CYBER STRATEGIES

By: Nevin Taylor

Given the growing dependence on the cyber domain, it is imperative that we remain vigilant as we operationalize cyber to assure competitive advantage. As we embark on this journey, we are well advised to heed the words of Carl Von Clausewitz…”Two qualities are indispensable: first, an intellect that even in the darkest hour, retains some glimmering of the inner light which leads to truth, and second, the courage to follow this faint light wherever it may lead.”

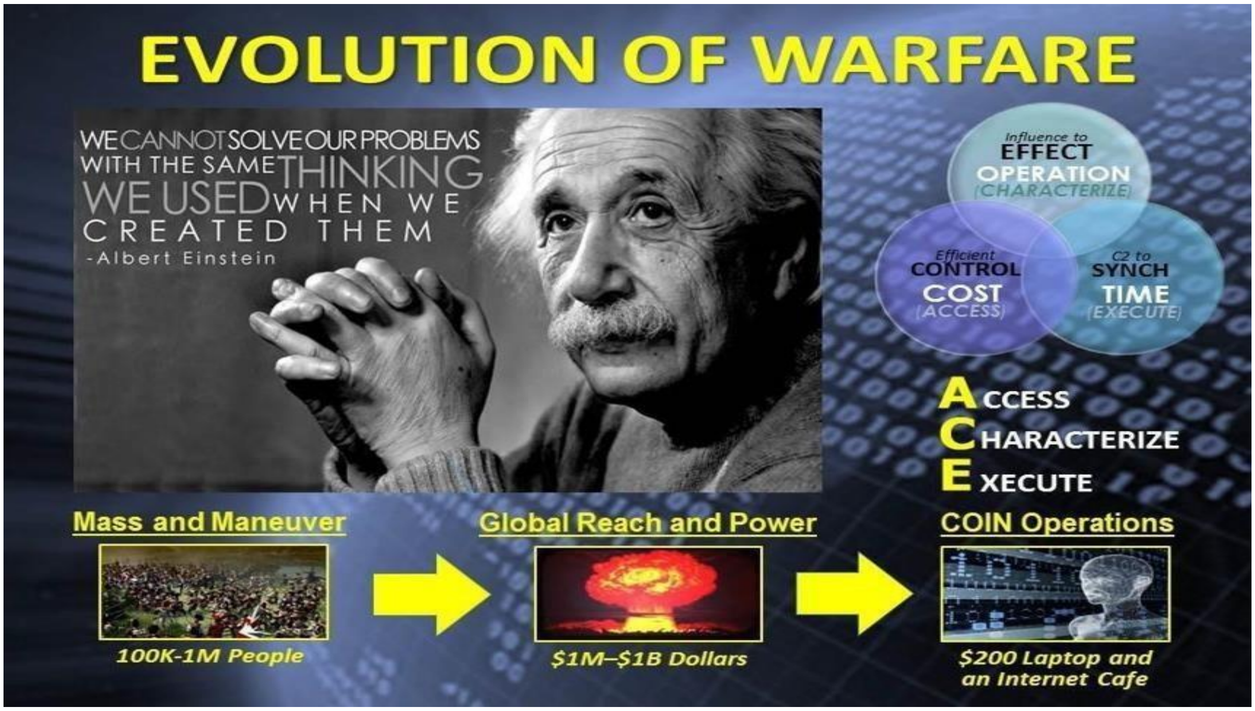
Thus, we must remain focused on the stated objectives as they operate in the new and ever-changing information environment. Moreover, as they operationalize the cyber domain, they must be cognizant and thoroughly consider their actions and how they are aligned to fulfill their objectives, void of unintended consequences, for it is within this information environment that their influence has a direct bearing on the outcomes that support and ensure the prosperity and preserve freedom of action within the digital domain.

Engagements in cyber not only support and enhance operations; they serve to assess and characterize the very nature of the information environment. Ultimately, the express and implied goals of cyber operations are to create the strategic advantage necessary to gain and maintain information superiority. By extension, therefore, dominance within cyber operations means wielding a strategic advantage or achieving information superiority.

History demonstrates repeatedly that victory typically goes to those best able to amass and direct substantial military might capable of imposing their will and protecting their interests. As technology continued to evolve, refinements and improvements in weaponry and tactics gave strategic advantage to the most innovative actors on the world scene by enabling them to overcome capacity shortfalls. The result is a strategic advantage achieved via superior capability. In today’s world, we seek ways to leverage the resources necessary to maximize the effects of our capabilities and capacity. In that search, information is the critical component that guides us in integrating and synchronizing operations in order to overcome adversarial threats.

