Winning Cyber Conflict

Military frameworks to understand, assess, and defend against cyber threats

Cyberspace is a domain of conflict akin to land, air, or sea. Cyber security needs to adapt to become cyber defense – replacing the fragmented lock-and-key, compliance-based approach with a holistic and analytical paradigm designed to win conflicts. Principles from military analysis can be modified and applied to the cyber environment to map out companies' cyber landscapes and help decision makers better understand cyber threats. DAMROD is a mnemonic in military operations used to assess the strength of a defensive position, and can be effectively applied to cyber. Damrod Analysis provides an integrative framework that helps organizations understand, assess, and defend against cyber-attack. The emphasis on human analysis over technology provides for efficiency gains and improved returns on investments without new spending.

MILITARY FRAMEWORKS TO UNDERSTAND, ASSESS, AND DEFEND AGAINST CYBER THREATS

CONTENTS

ABOUT DAMROD

Damrod Analysis is founded on the idea that cyber security must transition to cyber defense. The threats and risks of the modern world are ill-served by a philosophy that puts minimal compliance above independent analysis. Too often a regulatory checklist defines the cyber security of an organization. Damrod Analysis treats cyber as conflict, and provides the tools to win.

EXECUTIVE SUMMARY

There is an ongoing fight in cyberspace that extends from the server room to the darknet. Attackers can be professionals sponsored by nation states, or amateurs running open source scripts. Protecting against these attackers is a confused and disjointed process, with dozens of technologies and hundreds of vendors vying for attention.

Damrod Analysis provides tools and frameworks to understand cyber conflict, assess threats, and defend against them. It provides CISOs and their teams with a single model that interlocks system management, threat integration, and the myriad of cyber security products available today into a coherent defensive strategy.

To illustrate a company's cyber landscape, Damrod Analysis begins with a ***Cyber Geographic Framework***, on which conflicts can be mapped. It then draws on battle-tested military principles to develop a company's unique ***Cyber Terrain Analysis***. Next, it conducts a process of ***Threat Integration***, a visualization of threat intelligence that identifies the most likely and most dangerous paths attackers use to achieve their aims. Finally, it adds a ***Defense Overlay***, which plots a series of defensive techniques and technologies that block attackers from advancing. Together, these create the ***Cyber Strategic Framework***.

After mapping a company's existing ***Cyber Strategic Framework***, Damrod Analysis assesses the strength of its cyber defenses by using the mnemonic **DAMROD** –

- **Depth -** Layer defenses to delay attackers
- **All Around Defense -** Answer attacks from any angle
- **Mutual Support** – Explicitly interconnect defenses
- **Reserves** – Keep uncommitted resources to respond to the unexpected
- **Offensive Spirit** – Answer the question "How do I win?"
- **Deception** – Confuse and frustrate attackers with fake weakness

Damrod's six-step investigation helps cyber security teams review existing defenses and develop new plans to meet ever-changing threats, all without significant expenditure.

In sum, Damrod provides a single framework that helps the Board and other senior managers 'get' cyber conflict. With clear visualizations grounded in army tactics, Damrod Analysis's ***Cyber Strategic Framework*** brings it all together to demonstrate what needs defending, against what, and with what resources.

MOST COMPANIES SPEND ENOUGH MONEY ON CYBER SECURITY; DAMROD HELPS THEM SPEND IT BETTER.

CONFLICT IN CYBERSPACE

Conflict is a contest of wills and a competition over resources. It is a fight between humans that encompasses a mix of chance, risk, and policy. Land, air, and sea conflicts provide compelling drama and suggest violent contests between factions. Cyberspace, by its abstracted, non-corporeal nature, represents a distinct environment where the human contest is played out across countless miles, routed through proxy systems and accounts.

