



Creating Cyber Strategists: Escaping the 'DIME' Mnemonic

Timothy Thomas

To cite this article: Timothy Thomas (2014) Creating Cyber Strategists: Escaping the 'DIME' Mnemonic, Defence Studies, 14:4, 370-393, DOI: [10.1080/14702436.2014.952522](https://doi.org/10.1080/14702436.2014.952522)

To link to this article: <https://doi.org/10.1080/14702436.2014.952522>



Published online: 28 Aug 2014.



Submit your article to this journal [↗](#)



Article views: 2605



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 2 View citing articles [↗](#)

Creating Cyber Strategists: Escaping the 'DIME' Mnemonic

TIMOTHY THOMAS

This article offers a straw man cyber curriculum designed to initiate discussion on how to educate cyber strategists in the US, stressing the recent advances in technology moving us to the next generation of wearables, drivables, flyables, and scannables. With everything becoming interconnected, there is a need to extend instruction from the instruments of national power associated with DIME (diplomatic, information, military, economic) to a more holistic paradigm when considering cyber issues. This requires developing cyber strategists based on new curriculum components to capitalize on comprehensive views and analytical thought instead of mnemonic devices. It calls on digital and national security experts to reconsider the underlying concepts that will serve as educational guides for cyber strategists as they progress into the next decade.

Rat: How many languages do you speak?

Dr Zimsky: Five, actually.

Rat: I speak one: one, zero, one, zero, zero. With that I could steal your money, your secrets, your sexual fantasies, your whole life; in any country, any time, any place I want. We multitask like you breathe. I couldn't think as slow as you if I tried.¹

The application of cyber-related advancements to the instruments governing our daily lives (banking, buying, communications, national security, etc.) comes at a cost –the difficulty of developing a digital strategy to manage cyber's rapidly evolving nature. Even the notion of national borders is becoming obsolete, since photons moving at the speed of light can place Belarus virtually next door to Kansas City.²

Timothy Thomas, Foreign Military Studies Office, Training and Doctrine Command, Ft Leavenworth, Kansas, USA. Email: Timothy.L.Thomas20.civ@mail.mil

Currently there are few written explanations, at least in an unclassified form, of the educational requirements for developing a cyber strategist to handle these advancements as we have for the conventional strategic warrior. Now that the US Army has begun producing cyberspace warriors (military occupational specialty 25D, cyber network defender) and cyber specialists directly out of West Point, a discussion of such an educational curriculum has become more important. It appears a similar discussion began over ten years ago in China. Shen Weiguang, the so-called father of information war in China, developed an extensive cyber (he called it information at the time) program in his 2003 book *Deciphering Information Security*. Shen noted that network security and information warfare are both issues of technology but, above all else, they are issues of strategy. Initial courses he taught began with an explanation of military strategy in general and then proceeded to discuss US strategy before getting to the topics of writing code or developing viruses and hacker attack methods.³

It is important that guidelines are focused on developing a person who is knowledgeable in both strategic and cyber issues and can serve as a member or leader of a military/civilian Cyber Strategic Task Force, the unit that seems to be appropriate for implementing the concept. Individuals alone cannot hope to acquire the necessary skills in several disparate areas that are needed to create a cyber strategy. First, a task force member must be proficient in the concept of strategy. There is no general definition of strategy, as each nation defines the term according to its history and national use. You must understand an opponent's strategy if you are to counter it. Second, a task force member must be proficient in numerous cyber issues, and there are many to consider (writing code, examining adversary cyber, creating rules and regulations, etc.). A task force member should possess a special skill set in one particular area, such as writing code, and proficiency in other areas. The educational format for preparing a cyber strategist therefore must develop well-rounded individuals who are able to work as part of a team. As nations transition from the Internet of Things to the Internet of Everything the need for this educational format will only grow in importance and diversity.

This article offers several thoughts on the contents of an educational program for developing cyber strategists. It is general in nature and designed to initiate commentary on the topic, to include developing a definition of a cyber strategist. The discussion begins with the question 'who are America's cyber strategists' and proceeds to this author's potential definition of such a specialty. Next a few specific areas are proposed that might find their way into a cyber strategist's curriculum. These areas are: keeping one's finger on the pulse of the rapidly changing cyber

strategic environment, becoming familiar with the capabilities and programs of algorithm/software writers, understanding the layout of cyber terrain, looking at the *modus operandi* of various nations, assessing the impact of cyber developments in conjunction with law and ethics, attempting to understand the digital intent of actors and their use of electrons, decoding the topic of cyber deception, and examining the use of hacker and criminal plans. The article concludes with an offering of what a cyber strategist's qualities might look like.

It is hoped that the article will generate discussion on the topic and flush out more developed and germane definitions than those proposed here. There are already many outstanding information and cyber warfare courses currently taught in US military institutions. Perhaps these courses could now include (if they do not already) a one or two hour lecture that discusses what a cyber strategist might have to consider in his job and thereby develop the concept further. On the other hand, a potential finding also could be that the concept is simply not teachable, that the cyber age is too complicated and fast changing for such a specialty.

Who are Our Current Cyber Strategists and What is a Cyber Strategy?

National Security Agency (NSA) and commercial software developers, of course, are tacticians, as they analyze electron packets and attempt to uncover their purposes in order to construct defenses and counters to them. However, some of them examine the global digital environment and the development of methods and means of response, making them cyber strategists of a certain type 'at this point' in time. Other cyber strategists exist in think tanks, ministries, and policy forums. However, these people seldom realize that they are really cyber strategists in its narrowest, specialized meaning.

Strategy is an extremely important topic in an age where everything is or is going to be connected. It is unknown how much NSA and commercial software developers are studying the impact of cyber on strategy or if it is being studied at all. The front-line analysts often do not have the time or background to do so. Cyber issues are constantly developing new trends and strategy is a very complicated concept, defined according to person and context. Jomini (strategy is the art of making war on a map),⁴ Clausewitz (strategy is the use of engagements for the object of the war),⁵ Napoleon (strategy is the art of making use of time and space),⁶ and other icons of strategy have described the concept in varying ways. Their frame of reference, of course, was much more finite, slow, and localized than

today's cyber-based global context in terms of geography (cyber terrain), connectors (optical fiber, cables, satellites), and forces (cyber specialists, servers, etc.). Perhaps a new understanding of strategy is required to fit contemporary conditions.

Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, defines strategy as 'A prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives.'⁷ The 'instruments of national power' referred to in this definition are diplomatic, information, military, and economic (otherwise known by the mnemonic DIME). A proposed cyber strategist's curriculum should attempt to escape DIME's grasp, since this framework is too limiting and not indicative of either the many elements that compose cyber (engineering, systems, connectors, etc.) or the incredible speed of electrons with which modern day cyber strategists must contend. The situational context for a cyber strategist encompasses the entire interconnected globe and all the elements that compose it: social engineering, cyber terrain, digital and technological advances, the proliferation of tubes worldwide (optical fiber, submarine cables, etc.), the creative use of algorithms, satellites, sensors, etc. DIME is an insufficient template to handle these criteria.

In today's context networks and system-of-system lash-ups have integrated the cyber environment to such a degree that a movement in one area can be felt immediately in another or even several others. We are living at a time when the diffusion of power is moving into more and more hands, making it more difficult to control crises. And we are moving fast to the generation of wearables, drivables, flyables, and scannables,⁸ not to mention quantum computing. The cyber strategist's environment is interconnected, global, and continuous. Cyber can serve as both an enabler of joint action or as an agent of coercive strategic effect, both physically and cognitively. Today cyber weaponry makes the technology of the 1990s look archaic. More importantly, issues go well beyond a simple consideration of what combinations of hard and soft power to use. You have to know the lay of the cyber land and the strategic thinking of your adversaries that accompany it, among other issues.

For purposes of this paper, this author offers two definitions of cyber strategy. First, cyber strategy can be thought of as *the application of cyber technology and associated competencies to gain or maintain a relative power advantage and control (both offensive and defensive) in a competitive environment*. Second, cyber strategy can be thought of as *the achievement of cyber advantage and control (both offensive and defensive), based on an analysis of the strategic*

environment or situational context, through the thoughtful integration of cyber devices and human cognition in accordance with policy and political goals.

In the 2012 US Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy, the term 'military strategist' is used only three times in 359 pages: once in a quote from Liddell Hart and twice in John Warden's Five Ring Model. A strategist, in general, is often referred to as a person skilled in making plans for achieving a goal or someone who is good at forming or specializing in strategy. While it may seem adequate to simply slip the term 'cyber' in front of the word strategist or to call someone a military cyber strategist (and assume that the definition of a cyber strategist would then be fully developed and finalized), it is not that simple. We are not talking about an indirect approach or a five ring model. We are talking about a consideration of a global playing field where a holistic view of the strategic environment is required before an indirect approach or some other method can be applied.

Contending with the cyber environment, which is constantly changing due to new developments, will be a difficult task. While keeping a vigilant eye on the strategic landscape or environment, the cyber strategist must simultaneously adapt to new innovations, both friendly and adversarial, and adjust his cyber defense plan as appropriate in order to protect the nation's cyber capabilities and interests. As the curriculum below notes, this will very likely require the development of a task force composed of cyber strategic specialists in a number of fields, and headed by a general cyber strategist. There are simply too many variables and capabilities for one person to consider everything in detail. The lead cyber strategist will be dependent on the input of others as he develops his national security or military cyber plan. This requires a comprehensive cyber education; and a general understanding of the concept of strategy from its many vantage points.

So, with this background and the proposed definitions of cyber strategy in mind, let us explore the elements mentioned above that might be included in a cyber strategist's educational course. The course should include a mix of mandatory requirements to become a cyber specialist, as well as insights into the thinking of the cyber perpetrators, by culture and focus (criminals, terrorists, etc.), who will confront them after graduation. When basketball teams practice their defense, they do so against the offense of their next opponent. They do not practice against their own offense (the ends, ways, and means playbook), but that of the adversary. Cyber strategists will have to do the same.

Components to Consider for a Cyber Strategist's Curriculum

Continual Updates on Cyber's Emerging Context

Cyber requires something new from strategic theory. Other nations (the Chinese, Arabs, Russians, etc., although the Chinese example is used here) would appear to agree with this proposition. First, it appears that cyber can be thought of as a potentially independent force. For example, Stuxnet demonstrated the ability to shut down or destroy centrifuges through the insertion of a virus from afar, in the form of a file, that caused the damage. If systems or turbines spin out of control (as happened in Russia) and destruct due to a false cyber signal or a virus, leading to explosions or the collapse of a structure, then cyber has demonstrated that it has the power to influence, which, by definition, makes it a force. In extreme cases cyber can be regarded as approaching a nuclear-like capability. If scale is the measure of a nuclear capability or danger (destruction of a city or region, with massive deaths and pollution), then of course it is not the same as a nuclear weapon. However, cyber weapons can theoretically penetrate systems, including municipal and regional ones, and shut them down. Cyber may not be as coercively important as nuclear weapons are destructively and physically, but cyber can disrupt cognitively and it can inflict precision damage on high-value targets and thereby acquire a potential strategic effect that could change policy or politics. So cyber under such circumstances would appear capable of becoming a significant capability.

The Chinese book *On Military Strategy*, by Fan Zheng Jiang and Ma Bao, defines strategy differently than many nations. Fan and Ma's book states that the strategic environment is 'the important foundation upon which military strategy is dependent for its formulation, the extrinsic conditions upon which military strategy is dependent for its implementation, and the arena upon which the strategic directors are dependent for displaying their talent in planning and skill in directing'.⁹ The authors state that 'the relationship between the strategic environment and military strategy is the relationship between objective reality and subjective guidance. An understanding and analysis of the strategic environment is the prerequisite for properly formulating and implementing military strategy.'¹⁰ This Chinese definition of military strategy can be used for the planning and guidance of military struggles as a whole. A few of the objective realities of cyber are that surrogates can be used to hide a nation's participation, there is a lack of rules and regulations governing the use of cyber by nation-states, there are weak systems worldwide, and it is difficult to pin blame on a cyber perpetrator due to the anonymous

character of the Internet. Subjectively, China's strategists recognize these and other holes in objective reality (weak cyber defenses, etc.) and proceed to influence or manipulate cyber's objective environment to their benefit, such as through the extensive use of reconnaissance assets. Would ends, ways, and means thinking (a US military way of defining strategy) yield the same analysis and encourage similar actions (reconnaissance, etc.)?