By focusing on our ability to Support, Enhance, and Execute (SEE) operations and the cultural paradigm inherent in this domain, we can develop an understanding of WHY certain operations are essential, for it is through these efforts that we will acquire the requisite knowledge to ENHANCE HOW to proceed incrementally. Combined, this will afford us the strategic advantage of realizing WHAT is to be EXECUTED.

Since the Industrial Age, the Information/Knowledge Age has become critical for success. As we endeavor to embrace and harness the power of information, it has become the essence of strategic advantage in the global environment. This expansive area continues to evolve and transform at the speed of light. Thus, we must be cognizant of our growing dependency on technological capabilities or "critical mass" of the vulnerabilities inherent in cyber ops.


EVOLUTION OF WARFARE
WE CANNOT SOLVE OUR PROBLEMS WITH THE SAME THINKING WE USED WHEN WE CREATED THEM
-Albert Einstein
Influence to EFFECT OPERATION (CHARACTERIZE)
Efficient CONTROL COST (ACCESS)
C2 to SYNCH TIME (EXECUTE)
ACCESS
CHARACTERIZE
EXECUTE
Mass and Maneuver
100K-1M People
Global Reach and Power
$1M–$1B Dollars
COIN Operations
$200 Laptop and an Internet Cafe

The magnitude of the challenges confronting us in today's rapidly evolving information environment is compounded by a multitude of obstacles. Our constrained fiscal environment, inflexible organizational processes, and a risk-averse culture inhibit innovation. Within the cognitive phase, however, strategic tradeoffs within the decision space disclose opportunities that enable us to navigate the Volatile, Uncertain, Complex, and Ambiguous (VUCA) environment. It is within this risk-averse culture that we are precluded from overcoming threats and availing ourselves of the opportunities so prevalent in the new digital domain.

To remain vigilant—regardless of domain—it is vital to understand the complexity of our systems, which require continual patching across thousands of networks worldwide. However, it has proven difficult to establish a structure with the requisite visibility to defend this diverse network. We must characterize our adversaries' intentions and assess their capabilities to focus the efforts we need to mitigate the threat. In doing so, we must learn to manage this inherent risk and find ways to overcome actions focused against us by our adversaries. Most importantly, we must maintain our freedom of action in cyberspace so that we can either respond in kind or impose our will on those adversaries at a time and place of our choosing.

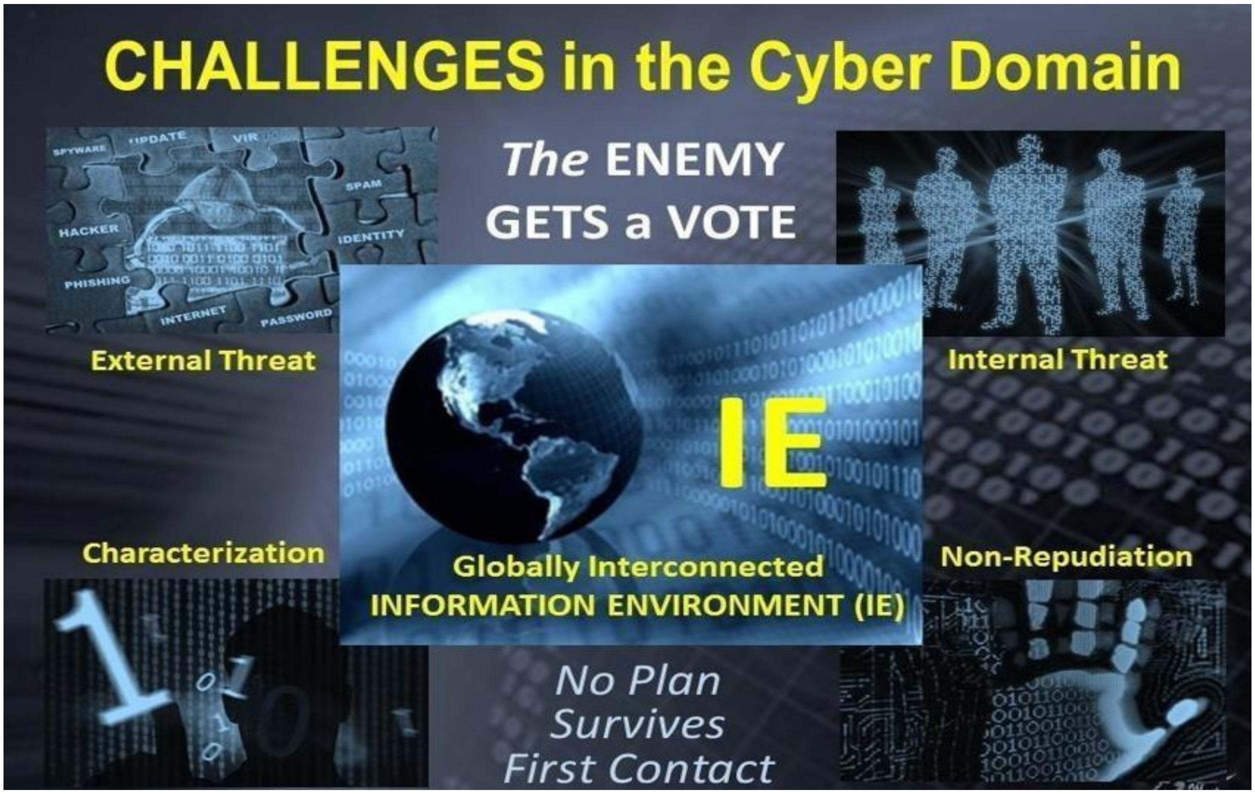
The unrelenting actions being taken by our adversaries have telegraphed their intentions to acquire disruptive capabilities and leverage the destructive capacity of the cyber domain. Stated otherwise, cyber actors are undercutting strategic and technological advantages by targeting our information systems. Even more alarmingly, the growing threats and complexities associated with our technological age make it more difficult, by an order of magnitude, to manage the confidentiality, accessibility and integrity of our information. Thus, it is imperative that we characterize, assess and act quickly on information to identify and overcome immediate threats and vulnerabilities.