Cyberspace is heating up, driven by increasing technological prowess and global instability. Operating in the cyber environment fosters asymmetry, providing the disenfranchised with significant reach and impact against mightier opponents. Technological superiority is less relevant when attackers can leverage a host of neutral machines to scale their attacks, or even use the defenders' size as an enabler for the attacks.

The British Army characterizes the future of conflict as congested, cluttered, contested, connected, and constrained. These characteristics may feel familiar to IT professionals. Networks are *congested* by ever expanding data needs, *cluttered* by legacy systems, *contested* by competitors and opponents, *connected* by a growing number of devices, and *constrained* by mounting government legislation.

In its current form, "cyber security" uses the imagery of locks and keys, of taking steps to protect private homes from opportunistic thieves. The stereotypical image of a hacker is a teenager in a hoody hunched over a laptop. This imagery is misleading and downplays the significance of the threat and the impact of failure. The attackers are not always amateurs. There are professionals who seek advantage – financial, strategic, or ideological. Those responsible for protecting society in the digital age need to treat cyber as a conflict between professionals.

PwC reports that the average UK organization budgeted £6.2 million for information security in 2016, up from £3 million in 2015.[1] This begs the question – are buyers getting return on their cyber security investments? Damrod Analysis argues that to maximize the value of their investments, companies must change their mindset: a transition from security to defense.

Damrod provides the tools and frameworks to win cyber conflict.

[1] PwC "UK organizations double cyber security spend but breaches continue" Oct 2016

DEFENSIVE OPERATIONS

The primary purpose of a defensive operation is to deter a threat. Its end goal is to defeat an opponent. Because the full defeat of an adversary is beyond the scope or reach of private business, Damrod Analysis focuses on threat deterrence, but the underlying thought of defense as an enabler for offense is one to which we will return.

To manage threats successfully, it is important to understand the relevant landscape, threats, and defensive tools in play. Once these are mapped out, we can assess the strength of existing defenses and propose strategic and tactical improvements.

CREATING THE CYBER STRATEGIC FRAMEWORK

In this section, Damrod Analysis maps out a company's cyber landscape with a series of easily understandable overlays.

Cyber Geographic Framework

Were IT professionals to step into an Army field headquarters, they may be struck by the concurrent use of analogue and digital tools. Dominating the HQ is a large map providing a bird's eye view of the battlespace. Atop this map are a series of overlays, each the outcome of analysis conducted by the headquarters staff.

While the analysis that goes onto these overlays often has digital origins, the synthesis occurs physically.

Knowledge of the terrain provides a decisive advantage in anticipating where and when a contest will occur. Three key takeaways from a military terrain analysis are:

- **the avenues of approach**
- **the key terrain**
- **the vital ground**

Avenues of approach are potential lines of attack. Key terrain is ground that will make the mission easier, or the opponent's mission harder. Vital ground is terrain that, if lost, results in mission failure.

From a cyber perspective, although movement is fluid through cyberspace, there are clear avenues of approach – paths along which 'movement' occurs. Key cyber terrain consists of networks and applications. Databases or other important pieces of the IT infrastructure are vital ground.

Conceptually treating the cyber environment as terrain aids in the assessment of what is important. To draw further deductions from the cyber terrain, we use a framework to organize observations and deductions.

The Army's 'Geographic Framework' divides a battlespace into three regions:

