I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

# Cyberspace Is Not a Warfighting Domain

MARTIN C. LIBICKI*

> Like everyone else who is or has been in a US military uniform, I think of cyber as a domain. It is now enshrined in doctrine: land, sea, air, space, cyber. It trips off the tongue, and frankly I have found the concept liberating when I think about operationalizing this domain. But the other domains are natural, created by God, and this one is the creation of man. Man can actually change this geography, and anything that happens there actually creates a change in someone's physical space. Are these differences important enough for us to rethink our doctrine?
>
> General Michael V. Hayden,
> USAF, Retired[1]

In the beginning was the land domain; with the discovery of flotation came the sea domain. A century ago, the air domain was added to the list; a half-century ago, the space domain was added as well. Within the last quarter-century, the combination of ubiquitous networking and universal digitization has given rise to cyberspace, the newest addition to the growing family of domains.[2] Cyberspace, we are

---

* Martin Libicki is a senior management scientist at the RAND Corporation. His research focuses on the impacts of information technology on domestic and national security. Libicki recievied his Ph.D. in economics and M.A. in city and regional planning from the University of California, Berkeley, and his S.B. in mathematics from the Massachusetts Institute of Technology.

[1] Michael V. Hayden, The Future of Things "Cyber," 5 STRATEGIC STUD. Q. 3, 4 (2011), *available at* http://http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf.

[2] By contrast with cyberspace, which is considered a domain and which, as a domain, is headed by a full general, radio-frequency spectrum, the control over which nations have sparred over since 1940, is not considered a domain. Even through far more money is spent on electronic warfare equipment than in cyberwar equipment, in no Service does the

told, pervades the other domains in the sense that warfighters in each of the prior domains would be severely handicapped if their access to cyberspace were successfully challenged. Thus understood, cyberspace has become the new high ground of warfare, the one domain to rule them all and in the ether bind them, which, as this essay will argue, is the wrong way to view cyberspace and what militaries can do by operating "within" it.

Whether cyberspace does or does not have the essence of a warfighting domain as per some platonic ideal is not at issue. Instead, this essay contends that understanding cyberspace as a warfighting domain is not helpful when it comes to understanding what can and should be done to defend and attack networked systems. To the extent that such a characterization leads strategists and operators to presumptions or conclusions that are not derived from observation and experience, this characterization may well mislead. In other words, connotations rather than denotations are the problem. The argument that cyberspace is a warfighting domain, only a really different one, begets the question of what purpose is served by calling cyberspace a domain in the first place. Our purpose is, therefore, akin to what our ancient Chinese friends would have called the rectification of terms: making the name of the thing match the nature of the thing.

To do this, I first characterize cyber operations and their tenuous relationship to cyberspace. Next, I examine how warfighting describes the set of tasks necessary to defend or, alternatively, offend networked information systems. Lastly, I describe some of the conceptual errors that may arise by thinking of cyberspace as a warfighting domain analogous to the traditional warfighting domains.

## I. FROM WHENCE CYBER OPERATIONS?

The networked systems used by countries and their militaries are designed to carry out the commands of their owner-operators. Whose orders these systems actually carry out, however, depend not on their design, but upon the code that reifies their design.[3] As a rule, the

person whose primary mission is to command electronic warriors rank higher than a brigadier general.

[3] It is possible to carry out cyber attacks by subverting not the code but the users. An authorized user can be a spy/saboteur or be persuaded to do the wrong thing using social engineering. From a system perspective, however, most users are clients. Good engineering practices would limit the damage that can be done to servers by the actions of rogue client machines, but the servers into which such principles are encoded may themselves have vulnerabilities, hence returning to the issue of code as a primary issue.

systems' code and design conform almost perfectly, but in the term "almost" lies the entire basis for offensive cyber operations. Information systems are complex and, in their complexity, there can often be minute cracks, no more than a bitstream wide, that hackers can take advantage of by issuing commands to systems to which they have no rights. These minute cracks are vulnerabilities; they are invariably specific and can usually be patched once discovered and understood. By depending on information systems to supply us the right information or to command machines, we rely on their correct performance, but this assumption is not always correct, particularly when such systems are under pressure.

