Military Cyber Affairs

Volume 1 | Issue 1 Article 3

2015

Cyberspace Operations Planning: Operating a Technical Military Force beyond the Kinetic Domains

Don E. Barber
US Navy

T. Alan Bobo
US Air Force

Kevin P. Sturm
US Army Reserves, kevinpsturm@gmail.com

Cyberspace Operations Planning

Operating a Technical Military Force Beyond the Kinetic Domains

DON E. BARBER, United States Navy
T. ALAN BOBO, United States Air Force, Retired
KEVIN P. STURM, United States Army Reserve

Traditional military planning has matured over the centuries and provides a proven foundation to achieve specific objectives. Planning for operations in cyberspace, however, goes beyond what is typically required in planning for 'kinetic' military operations, employing munitions against physical targets. To capture the incredible nuance required to conduct cyber operations, it is useful to conceptualize a deeper, more technical level of warfare planning that illuminates the role of technical implementation that supports tactical planning. The technical details associated with cyberspace operations are not as intuitive to planners and commanders as the capabilities and limitations of tanks, ships, and aircraft. In cyberspace planning this additional technical level is required to translate impacts on non-intuitive components into readily understandable effects on adversary operations. Noting the importance of technical cyber planning, it nevertheless remains critically important to ensure that focused technical operations continue to clearly tie back to a commander's operational effect requirements and national strategic objectives. This paper attempts to capture the highlights of U.S. Joint military doctrine and incorporate best practices from the commercial sector to outline a process that the DoD's new cyber mission force could employ.

1. INTRODUCTION

As cyberspace continues to become increasingly integral to our way of life, threats from cyber criminals and nation state actors continue to grow ever more pervasive. We depend on computers in almost every aspect of our lives, from controlling our cars and communications, to maintaining our bank accounts and medical records, and even running public utilities. Like the broader population, our government and military also depend heavily on cyberspace to operate and communicate.

While networked computers offer tremendous opportunities for unprecedented collaboration, high speed processing, and big data analytics; time and again hackers have been able to find vulnerabilities to exploit these same systems to malicious ends. Malicious cyber activity runs the gamut, from stealing money, personal information, and intellectual property, to vindictively damaging systems and networks through denial of service attacks, to the possibility of damage to critical infrastructure. Hackers have attacked the financial sector across the spectrum from denial of service attacks on banks to stealing credit card data during point-of-sale transactions at major retailers.[1,2,3] Large, orchestrated attacks against a major casino and movie studio appear to be targeted attacks by nation states to achieve political objectives.[4,5] Ongoing theft of intellectual property, including details of a next generation military fighter aircraft, undermines national strategic investments.[6]

[1] Joseph Menn, "Cyber attacks against banks more severe than most realize," Reuters, May 18, 2013, http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518.
[2] Chris Isidore, "Target: Hacking Hit Up to 110 Million Customers," CNN, January 11, 2014, http://money.cnn.com/2014/01/10/news/companies/target-hacking.
[3] Shelly Banjo, "Home Depot Hackers Exposed 53 Million email addresses," Wall Street Journal, November 6, 2014, http://www.wsj.com/articles/home-depot-hackers-used-passwords-stolen-from-vendor-1415309282.
[4] Bill Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," Bloomberg, December 11, 2014, http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.
[5] Kim Zetter, "Sony Got Hacked Hard: What We Know and Don't Know So Far," Wired, December 3, 2014, http://www.wired.com/2014/12/sony-hack-what-we-know.
[6] Bill Gertz, "Top Gun takeover: Stolen F-35 secrets now showing up in China's Stealth Fighter," Washington Free Beacon, March 13, 2104, http://www.washingtontimes.com/news/2014/mar/13/f-35-secrets-now-showing-chinas-stealth-fighter.