Strategy, at least from the Chinese viewpoint, should pay attention to and adapt to technological change, since the latter (in the case of cyber technology) can affect targets anonymously from great distances and with blinding speed. If directed at a key digital target, cyber could potentially induce strategic change overnight and invite an overwhelming response from those affected. Strategic thought and planning will have to adapt accordingly. Jomini and Clausewitz would have no idea what had happened strategically under these circumstances, since their concepts of strategy bear little relation to today's integrated environment. Napoleon, on the other hand, due to his interest in time and distance, perhaps would have understood the impact of cyber best (based on these old definitions) among the three men if they were alive today.

Cyber-generated images and communications, especially when conducted without retribution, motivate and unite people and give them courage to confront wrong and request fair hearings for their concerns. Anonymous communications can also generate unity among individuals and groups. Such activity causes security agencies in some nations to erect firewalls and sensor information or conduct Internet espionage on civilian protests. Two Chinese cyber experts from the Academy of Military Science have noted the reason for such concern:

Network psychological warfare is a mental and psychological game that unfolds in cyberspace. It has been referred to as 'the politics of the heart'. It is the extension and development of traditional psychological warfare in cyberspace. It is worth noting that the targets of network psychological operations have already expanded from the military to society and the people to achieve the 'butterfly effect' and directly achieve political goals.¹¹

Intelligence and information are equally important, it appears, since is not intelligence nothing more than analyzed information? Information is what GPS, satellites, and all sorts of devices utilize or provide, without which soldiers in the field now find it hard to operate. Information becomes intelligence or it could be used to communicate or navigate. Without information there would be no strategy that makes sense. It is

not just men and machines that sink ships nowadays, but also men assisted by cyber-enabled command and control, cyber-enabled precision weapons, and other types of cyber-enabled and cyber intelligence assistance from satellites and radars. An understanding of a potential cyber catastrophe's impact and form has widened our concern and put us on constant watch, just as nuclear once did.

The ability of cyber to put nations on constant infrastructure and intelligence watch indicates that the calls of cyber alarmists should continue to be taken seriously. There are numerous businessmen, bankers, national security experts, and others who comment almost daily on this important issue. The Obama administration urged companies to do more to protect their networks. Companies are now taking out 'cyber insurance' for a reason. On 26 February 2014 the following comment appeared in the editorial section of the *Wall Street Journal*, indicating once again the fear of a cyber attack against the nation's economic stability:

Hardly a day goes by without news of another cyber attack. Supposedly well-guarded corporate, government, or consumer data land in the wrong hands thanks to crafty hackers who attack allegedly impenetrable networks in search of valuable data. On January 30 Yahoo surfaced as one of the latest victims when the company disclosed that its users' email accounts had been compromised ... so it should come as no surprise that US intelligence officials ranked cyber security as the number one threat to US interests during a recent congressional hearing.¹²

Banks are having the same issues and, as is often noted, seldom report losses of cash nationally to avoid losing customers. National security experts, as numerous examples (Lockheed Martin's Joint Strike Fighter Program, Pentagon data thefts, etc.) have shown would be absolutely wrong to think their systems are fail-safe. Members of the US Computer Emergency Response Team (CERT), who have tended to numerous intrusions (compromised tokens, loss of data, etc.), also take cyber alarmism seriously.

Algorithms

Algorithms allow processors to think faster. They enable complex decisions almost instantaneously. To observe the speed of an algorithm, one only needs to browse for a topic and observe the 300,000 plus hits one receives in two seconds or less. As a demonstration of the speed and

importance of algorithms and perhaps their ability to induce strategy, one is reminded of the exchange from the movie *The Core* in 2003:

Rat: How many languages do you speak?

Dr Zimsky: Five, actually.

Rat: I speak one: one, zero, one, zero, zero. With that I could steal your money, your secrets, your sexual fantasies, your whole life; in any country, any time, any place I want. We multitask like you breathe. I couldn't think as slow as you if I tried.¹³

Rat's response suggests that, if all his actions could be accomplished as fast as he indicates, the recipient of the attack is in dire trouble. Not only must multiple counter capabilities be available to the person under attack, but the person must also have some knowledge of the type or methodology of the attack he is facing (criminal, nation-state, etc.) if he hopes to construct the correct response. Strategies might include those for limited attacks on privacy, more stringent strategies for attacks on financial resources, and escalation-type strategies for attacks on infrastructures. Further, the cyber strategist swims in a sea of limited or no rules and regulations at the moment, as well as unknown intent and methodologies.

Algorithms can provide us with reams of information, but they can manipulate us and sometimes inhibit our innovative talents as well. As anyone knows, a slick algorithm writer can direct interested parties to specific locations, thus influencing their thinking. It will be hard to get the algorithm writer to share his code and perhaps the purpose behind it, since algorithm writers have mathematical secrets to protect as well, especially if they are hackers. With regard to inhibiting our innovation, we can become so accustomed to these quick response algorithms that we forget algorithms are behind this speed. We accept what the algorithm provides and with that acceptance we surrender some of our ability to innovatively think and manage our responses to searches. Innovation can also be affected by local or some specific context.

In a discussion of the book *Automate This*, noted digital expert Evgeny Morozov stated that we can live with algorithms but must learn how to do so. Most important is that we do not accept things at face value. 'An uncritical embrace of automation', he notes, 'for all the efficiency that it offers, is just a prelude to dystopia.'¹⁴ No one wants to become unhappy and live in an imaginary place. Instead, we have to skeptically recall the inherent dangers of algorithms and learn to stay cognizant of their manipulative ability. This will help us adapt to algorithms correctly and to our advantage, while remaining innovative. Further we will have to become

acquainted with the various strategies that algorithm writers may hide within the digits and maths. This awareness should be part of a cyber strategist's curriculum. In the end, maths superiority has become crucial to a state's security, especially software security. The ability of an opponent to manipulate software to his benefit can spell the doom of infrastructures, financial assets, and even key weapon technologies.

