is available. Choose wisely and don’t pursue perfection. You’ll never achieve it.

3. Mass

> *Concentrate the effects of combat power at the decisive place and time. The purpose of mass is to concentrate the effects of combat power at the most advantageous place and time to produce decisive results.*

You can’t win every battle; it’s just not possible. But the wise leader knows when to apply political and organizational clout to get things done. If you try to fight every battle with 100% of your army, you will not only burn out your troops, your commanders will not take you seriously when you really need their support. A big part of this principle is the ability to read the terrain and understand when, where and how to strike.

While it may be counterintuitive, don’t be trapped into focusing on reinforcing an unimportant weak line. Often, the better strategy is to reinforce strength. All too often we get caught up in security trying to do too much. Define a strong service catalog, build your capabilities, execute on those with focus and determination. For example, if the organization is strong at detecting attacks, build on this strength to

become world-class. If managing audit and compliance detracts from this mission, it may be time to find another battalion commander to run that division so you can focus your mass on the mission at hand.

4. Economy of Force

> *Allocate minimum essential combat power to secondary efforts. The purpose of economy of force is to expend minimum essential combat power on secondary efforts in order to allocate the maximum possible combat power on primary efforts.*

Like all organizations, we only have so many resources we can expend. Those resources may be money, people, technology, time, etc. but whatever the precious commodity we have, we must focus our efforts on the most important things. It's always amazing to see organizations who cannot articulate what is "important" to them. For example:

- What risks must we manage?
- What assets must we protect?
- Where are we exposed?
- Who poses the biggest threat?
- What tactics, techniques and practices must we defend against?

Answering these questions paints a composite picture of risk. Not as an academic exercise but as a means of prioritizing the limited resources that we have to address these risks. Why would we focus all our efforts protecting low value technology assets? It just doesn't make sense. Target your security strategy on the most important things and reserve secondary efforts for when the primary objectives have been achieved. Be specific about where to spend your resources. Discussing "threat actors" is always interesting however we often cannot derive enough specific intelligence to produce practical and actionable solutions. Discussing an adversary's tactics on the other hand will likely provide insight in to necessary countermeasures to defend against such an attack.

5. Maneuver

> *Place the enemy in a disadvantageous position through the flexible application of combat power. The purpose of maneuver is to place the enemy in a position of disadvantage through the flexible application of combat power.*

Things change. That's what they do. All. The. Time. Your strategy must remain flexible and adapt to the changing situation. In the theater of information security warfare, hackers are like terrorists; they are not bound by organizational rules and operational doctrine. They attack for maximum impact and they move quickly and nimbly. Your ability to remain flexible and shift strategies may mean the difference between headline news and preventing a breach. Maneuverability can be a difficult concept for non-IT people to comprehend. In business, when you buy an asset, it generally lasts for a period of time. In security, it's a constant battle and ever-escalating arms war to out-maneuver your attacker. However, you have an advantage: like the revolutionary rebels in the US war for independence, you know your terrain. Use the knowledge of your environment to your benefit. You know your assets (targets), you know your weapons (security tools/controls), you know your geography (your network and architecture), right? The reality is: some do and some don't. To stay nimble and maneuverable, you must have a good understanding of your environment, create a culture that enables change and leverage both to your advantage.

6. Unity of Command

> *For every objective, ensure unity of effort under one responsible commander. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective.*

How many times have you received conflicting direction from multiple bosses? There's nothing more frustrating than hearing differing answers to a simple question. Do I go left or right? Do I charge ahead or retreat? Do I shoot or stand down? In business, this duality can generate frustration, or at its worst, attrition of your people. On the battlefield, it could mean the difference between life and death. A single voice of command ensures alignment to one vision.

In information security, nothing is more dangerous than the live-fire exercise of an active security incident. It's a strange organizational dynamic, but often when an incident is declared, people come out of the woodwork to get involved. Lawyers, auditors, compliance officers, architects…and nothing can be worse than senior executives trying to wrestle control or influence activity from an attack in progress. It is during an incident that command and control must be clear, understood, disciplined and followed. Yet, not every incident requires the same command and control structure. Careful planning should determine the level of command required in advance and then followed with military precision. The traditional focus on rigid technology, structure and mechanics of command, while important, tends to confound decision-making and may be of marginal value in today's fast moving cyber events. Today's view of command should acknowledge the dynamic and stochastic nature of cyber warfare and focus on function, understanding and decision-making. Our command and control systems must:

- Support human decision-making.
- Reduce uncertainty while acknowledging that uncertainty cannot be eliminated.
- Decrease the complexity of coordinating, integrating and applying resources.
- Possess flexibility to respond to real-world dynamics.

7. Security

> *The purpose of security is to prevent the enemy from acquiring unexpected advantage.*

How do you prepare for the unexpected? Train your people how to think independently and make informed decisions based on objective criteria and facts. Military practitioners are familiar with the "O-O-D-A Loop" – Observe, Orient, Decide and Act (**click here** for more information). This model provides a method for making informed decisions and acting based on feedback from various sources. In business, we get feedback all the time: assessments, studies, investigations, reports, etc. But many of the recommendations from that feedback fall on deaf ears and the issues are never acted upon. Inevitably this results in worsening problems and ultimately provides attackers with an advantage. The question is:

is this advantage unexpected? No. The fact is: to prevent your enemies from gaining the upper hand, decisive action – based on multiple sources of feedback – is required. In combat, failure to act can compromise the security of the mission. In security, the mission is to take action so you are not compromised.