1.1 The Department of Defense Strategy

As outlined in the recent 2015 Department of Defense (DoD) Cyber Strategy, the DoD plans to work in concert with other government agencies and international allies to counter these pervasive threats. The DoD's first goal is to protect its own networks, systems, and information. Their second mission is to be prepared to defend the U.S. and its interests against cyber-attacks of significant consequence, which "may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact .[7] To accomplish these goals, the DoD is investing in building a cyber mission force to provide resilience, deny attacks, and respond to cyber-attacks as directed.[8]

Military planning and operating concepts have matured over the centuries and provide a proven foundation for operating as a team to achieve objectives; so much so that countless books have applied military principles to business management. However, while a military organization must also tackle cyber threats to the nation in a deliberate and organized manner, the nuances of conducting operations in cyberspace go beyond what is typically required in planning for 'kinetic' military operations employing munitions against physical targets. This paper attempts to capture highlights of U.S. Joint military doctrine and incorporate "best practices" principles from the commercial sector to outline a process that the DoD's new cyber mission force could usefully employ.

1.2 Layers of Military Planning

The U.S. process of planning and employing military capabilities and countermeasures to deter, and ultimately defeat, aggression is captured in Joint Publications from the Joint Chiefs of Staff. Strategic guidance, coupled with those missions found in the DoD Cyber Strategy, is passed down the chain of command in campaign plans to allow operational planners to develop concepts of operations. Joint Publication 3-0 captures the relationship between strategic and operational art, linking tactical actions by military commanders to a strategic purpose, as articulated by the President and National Security Staff.[9] These gears are inextricably linked. Overarching strategic policy objectives steer the development of operational plans, while the resulting tactical outcomes provide feedback as they influence the larger strategic and operational environments. Leveraging this paradigm, cyber forces are structured in a military hierarchy to allow operational unity of effort, while maintaining proper planning division of labor at the strategic, operational, and tactical levels to accomplish the mission of defending the U.S. in cyberspace.

Cyber operations can be very complex, and it is useful to conceptualize a deeper, fourth technical level of warfare in order to conduct effective planning. Figure 1 illustrates the critical importance of properly incorporating technical aspects of cyber into the tactical planning phase. The technical details associated with cyberspace operations are not grasped as intuitively by planners and commanders as are the capabilities and limitations of tanks, ships, and aircraft. While advanced research and engineering are inherent in the development of modem military systems, they are "baked-in" before the platforms are provided to tactical commanders. The complex and dynamic nature of cyberspace often drives technical analysis and planning to a level beyond those planning practices and procedures accommodated by traditional Joint doctrine.

Noting the importance of technical cyber planning beyond traditional military planning, it remains critically important to work through the disciplined military hierarchy of planning to ensure focused technical operations continue to clearly tie back to national strategic objectives. It can be easy to lose the forest for the trees, or even leaves, if operations directors become fixated on nuanced technical operations without keeping sight of the desired end state.

---

[7] U.S. Department of Defense. DoD Cyber Strategy. (Washington, D.C.: Government Printing Office, April 17, 2015), 4.
[8] Ibid., 4-5.
[9] U.S. Joint Chiefs of Staff, "Joint Operations," Joint Publication 3-0. (Washington, D.C.: U.S. Joint Chiefs of Staff, August 11, 2011).

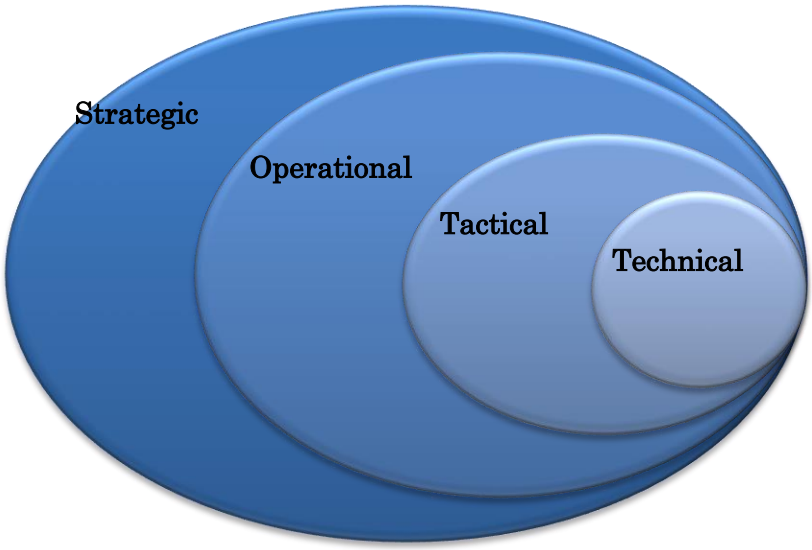

Fig. 1. Layers of Cyber Planning

2. OPERATIONAL PLANNING

In brief, operational planning decomposes the strategic objectives, such as preventing malicious cyber-attacks to critical U.S. networks, in order to identify adversary centers of gravity and potential vulnerabilities.[10] This process informs development of courses of action necessary to effectively impact those centers of gravity.