Offensive cyber operations attempt to exploit such vulnerabilities to create effects that interfere with the ability of their victims to carry out military or other tasks, such as production. As a rule, the more these tasks require correct working of the systems, the greater the potential for disruption or corruption that can be wreaked by others. Similarly, the more widely connected the information systems, the larger the population of those who can access such systems to wreak such havoc. Conversely, the tighter the control of information going into or leaving information systems, the lower the risk from the threat. Stated more broadly, the sounder the security design of an information system, the lower its susceptibility to such threats, the faster such threats can be recognized, the easier they can be thwarted, the less the damage, and the faster the recovery. Ultimately, the ability to carry out offensive cyber operations is a direct function of the weakness of the target system—something that cannot be said for, say, cities threatened by nuclear weapons. To be sure, clever hackers can do more damage than mediocre ones—but a large part of their skill set rests on the ability to discover and discern how to exploit these vulnerabilities,[4] if they exist in the first place.

What is there about such effects that necessarily describe a medium of combat? The answer is empirical: the most common way of accessing one information system is to take advantage of the fact that systems are typically connected to other information systems, and ultimately to all information systems, usually through the Internet. The Internet is basically tantamount to cyberspace; everything

Why???

[4] To wit, those who discover a vulnerability can usually generate the tools required to exploit it—but a set of tools without the requisite vulnerabilities is not particularly useful. A similar point is made about nuclear bomb making—no state that has the requisite fissile material has failed to figure out how to make a bomb from what it has. *See* Peter D. Zimmerman, *Proliferation: Bronze Medal Technology Is Enough*, 38 ORBIS 67, 75–78 (1994).

If one can discover a vulnerability, one has the capacity to exploit it. Really?

connected to the Internet is connected to cyberspace and, therefore, part of cyberspace. The connection even extends to systems where the connection is intermittent and asynchronous—the best example being how bytes can be inserted into and extracted from supposedly closed systems, such as those that run Iran's centrifuges at Natanz or the Department of Defense's (DoD's) SIPRNET, using removable media, such as USB drives.

Internet connectivity is an epiphenomenon of system attack, but there are other ways to introduce errors into computer systems. An authorized user could be a foreign agent. A special forces operator could gain illicit access to a system and command it for long enough to make it err. The system may contain rogue logic components that create certain types of errors based on particular circumstances (e.g., if the radar sees a U.S. warplane, a circuit in the radar instructs the screen not to show anything). A message sent over a short-range, point-to-point radio-frequency connection could be overwritten by a long-range, high-power signal from outside the supposed perimeter. None of these methods require cyberspace to work, but they can create the same effects. Nevertheless, operating through cyberspace is the preferred method of entry for reasons of economy, certainty, and risk.

## II. CYBERSPACE, THE MALLEABLE MEDIUM

It is one thing to recognize that the ability of advanced militaries to carry out missions in the four physical domains requires that they alone can command their systems. It is another to conflate the epiphenomenon of Internet-connectivity of such military systems with the proposition that cyberspace is a military medium subject to the tenets of warfare that exist in the other physical media.

Everyone concedes that cyberspace is man-made. This is what makes it different from its predecessors. Most then proceed as if the difference between a natural and a man-made combat medium is of no greater importance than the difference between natural and man-made fibers. But it is not the man-made nature of cyberspace that makes it different. Cities are man-made, but city combat shares many of the rules of country combat. What matters is that cyberspace is highly malleable by its owners, hence its defenders, in ways other media are not. Cities, although man-made, are not particularly malleable (at least not by those defending them).

How malleable is cyberspace? In the commercial world, there are many givens: the overwhelming majority of all machines run some version of Microsoft Windows; most software products are dominated

by a handful of firms, often just one; communications with the outside world have to use various protocols of the Internet suite (e.g., TCP/IP, the Border Gateway Protocol); and major communications companies transmit most of the traffic over what are, in the short run, fixed hardware infrastructures. This still leaves a great deal of discretion for the average user, even in the short run: which systems are connected to the outside; what is accessible through systems so connected; what provisions are made for back-up or process validation; how networks are managed and secured (including which products and services are purchased); where encryption and digital signatures are used; how user and administrator identities are authenticated; how such individuals are vetted for their responsibilities; what version of software is used and how diligently its security is maintained; what security settings are applied to such software (and who gets to change them); how personnel are vetted; and so on.