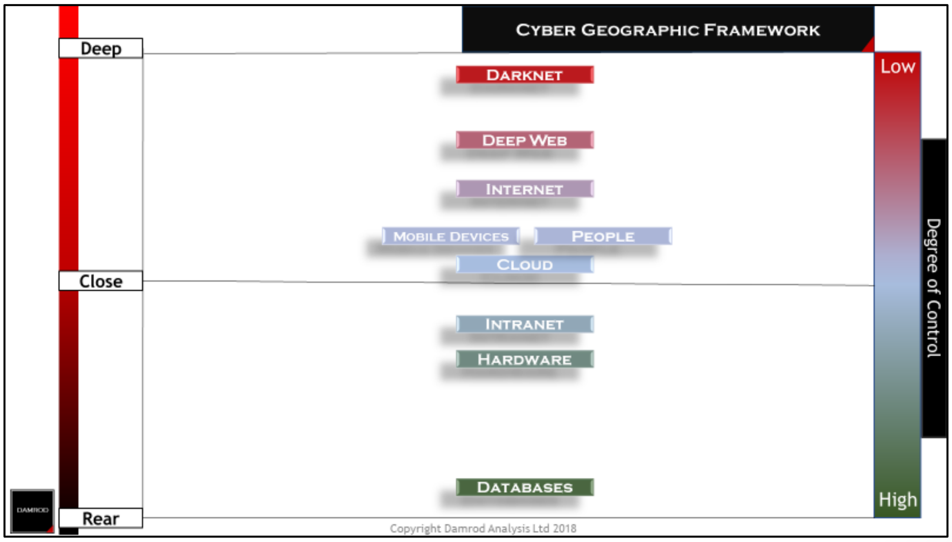
- **Deep**
- **Close**
- **Rear**

Deep is where an opponent's force operates. In other words, the defender does not control it. Close is where the conflict occurs, where opposing factions meet in a contest of wills. The Rear is the region over which the defender exerts the most control.

In cyber terms, Deep is synonymous with the deep web and darknet, while Close is the internet and common interactions with cyberspace. There is an interplay in the Close between cyber and physical assets. The Rear is analogous to an organization's own networks and databases.

We can refine terrain analysis for use in cyber conflict by keeping this degree-of-control framework in mind. The substitution of 'control' for 'geographical space' is necessary because while physical distance often makes access difficult in the real world, in cyberspace physical distance is negligible. By organizing the cyber terrain based on Deep, Close, and Rear categories linked to a defender's degree of control, the Cyber Geographic Framework allows for visual orientation, much like North or distance markers on a map.

FIGURE 1: CYBER GEOGRAPHIC FRAMEWORK



We can overlay additional analysis onto this framework to increase our understanding. The first overlay should be a representation of the cyber terrain.

Cyber Terrain Analysis

Instead of hills, rivers, or roads, cyber has prominent features like networks, databases, and applications. There is no constraint on what constitutes a cyber terrain feature, provided that the cyber terrain is:

- ✓ representative of an element relevant to cyber, and
- ✓ something of interest to attackers or defenders.

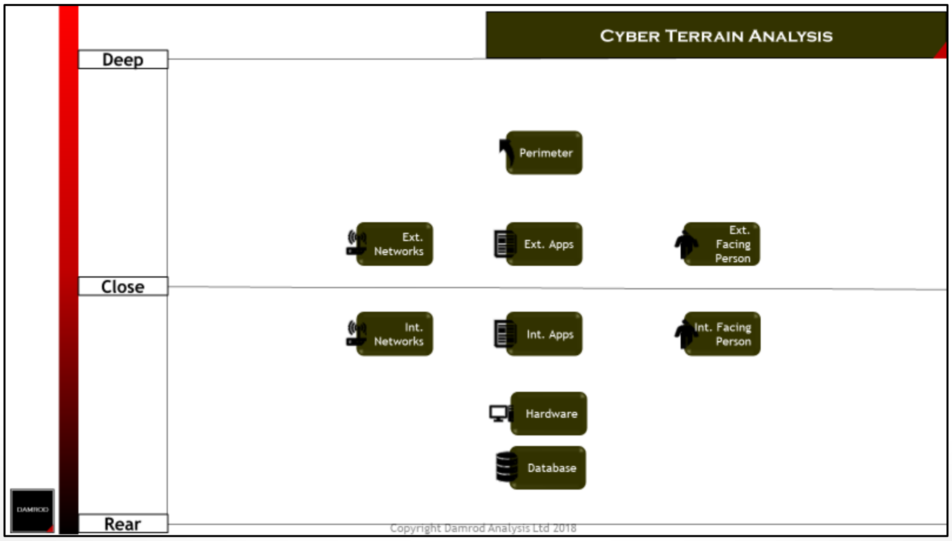
Some prominent examples of cyber terrain are:

- **Perimeters**
- **Networks**
- **Applications**
- **Hardware**
- **Databases**
- **People**

These broad terms can be further split based on additional criteria, such as being internal or externally facing, or cloud, or legacy. So long as some analysis has gone into the planning, it is a valid observation of the cyber terrain.

