Combatting Asymmetric Threats: Dominating the EMS, Defending the Homeland

For the past 13 years, the U.S. has been engaged in a counterinsurgency and counter-terrorism fight, primarily in Southwest Asia (Iraq and Afghanistan) and Africa. These "wars of shadows" will continue unabated, potentially growing even more vicious, as the stakes become the very essence of life: food, water, energy. Concurrently, conflicts in regions of vital U.S. security interest are escalating, with additional festering rivalries teetering perilously on the brink. Such conflicts entail both traditional "wars of iron" – tanks, jets, drones, ships, bombs, and missiles – as well as "wars of silicon" – electronic warfare, cyber, and novel applications of electromagnetic energy.

As America's strategic focus shifts away from conflicts in which it held an overwhelming advantage to operations in denied environments – against adversaries with both greater economic heft and more sophisticated technology than encountered in Southwest Asia – immunity from coercion can no longer be taken for granted.

Today's security challenges are predominantly hybrids: foreign and domestic; offense and defense; high tech and low tech; symmetric and asymmetric; synchronous and asynchronous; regular and irregular; geographically focused and globally ubiquitous. This reality requires multi-dimensional, nuanced, innovative approaches. To triumph against today's and tomorrow's threat array, the U.S. must retain the freedom to attack and the freedom from attack in and through: terrain, atmosphere, oceans, space, and the electromagnetic spectrum. This, in turn, requires integration of systems, capabilities, and operations to maximize the synergies that generate simultaneous, synchronized effects on land, at sea, in the air, space, and cyberspace – all while defending the Homeland.

From this point forward, the U.S. should expect to be challenged at home and abroad in all domains, including in and through space and cyberspace, across the electro-magnetic spectrum (EMS), as well as on land, at sea, and in the air. The race is to the swift: he who masters the EMS and denies it to the adversary, wins. To this end, Chinese Information Operations/Cyber Units have been fully integrated with Electronic Warfare to operate across the Electromagnetic spectrum, termed in Chinese military doctrine as the "5th battlefield."[1] Likewise, specialized Russian units target computer and communications networks gaining hands-on experience in their ongoing operations against Ukraine, while training for high-end, terrestrial, and space-based "radio-electronic combat."[2] Both countries, as well as other state and non-state actors, also field advanced encryption-cracking capabilities to penetrate, corrupt, or co-opt friendly systems. The electron is fast becoming the ultimate precision guided munition (PGM), capable of devastating the targeted nation's economy, critical infrastructure, and military.

The concern with cyber and the critical infrastructure it undergirds is not new. It is, however, becoming increasingly visible. A Pew Research Center opinion poll conducted in December 2013

---

[1]Brendan Koerner, "Inside the New Arms Race to Control Bandwidth on the Battlefield," *Wired*, February 18, 2014, http://www.wired.com/2014/02/spectrum-warfare/; Joshua Phillip, "Chinese Military Gets Trained on Electronic Warfare," *Epoch Times*, October 18, 2013, http://www.theepochtimes.com/n3/322299-chinese-military-gets-trained-on-electronic-warfare/.

[2] Andrei Kislyakov, Russian Military Makes Strides in Electronic Warfare," *Russia Beyond the Headlines*, December 20, 2013, http://rbth.com/science_and_tech/2013/12/20/russian_military_makes_strides_in_electronic_warfare_32797.html; Patrick Tucker, "Why Ukraine Has Already Lost The Cyberwar," *Defense One*, April 28, 2014, http://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350/.

noted that the public ranked cyber as the #1 threat to U.S. national security. Likewise, a more recent Defense News Leadership Poll, surveying senior officials at the White House, Pentagon, Congress, and the defense industry, concluded that 45% of the respondents named a cyber attack as the single greatest threat – nearly 20 percentage points above terrorism, which ranked second.

Growing awareness, while important, is not enough. To produce effective, timely actions, vigilance must be guided by a coherent strategy, based on a clear understanding that the price of failure is nothing less than America's very way of life. The following tenets should underpin the necessary holistic approach:

Cyber is a domain defined by the physics of the electromagnetic spectrum (EMS), electronics, and the systems used to access and exploit their characteristics. As such, Cyber is on par with Land, Sea, Air, and Space – vitally important to the Nation's economic, political, diplomatic, financial, informational, and military power. Indeed, Cyber is America's Center of Gravity; the neural network upon which all activities hinge. No nation is as reliant on and, consequently, as vulnerable in this domain. Cyber enables such indispensable daily functions as power generation, transport and traffic control, industrial processes, global positioning, navigation and timing, communications, intelligence collection (in all disciplines), logistics, security, financial and legal transactions, etc. Likewise, cyber superiority is the prerequisite for effective operations in all domains, from the tactical to the central strategic levels.