8. Surprise

> *The purpose of surprise is to strike at a time or place or in a manner for which the enemy is unprepared.*

It's easy to understand that, in the theater of battle, the element of surprise can work in a combatant's favor. If you can surprise your enemy with a surprise show of force, you can often disable front-line defenses and weaken key points in the enemy's line. Business calls this "first mover advantage" and it's no doubt that first to market has a distinct advantage in capturing the market over the subsequent entrants.

In security, the element of surprise takes on a couple dimensions. The first dimension is preventing the enemy from surprising you. If the enemy cannot see your detection mechanisms, then they are unable to deny or disable them. Layer your defenses, but above all, protect your core defenses. You may find the adversary disables an intrusion detection system (IDS) sensor or an anti-virus (AV) program, but fails to understand additional detection techniques are in play on your network. The second dimension is surprising your enemy. You may direct the adversary to a field of battle that provides your team with the "high ground" such as funneling the attacker to a shadow network for which we can gain greater insight into the tactics, techniques and practices. Nothing is more educational than watching your attacker's behaviors under a controlled microscope. How's that for a surprise?

9. Simplicity

> *The purpose of simplicity is to increase the probability that plans and operations will be executed as*

intended by preparing clear, uncomplicated plans and concise orders.

Complexity can be the enemy of security! Especially when it comes to the mountains of data we typically generate in a technology organization. If we have to process thousands of logs and hundreds of events per hour provided by multiple systems and technologies it is very likely we will battle a self-induced “fog of war.” We are living in the age of “big data analytics” and while many resources are available to us, at what point are we introducing data for the sake of data? Data is important but only if it is accurate, timely, and relevant to some decision a commander will make. Data does not equate to knowledge, communication flow does not guarantee effective decision-making, and hierarchy cannot guarantee efficient and effective coordination. Do we have the right data to reduce uncertainty and support the important decisions that must be made in a timely manner or are we overloading decision makers and increasing uncertainty? The key is to define – simply and clearly – the information we care about; the information that will prompt attention and action. While our security analysts continue to innovate and watch for trends outside of the known signatures and heuristics, it is important that we do not drown our operational personnel in data causing paralysis.

10. Perseverance

The purpose of perseverance is to ensure the commitment necessary to attain the national strategic end state. (2)

Our mission is not to just detect and defeat the impending attack, but to break the will of the enemy. At some point, an attacker is going to give up the fight and move off to a less prepared target. If each tactic is thwarted, every campaign shut down and all advances pushed back, at some point the enemy will tire… and retire. Sure the true Advanced Persistent Threat (APT) actors have demonstrated patience and staying power, yet at some point, their investment in resources will devalue. That’s why it is important to see each campaign to its final conclusion. Do not retreat early. Be certain the field commanders (aka executive management) understand that we are in this for the long haul.

11. Legitimacy

The purpose of legitimacy is to maintain legal and moral authority in the conduct of operations. (2)

Military legalities can often be blurry. What is a legitimate military action? When the US president approves? When foreign prime ministers approve? That's why we have guidelines to justify our acts of war and rules of engagement. Similarly, the security profession is bound by a code of ethics and conduct that outline the "dos" and "don'ts." Yet sometimes the line blurs when fighting attackers representing hostile nation-state actors. It is important to uphold and adhere to the legal obligations by which we are bound. The line between white hat and black hat hackers is separated by an ocean of moral fiber, which can be tested and tempted with the promise of bitcoins and fame. While many investigations are never exposed outside the confines of the corporation's area of responsibility, no one of us could ever know completely how the investigation will evolve. This means we must do everything possible to preserve forensics evidence – from the first indication of the "event" through to the completion of the investigation.

12. Restraint

Limit collateral damage and prevent the unnecessary use of force. (2)

It may be that the best course of action is to disengage. I can choose to fight the attacker on their terms, or fight them on ours. If we can isolate the domain controller or shut down the server, that may be our best course of action. That is, it may be worth allowing the adversary to make his first move or two to understand their tactics and techniques. What tool sets do they apply? What seems to be their objective? Is it possible that they leave indicators that will help in assigning attribution? Using some restraint in countering attacks takes patience, maturity and experience. Sometimes it's not about sending that kill pill to the attacker; it's about gathering intelligence and making your move at the right time.

Conclusion

The twelve principles of warfare reveal many parallels that can be applied to a variety of professions. There is much we can learn from studying the techniques that have served the military effectively for hundreds of years, especially when battling an enemy with nearly unlimited resources and whose weaponry is only limited by the creativity, imagination and innovation of a global network of ever-growing hackers. It is our belief that the application of these principles will serve you well in your ever-escalating arms war to protect your most valuable information assets.

Footnotes

1. Now, arguably, unlike the military, information security departments these days are always under attack and in a state of combat. But for the purposes of this article, let's assume that attacks within normal operating limits are "peace time" and major incidents are considered "war time."
2. Additional principle from Joint Publication 3-0 (JP 3-0).

justin greis

hi, i'm justin

(nice to meet you)

I post weekly **professional insights** and **personal stories** from my life as a management consultant, a dad, and an eternal optimist.

Click here to learn more about my **professional**, **personal**, and **"perfessional"** background.

connect with me

- **Visit JustinGreis.com**
- **Learn more about Justin**
- **Subscribe to newsletter**
- **Contact Justin**