The Spectrum of Cyber Attack

Maj David Musielewicz, USAF

Introduction

Despite the extensive high-level guidance given by America's senior leaders in cyberspace, the risk of strategic failure and wasted resources remains high in offensive cyberspace operations. Former Secretary of Defense Ash Carter reflected on these failures in his description of countering the Islamic State of Iraq and Syria (ISIS) from 2015–17: "I was largely disappointed in Cyber Command's effectiveness against ISIS. It never really produced any effective cyber weapons or techniques. . . In short, none of our agencies showed very well in the cyber fight."[1]

This failure is due to the broad gap in the understanding of how leaders should pursue strategic objectives and goals at the tactical level. Although the Department of Defense most recently requested $3.7 billion for 2020 offensive cyberspace operations alone,[2] a clear, executable cyber attack framework that allows commanders to achieve senior leader visions does not currently exist. How can commanders reliably achieve the visions put forth by senior leaders given such a gap? I propose the following operational framework that bridges this gap and lays a foundation for the seamless pairing of tactical tasks and effects with desired strategic objectives.

If the United States is to have a distinct military advantage over its enemies, it must aggressively stay ahead of other nations in cyberspace through a framework at the operational level that offers speed and flexibility, while also succinctly connecting strategic guidance to tactical employment. A seamless flow from the strategic to tactical level will enable the alignment of action plans with overarching strategic goals throughout all echelons of cyberspace.

In the following sections, I draw on the previous decade of historical and currently active cyberwarfare alongside my 10 years of experience executing offensive cyberspace operations to frame attacks into a series of five levels that I collectively refer to as the "Spectrum of Cyber Attack." Each section defines and describes a particular level, provides real-world examples, and then explores the costs and benefits of conducting such attacks. A condensed depiction of these tradeoffs between cyber-attack levels is then estimated and summarized in the table. Fi-

nally, I propose future areas for consideration alongside the overall benefits of employing this framework throughout the various levels of leadership.

The Framework

By understanding the various attacks at each level within the spectrum, leaders and planners at the operational level will be better positioned to pursue objectives, describe expected end-states, and express various tradeoffs between methods. This will allow for the proper allocations of time, resources, and effort toward a particular objective. Ultimately, commanders will be able to present a menu of options for achieving strategic goals, all with varying levels of risk, reward, and resource commitment.

Throughout the brief history of cyberwarfare, actors at all levels have performed a wide range of attacks. Despite individual differences, these attacks can be arranged into five categories or levels that build upon one another to form a spectrum: Network Denial, Enterprise Denial, Enterprise Manipulation, Mission Denial, and Mission Manipulation.

The term *level* is best suited because of the compounding factor that exists between different attacks as they become more sophisticated. Once an actor can execute an attack at a higher level, they can also execute attacks at the lower levels. Conversely, conducting a denial attack at a lower level will likely cut off access to the systems required for higher-level attacks.

The following sections categorize these levels based on the estimated time required to execute an attack, their cost, their likelihood of success, how long they affect an organization, and their overall impact. In cyber warfare, almost all time is spent on gaining access to a particular system or systems crucial to the desired attack, while the time to execute the attack is negligible. Similarly, the policies and procedures to gain the appropriate approvals to conduct various attacks vary widely between organizations. Therefore, the time frames discussed throughout this article only refer to the operational time required to gain the requisite access, not the time required to initiate the attack or for various policies and processes.

The "Spectrum of Cyber Attack" incorporates the definition of denial from Joint Publication (JP) 3-12, *Cyberspace Operations*, "to prevent access to, operation of, or availability of a target function"[3] as the foundation for the three levels designated as denial attacks: Network Denial, Enterprise Denial, and Mission Denial. The spectrum builds upon JP 3-12's definition of manipulation, "controls or changes. . . to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification and other similar techniques,"[4] for the remaining levels designated as manipulation attacks: Enterprise Manipulation and Mission Manipulation. In this definition, *physical* simply refers to the fact that manipulation

effects have an impact outside of cyberspace. This definition not only refers to the physical systems themselves, but also the cognitive layer, or users, of those systems. This describes manipulating a system to in-turn manipulate or drive an effect in the human element. Manipulation attacks require a more complete understanding of the systems involved along with deeper, more intrusive network access. This knowledge and access are required to successfully manipulate, deceive, or otherwise influence the behavior of users within a target organization.