In military terms, cyber comprises all operations conducted in and through the EMS, from C5ISR, through Computer Network Defense, Exploitation and Attack, to Electronic Warfare (EW), Directed Energy Weapons, Electromagnetic pulse (EMP), and technologies not yet conceived. The first battle of any future war will be for command of the air, space, and the EMS. Yet the U.S. is neither adequately prepared to withstand and counter the growing threat, nor armed with sufficiently robust offensive capacity.

The peerless network connectivity that the U.S. has used to tremendous economic, political, and military advantage has rendered it more vulnerable than ever, particularly as cyber operations have moved from disruption to destruction. The inflection point in this context has been the Stuxnet worm, reportedly unleashed on Iran's nuclear program. By making the uranium-enriching centrifuges spin out of control, while deceiving the operators as to what was really taking place by showing all gauges to be operating within the required parameters, Stuxnet physically damaged the centrifuges, producing effects that, till then, could be achieved only through kinetic means of blast and fragmentation.[3]

Though the EMS/cyber domain is highly complex, the cost of entry is comparatively low. Electronic attacks are widely seen as a relatively cheap and easy way to wreak havoc on unprecedented scale. Dual-use, readily-available technologies abound. Trillions of dollars in daily global electronic transactions and petabytes of critical, exploitable data offer lucrative target sets. Not surprisingly, cyberspace is rife with criminals, terrorists, and nation-states seeking a high-impact asymmetric advantage at relatively low cost.

To address the increasingly sophisticated threats that both the public and private sectors face, the Department of Homeland Security (DHS) develops National Infrastructure Protection Plans (NIPP) "through a collaborative process involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry." The NIPP is designed to "leverage

[3] Kimberly Peretti and Jared Slate, "State-sponsored Cyber Crime: From Exploitation to Disruption to Destruction," *The SciTech Lawyer*, Winter 2014, http://www.americanbar.org/content/dam/aba/publications/scitech_lawyer/2014/winter/state-sponsored_cybercrime.authcheckdam.pdf.

partnerships, innovate for risk management, and focus on outcomes." In its most recent, 2013 iteration, the NIPP is promulgated as a national plan, "streamlined and adaptable to the current risk, policy, and strategic environments" and designed to facilitate "an integrated and collaborative approach to achieve the vision of a Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened."[4]

The DHS also hosts a biennial, Congressionally-mandated "Cyber Storm" exercise series, providing a framework for the most extensive, government-sponsored cybersecurity exercise of its kind. These exercises, simulating large-scale, coordinated attacks on critical infrastructure, test the processes, procedures, tools, and organizational responses to a multi-sector, coordinated attack. According to DHS, Cyber Storm exercises:

- Examine organizations' capability to prepare for, protect from, and respond to cyber attacks' potential effects;
- Exercise strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures;
- Validate information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response, and recovery information; and
- Examine means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests.[5]

Yet Cyber Storm, along with similar exercises conducted by other departments and agencies, also demonstrates that small "Red Teams," using exploits downloaded from the Internet, consistently disrupt the "Blue (friendly) Actors."[6] This leads to a series of poignant questions: if a significant level of damage can be inflicted by a few smart people, in a few days, using tools available to everyone, how much damage could be inflicted by a determined, sophisticated adversary with large amounts of people, time, and money? What would happen in an America suddenly deprived of electricity, water, money, communications, and fuel? What would happen if food and medicine distribution were rendered ineffective? What if the entire transportation system – trains, planes, ships, and automobiles – came to a screeching halt? What if law enforcement and emergency personnel were unable to function? Would the damage equal a weeks-long power outage, or pose existential consequences similar to the Cold War nuclear threat? How effective and realistic are extant response plans and mitigation approaches, given that the lion's share of the critical infrastructure is privately owned and compliance is voluntary and, thus, unenforceable?