Once the initial list of cyber terrain is assembled, it can be mapped onto the Cyber Geographic Framework. Recalling that the framework provides a top to bottom axis based on low to high degrees of control, we overlay each aspect of cyber terrain, as in ***Figure 2***:

FIGURE 2: CYBER TERRAIN ANALYSIS



In this example, we have divided the networks, applications, and people into distinct terrain features based on their level of externality. This allows for greater granulation of risk and to identify which aspects are further forward in the cyber conflict and thus less controlled.

Following on from the evaluation of the cyber terrain, we assess the threats in cyberspace and the steps opponents will take to achieve their objectives.

Threat Integration

Broadly speaking, there are four primary threat actors in cyber conflict:

- **Advanced Persistent Threat (APT) – or state sponsored**
- **Cyber Criminals**
- **Hacktivists**
- **Insider Threats**

There are additional categories and hybrid threats, which specialized threat intelligence organizations can identify. More detailed threat assessments yield more detailed and valuable threat integration.

Damrod's aim is to assess how these threats will move through the cyber terrain to realize their objectives.

Damrod Analysis's Threat Integration overlay is a visual representation of the complicated paths attackers use to breach IT systems. While Cyber Terrain Analysis identifies what you are protecting, Threat Integration identifies what you are protecting it from.

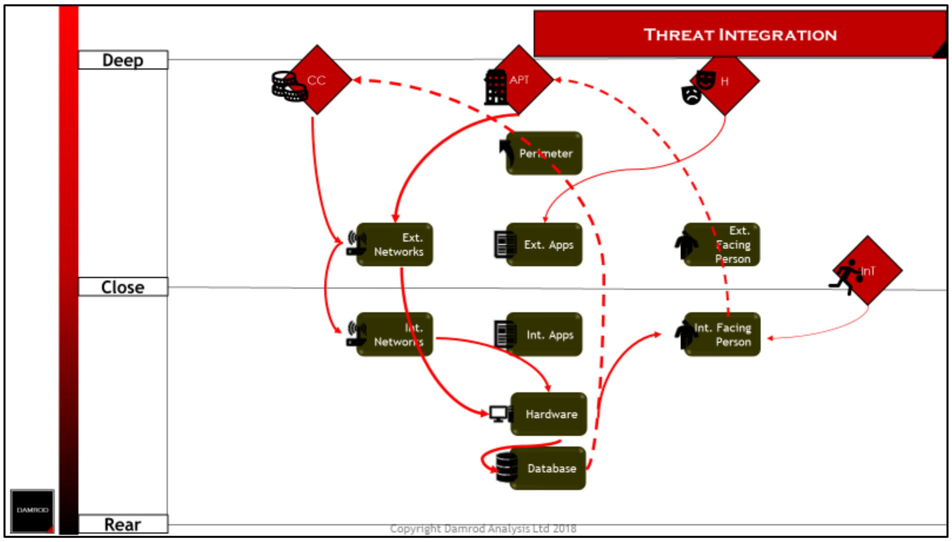
We show higher probability threats with large and thick red lines, and less likely or less dangerous attacks with thin red lines. The exfiltration of data is also important, and is represented as a dashed red line.

Figure 3 is a summary of multiple attacks threatening a hypothetical large enterprise. In this example, the primary threat originates with a state-sponsored **APT**. Threat intelligence indicates the attackers will be targeting external networks to gain access to hardware and databases, and will then be exfiltrating the data back to the state actor.