In the slightly longer run, radically better system architectures and ecologies are possible. Take Apple's iPad. Little, if any, malware has been written for it.[5] Why? The iPad operating system will only run software acquired through Apple's iStore and such offerings are vetted and never anonymous. Thus, while apps are not foolproof, they are small, not resident (because iPads do not support multitasking, few apps are on all the time), and much less likely than web pages to deliberately become sources of malware (unfortunately, apps can be quite nosy.) The iPad version of the Safari web browser limits plug-ins (most famously, Adobe's Flash player) and web downloads. The iPad's apps tend to be much simpler than those designed for personal computers. The iPad also shuts down (but in a state-full way) when not in use, thereby flushing memory-resident processes. It is unclear how robust the iPad model is for general-purpose computing (its apps come with far fewer user-set options than PC applications and heavyweight database processes, for instance, have little presence on the iPad). Yet the iPad demonstrates how alternative architectures may radically change the security equation.

The U.S. military has a real need to shape its information systems. Unlike most of us, it faces more competent, potentially serious foes

[5] As of April, 2012 there has been no known malware for systems built with Apple's iOS5, which runs not only the iPad, but the iPhone and the iPod touch. Yes, the iPad itself is new, but 25 million had been sold by mid-2011. Sam Costello, *What Are iPad Sales All Time?*, ABOUT.COM, http://ipod.about.com/od/ipadmodelsandterms/f/ipad-sales-to-date.htm (last visited Apr. 9, 2012). Furthermore, the same generalizations apply to the iPod Touch and the iPhone which use the same operating system and which all together have sold over 250 million units. Charles Jade, *iPod Touch Now Outselling iPhone*, GIGAOM, Jan. 28, 2010, http://gigaom.com/apple/ipod-touch-now-outselling-iphone.

with a clear interest in preventing its operations from working, particularly while fighting a war, when its capabilities are most important. Foes are more than willing to penetrate the military's computers to do so. Thus, the DoD should be and is willing to make tradeoffs that ensure its systems do as they are told even if doing so makes systems somewhat costlier and more inconvenient. Many of its systems are air-gapped, that is, with no electronic links to other networks.[6] Encryption is widespread, particularly on RF links, which characterize communications among warfighting platforms. The DoD imposes many restrictions on what its users can do; access, for instance, requires a Common Access Card (CAC). The DoD has its own Internet domain and runs its own domain-name server. It has acquired most of the source code for Microsoft Windows so that it can understand, and in some cases alter, its security features. It vets users tightly. It operates a complex system of document security (classification). It has hired some of the world's smartest people in information security, many of whom work for the National Security Agency (NSA). In sum, the DoD has even more scope to shape its share of cyberspace than most organizations do and uses this discretion vigorously. In other words, its cyberspace is definitely malleable. Unlike the physical domains, cyberspace is not a given environment within which the DoD must maneuver on the same basis with its foes. Indeed, the task in defending the network is not so much to maneuver better or apply more firepower in cyberspace but to change the particular features of one's own portion of cyberspace itself so that it is less tolerant of attack.

## III. CYBERSPACE AS MULTIPLE MEDIA

The use of "its cyberspace" when discussing the DoD suggests another feature of cyberspace—it is not a single medium as, say, outer space. Cyberspace consists of multiple media—at the very least, yours, theirs, and everyone else's. Each of these media often contains sub-media. Your cyberwarriors are trying to get into their cyberspace as a way of getting their systems to misbehave and theirs are trying to get into yours for the same reason. The question of who controls the

[6] Air-gapping is no panacea. (What is?) To be perfect, air-gapping has to exclude removable media, intermittent connections (*e.g.*, for software updating), and stray RF signaling. Even then, an air gap can be defeated by those willing to penetrate physical security perimeters or by the insertion of rogue components. But efforts to penetrate air-gapped systems are costly and do not scale well.

public share of cyberspace, while important, is usually ancillary to the ability of each military to carry out operations.