Level 1: Network Denial

Definition. A cyber attack that prevents a network from communicating with external networks

Description. The first level of attack is the most simple to conduct, difficult to stop, and thus commonly used. Level 1, Network Denial, targets only the transmission of information, not the actual information itself.

These attacks may affect only a part of the network or the network in its entirety. They can be accomplished through several different methods, many of which are exceedingly difficult for the victim to stop. Level 1 attacks primarily differ from other levels in that they affect the target's ability to interact with other organizations while internal processes are largely unaffected.

Examples. A simple example of Network Denial is characterized by an attacker that logs into a router at the border of an organization's network and stops it from transferring data. This example results in the blocking of all traffic on a network and isolates the target organization, temporarily preventing it from transmitting any information in or out using computer networks. This type of network isolation degrades the operations of any organization but only as long as the target is unable to restore proper functionality.

More advanced level 1 attacks require national-level resources or access to central backbones of the internet. These include Border Gateway Protocol hijacking, Domain Name Server hijacking, and large-scale Distributed Denial of Service, all of which have been used by either Russia, Iran, or China.[5] These attacks take advantage of the fundamental trust that the internet is built on, giving them the added benefit that there is very little a victim can do to stop them, and they are always at the disposal of a nation.

Tradeoffs. Network Denial attacks are conceptually simple to execute but only provide temporary paralysis of a target's operations. Fewer moving pieces at the technical level results in the highest chance for success compared to all other levels and requires far less knowledge about the target. New targets can be attacked within hours or days and require little preparation. The trade-off, however, is that level 1 attacks draw significant attention and are quick to diagnose. Overall,

level 1 attacks require less time, less funding, and thus less commitment, yet they are only expected to disable an organization for hours to days depending on the sophistication of the target's personnel.

Level 2: Enterprise Denial

Definition. A cyber attack that denies an organization's users access to their data

Description. The next level of cyber attack also disables an organization, but in a manner that inhibits the daily activities of end-users. The term *enterprise* is used to describe the systems and applications users rely on to perform day-to-day tasks. Examples of daily activities affected by level 2 attacks include the ability to log into computers, send e-mail, and alter documents. Level 2 attacks differ from level 1, Network Denial, in that they specifically disrupt information that an organization's users interact with directly.

Examples. The most common example of a level 2 attack is ransom malware, or "ransomware," currently in vogue with cybercriminals. Ransomware does not need to know anything about an organization before executing its core objective, to deny users access to their data by encrypting it. The files that become encrypted are critical to the system users as the malicious software attacks all files, historical records, activity records, and any others used to carry out daily tasks and company function. This is precisely why it is so devastating for companies hit by such attacks.

The most destructive level 2 attack to date has been the "NotPetya" ransomware that caused an estimated $10 billion in damages worldwide in 2017. As an example of the financial impact caused by NotPetya, the international shipping company Maersk alone suffered $300 million in damages and experienced a complete operational shut down for almost a week. This level of disaster is not unique to Maersk,[6] or even NotPetya itself. "WannaCry," "SamSam," and "Ryuk" are all well-documented ransomware attacks dating back to 2017 that inflicted millions in financial costs and achieved wide-scale operational impacts across numerous organizations.[7]

Tradeoffs. Level 2 attacks are likely to cost more financially than any other cyber attack, purely based on the scope and number of systems they affect. Similar to level 1, level 2 attacks require very little target knowledge, and thus, require less time and monetary investment than other levels. However, the likelihood of success of level 2 attacks is also less than that of level 1 attacks due to the deeper network access required. Additionally, the most damaging level 2 attacks to-date only managed to take organizations offline for a few days despite the severe financial costs, and all operations were restored in a manner of weeks.

Level 3: Enterprise Manipulation

Definition. A cyber attack that manipulates the decision-making of an organization's users without being detected

Description. Enterprise Manipulation is the first level on the spectrum that tailors more toward affecting the behavior of the adversary than removing their ability to operate. These attacks target the same computer systems as level 2, Enterprise Denial, attacks but utilize a deeper understanding of the organization to influence or corrupt, but not deny, common organizational processes. Further, a key objective in executing a level 3 attack is to do so without the user being aware of the attack. This is the key distinction between level 3 and the first two levels.