Joint Publication 5-0 illustrates the mission analysis process examining an exemplar adversary armored corps as the center of gravity within a larger army. One critical capability that supports the adversary armored corps is an integrated air defense system, protecting their tanks from attacks by aircraft. The air defense network itself requires radars, launchers, and command and control capabilities. Operational-level analysis identifies these critical capabilities and critical requirements to uncover critical vulnerabilities that can be targeted to significantly degrade the threat posed by the adversary. Rather than directly confronting the adversary's full supported army, it may be possible to first neutralize adversary enablers, such as radar or communications, to indirectly defeat the threat rather than attack it head on.[11]

In order to defend in cyberspace, a similar analysis of centers of gravity for malicious cyber actors is needed to identify and characterize the threat at the technical and granular level necessary to operationally implement the broad strategic guidance of 'protect DOD and other U.S. networks'. Similar to identifying the defeat of an armored corps as critical to defeating an attacking army, there may be specific hacker groups that are centers of gravity in malicious cyber activity targeting U.S. networks. Through the application of intelligence resources, operational level commanders will identify these functional groups to enable operational planners to study them and identify the requirements and vulnerabilities in the hacker's cyber-attack processes. As military air defense needs radar to target missiles, likewise, a hacker may require network mapping of their target to conduct targeted cyber-attacks as a critical requirement.

2.1 Kill Chains

Numerous academic and commercial efforts engaged in network defense have already created basic models of the lifecycle of a cyber attacker which can be leveraged as a baseline to help identify hackers' processes and requirements. One frequently used network security textbook provides six

[10] U.S. Joint Chiefs of Staff, "Joint Operation Planning," Joint Publication 5-0. (Washington, D.C.: U.S. Joint Chiefs of Staff, August 11, 2011), IV-4.
[11] Ibid.

phases of an attack: targeting, access/compromise, reconnaissance, lateral movement, data collection/exfiltration, and administration and maintenance.[12] In a 2015 trend report, a computer security firm outlined attacker techniques seen during recent point of sale compromises (including those mentioned in the introduction) as being composed of: initial compromise, establish foothold, escalate privileges, internal recon, move laterally, maintain persistence, and complete mission.[13] A major defense contractor proposed a similar "cyber kill chain" framework consisting of: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objective.[14] Even from just these three examples, we can see diverse organizations using the basic process of operational analysis to decompose cyber threats and the emergence of a relatively uniform set of critical requirements needed for any cyber attacker to carry out sophisticated attacks.

In 2013, the Chief of Naval Operations, ADM Jonathan Greenert, and Chief of Staff of the Air Force, General Mark Welsh began to publically discuss the concept of breaking the kill chain in a traditional military context to counter adversary threats.[15] As previously articulated by other works, breaking a function or even a single step within the adversary process can interrupt the entire process, requiring a restart or adaptation to be made in order for the adversary to continue.[16]

Thicker armor and point defense systems are very expensive and bring risk right to the defended platform in a conventional conflict as well as in cyberspace. Where it is possible, it is safer and more cost effective to stop the archer than the arrow. Also, whenever possible, it is preferable to work against earlier phases in the kill chain to disrupt processes like reconnaissance or initial compromise, as it preempts overall adversary functions and eliminates the need for point defense or remediation within the protected networks.

2.2 Targeting

Operational plans drive tactical planning analysis by identifying specific threat actors and functions that must be countered to achieve the strategic end state. Tactical level planning then specifies key processes through kill chain analysis that can be impacted to create the desired operational level effects. After critical processes in the kill chain are identified, further technical analysis identifies tangible component elements, which are critical to the processes and functions they support, that can be directly impacted through tactical level actions. In cyberspace, an additional level of technical planning, beyond traditional tactical military planning, is required to translate impacts on non-intuitive cyber components into readily understandable effects.