The extent to which our adversaries' systems are an undifferentiated subset of the greater Internet, and thus of public cyberspace, varies. As a rule, the more sophisticated and well-financed the adversary, the more it maintains its own communications links. In any case, connectivity among mobile units has to use a different architecture than the land-line Internet. Conversely, the less sophisticated and well-financed the adversary, the less likely it is to be able to afford the kind of networking upon which the United States and comparable militaries have grown so dependent. Countries are either too technically sophisticated to allow the systems on which they depend to rely heavily on the Internet or countries lack the technological sophistication to afford the systems upon which their warfighting would depend. In other words, the ability to command or at least to confound the Internet of foreign countries is likely to be of modest *military* value. This is far from saying that such countries are impervious to operations against their systems. It does mean, however, that carrying out such operations requires playing in *their* corner of cyberspace and they too have considerable scope to shape what they become dependent upon—cyberspace is not a given for them either.

What about this broad cyberspace in the middle—is it worth trying to dominate or preventing others from dominating? To some extent, it is. Cyberspace operations can keep a state's leaders from communicating with its population easily, as Russia's operations did against Georgia in 2008. It can make life uncomfortable for citizens of another state, as the operations of Russia against Estonia did in 2007. The ability to interpose messages into media can have psychological effects. The ability to take down web sites (e.g., Jihadist sites) can complicate recruitment efforts. Interfering with services from, for example electric and transportation utilities or maintenance organizations, can reduce the support that militaries receive from them. But these operations are carried out, not so much against cyberspace which is to say the Internet per se, as against systems connected by cyberspace to the rest of the world. Such systems, and to some extent their connections, are themselves malleable. Thus, Estonia reduced its vulnerability by having Akamai redo its network architecture and Georgia did similarly by having U.S. companies, such as Google and Tulip, re-host their web sites. Power companies do not have to be vulnerable to hackers; they can air-gap their generation, transmission, and distribution systems in advance. If they feel the consequences of their failures to do so beforehand, they can correct matters afterwards, albeit not instantly. Maintenance activities for the

electric grid companies can adopt back-up methods (e.g., phones and modems, VSATs) so that they can continue to serve their customers should the need arise. Trying to control the Internet in order to interfere with civilian activities may contribute to an overall warfighting effort, but, as a general rule, what lies on the civilian Internet is usually secondary to how physical wars are fought.

We are left to conclude that in great contrast to other domains, cyberspace is composed of multiple media and is malleable in ways that advantage its various owner-operators.

## IV. DEFEND THE DOMAIN OR ASSURE MISSIONS?

Thinking of cyberspace as a warfighting domain tends to convert the problems associated with operating in cyberspace—creating useful effects in your adversaries' systems and preventing the same from being done to you—into a warfighting mold shaped by the four older domains. This shifts the focus of thought from the creation and prevention of specific effects to broader warfighting concepts, such as control, maneuver, and superiority. This approach emphasizes the normal attributes of military operations, such as mass, speed, synchronization, fires, command-and-control, and hierarchy, at the expense of other ways, such as engineering, as a way of creating or preventing effects.

Start with the problem of preventing effects arising from mis-instructed systems, often understood as "defending networks." As noted earlier, such a task might otherwise be understood as an engineering task—how to prevent errant orders from making systems misbehave. One need look no further than Nancy Leveson's *Safeware* to understand that the problem of keeping systems under control in the face of bad commands is a part of a more general problem of safety engineering,[7] a close cousin of security engineering as Ross Anderson's classic of the same name expounds.[8] *Safeware*, incidentally, has no mention of militaries or military metaphors.[9] *Security Engineering* rarely discusses military matters and much of what it does cover is the safe command and control of nuclear

---

[7] NANCY G. LEVESON, SAFEWARE: SYSTEM SAFETY AND COMPUTERS (1995).

[8] ROSS ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS (2d ed. 2008).