Moore's Law holds that technology evolves every 18 months. By extension, the Internet is growing beyond the ability of most people to conceive both in its breadth and scope. For instance, the "Internet of Things" stems from our sustained demand for greater awareness through an always-connected profile. In 2015, the Internet Society—a non-profit entity dedicated to preserving the Internet as an open platform—estimated that the number of Internet hosts and users worldwide would increase to 1 billion and 3 billion, respectively. Similarly, Cisco Systems, Inc. estimates that 15 billion Internet-connected devices are currently in use. A joint Cisco-IBM research study projected that worldwide data volume will double every 18 months, reaching a rate of quintillion bytes per day.

There is indeed a clear and present need for us to develop a comprehensive cyber deterrence strategy. For our adversaries are lurking, right now, in this amorphous and limitless domain. The actions being taken by those adversaries place our systems at considerable risk. Specifically, the global proliferation of malicious code—malware—which continues to threaten U.S. networks, the data they store, and the mission they support.

One of Von Clausewitz's most renowned aphorisms is that “War is merely the continuation of politics by other means.” State and non-state actors conduct cyber operations or wage cyber warfare to destroy, manipulate or disrupt our industrial control systems. This allows them to influence public safety and national security to subvert trust and confidence. As deleterious as this may seem, however, those actions can be defeated by employing heightened situational awareness, which allows us to manage and mitigate the risk.

By applying a credible strategic aim to push and pull trusted information within the information environment, we can increase situational awareness and advance knowledge to make better-informed decisions. In short, the cognitive process facilitated by efforts to Assess, Characterize, and Execute (ACE) cyber operations affords a predictive capability to outthink adversarial attempts to create and inflict havoc.



We must capitalize on ACE's predictive capacity to determine the best way forward to execute actions and gain and maintain dominance within the information environment. This will enable us to overcome a broad range of threats and unpredictable challenges levied by adversaries, from non-state actors to nation-states. Moreover, despite the rapid and exponential advancement of the digital domain, we must exude agility in this inherently VUCA environment. Therefore, in coordination with other services and agencies, today’s cyber professionals are expected to establish resilient and trustworthy systems with tighter human-machine interfaces to provide our personnel with dependable information when and where they need it most. By organizing, training, and equipping cyber professionals to be experts in their field, we can and will protect and assure a competitive advantage.

Despite the current fiscal constraints, we must optimize the planning, programming, and execution of information technology investments to sustain the synergistic advantage on which our nation depends. By collecting information to evolve our Frame of Reference (FOR), controlling it to safeguard its strategic value, and exploiting opportunities that ensure our ability to fulfill our mission objectives, we will maximize effectiveness in the following areas.