A secondary threat is cyber criminals **[CC]** targeting similar vulnerabilities in external networks to spread through internal networks and hardware.

Less severe threats come from hacktivists **[H]**, who target external applications to bring down external networks, and insider threats **[InT]**, who are internally facing employees with access to databases.

FIGURE 3: THREAT INTEGRATION



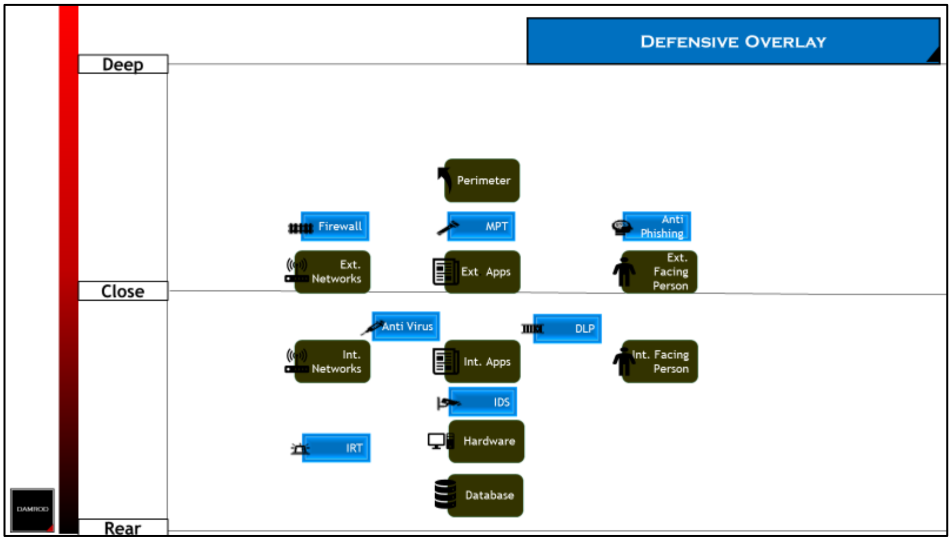
This high-level overview of likely attacks informs how the cyber defense team should be organized, empowered, and resourced to defend against potential attacks. Team leaders within IT can conduct their own Cyber Terrain Analysis and Threat Integration to better defend their assigned regions.

DEFENSE OVERLAY

Damrod's Defense Overlay maps out a company's cyber security apparatus. ***Figure 4*** is a summary of various resources protecting a hypothetical large enterprise. In this example of a typical enterprise cyber security setup, **Firewalls** protect the external networks, and manual penetration testing **[MPT]** is performed on externally facing applications. Employees receive **Anti-Phishing** training, and **Anti-Virus** programs protect internal networks and applications. Data Loss Prevention **[DLP]** is in place, as are Intrusion Detection Systems **[IDS]** and an Incident Response Team **[IRT].**

By adding the Defense Overlay to the Cyber Terrain Analysis, it is evident how existing cyber tools already form a web of security. The graphical representation makes it simpler to make observations and draw deductions from a complicated cyber security setup.