Identifying specific target elements that support the overall target systems, and in turn critical functions of the center of gravity, allows commanders to prioritize and assign forces to take actions to impact tangible target system elements. Joint Publication 3-60 provides an example of identifying targets in a notional adversary air defense system. A successful air defense system performs several functions in order to achieve its aims - a failure to complete one of these functions, like radar identification, launching intercept aircraft, or firing surface to air missiles will likely result in the overall failure of the system. In order to affect an air defense target system, planners assess the component processes supporting those air defense functions that can be affected with the resources available and that will have the most significant impact on the overall target system.

---

[12] Stewart McClure, Joel Scambray, and George Kurtz, Hacking Exposed 7: Network Security Secrets and Solutions. (New York: McGraw-Hill, 2012), 316-317.
[13] "M-Trends 2015: A View from the Front Lines", Mandiant, 2015, http://www2.fireeye.com/rs/fireeye/i mages/rpt-m-trends-2015.pdf.
[14] Eric Hutchins, Michael Cloppert, and Rohan Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns, and Intrusion Kill Chains," Leading Issues in Information Warfare and Security Research (2011).
[15] Jonathan Greenert and Mark Welsh, "Breaking the Kill-chain: How to keep America in the game when our enemies are trying to shut us out," Foreign Policy, May 17 2013.
[16] Hutchin, Cloppert, and Amin, 4.

Continuing our example, consider an airfield. Airfields are a component of an air defense system, but their value lies in the function that they perform for the overall air defense system - providing a nearby launching point for intercept aircraft. An airfield, in turn, is composed of numerous elements that allow it to perform its function, and specific physical attributes (instantiations) that affect how it can be engaged. Some specific instantiations include the overall dispersion of the operations area, the hardness of concrete on the runways, and the vulnerability of combustible fuel depots. Planners consider these specifics when assessing how the airfield can be impacted. By impacting elements that support adversary processes, the overall components are degraded. With sufficient impacts to components, the functions that support the adversary processes, and ultimately the adversary system itself, can be stopped.[17]

Returning to countering cyberspace adversaries, it is important to operationally assess the hackers and cyber threats across their entire kill chain to identify potential functions that can be impacted through critical components and elements where an attack could be stopped during reconnaissance, exploitation, or any other phase. Like the kinetic example, preempting adversary exploitation efforts during earlier steps in the kill chain will likely be more cost effective and lower risk than trying to combat every cyber-attack as it comes – effectively swatting at arrows.

However, as with the kinetic military examples, trying to counter some early foundational activities supporting the kill chain may induce significant collateral effects while still not stopping a committed adversary. Like trying to preempt adversary air defense by targeting oil wells and refineries, attempting to stop hackers by causing ISPs to stop all traffic from large areas would likely be an affront to international norms and might only be feasible in extreme situations requiring necessary authorities.