[9] LEVESON, *supra* note 7.

weapons.[10] Together with engineering, one could add the related disciplines of architecture (how the various parts fit together influences how faults echo throughout a larger system), administration, and policymaking (how to make intelligent tradeoffs between values such as security on the one hand and cost and convenience on the other). For systems so complex that predicting what they do by analyzing their components is difficult, warding off unwanted effects may also call on the talents of a scientist used to dealing with complexity theory.

Granted, there may well be ways of managing networks which require activities that may be likened to warfare. Even well-designed systems have to be tended to constantly. (Indeed, well-designed systems facilitate such management.) Systems managers may even be lucky enough to see incoming or circulating malware and intervene to limit its malign effects by isolating and neutralizing it. In other words, there may be something worthwhile about having warriors "live in the network." But is such a reactive ability important compared to systems engineering or is it simply something to be emphasized in order to make network defense look like warfighting? Perhaps another analogy may be illuminating. If illegal migrants entered the United States in large gangs, forcing their way past border guards, a military response to their penetration attempts may be appropriate. As it is, illegal migrants enter this country using guile by sneaking across lightly guarded terrain or by overstaying their visas. Staunching their flow is rightly seen as a police problem. Similarly, the problem of bad bytes traversing borders is not a matter of force but guile and the military metaphor just does not fit.

The same question may be asked of certain aspects of "active defense."[11] Cyber warriors want to take the fight to the enemy by finding, targeting, and disabling the servers from which the intrusions came. This is probably not a bad idea if foes lack the care or sophistication to launch an attack in other ways, for example by using fire-and-forget weapons (Stuxnet[12]) or by operating from multiple

---

[10] ANDERSON, *supra* note 8.

[11] "Active defense" comprises a large number of defensive activities which are "active" in the sense of doing something other than waiting for the detection of malware or an intrusion before acting. One component, for instance, is the collection of malware signatures from the outside to constantly upgrade the list of material whose ingestion is forbidden.

[12] Stuxnet was a worm that infected and likely destroyed uranium centrifuges in Iran's Natanz facility. Once released, it carried instructions on how to destroy such centrifuges without requiring further human command.

servers up to and including peer-to-peer networks of bots. Against better foes, search and disable missions are likely to be much less productive. Here, again, the conventional imagery of cyberspace as a warfighting domain distorts how cyber operations are understood.

More broadly, the emphasis on defending the domain puts the information assurance cart before the mission assurance horse. Militaries adopt networked systems in order to facilitate kinetic operations. Adversaries target these networks in order to neutralize the help that networked systems provide to operations or, even worse, to exploit the dependence on such systems to render militaries less effective than if they had never adopted network systems at all. Information assurance refers to how militaries minimize such a threat, but what these militaries really need is mission assurance. A large component of mission assurance is being able to carry out operations in an environment in which the enemy has penetrated their networks. This component requires understanding the relationship of operations to information flows and adjusting accordingly in order to manage risk. It also includes training to ensure that warfighters can function in an environment where networks are occasionally unavailable and information from a single source is not always trustworthy. But if cyberspace is viewed as a domain that needs to be mastered by warfighting, the subsidiary nature of this domain to kinetic operations is lost and the emphasis shifts to achieving control in this domain for its own sake rather than understanding exactly why such control was needed in the first place.

## V. UNDERSTANDING WHAT IT TAKES FOR OFFENSIVE OPERATIONS

If understanding cyberspace as a warfighting domain is a poor way to approach mission assurance, might it nevertheless be a good way to understand *offensive* cyber operations? At first glance, yes. Envision teams of cyber warriors entering the networked systems of adversaries—controlling, disrupting, and corrupting as they go.