With regard to technology, there is a growing emphasis on the concept of STEM – science, technology, engineering, and maths. Barriers to entry are low, and a highly qualified STEM nation, even one without military hardware, can theoretically damage the capabilities of other nations. Some countries or groups are developing what is often referred to as talent, techniques, and technology.¹⁵ The 'three Ts' are important to keep in mind, especially the middle one. It is the most difficult for the cyber strategist to conceptualize, since it lies in the minds of those with talent. STEM capabilities could be used in strategic ways to change policy and politics. STEM, then, demonstrates other activities that must be considered by a cyber strategist, and indicates that a reliance only on DIME will cause strategists to come up short in assessing the evolving cyber environment. Strategists must be aware of the advantages that algorithm writers provide. They should be included as lecturers in any cyber strategy class and tapped for their ideas.

Cyber Terrain and 'Mapping'

A cyber strategist's terrain includes optical fiber, internet service providers (ISPs), routers, switches, wireless links, terrestrial gateways and underwater cables of all types, satellites, power stations, and many other features often described as tubes, both visible and invisible. These links and connecting points comprise the terrain that, like Jomini studying terrain and forces on his map, a cyber strategist must consider. These points are important, since each could control access to millions of computers or to key sections of digital infrastructure. They must be protected and monitored, but they also represent key areas of influence or manipulation. The terrain can be used, similar to a manipulated voting machine, to fool someone, to force him into making certain decisions, or to shut down an infrastructure.

Another aspect of key cyber terrain is the ability of modern day digital processing elements to basically make maps of one's choosing, to 'map a map' (for example, specifically map an existing map in various ways). Adam Fisher, writing in the *New York Times*, noted that there have been three great Internet land grabs to date. Google won the first, which was

the search algorithm. Facebook won the second, which was snaring people and their egos. The third, mapping places, is still a competitive fight that is underway. Location awareness will allow mobile devices to know where one's possessions or 'stuff' is: 'Your house keys will tell you that they're still on your desk at work. Your tools will remind you that they were lent to a friend.'¹⁶ Key cyber terrain will also beckon to be exploited or damaged by a criminal or adversary.

Google cars, often visible in towns across the US, having been mapping most of the country and have started to do so in other nations as well. A green orb is placed on a rod that is attached to the car. It captures images with a panoramic camera, making Google's Street View possible. Pattern-recognition bots search the archive for addresses. Google's computer-vision programs look for house numbers, street signs, and even well known landmarks (fast food venues, etc.). Even the bottom of the Grand Canyon has been captured on camera with a similar device, known as the Trekker. Amazon had a similar technology called Block View, and Microsoft had a version called Streetside.¹⁷

Google's innovation was its web interface, which made its map dragable, zoomable, and panable. One could interact with maps, which MapQuest did not allow. To Google's chagrin, its map soon became co-opted and used by many other groups for their particular interests. HousingMaps.com, for example, overlaid Google's map with apartment listings from Craigslist for accommodation availability in San Francisco, an example of 'mapping a map'. However, Google understood the opportunity here and created an application programming interface for Google Maps, allowing a programmers-only side entrance into the Google mapmaking machine. Entire companies could then be based on Google Maps,¹⁸ and Google could charge for the opportunity to use the side entrance. Are the interior of buildings the next thing Google will map?

This mapping prowess can allow new insights for strategists simply due to the amount of data being collected and available. An entire operational environment can be laid out before the cyber commander as he tries to develop a successful plan. Cyber geography is important and will grow in its capacity to serve leaders. It will be an area of intense study in the coming days.

Modus Operandi of Nations

Different nations comprehend the use of cyber assets in various ways. For example, the Chinese look at strategy as the ability to apply methods to influence to their advantage the strategic environment before them.

China has a very long history of strategic thought. One need only access their military encyclopedia to get a feeling for the hundred or so Chinese terms that are defined and include the word 'strategic': for example, strategic cover, strategic concept, strategic target, strategic thought, strategic pivot, and strategic maneuver.

Listening to the leading military thinkers of any country can better expand one's understanding of strategy. Analysts can improve their own understanding of strategy, gain new templates for contemplating the global environment, and find ways to counter an adversary's concepts. China, for example, has 5,000 years of military history on which to draw. Its leaders are calling for a grand strategy, one that desires to set up a system of systems of laws and regulations with the guideline-oriented *Cyber and Information Security Management Law* as the superior law. Most likely there is a hidden strategic advantage for China in this law, an advantage that represents the essence of this strategic move. Understanding this template enables other nations to find ways to counter it or expose hidden agendas.

Chinese strategic planning includes industrial development of controllable core technologies and big data-mining technologies. China wants to produce specialized personnel and enhance the forward-thinking and application studies of key cyber subjects. In addition to the standard geographical (land and water), weather, human, space, and hydrological environments, there are now sophisticated electromagnetic and network environments with which to contend, according to Chinese specialist Li Qiang.¹⁹

Russia, like China, has its own understanding of cyber. That nation has a multitude of outstanding mathematicians and software writers similar to the Chinese. US stores such as Best Buy sell the anti-virus product of one of them, Eugene Kaspersky. Not long ago, Russia's Defense Ministry hired the Kaspersky Laboratory to install software to protect the official Defense Ministry website against hacker attacks. The Kaspersky DDoS Prevention Ultimate Level set of programs should provide protection against attacks and filter parasite traffic with a 98-percent guarantee, with the possibility of blacklisting certain regions' IP addresses, according to writer Aleksey Krivoruchek. The license for the set of programs includes 24-hour technical support from the Kaspersky Laboratory, and the maximum time for troubleshooting problems in the case of a Defense Ministry website crash, under the contract terms, does not exceed four hours. The provision of such services for one year will cost the military 3.4 million rubles.²⁰

For the Russians, both technical and cognitive issues are important. They do have some fear of cyber matters getting out of control, it seems. When asked a few years ago about developing an order of merit list of the top ten cyber items of concern that are of worry, they responded as follows: escalation models, civil infrastructures, definitions, cyber law, codes of conduct, cyber terrorism, cyber crime, technical cooperation, protection of the world community, and industrial espionage. Thus technical and cyber issues that could lead to escalation are the most worrisome.