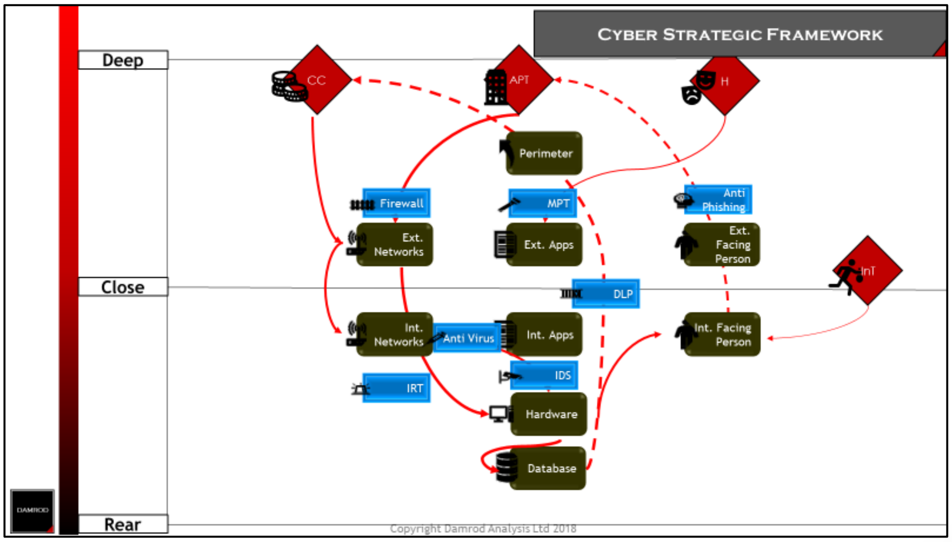
FIGURE 4: DEFENSE OVERLAY



CYBER STRATEGIC FRAMEWORK

Combining the ***Cyber Geographic Framework*** with the ***Cyber Terrain Analysis***, ***Threat Integration*** and ***Defense Overlay*** creates the ***Cyber Strategic Framework*** – a visual representation of cyber conflict to aid decision makers craft cyber defense strategies. ***Figure 5*** shows what a simple, high-level Cyber Strategic Framework for a hypothetical enterprise could look like.

FIGURE 5: CYBER STRATEGIC FRAMEWORK



In the ***Cyber Strategic Framework***, defensive icons move to align with avenues of attack – demonstrating the intent behind their deployment. It should be quickly evident that this organization is relatively well defended, though should consider a response to the Insider Threat **[InT]**, which goes unblocked.

Beyond the visualization of the cyber conflict, Damrod's frameworks provide context for the selection and implementation of products and services – creating opportunity for efficiency gains and improved return on investments.

Cyber security vendors are legion and well-funded. Research from the International Data Corporation indicates that worldwide revenues for security-related hardware, software, and services will grow from $73.7 billion in 2016 to $101.6 billion by 2020.[2]

Technology and services will continue to improve and evolve, but the total spend by companies does not need to keep growing at a comparable pace.

Damrod contends that technology is only a partial solution to cyber conflict. Transitioning from security to defense requires a change in mindset. **First**, a company needs to adopt an analytical approach grounded in military thinking: a survey of the cyber terrain and likely threats will help determine the defenses required by the business. **Second**, a company needs strong leadership: overlaying multiple technologies and services into a coherent defensive strategy requires vision, not just money and technology.

ASSESSING THE CYBER STRATEGIC FRAMEWORK

Each company has a unique Cyber Strategic Framework, which it can use to determine the strengths and weaknesses of its existing cyber defense.

A strong defense has six traits:

- **Depth**
- **All Around Defense**
- **Mutual Support**
- **Reserves**
- **Offensive Spirit**
- **Deception**

[2] International Data Corporation Press Release Oct 2016

Collectively, these form the mnemonic DAMROD, from which Damrod Analysis takes its name. In this section, we discuss how each of these facets is applied to cyber to help companies evaluate the strength of their defenses.

Depth

Defense in depth is a common cyber security phrase that has military origins. In its original context, defending in depth refers to a tactic that defeats an attack by absorbing momentum. ***There is an explicit trade to give attackers space in order to buy defenders time***.

To defend in depth means more than piling on layers of security. It is a philosophy that acknowledges that an attacker will break through the initial lines. An IT system with suitable defense in depth will have multiple layers to prevent breach, but also buy time to detect the attack and respond to it.

Implicit is the requirement that all defenses be integrated, sited with analytical insight and clear purpose. It is insufficient to simply buy and layer a host of cyber security tools. The cyber defender must think through how each piece of technology or policy adds to the defense of the organization and what effect is intended.