However, at second glance, not quite. The metaphor of warfighters living in cyberspace is exactly that, a metaphor. In practice, a great deal of what offensive cyber warriors do is reconnaissance, or exploration; in no other military endeavor is intelligence so integral to warfighting. But the nature of the reconnaissance is not simply to observe and report. The real purpose of cyberspace reconnaissance has a more scientific bent—to examine a logical structure and determine its flaws, either by observation or by experimentation. As it is, the relationship between reconnaissance and operations in cyberspace has changed a great deal in the last dozen years and may

change yet again. In the late 1990s, the act of exploration consisted of lone hackers getting past barriers and interacting in real-time with the target system. In that respect, it was much like special operations. These days, the entry point is more likely to be some malware that has been downloaded by some client. (A half-dozen years ago, servers were a more logical entry point than they seem to be today.) Offensive cyber warriors then communicate to the target system via the malware. The center of gravity of such an operation is the act of determining the target system's vulnerabilities and creating a tool embodied in malware to exploit them. In a sense, if defensive cyberwar is largely a question of engineering systems to make them resistant to attacks, then offensive cyberwar is reverse-engineering target systems to understand how they may be vulnerable to attacks. All this dynamism further argues against trying to force-fit cyber operations into any mold, not the least of which is domain dominance. None of these is alien to warfighting, but they do have different rhythms.

Such rhythms necessarily derive from the unique nature of cyberspace. A key characteristic of offensive cyberspace operations is that most of them are hard to repeat; once the target understands what has happened to its system in the wake of an attack, the target can often understand how its system was penetrated and close the hole that let the attack happen. Even if it cannot find the hole, the target learns where its system is vulnerable and may rethink the accessibility or trustworthiness of its system. The strong likelihood that targets of cyberwar will make such adjustments suggests that offensive cyber operations may be front-loaded over the course of a campaign. The use of offensive operations against a naïve target set is likely to be considerably more effective than against the harder target set several weeks later. This is not so characteristic of other warfighting domains which retain their importance throughout a campaign.

Indeed, one can characterize offensive cyber operations as a set of carefully prepared one-offs that have a well-defined role to play as niche operations in certain phases of a conflict. Stuxnet could be described that way. But such a characterization ill fits the notion of cyberspace as a continuous warfighting domain in the same way as land, sea, air, and space.

How does that relate with the Clausewitzian contention that war is "war does not consist of a single instantaneous blow." (Book 1, chapt. 8)

Finally, focusing on cyberspace as a domain suggests that cyber warriors be organized the same as warriors in other domains. Using/Implementing a division of authority in which the enlisted greatly outnumber officers (typically by more than four-to-one) implies converting cyber warfare into a set of operations in which most elements can be broken down into routines and taught to people

who are well-trained but not extensively educated. The wiser alternative is to determine what skill mix the domain requires, then recruit and train appropriately without worrying too much about whether the resulting hierarchy characterizes what are understood to be warfare domains.

## VI. OTHER MISBEGOTTEN CONCEPTS FROM CALLING CYBERSPACE A WARFIGHTING DOMAIN

Calling cyberspace a warfighting domain also promotes the urge to force-draft warfighting concepts from the earlier domains of land, sea, and air,[13] which may be required because everyone in the field, particularly at the senior officer level, started in a service dedicated to a historic domain and came equipped with frameworks that can be used to shape how cyberspace is understood.

Perhaps the most pernicious concept is the notion of domain superiority—the notion that power in a domain can prevent adversaries from doing anything useful in it. In the air or seas, whoever's fleet can keep the other from taking off or leaving port has achieved superiority. But, as argued, cyberspace is not unitary. In a war of two sides, there are at least three sub-domains: mine, yours, and, least relevant for warfighting, everyone else's. The best hackers in the world can do little to interfere with a truly air-gapped network of their adversaries. Enough said.

Notions of cyberspace as a high ground whose dominance presages the dominance of all other domains are similarly meaningless. The ability to get useful work done with one's systems and make it difficult for adversaries to do likewise is helpful, but only instrumental. The traditional, and partially obsolete metaphor, that air control means I can hit you *and* you cannot hit me is not even close to an accurate précis of what competent cyber warriors permit.