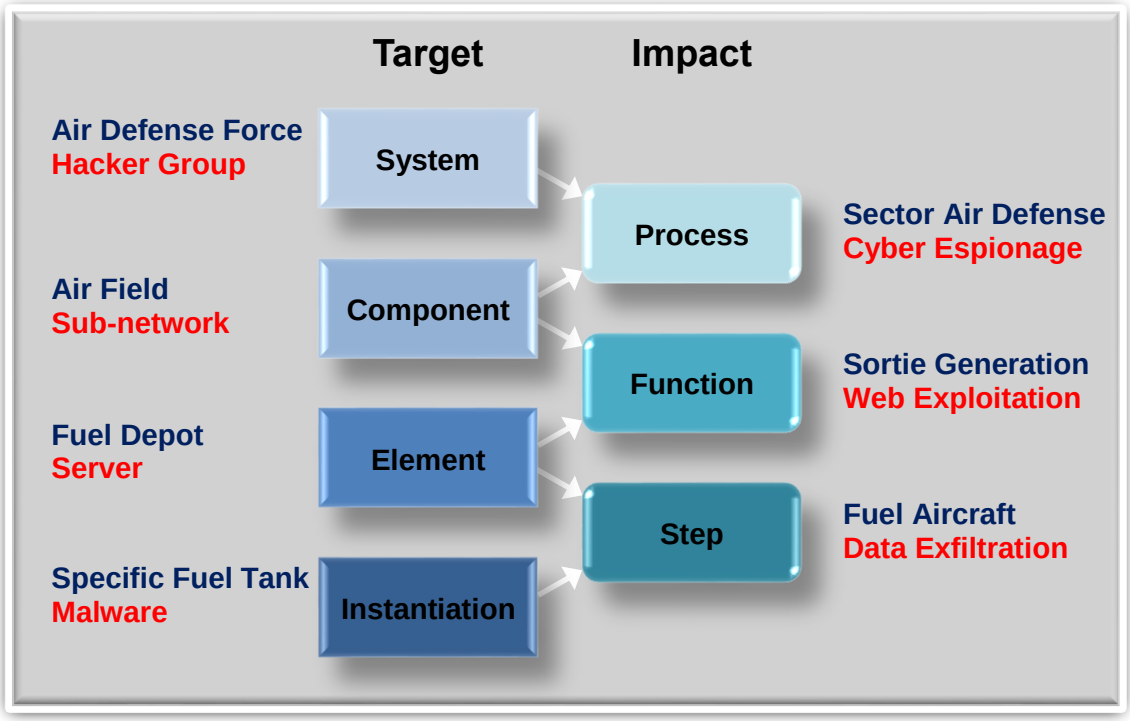

Fig. 2. Example Target System Components And Elements

[17] U.S. Joint Chiefs of Staff, "Joint Targeting," Joint Publication 3-60. (Washington, D.C.: U.S. Joint Chiefs of Staff, January 31, 2013).

2.3 Brass Bullets

While acting earlier in the kill chain can be more effective, it is apparent that extreme actions affecting bystanders are neither appropriate nor effective. Rather than a single 'silver bullet' solution to cyber threats, a collection of constrained effects against target system elements is needed. In aggregate, a planned implementation of these 'brass bullets' can achieve the intended effect, either a denial or manipulation of the targeted functions.

To counter an adversary air defense system like the example, targeting only a single component is unlikely to succeed.[18] However, degrading multiple components, like the radar system and airfields, increases the likelihood of having a significant aggregate effect against adversary air defense functions. In order to delay and disrupt airfield operations, numerous elements of an airfield could be impacted that in sum significantly degrade the airfield's operation.

The planning and targeting process begins with assumptions and continues to refine an understanding of the adversary's composition and processes through observation and intelligence. By studying how the adversary operates, it is possible to identify its critical requirements and vulnerabilities. Ultimately, by targeting significant critical requirements via associated vulnerabilities, impacts are generated against target components, degrading those adversary functions that threaten allied strategic goals.

In order to conduct cyber operations planning, operational planners study the cyber threat in the context of a kill chain framework across the three layers of cyberspace (physical, logical, and persona), to identify target system components, perhaps specific hacker sub-networks, to counter.[19] Studying malicious cyber activity can identify elements within target components, such as malware or bots, making it possible to counter them. At this point in planning traditional military operations, specific aim points, like a building or server, are impacted by employing ordnance against them. However, in planning cyber operations, there remains yet another iteration of intelligence gathering and planning to be accomplished in order to non-kinetically deter or defeat a cyber-attack through cyberspace.

3. TECHNICAL OPERATIONS

A cyber threat target system element, such as a malicious executable, network control device, or database of hacker targets may be identified as one of several critical elements that could be impacted to diminish the overall cyber threat from a hacker group. The nuanced specifics related to software versions and threat network configurations must be accounted for when planning to impact them. Rather than simply engage an airfield or its fuel depots, this level of exquisitely detailed targeting is analogous to targeting specific rivets in the fuel tanks, well beyond the traditional tactical planning analogy.