All Around Defense

No endeavor is free from risk – particularly in conflict. No leader has sufficient resources to eliminate risk from every angle. However, astute leaders have thought about every angle and will provide threat mitigation on all fronts. While a soldier in the field may not expect a flanking attack, it is still something an intelligent defender will consider.

Likewise, in cyber, threats come from unexpected directions, ranging from the new and novel to the tried and tested. ***To consider the all-around defense is to design your defenses to respond to threats from any angle***. If a technology or service protects against only a single threat it may not be an efficient allocation of resources.

Mutual Support

A key consideration in cyber security is that many of the providers are private businesses. Without disparaging their intent or ability, their ultimate driver is profit in a zero-sum game – customers have limited budgets, and each vendor maximizes its share of it. It is natural then that cyber security vendors will compete rather than collaborate. Ensuring that the offerings of one vendor are supported by the offerings of another is a vision and leadership piece that belongs to the cyber defender.

Each part of a company's cyber defense should be supported by at least one, but ideally two other elements of the defense. This is particularly important for the threat integration analysis. ***If an avenue of approach is a likely attack vector, multiple defenses must be deployed to mutually support each other***. This prevents circumvention and limits the impact of novel attacks.

Reserves

No defense is complete without a capability to react to the unexpected. While threat intelligence may paint a picture of what your opponent may do, a key feature of conflict is that it is a contest, and the attacker is a thinking enemy that develops its own methods to defeat your defenses.

The reserve is an uncommitted resource to respond to new threats and opportunities. A dedicated Incident Response Team is the most obvious example, but providing security training to existing employees who can be called from their normal tasks to reinforce the defense is another workable approach. Cyber insurance that provides a ready injection of funds following a breach may also fall under the aegis of the reserve.

The most proactive approach to the reserve concept is to keep some resources uncommitted, which can be drawn upon to take advantage of new technologies as they become available. For the right companies, this may represent excellent return on investment to protect against emergent threats and seize new opportunities.

Offensive Spirit

Trite but true, the best defense is a good offense. ***A sound cyber defense goes beyond achieving compliance with regulation, and answers the question - How do I win?*** A passive mentality will not protect organizations from cyber conflict. Defenders must think like attackers, modifying defenses with an eye for victory.

In army environments, this is achieved by walking the ground and war gaming how an attack might unfold. War gaming is an equally valid tool in cyber and committing red teams to test an organization's defenses is a sound strategy.

Aggressive patrolling is a hallmark of a sound defense. Looking into the cyber Deep to identify and disrupt upcoming or planned attacks could prove effective if properly resourced.

Deception

Conceptually related to the offensive spirit, ***the principle of deception looks to put adversaries on their back foot - confusing them and delaying their attack***. Fake variants of key assets are deployed to deceive attackers about how the defenses are arrayed, how many defenders there are, and the location of important hubs.

Artificial networks with planted vulnerabilities force an attacker to reveal their presence and waste their opportunity to enter undetected. To be effective, deception requires mutual support and reserves: the first to cover and observe the deceit, and the second to respond to attacks against it.

CONCLUDING THOUGHTS

Damrod Analysis applies defensive principles to cyber security to create cyber defense. It is a step away from checklists and compliance to look at cyber like the other fields of conflict.

Damrod Analysis's approach realizes the full value of technology by integrating disparate elements into a detailed and structured defensive plan suitable to defeat the threats facing modern organizations.

The Cyber Strategic Framework enables CISOs and their staff to:

- **Understand their cyber terrain**
- **Assess the cyber threats to their business**
- **Communicate complex cyber information to non-expert decision makers**

The six-step DAMROD defense assessment empowers CISOs and their staff to:

- **Test the strength of their cyber security and mitigate weaknesses**
- **Allocate resources to maximize return on investment**
- **Integrate technology, services, and policy efficiently**

Book a free initial consultation at www.damrod.co.uk

DAMROD