Other misleading metaphors come from ground warfare. For example, take "key terrain." True, in any network some physical nodes and services are more important than others. But offensive cyberspace operations generally cannot break physical nodes and the services

---

[13] Why not outerspace? Fortunately for warfighters in that domain, it has yet to produce its first Clausewitz, Mahan, or Douhet. Although many have tried, all have thankfully failed to achieve such conceptual heights. Part of the problem is that the physics of orbital mechanics are so daunting, and the art of the possible is quite constrained. Despite the recurrent urge felt among space warriors that their instruments should be designed for combat amongst each other, satellites are entirely used to support the terrestrial campaign, so far at least.

provided by networks can be and are increasingly virtualized. The very plasticity and malleability of software makes gaining the "possession" of key terrain an empty victory. Or take "maneuver." Again, no self-respecting cyber warrior wants to stay in one place waiting for the enemies to hone in, but, by the time this metaphor of place is translated into cyberspace, it may be drained of all effective meaning. Should malware be polymorphic? Should it be hopping from client to client? Should systems dynamically reconfigure their address space? Should server capacity be distributed across the cloud? These are all good questions, but it is unclear how translating all of them into some aspect of maneuver is particularly helpful in answering them.

If cyberspace is like other domains, then under current rules of engagement for kinetic combat, U.S. forces are allowed to fire back when under fire. This particular rule provides a robust rationale for disabling machines that appear to be sending bad packets to military networks. Such a rule arises in part because it is deemed unreasonable to order people to be put in harm's way without being able to protect themselves—and people do put themselves in harm's way in cyberspace. As noted above, this perspective puts too much emphasis on firing back as a way of protecting networks despite the likely ineffectiveness against even a halfway-sophisticated adversary. Interpreting this doctrine more broadly carries substantial risks, particularly given the problems of attribution. A closely related assumption is that conflict in cyberspace features an opposing force that one is supposed to disarm or destroy. But hackers cannot be destroyed by a cyber attack and they cannot be disarmed because none of the three weapons in their arsenal—intelligence, computers, and networks—can be destroyed by a cyber attack in the same way that kinetic warfare makes possible. Hence, such a quest is futile.

Fortunately, although these issues make writing concepts and doctrine an error-prone exercise, the influence of concepts and doctrine on what people actually do on a day-to-day basis is limited. But why not start by not having to jettison such inaccurate concepts in the first place?

## VII. YET ANOTHER DOMAIN TO PROTECT THE NATION FROM

Anointing cyberspace as a domain creates expectations that the DoD, notably the U.S. Cyber Command (USCYBERCOM), will protect the nation's cyberspace in the same way that the Army, Navy, and Air Force keep hostile forces away from our borders. The U.S. Department of Homeland Security has signed technical-assistance agreements with DoD knowing the latter brings the lion's share of expertise into

the domestic fight for cyberspace protection. U.S. defense officials argue that, notwithstanding their intention to concentrate on protecting the military domain, should some digital Pearl Harbor ensue, the DoD will have to answer for why it stood aside and did nothing to protect the country in this domain.

Can the United States be protected by USCYBERCOM from hostile forces[14] in this domain? Clues to that possibility may be found in the Einstein III program which is being rolled out to protect the U.S. government's portion of the Internet (.gov). Proponents have advocated extending the protection to the nation's critical infrastructure[15] and the defense-industrial base.[16] Such a program would sit between the Internet and the protected networks, inspecting the contents of all incoming packets and neutralizing those that contain the signature of known malware—a firewall to end all firewalls. But would it work, or at least work better than what already exists? Bear in mind that these institutions can also contract with professional information security companies to obtain the same services without raising government-spying issues. If USCYBERCOM has an edge, however, it could only be because it knows something about malware signatures that these private companies do not, either arising from harvested intelligence unavailable to private firms[17] or from having found a vulnerability themselves and telling no one. There is surely some malware known to the intelligence community that has not yet been seen in the wild, but there is undoubtedly even more malware unknown to the intelligence community by dint of being developed in small cells that do not display their wares over the unencrypted Internet. It is hard to imagine, for instance, that an Iranian equivalent would have discovered Stuxnet.

The (un)importance of the USCYBERCOM

---

[14] Chris C. Demchak & Peter Dombrowski, *Rise of a Cybered Westphalian Age*, 5 STRATEGIC STUD. Q. 32, 38–39 (2011), *available at* http://www.au.af.mil/au/ssq/2011/spring/demchak-dombrowski.pdf (suggesting that many states are likely to try anyway).