There is little doubt that there is concern in Russia over cyber's ability to manipulate and influence the cognitive capabilities of their population. Some still consider the loss of communist ideology in the 1990s to be the Third World War, a psychological one in their understanding that the West was able to win. When dividing information warfare into parts, the psychological aspect is equally as important to Russia as the technical aspect. They lost an ideology once and want to make sure it never happens again.

Cyber strategists will be wise to become familiar with the methods, definitions, and concepts of the most capable cyber nation-states. The largest of these by population, such as India, Russia, or China, are able to aggregate the greatest amount of relevant resources (mathematicians, etc.) and present the greatest potential cyber capabilities. On the other hand, one genius (a talented algorithm writer) or insider (Edward Snowden) can do catastrophic harm on his own if he is able to access, download, and share information with would-be law breakers or potential adversaries.

Law and Ethics

There are a few rules and regulations that some categories of cyber perpetrators, such as criminals and terrorists in particular, violate, although nation-states have also gone the way of independent destructive actions at times. Rules that do exist cover areas such as fraud and financial scams. There are no caution signs or white flags to slow down the criminal or terrorist (unless they are struck hard) and such groups have little cause for extended discussion of the use of cyber assets. A lack of rules, regulations, and customs, along with the issue of anonymity, allows them to continue cyber perpetrations with little thought of being caught or prosecuted.

Mike McConnell, former White House National Intelligence Director and, before that, NSA Director, supported this contention of a lack of rules and regulations, stating in February 2014 that cyber security's laws are outdated.²¹ In February 2014 the 'Obama administration released voluntary cyber security guidelines for utilities, banks, and other crucial

industries',²² which stem from an executive order issued last year. It is ironic that, in the age of instant communications, the rules and regulation process works at 'turtle speed' by comparison. The steps to improve security do not include incentives for companies to take part, and companies worry this could be the first step toward regulation. An effort to pass legislation with security requirements for companies possessing or developing critical infrastructure failed in the Senate in August 2012, yet another indication of the slow pace of change in the US legal system.²³

This past year in the US and abroad the discussion of privacy issues became a focal point for law and ethics, highlighted by the revelations of Bradley Manning and Edward Snowden. Fingers pointed directly at the NSA for dipping into the public domain's phone records. In hindsight, there are so many invasive technologies these days that the NSA's surveillance (of some 20 percent of the populace, according to one report) is only one of many to contemplate. Francis Clines, in a *New York Times* editorial, stated that since the cloud is 'powered by tens of thousands of computers at server firms owned and managed by companies like Google, Amazon, and Facebook', we have collectively ceded our privacy bit by bit.²⁴ We have given up privacy for free services:

Facebook wants to know why you did not publish that status update you started writing –that is, things you start to type and erase are searchable and locatable on Facebook.²⁵ Facebook has a listing of you, your friends, personal likes and dislikes, photos, recent events, anything you desire to post

Amazon wants to know about all your preferences.

Google maps shows the world street views of our homes and targets ads based on e-mail content.

Skype can show elements of the inside of our homes.

Hidden cameras placed throughout towns and on buildings watch us as we move through our day.

Trackable traces are left on our phones and computers everyday.

Web retailers save your credit card numbers so that you do not have to type them in.

To demonstrate just how porous our privacy has become, comic Jack Vale offered an example. He showed how, through a simple search of social media services, he could see who was nearby and what he could learn from them 'at that moment'. Vale went to a social media site and

searched to see who was near his location, which was a shopping district in Irvine, California. He states clearly in an online video, 'I got all of this information just by searching their personal social media posts.'²⁶ The video, located at <http://bit.ly/vale1202>, has been viewed more than 2.5 million times. Vale states he could call people out by name on the street, congratulate them on a recent birthday, or name their pets. And this was done on a lark by a comedian, not a criminal with other intent.

There are now apps for phones in particular cities that enable places to find you as you pass by. They might explain the layout and offerings of a restaurant or the history of a place or building.²⁷ At the same time, the places your phone finds will enable others to find you. A cyber strategist could use this information about phones and other devices.

One well-recognized effort to overcome a perceived global shortcoming in understanding the impact of cyber on warfare (from the vantage point of international law) was the development of the Tallinn Manual. As NATO's Cooperative Cyber Defense Centre of Excellence (CCD COE) website notes:

The Tallinn Manual on the International Law Applicable to Cyber Warfare, written at the invitation of the Centre by an independent 'International Group of Experts', is the result of a three-year effort to examine how extant international law norms apply to this 'new' form of warfare. The Tallinn Manual pays particular attention to the *jus ad bellum*, the international law governing the resort to force by States as an instrument of their national policy, and the *jus in bello*, the international law regulating the conduct of armed conflict (also labelled the law of war, the law of armed conflict, or international humanitarian law). Related bodies of international law, such as the law of State responsibility and the law of the sea, are dealt within the context of these topics.

The Tallinn Manual is not an official document, but instead an expression of opinions of a group of independent experts acting solely in their personal capacity. It does not represent the views of the Centre, our Sponsoring Nations, or NATO. It is also not meant to reflect NATO doctrine. Nor does it reflect the position of any organization or State represented by observers.²⁸

Actor or Electron Intent

In addition to monitoring and detecting probes or attacks the cyber defender would be well assisted if he knew how to analyze the source

behind the electrons and their potential intent and methodology. Developing the capacity to make informed analytical judgments of another government's or group's cyber exploits has become important. It not only allows for the development of a way to thwart reconnaissance or other types of actions but it enables one to perhaps trace an event back to its origin.

The cyber strategist must understand how competitors, potential adversaries, terrorists, and criminals differ in their employment of electrons and their associated goals or objectives. This requires giving some depth of thought to both the concept of strategy and its electron employment by other cultures. One must abandon the thought that electrons can only be used in certain ways. On the contrary, cultural applications of electrons are only limited by one's creativity and imagination. For example, some cultures use packets of electrons as stratagems, which are designed to fool perceptions. Strategy, to some, is not a prudent idea as it is to the US military but rather the application of subjective thought to objective reality. This is a strategic concept used by several nations. Others might consider strategy as the ability to make someone do something ostensibly for themselves but in reality for you. Phishing would be a cyber example of this concept. The composer of an executable file works to get you to open it and do something supposedly for your benefit (reveal a message that you think is important). Meanwhile, you are downloading files that the strategist or executer of the file wants to introduce into your system, where they could cause harm. You are, in fact, doing something for the file's developer that you thought you were doing for yourself.