Level 3 attacks must be performed in a manner that is not predictable nor widespread throughout the target organization. Enterprise users have been conditioned over time to be mistrusting of computers and software due to confusing interfaces, technical user manuals, overall complexity, and frequent data loss. By introducing outside gremlins into the systems, end-users can further lose confidence in their ability to effectively perform tasks, thereby leading to loss in productivity and organizational effectiveness.

Examples. Although data manipulation has only started to be openly discussed in the past few years,[8] it is easy to envision the potential chaos that can result from such attacks and has captured the imagination of television producers in series such as "Mr. Robot."[9] These attacks can be as simple as removing key e-mails, locking particular user accounts, or corrupting vital user files. More robust and potentially far-reaching attacks can be catastrophic, such as manipulating financial or human resource data.

According to *Forbes*, the manipulation of financial data is already extensively practiced by North Korean hackers. North Korea has stolen a staggering $2 billion in 35 compromises across 17 nations.[10] For example, North Korea drained $498K from the city of Tallahassee by manipulating payroll data.[11] These attacks were designed to obtain funds rather than impose crippling costs on the underlying organizations, yet the devastating impact to the organizations were the same.

Tradeoffs. Enterprise Manipulation attacks strike at the psyche of an organization with the aim of crippling its effectiveness for a prolonged period of time. Levels 1 and 2 cause overt disruptions resulting in temporary outages, but level 3 attacks can hinder an organization for an indefinite period of time. These attacks require a nearly identical preparation time as level 2 but have a much lower chance of success and less quantifiable results. Level 3 attacks also cost more to execute because they must use more sophisticated tools to remain undetected in the target network. Level 3 attacks will not likely impose costs similar to the other levels, but

they allow attackers to remain within the network undetected while eroding the productivity of an organization.

Level 3 attacks also provide the ability to engage a target without the increased risks of retaliation or escalation because of their inherent stealth and plausible deniability. As long as level 3 attacks remain hidden, they allow the perpetrator to develop level 4 and level 5 attacks, all while the target simultaneously suffers negative impacts on efficiency and productivity.

Level 4: Mission Denial

Definition. A cyber attack that specifically prevents the operation of processes or systems critical to an organization's mission

Description. The final two levels of the Spectrum of Cyber Attack focus solely on the chain of systems and processes that are essential to an organization carrying out its core mission. This focus may be the destruction of mission-critical data or even—in very specific scenarios—the physical destruction of hardware through industrial control system manipulation. The precision of these attacks is what specifically distinguishes level 4, Mission Denial, from level 2, Enterprise Denial.

Example. The 2015 Russian attack on the Ukraine power grid is a prime example of a level 4 cyber attack. During this attack, Russia gained critical access to three primary Ukrainian power companies undetected. Once inside the networks, the malicious actors immediately targeted the systems used by internal operators to control the generation of power. The actors surveilled the system operators long enough to learn which interfaces were used to control the power generators. Once known, the attackers systematically shut the generators down and disabled remote access to the controlling computers.[12] By preventing the power generator operators from remotely bringing the systems back online, technicians were required to physically travel and manually restart each generator, a process that took six hours to complete.[13]

What makes this example a level 4 attack instead of a level 2 is that the actors were specifically targeting those systems that were essential to the organization executing its core mission—generating power. If these same actions were conducted against systems not vital to this mission, they would be classified as a level 2 attack.

Tradeoffs. From an attacker's perspective, level 4 attacks are much more predictable than level 2 because of their precise nature. These attacks are far more likely to create the specific effect desired. Reducing the scope of an attack and executing with precision allows the attacker to tailor to specific strategic objectives and execute with a higher level of certainty. In contrast, level 2, Enterprise Denial, has the potential to prevent an organization from accomplishing its pri-

mary mission, but only as a byproduct of the primary attack. It is easier for a victim to restore mission-critical functions following a level 2 attack because of the universal aspect of level 2 attacks versus the subtlety required for level 4. Level 2 attacks are far more common and less sophisticated, making them more likely to be anticipated and mitigated by network defenders.

Level 4 attacks require notably longer time commitments than levels 1, 2, and 3. This is due to the in-depth understanding required to learn the specifics of how an organization conducts its mission and the time required to maneuver to those systems that enable that mission. These longer time commitments naturally cause the overall cost of operations to go up. The longer an actor must remain in a network, the more sophisticated their tools must be to stay undetected. Once a level 4 attack is executed, it will quickly be discovered by network defenders and the remedy will likely be straightforward. The effective downtime of the organization relies heavily on the extent of any physical damage and is further influenced by the scarcity of any specialized hardware required.