[15] Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, WALL ST. J., Jul. 8, 2010, at A3, *available at* http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html.

[16] Marc Ambinder, *Pentagon Wants to Secure Dot-Com Domains of Contractors*, ATLANTIC, Aug. 13, 2010, http://www.theatlantic.com/politics/archive/2010/08/pentagon-wants-to-secure-dot-com-domains-of-contractors/61456.

[17] The larger information-security companies (including Microsoft) have so many monitors in place that they do, in fact, gather a great deal of what would be called intelligence if done by governments.

How to curtail something such as the Stuxnet threat?

What Einstein III offers, a better firewall, is just one element of a more complex array of information security measures. Returning to Stuxnet, relying on such a firewall could have blinded defenders to the need for inherent defenses, including eliminating USB ports on the air-gapped network, ensuring that the programmable logic chip (PLC) that governed the centrifuges could not be reprogrammed *in situ*, or separating the mechanisms that controlled the centrifuges from the mechanisms that monitored what the centrifuges were actually doing. Indeed, creating something like Einstein III under government auspices may well *reduce* the amount of real effort expended on cybersecurity, just as USCYBERCOM has provided the Services with excuses for not defending their own networks. Then, users can hide behind the fiction that they are being fully protected and can no longer be compelled to protect themselves, thereby limiting potential lawsuits arising from third-party damage. After all, no one expects private firms to mount their own anti-aircraft weapons.[18]

## VIII. CONCLUSION

The notion that cyberspace is a warfighting domain is deeply engrained in doctrine and the minds of those who carry out such doctrine. This essay argues that this concept is misleading, perhaps even pernicious. Faced with the question—if cyberspace *is* not a "domain" what is it—one answer may be that "it" does not exist in a sufficiently meaningful form to make conflict-related statements about it. Such a stance suggests that the term be totally avoided, but since the author himself has no intention of following such advice, the second-best alternative is to use the term carefully. Take a sentence with the offending word in it—for example, the United States must achieve superiority in *cyberspace*—and restate it without that term. The resulting sentence will likely be wordier, but if it is also nonsensical or excessively convoluted, perhaps the underlying thought needs rethinking as well. As for the argument that the military's calling cyberspace a domain is necessary if it is to organize, train, and equip forces for combat in that medium,[19] what is wrong with focusing

[18] More likely, such enterprises will object vociferously because they do not want the U.S. government reading the contents of all their incoming traffic. Commercial satellite operators, for which the case for protection is somewhat stronger, are adamant about not wanting the DoD's help.

Link with Brazil!

[19] The first strategic initiative of the DoD Strategy for Operating in Cyberspace is, "treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential." DEP'T OF DEF., STRATEGY FOR OPERATING IN

on the problems that such forces must solve—defending networked systems, interfering with those of the adversary—and then organizing, training, and equipping to solve such problems? Militaries do this for electronic warfare without the latter, as noted, having been elevated into a separate domain.

Nevertheless, is the fight over calling cyberspace a domain over even before it has begun? Is it time to move on? A dozen years ago, a similarly misguided notion plagued the defense community. The concept of information warfare created a false unity binding diverse activities such as cyberspace operations on the one hand and psychological operations on the other. Fruitless hours were spent developing a comprehensive theory covering this agglomeration. When questioned about whether such a unity was not illusory, high defense officials retorted: be that as it may, the concept was established and that was that. But things did change. The term information warfare, in the process of morphing into "information operations," created "influence operations," which covers psychological operations and concomitants, such as strategic communications. The cyber part of this formulation, computer network operations, married the "cyber" prefix and separated itself completely from matters psychological. Electronic warfare returned to its own aerie. So, at least the term, information warfare, has been rectified.

---

CYBERSPACE 5 (2011). Although the Strategy never uses the term "warfighting domain" as such, cyberspace is to be treated no differently than the historic four, "As directed by the National Security Strategy, DoD must ensure that it has the necessary capabilities to operate effectively in all domains[—]air, land, maritime, space, and cyberspace." *Id*.