It is not easy (nearly impossible?) to determine whether a cyber activity is designed to damage or simply vandalize a file at this point in time. Likewise, it is difficult to determine the intent of a human conducting a physical attack on an ISP or some other cyber device. Is this activity designed to destroy the device, to monitor a device, or simply to terrorize or to vandalize populations and property? For example, on 5 February 2014 the *Wall Street Journal* disclosed that an armed attack had occurred on an electrical substation. The attack at PG&E Corporation's Metcalf transmission substation is being termed by some as a terrorist attack. If widely replicated across the country, some believe the attacks 'could take down the US electric grid and black out much of the country'. It was the greatest attack against the grid to date, the article noted, and it was not done electronically. Using rifles, the attackers aimed at the transformers' oil-filled cooling systems, which began to bleed oil. They were out to shoot to kill a container.

Some believe an even larger attack could be in the works, as this attack could have been a 'dress rehearsal for a larger event'. In the past three years, companies have reported 13 cyber incidents requiring emergency reports. With this focus on Internet attacks, it appears less focus had been placed on substations. Some feel that physical attacks present a larger threat to cyber security than the maths-or-electron-based cyber attacks. Cyber strategists understand that the physical connectors or power providers are also strategic targets and, implicitly, key terrain. Massive outages can cause policy or even political change. Cyber advocates cannot be limited to the 'virtual' world. For example, in September 2013 in Caracas, Venezuela a blackout deprived some 70 percent of the country of electricity. The failure was reportedly in the 'backbone' that carries electricity from the Bajo Caroni region, where some 60 percent of Venezuela's power is generated. Major electrical malfunctions there led to the interruption of subway services and other transportation programs. President Nicolas Maduro claimed the outage was 'part of a low-level war' on his government.²⁹

Deceptive Web Traffic

Some criminals or other groups have established botnets, which are zombie armies of hijacked computers controlled from unknown locations. Command and control servers can instruct the bots to send mass spam, initiate a distributed denial of service (DDoS) attack, redirect web searches, intercept legitimate web traffic, or reroute traffic to capture personally identifiable information (PII). The bots visit websites (instead as people) in the thousands. These visits encourage advertisers to pay for the traffic, which they think is human. The bots can 'mimic the behavior of online consumers, clicking from one site to the next, pausing at ads, watching videos, and even putting items in shopping carts'.³⁰ Such tricks are becoming standard for the industry, with digital foolery growing in number and sophistication. Today there are chatbots (they greet users when entering an online chat room), spambots (which produce e-mails advertising miracle developments), bimbots (which offer photos of beautiful women who hawk products), and socialbots (which are programmed to tweet and retweet). The latter are, according to researchers, being designed to sway elections, influence the stock market, attack governments, and flirt with people and one another. They also are acquiring accounts on Facebook, Reddit, or Foursquare to give them an online footprint and appear more human. This is accomplished via so-called persona management software.³¹ These bots are real and act well beyond the artificial capabilities of those 'fembots' popularized by Austin Powers in

the movie *International Man of Mystery*. So are we dealing with humans or cyborgs? The cyber strategist will have to contend with these bots as part of the strategic environment.

Social engineering is a well-known form of deceptive web traffic. It tries to fool decision makers, and is really nothing more than an updated form of the use of stratagems, which were used thousands of years ago for similar purposes. There are many social engineering techniques, several of which are highlighted below:

- Pretexting –the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action, typically done over the telephone.
- Phishing –a technique of fraudulently obtaining private information, typically by sending an e-mail that looks legitimate.
- IVR/phone phishing –technique using an interactive voice response (IVR) system to recreate a legitimate sounding copy of a bank or other institution’s IVR system.
- Trojan horse/gimmies –technique taking advantage of a victims’ curiosity or greed to deliver malware.
- Road apple –a real-world variation of a Trojan Horse using physical media and relying on a victim’s curiosity (e.g., leaving a CD or USB flash drive in a place where it will be found).
- Quid pro quo –technique involving a random caller who states that he is from technical support in an attempt to find someone with a problem and then guide him through commands, thus giving the caller access or the ability to launch malware.³²

Cyber strategists must be aware of cyber deception methodologies. Good cyber awareness is not enough. While everyone knows this, they often disregard the requirement to understand adversary methodologies and how they apply cyber deception.

Narrative through Images

Cyber is most often associated with being an enabler of a physical effort, such as an attack on infrastructure, since computers, sensors, and other digital devices compose its basic elements and carriers. But in addition to affecting infrastructure, cyber empowers people and influences them due to its rapid information processing and dissemination capability. Cyber images can impart a cognitive effect that can have strategic consequences. Russia attempts to work with this effect doctrinally, including cognitive issues as part of its understanding of information conflicts. That country’s cyber experts continue to stress the importance of two information-age

aspects, information-technical devices and information-psychological ones. Other governments must contend with both of these aspects as well, whether they agree or not with the division of labor inherent in the Russian concept.

The danger of cognitive manipulation lurks constantly in the connection among technology, images, and our minds. Images can be sent around the world in a matter of seconds, without relation to reality, from an iPhone, computer laptop, or some new-fangled camera. These images can incite emotions and responses if one is oblivious to contextual consideration or is not a skeptic. People with agendas can influence others by making specific points to interested audiences. The media (and sometimes diplomacy) then have to catch up with these postings and analyze them as to content and truth. Today in Syria, for example, there are horrific images, some staged and some real, which are influencing decision-makers worldwide. Extreme care must be taken to correctly understand and comment on them; otherwise, they can take on a life of their own. In that sense this is a dangerous world of individual power. The military speaks of the strategic corporal in this respect, the ability of a lone person to say something on camera and have that sound bite transferred globally as representative of a unit at large. One US editorialist noted that 'an idiot with a video camera has the terrifying power to change the world'.³³ Such reporting could be considered as strategic, whether idiotic or not. The effect would be the same.