Level 5: Mission Manipulation

Definition. A cyber attack that specifically manipulates the systems or processes critical to an organization's mission without being detected

Description. Mission Manipulation is the most sophisticated and strategically complex cyber attack within the spectrum. Mission Manipulation allows for the repeated, sustained disruption of the fundamental mission of an organization. Level 5 attacks are identical to level 4 except for the critical fact that they are executed without being detected. This is a small distinction but is exceptionally difficult to achieve.

Example. The destruction of mission-critical systems and the manipulation required to hide those actions has only been demonstrated by one publicly disclosed cyber attack to date: Stuxnet. Extensively documented, Stuxnet is known for the physical destruction it inflicted on Iranian centrifuges from April 2009–June 2010.[14] Yet, the true brilliance of Stuxnet was its skillful deception of the end-users of these systems. Stuxnet systematically destroyed these mission-critical centrifuges while at the same time manipulating the monitoring components to tell the engineers they were functioning properly.

Because of the criticality of these centrifuges, the paired destruction and deception of Stuxnet disrupted the organization's ability to perform its primary mission and set back Iran's nuclear program a minimum of two years.[15] The attack exacerbated financial burdens and according to a report by the Center for Security Studies, "likely culminated in an overall feeling of insecurity throughout Iranian society."[16] Even after the discovery of Stuxnet, Iran was not able to fully trust their

systems—not knowing whether a failure was generated by human error or the actions of malicious code lurking in their systems.

Tradeoffs. Level 5 attacks require substantially more resources than any other level, both in time and human capital. Mission Manipulation is expected to require a combination of customized tools, in-depth knowledge, sophisticated cyber expertise, specialized engineering knowledge, and significant amounts of time. It requires time to gain network access, time to harvest information, time to develop tools, time to maneuver within the network, and time to execute. It was speculated that Stuxnet required the combined efforts of Israel and the United States[17]—two of the most technologically sophisticated nations in the world—a minimum of three years of preparation, a year of continuous execution, and an estimated $100 million dollars.[18]

The target knowledge, commitment, and technical expertise required to execute attacks at level 5 demands real-time development as the exact configurations and nuances of mission systems are almost impossible to know before accessing them. The skills and tools for such specialized or indigenous mission systems may be extremely hard to find, or may not exist, requiring them to be built from the ground up.

In spite of these heavy constraints, a level 5 attack has the ability to cause massive high-level impacts that rival the sophistication of any operation in the other warfare domains. It can single-handedly achieve strategic objectives through non-kinetic means, and importantly, allow for plausible deniability that reduces the risk of retaliation and conflict escalation. As seen in the Stuxnet example, the culmination of such high levels of investment can produce powerful effects that last for years.

Conclusions and Expansion

By defining the attributes and characteristics of attacks at each level within the Spectrum of Cyber Attack decision-makers are better positioned to understand and pursue strategic objectives. Strategic guidance can be succinctly delivered, and tactical tasks can be determined more rapidly. Moreover, this operational framework presents a clear roadmap for building out a menu of options that incrementally increases the required resources and effectiveness when engaging a target. Although each described level presented several examples, the creative opportunities within or between levels are largely unlimited—especially as this field of knowledge continues to expand.

While this framework was developed with offensive cyberspace operations in mind, there may also be ways it can be used in defensive cyberspace operations to interpret the intent and resources of an adversary's attack. The framework may

allow defenders to quickly triage the holistic threat to a network, not just the immediate threat to a single host, and allocate resources accordingly.

Additionally, operations using this framework could greatly benefit from a more thorough exploration of the possible psychological effects that could result from cyber attacks at each level. Since cyber operations are nonkinetic in nature, attacks leveraging psychological operations—particularly level 3 attacks—could have significant impacts on an adversary in ways kinetic attacks cannot. Using this framework as a prism, a focused examination of combined arms that uses both psychological and cyber operations could yield even more effective methods for influencing an adversary.