Goal 1: Provide trusted information when and where it is needed:

- compress the information flow within the kill chain
- apply common data standards in all mission areas
- attain operational and technical resilience
- improve interoperability and effectiveness
- prioritize secure capabilities

Goal 2: Organize, train and equip cyber professionals to be experts in their field:

- cultivate innovation to capitalize on cyberspace capabilities
- provide cyber professionals with the means to execute, enhance, and support organizational objectives

Goal 3: Strengthen mission assurance for freedom of action in cyberspace:

- provide cyber capabilities for mission assurance
- shorten the kill chain and increase decision-making speed

Goal 4: Optimize planning, programming, and execution of cyberspace investments:

- flexible dynamic processes for capital planning and investment
- ensure competitive advantages to sustain and modernize cyber

All plans begin with the end state in mind, since that objective enables us to focus clearly on goals that will fulfill our intermediate and ultimate objectives. Thus, developing a top-down perspective makes our personnel aware of themselves, their adversaries, and their environment, all of which are vital to understanding the best way to achieve their objectives. Supporting and enhancing their actions by making informed decisions and capitalizing on their strengths (while mitigating their weaknesses) will enable us to gain an asymmetric advantage over our adversaries.

We must therefore cultivate actions that control escalation and shape the conflict environment at all stages by integrating cyber options into all aspects of planning to apportion the cyber domain effectively. The result of this will ensure adequate campaign planning that assesses and identifies gaps and establishes initiatives geared to pursue a cyber deterrence posture and strategy that will inhibit adversaries from conducting cyberattacks.

By characterizing, assessing, and mitigating risk in the rapidly evolving cyber domain, we will ensure strategic global stability by engaging in information sharing, interagency coordination, and building bridges to the private sector, thereby establishing alliances and partnerships. Such collaboration will ensure our ability to achieve our three primary cyberspace missions successfully:

> **FIRST**: Defend networks/systems/information in and through the cyberspace domain
>
> **SECOND:** Defend against cyberattacks and conduct operations to counter attacks that could threaten loss of life, significant property damage, and adverse consequences. (The achievement of this mission is challenging since limited and specific roles play into defending against cyberattacks. As the private sector owns and operates over 90% of all networks and other examples of cyberspace infrastructure, it represents the first line of defense. Accordingly, they must prioritize the protection of those networks and data by investing in improving their own cybersecurity.)
>
> **THIRD**: Organizations must provide integrated cyber capabilities in support of their operations and contingency planning to:
>
> - *disrupt an adversary's potential to impact their networks or infrastructure*
> - *deter or defeat strategic threats in other domains*

By investing in technical capabilities to conduct cyber operations, we can develop capabilities that validate and continually refine adaptive command and control mechanisms. This will ensure the presence of efficient and reliable C2 nodes that promote unity of effort across all three cyber missions. To field a cohesive, well-integrated, and enterprise-wide cyber modeling and simulation capability, we must establish a data schema comprising databases, algorithms, and modeling and simulation environments. Such advancements will ensure our ability to defend the information environment, secure the network, and mitigate mission risks.

Through continuous network monitoring coupled with improved cybersecurity training and reporting of suspicious behavior, we will cultivate a culture of awareness to anticipate, detect, and respond to insider threats before they can adversely impact our mission. In general, cyber protection will ensure the technology is leveraged appropriately to produce information that feeds the decision-making process.

In taking steps to identify, prioritize, and defend its most important networks and data, we will plan and conduct exercises that will operate within degraded and disrupted cyber environments. We will also strive to advance technology to develop innovative approaches to enhancing, building, and employing a collaborative information environment network architecture that is more defensible, thereby mitigating and protecting against cyberattacks.

Ongoing efforts to build a single security architecture (intended to adapt to and evolve in response to current and future cyber threats) will enable robust network defense and shift the focus from protecting service-specific networks to establishing a unified approach to securing the enterprise. The resulting framework integrates and advances the cybersecurity architecture by including anomaly-based detection capabilities and data analytics intended to identify vulnerabilities. Awareness of these threats and the application of advanced encryption methods will establish a best-in-class cybersecurity practice that ensures situational awareness of network threats, enabling risk assessment and mitigation.

In Summary, as the information environment continues to evolve at a blinding speed, we must remain flexible and versatile, and shift to inherently agile, deployable, and networked systems. As mentioned, such systems must be resilient and trustworthy, and they must feature improved interfaces, exemplified by cloud computing and intelligent machines. This combination will provide trusted information when and where they need it most.