Andy Carvin, a former National Public Radio social media strategist, noted with regard to the Middle East that 'basically every potential player in the conflict, from individuals in the grassroots to NGOs all the way up to governments and para-government organizations, now has a stake in the game in which they can potentially influence the public'.³⁴ Each individual, whether prime minister or average citizen can, in only 140 characters, influence someone with a Tweet, so social media is a very democratic platform. These platforms, which once were only in the hands of the state, are equalizers that enable the invasion of pocket technology to be 'like a viral tsunami, and we still don't yet know the effect it will create'.³⁵ Cyber strategists must remain eternally vigilant to be able to separate virtual truth from actual truth. They will most likely be confronted with this complex situation on multiple occasions.

Hacker and Criminal Strategies

Two years ago NSA director General Keith Alexander, in testimony before congress, warned that in a year or two the hacking group Anonymous

might be able to conduct a limited power outage through a cyber attack on US systems. To date this has not happened, but his warning did signal how federal concerns have grown over hacker capabilities in the recent past. It thus is wise to become acquainted with the methodologies of various hacker and criminal groups in order to better identify who is hacking one's systems.

Hackers have their own *modus operandi* and intentions. Gamers do as well. They speak the language of ones and zeros that most average Joes do not, especially to their degree of fluency. When hackers link with criminals or terrorists the world pays attention. Under that circumstance the quick mind is bonded to the sneaky mind, where strategies are developed in willful defiance of rules, regulation, or decency. For a military leader to take down the hacker, it 'will require observance of the military operational principles which, in turn, will require careful study of the physical and human geographies in which counter-nerd operational art will play out'. It will also require an inherent knowledge of hacker, criminal, and terrorist digital thought. The recent attacks on retailers Target and Neiman Marcus indicate the sophistication of such attacks. Extensive reconnaissance was conducted of the point-of-sale system, watching how it processes transactions. This is where most of the theft occurred. To create the ability to steal information, cyber gangs have specialists 'in areas of infiltrating systems, designing malware, mapping networks, and selling stolen data, and they employ them to work on different phases of the attack'.³⁶ They may, for example, create an illegal cyber 'man in the middle' that intercepts data (unknown to the sender) and then allows the message to proceed to its original designated recipient. Meanwhile, important data is harvested by the illegal cyber intercept accomplished by a bot. Cyber strategists must be taught to counter each of these areas.

Cyber gangs have time on their hands, so they sit and innovate. Meanwhile, the law abiding population can only sit and implement or install comprehensive counters, since they have little grasp of coding or an idea as to which particular stratagem or manipulation the cyber gangs will fire at them. One such counter group has been a startup called Shape Security. It sells an appliance that plugs into a network and 'obfuscates the code behind the customer's website. It replaces variables with random strings of characters that change every time a page is loaded, all without altering the way the site appears to human visitors'.³⁷ Called a ShapeShifter, the appliance uses a trick known as polymorphism, which makes it more difficult to use automated tools to enter websites and crack passwords. It must become mandatory that the cyber strategist be familiar with such tools and be able to imbed them in US systems to keep adversaries out.

Conclusions

One of the main conclusions reached in this discussion is that it 'will take a Task Force' to develop competency in cyber strategy. A second conclusion is that America's cyber specialists will require a well-rounded curriculum in order to develop a good cyber strategist, a curriculum that meets the challenges of the current and evolving cyber strategic environment. A third conclusion is that this means moving beyond the DIME mnemonic (that is, adding to it), which has served as a foundational element of strategy's definition in this country for years. The cyber issue requires a broader range of considerations that must be taken into account.

The curriculum suggestions offered several ways of organizing thoughts regarding how to prepare a cyber strategist for the challenges before him. The cyber environment was described by one strategist in the following way:

The intersection of these forces (globalization, the information revolution, proliferation, numerous actors, resources that shape strategies, etc.) is creating future security environments characterized by greater complexity, compressed decision-making timeframes, rapidly unfolding contingencies that are more likely to radiate across borders, greater access to information and misinformation and growing uncertainty about the true nature of capabilities that both state and non-state actors may possess.³⁸

Whatever direction the development of a cyber strategy curriculum takes, the topics discussed above indicate that a holistic approach is required to develop a cyber strategist due to the global nature and blinding speed of digits. A current cyber strategy approach may require the aptitudes and capabilities of engineers, mathematicians, neuroscientists, and other specialists. Of particular importance for the assault on the mind is the large assembly of social engineering methods that are able to influence and deceive both humans and digits. For example, one analyst noted that 'our vision is that in the near future automatons will eventually be able to rally crowds, open up bank accounts, write letters, all through human surrogates'.³⁹ In July 2013 it was revealed that Carina Santos, a much-followed Twitter journalist, was a bot or automaton created by computer scientists. She was said to have more online 'influence' than Oprah Winfrey.⁴⁰ It is possible to envision that people behind these methods could potentially have strategic goals in mind, such as changing policy or politics, and not simply social chat. Engineering methods and carefully written software may one day be able to fool data links and

connections, forcing specific files to send packets of electrons in the wrong direction or perform the wrong function.

The development of a cyber strategist is thus a complicated endeavor that will require serious training. Strategists of the past had time to analyze a limited number of forces and the terrain on a map. A cyber strategist is faced with a global domain, different types of key terrain (in the sky, on and under land, under water), and unknown forces and methodologies. The qualities indicative of a worthy cyber strategist would include, but not be limited to, the ability to perform some of the following functions:

- Make analytical judgments of the many competencies and approaches for using cyber in order to obtain as accurate a picture as possible of the cyber situation (cyber terrain, etc.) and methodology that is confronting the US.
- Decide what it is that must be manipulated, changed, or countered in order to attain a cyber strategic advantage and implement it.
- Constantly be aware of social engineering constructs and strategies used to fool cognitive rather than technological issues.
- Provide expert analysis of cyber gangs who specialize 'in areas of infiltrating systems, designing malware, mapping networks, and selling stolen data, and employing them to work on different phases of the attack'.
- Become expert in understanding the routing of cyber via optical fiber, satellites, routers, etc., and the use of hardware and software technologies.
- Become expert in domains, terrains, environments, consequence management, and unanticipated risks.

An element of the areas discussed above (algorithms, cyber terrain, etc.) could be shoehorned into one or more of these functions.