Overall, the Spectrum of Cyber Attack is a straightforward framework that works to bridge the gap between strategic doctrine and the appropriate tactical tasks pursued through offensive cyberspace operations. As this framework is adopted and further refined, the end-result will allow commanders and planners to pair desired end-states with the proper actions based on resource requirements and constraints. By understanding strategic objectives and aligning them with a given cyber-attack level, commanders can more effectively prosecute targets, produce desired strategic outcomes, and uniquely contribute to winning our nation's conflicts. ✪

Table. Estimated tradeoffs between cyber-attack levels

Level	Cost to execute	Preparation time	Likelihood of success	Impact duration	Severity of impact
1	$1K+	Days	High	Days	Low
2	$10K+	Weeks	Medium	Weeks	Medium
3	$50K+	Weeks	Medium	Years	Low
4	$100K+	Months	Low	Weeks	Medium
5	$1M+	Years	Low	Years	High

Key: K = thousand, M = Million

Maj David Musielewicz, USAF

Major Musielewicz (BS, USAFA; MS, Georgia Institute of Technology) is a combat mission team lead for US Cyber Command, Lackland AFB, Texas. With more than 300 missions and 2,100 hours on offensive cyber platforms, he previously served as a cyber-attack operator at the National Security Agency, Fort Meade, Maryland.

Notes

1. Ash Carter, "A Lasting Defeat: The Campaign to Destroy ISIS," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, October 2017, https://www.belfercenter.org/.

2. Mark Pomerleau, "What's in the $9.6B Cyber Budget Request?" *Fifth Domain*, 14 March 2019, https://www.fifthdomain.com/.

3. Joint Publication (JP) 3-12, Cyberspace Operations, 8 June 2018, II-7, https://www.jcs.mil/.

4. JP 3-12, *Cyberspace Operations*.

5. Justin Sherman, "Hijacking the Internet Is Far Too Easy," *Slate Magazine*, 16 November 2018, https://slate.com/; Brian Krebs, "A Deep Dive on the Recent Widespread DNS Hijacking Attacks," *Krebs on Security*, 18 February 2019, https://krebsonsecurity.com/; and Jon Porter, "Telegram Blames China for 'Powerful DDoS Attack' during Hong Kong Protests," *The Verge*, 13 June 2019, https://www.theverge.com/.

6. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired Magazine*, 22 August 2018, https://www.wired.com/.

7. Phil Muncaster, "WannaCry Cost NHS £92 Million," *Infosecurity Magazine*, 15 October 2018, https://www.infosecurity-magazine.com/; Zack Whittaker, "Atlanta Projected to Spend at Least $2.6 Million on Ransomware Recovery," *ZDNet*, 23 April 2018, https://www.zdnet.com/; and Sam Dean, "What Is Ryuk, the Malware Believed to Have Hit the Los Angeles Times?," *Los Angeles Times*, 1 January 2019, https://www.latimes.com/.

8. Sean Lyngaas, "Former NSA Chief: Data Manipulation an 'Emerging Art of War,'" *FCW: The Business of Federal Technology*, 22 October 2015, https://fcw.com/.

9. Kayleena Pierce-Bohen, "10 Technological Threats in Mr. Robot That Are Actually Real," *Screenrant*, 27 May 2019, https://screenrant.com/.

10. Kate O'Flaherty, "North Korean Hackers' $2 Billion Heist Is 'Funding WMD Programs,'" *Forbes Magazine*, 7 August 2019, https://www.forbes.com/.

11. Karl Etters, "Almost $500,000 Swiped in City of Tallahassee Payroll Hack," *Tallahassee Democrat*, 5 April 2019, https://www.tallahassee.com/.

12. Robert M. Lee, Michael J. Assante, and Tim Conway, "TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid," *SANS*, 18 March 2016, https://ics.sans.org/.

13. Darren Pauli, "Malware 'Clearly' behind Ukraine Power Outage, SANS Utility Expert Says," *The Register*, 15 January 2016, https://www.theregister.co.uk/.

14. Jim Finkle, "Factbox: Cyber Warfare Expert's Timeline for Iran Attack," Martin Howell, ed., *Thomson Reuters*, 2 December 2011, https://www.reuters.com/.

15. Yaakov Katz, "'Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years,'" *Jerusalem Post*, 15 December 2010, https://www.jpost.com/.

16. Marie Baezner and Patrice Robin, "Stuxnet," *ResearchGate, ETH Zurich*, 15 February 2018, https://www.researchgate.net/.

17. William J. Broad, John Markoff, and David E Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, 15 January 2011, https://www.nytimes.com/.

18. Finkle, "Factbox: Cyber Warfare Expert"; Dennis Fisher, "Cost of Doing APT Business Dropping," *Threatpost*, 6 February 2014, https://threatpost.com/.