At this technical level of planning, understanding specifically how malicious code propagates through victim networks, escalates privileges, and exfiltrates data creates a need for frequent rediscovery. Cyberspace morphs and develops at a pace exceeding conventional military analog. While militaries face an ongoing evolution of attack and defense capabilities over an arc of months to years, new variants of malicious code emerge daily. While the physical terrain of a battlefield is static, changes to logical networks can shift topology of cyberspace terrain almost instantly. Tactical planning identifying nodes as key target system elements alone is not enough; detailed technical data must be gathered continuously to stay abreast of dynamic components and their attributes, as well as to properly attribute the activity of those components to the correct sponsor. This data is complex, ever-changing, and will require a dynamic database environment to ensure that it is secured and organized logically. Access to this information will be critical for technical level planners to ensure that cyberspace capabilities at their disposal are appropriately matched to the environment that they

[18] U.S. Joint Chiefs of Staff, "Cyberspace Operations," Joint Publication 3-12(R). (Washington, D.C.: U.S. Joint Chiefs of Staff, February 3, 2015), ch 2.
[19] Ibid.

will be employed in, while an operational planner may only be concerned with the sum of impacts on adversary functions. Appropriate amounts of information on the component elements and proposed impacts must be coordinated through the tactical level to ensure overall alignment with the commander's intent.

The rapidly changing cyber environment challenges deliberate planning and, in fact, necessitates, at times, a continuous planning effort. Fortunately, planning at the target system level can proceed at a pace similar to traditional military planning, but it becomes critically important to select the right adversary requirements and vulnerabilities to target to allow technical operations to track and action cyber threat elements.

3.1 Implementation

While specifically proposing how DoD cyber forces might take actions against adversary cyber target systems is beyond the scope of this paper, it is easy to appreciate how critical the concept of threat decomposition and 'brass bullet' solutions are to cyberspace operations. While there is a broad range of cyber threats, from script kiddies to hacktivist groups to nation state actors, network defenders must make resource investment decisions to prioritize their focus based on a strategic end state.[20] Once focus areas have been determined, either specific threat actors or types of cyber-attacks, a deliberate framework is needed to study the life cycle of an attack. Once a threat's functions, requirements and vulnerabilities are identified, plans are developed to target the supporting components of the kill chain.

However, no single solution alone is likely to provide a robust response capability against a dynamic threat. Continual intelligence collection and detailed analysis is required. In no other endeavor is timely and accurate intelligence of such critical importance.[21] A virus signature today may defeat an element of a threat's exploitation, but new or modified Trojans require development of new signatures. Blocking a malicious IP addresses may break an instantiation of a cyber threat's initial access, but a hacker could rapidly move to another IP range. In order to effectively defend against threats, it will be necessary to engage at multiple points along the kill chain so that the aggregate degradation of the threat allows an assured availability of protected networks and systems. By engaging multiple target system elements even when some change, other can still be preempted, preventing a full on cyber-attack.

4. CONCLUSION

The military planning process is composed of deliberate steps that begin with the strategic ends in mind to shape plans and operations that force adversary threats to that desired end state. Analysis of components and elements of target systems identifies where forces can exert effects to disrupt the target system's function. Activities across the spectrum of operations from strategic to tactical are interdependently linked through feedback from actions at each level. This same process holds true in the cyberspace domain, with the addition of a nested level of technical planning and operations that translates between non-intuitive component-level impacts and readily understandable effects.

BIOGRAPHIES

LCDR Barber is a naval officer with over a decade of technical and planning expertise. He is a graduate of the United States Naval Academy and Naval Postgraduate School, with a focus of study on electronic communication networks. He holds a professional project management certification and his military experience consists of multiple leadership tours at home and abroad, including work in D.C. and the Middle East.

Mr. Bobo retired from the US Air Force after 20 years of planning, conducting, and teaching computer network operations in a Joint environment. He has a Master’s degree in Electrical

[20] P.W. Singer and Allan Friedman, Cyber Security and Cyber War: What Everyone Needs to Know. (Oxford: Oxford University Press, 2014), 68.
[21] Martin C. Libicki, Cyber Deterrence and Cyberwar. (Santa Monica: RAND Corporation, 2009), 330.

Engineering with an emphasis in network design from the Air Force Institute of Technology and now works as a cyberspace operations planner for the U.S. Government. His experience includes operations in Iraq, Afghanistan, and Kosovo in both an operational and planning capacity.

MAJ Sturm is an Army Reserve Officer and Department of the Army Civilian who has served in a wide variety of assignments spanning across tactical and strategic levels overseas and stateside, with a focus on operational planning and analysis. His Master's degree focused on cyberspace operations in a strategic context.

DOI: http://dx.doi.org/10.5038/2378-0789.1.1.1003