The development of this list indicates the difficulty of becoming a bona fide cyber strategist. It may be asking too much of one individual, since there are several layers of specialized knowledge that must be accumulated: algorithms, cyber terrain, national methodologies, and so on. This indicates that a cyber strategist might stand at the head of a task force assembled with specialists in each area. The cyber strategist would, after consultation with his team, arrive at a conclusion for strategic objectives and direction.

It will be interesting to watch how this area develops in the coming years. What is important is developing the talent to handle the number of competencies that are required and to develop personnel or even agencies

equipped to handle the focus areas of this article. And, as soon as this curriculum is developed, quantum computing will outdate it and the race to develop quantum strategists will be on!

Disclaimer

The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the US government.

The Foreign Military Studies Office (FMSO) assesses regional military and security issues through open-source media and direct engagement with foreign military and security specialists to advise army leadership on issues of policy and planning critical to the US Army and the wider military community.

NOTES

- 1 See Geoff Demarest, *Winning Irregular War*, FMSO publication, cited from a section titled 'Nerd Globe', 2014, p.515.
- 2 Mark Morris, 'FBI Director Comes to KC to Emphasize Local Work', *Kansas City Star*, 20 Feb. 2014.
- 3 Shen Weiguang, *Deciphering Information Security* (Beijing: Xinhua Publishing House July 2003) pp.26, 199. To view the entire curriculum, see Timothy Thomas, *Decoding the Virtual Dragon* (Fort Leavenworth, Kansas, 2007) pp.152–7.
- 4 Baron Antoine Henri de Jomini, *The Art of War*, translated by Capt. G.H. Mendell and Lt. W.P. Craighill. (Philadelphia, J.B. Lippencott, 1862), pp. 69–71, in Michael I. Handel, *Masters of War* (London: Frank Cass 2001) p.37.
- 5 Carl Von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton UP 1984) p.128.
- 6 See, for example, <www.military-quotes.com/Napoleon.htm>.
- 7 *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, as amended through 30 Jan. 2011, p.350.
- 8 L. Gordon Crovitz, 'Techies Cheer Creative Destruction', *Wall Street Journal*, 3 June 2013, p.A15.
- 9 Fan Zheng Jiang and Ma Bao An, *On Military Strategy* (Beijing: National Defense UP 2007) p. 43.
- 10 Ibid.
- 11 Ye Zheng and Zhao Baoxian, 'How Do You Fight a Network War?' *Zhongguo Qingnian Bao* Online, 3 June 2011.
- 12 John Walecka, 'Next-Generation Cybersecurity Ratchets Up', *Wall Street Journal*, 26 Feb. 2014, p. A17.
- 13 See Geoff Demarest, *Winning Irregular War*, FMSO publication, cited from a section titled 'Nerd Globe', 2014, p.515.
- 14 Evgeny Morozov, 'The Tyranny of Algorithms', *Wall Street Journal*, 20 Sept. 2012, p.A15.
- 15 Brian Contos, 'Why Cyberwarfare is the Great Equalizer', *USAToday.com*, 30 May 2013.
- 16 Adam Fisher, 'Google's Road Map to Global Domination,' a *New York Times* article at <www.nytimes.com/2013/12/15/magazine/google-plan-for-global-domination-dont-ask-why-ask-where.html?pagewanted=8&_r=0>.
- 17 Ibid.

- 18 Ibid.
- 19 Li Qiang, 'A Scientific Understanding of Complex Battlefield Environments', *Zhanyou Bao*, 9 Nov. 2013, p.3.
- 20 Aleksey Krivoruchek, 'The Defense Ministry Has Prepared Itself for DDoS Attacks', *Izvestiya Online*, 5 Nov. 2013.
- 21 John Bussey, 'How Cybersecurity Laws are Outdated', *Wall Street Journal*, 11 Feb.2014, p.R5.
- 22 Gautham Nagesh and Danny Yadron, 'Guidelines Offered for Cybersecurity', *Wall Street Journal*, 13 Feb. 2014, p.B6.
- 23 Ibid.
- 24 Francis X. Clines, 'Notebook: Can't Hide in the Cloud', *New York Times*, 16 June 2013, p.10.
- 25 Jennifer Golbeck, 'Facebook Wants to Know Why You Didn't Publish That Status Update You Started Writing,' part of *Future Tense*, collaboration among Arizona State University, the New America Foundation, and Slate. The article notes that it is the browser code, not Facebook that reads whatever one types.
- 26 L. Gordon Crovitz, 'Smile, You're on Candid Webcam', *Wall Street Journal*, 2 Dec. 2013, p. A17.
- 27 Katherine Boehret, 'Oh, the Places Your Phone Will Find Just by Passing by', *Wall Street Journal*, 4 Dec. 2013, p. D3.
- 28 Downloaded at <www.ccdcoe.org/249.html>.
- 29 Fabiola Sanchez, 'The Big Story: Power Blackout Hits 70 Percent of Venezuela,' Associated Press, 4 Sept. 2013.
- 30 Christopher S. Stewart and Suzanne Vranica, 'Phony Web Traffic Tricks Digital Ads', *Wall Street Journal*, 1 Oct.r 2013, p.B1.
- 31 Ian Urbina, 'I Flirt and Tweet. Follow Me at #Socialbot', *New York Times*, 11 Aug. 2013, p.5.
- 32 Timothy Thomas, 'Cyberskepticism: The Mind's Firewall,' *IO Sphere*, Spring 2008, p. 4.
- 33 Peggy Noonan, 'The Age of the Would-Be Principis', *Wall Street Journal*, 15–16 Sept. 2012, p. A13.
- 34 'Dara Kerr, 'How Israel and Hamas Weaponized Social Media', <http://news.cnet.com/8301-1023_3-576168890-93/how-israel-and-hamas-weaponized-social-media/>, 13 Jan. 2014.
- 35 Ibid.
- 36 Paul Ziobro and Danny Yadron, 'Hackers Tailored Malware to Retailers', *Wall Street Journal*, 6 Feb. 2014, p.B3.
- 37 Andy Greenberg, 'Tricking the Hackers', *Forbes*, 10 Feb. 2014, p. 44.
- 38 Tate Nurkin, 'Getting Creative to Fight Future Battles', *Jane's Defence Weekly*, 23 Nov. 2011, p.25.
- 39 Urbina.
- 40 Ibid.