Likewise, prudent planning should assume that in a full-scale conflict with a mature adversary, the U.S. would have to deal with any and all of the following: denial of service; data and supply chain corruption; jamming; spoofing; traitorous insiders; and kinetic and non-kinetic attacks at all altitudes – in and through all domains. Weapons systems might not work, or, worse, fire on friendly forces. Critical resupply – ammunition, spare parts, food, water, and medical evacuation – might not arrive

[4] National Infrastructure Protection Plan 2013, http://www.dhs.gov/national-infrastructure-protection-plan.
[5] Department of Homeland Security, "Cyber Storm: Securing Cyber Space," http://www.dhs.gov/cyber-storm-securing-cyber-space.
[6] The most famous and publicly discussed of those exercises is "Eligible Receiver" in 1997. Bradley Ashley, "Anatomy of Cyberterrorism," Air University Press, February 27, 2003, http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA424625. See also, *Final Report of the Defense Science Board's Task Force on Resilient Military Systems*, October 11, 2011, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

when or where needed. Leaders trained to trust information displayed on their various plasma screens are particularly vulnerable to deception and manipulation. As a result, operators would lose trust in the data they receive, further degrading the ability to command forces and control systems.

Risk is a function of threat (capabilities and intent); one's own vulnerabilities (inherent or operationally introduced); and consequence (fixable or fatal to the impacted systems). There is no credible mechanism to reduce any of these three risk parameters to zero, thus obviating the threat. Therefore, the threat, vulnerability, and consequence equation cannot be managed in isolation. A systems solution is required.

Today, the preponderance of money and effort are spent defending against the inherent vulnerabilities that exist in all complex systems. In 2014, the global cybersecurity market is said to be worth $77 billion, doubling to $155.7 billion by 2019.[7] Yet defense-only, especially perimeter defense which tries to keep attackers from gaining access in the first place, is simply not enough.

Defense buys tactical breathing room, much like treading water: if one finds oneself in the middle of the ocean, treading water is a good thing, but insufficient as a long-term strategy. Currently, it is both cheaper and easier to attack a network than to defend it. To win, what must be changed is the cost equation and adapt an approach that assumes the adversary is already inside our networks. This will shift the focus to solutions that would allow both the U.S. Government – at the federal, state, and local levels – as well as the equally-reliant, but even more vulnerable private sector, to continue operations, while protecting essential data. To prevail, the U.S. must field knowledge-centric systems that process, filter, integrate, and convey data in ways that enable quick, logical decisions…no matter the external stresses and disruptions. Resilient, self-forming, self-healing networks are required to sustain and recover essential functions, fight through, and win.

The U.S. urgently needs new approaches and authorities to ensure the resilience of its vulnerable critical infrastructure in the diverse sectors theoretically integrated through DHS's array of "self-organized, self-run, and self-governed" Sector Coordinating Councils, interacting with an equally loose set of Government Coordinating Councils.[8] Likewise, DoD and the Intelligence Community require immediate, innovative solutions to deliver command, control, communications, computers, cyber, intelligence, surveillance, reconnaissance (C5ISR); EW; and other kinetic and non-kinetic effects in a contested, full-spectrum, electronic and cyber warfare environment. The ability to anticipate, plan for, coordinate, and execute operations against adversaries capable of simultaneously threatening the Homeland and harming U.S. forces, allies, and friends is paramount. The price of failure is nothing less than America's prosperity and global stature as the indispensable power for good, and, ultimately, its very way of life.

---

[7] "Cyber Security Market to Hit $77B," *Federal Times*, February 21, 2014, http://www.federaltimes.com/article/20140221/CYBER/302210004/Cybersecurity-market-hit-77B.

[8] In February 2013, President Obama issued a Presidential Policy Directive (PDD) requiring federal agencies and critical infrastructure owners and operators to work cooperatively to minimize risks and strengthen resilience. The order gave the DHS Secretary wide latitude to designate critical infrastructure, though it remains to be seen whether broadening the list will make much of a difference in heading off cybersecurity threats. Nothing in the PPD clarifies what the mechanisms for the required "timely information sharing" are or, more crucially, how the expanded definitions would actually transform the fragmented, essentially voluntary compliance system. http://www.dhs.gov/critical-infrastructure-sector-partnerships.
In July 2014, the SANS Institute, which specializes in information and cybersecurity, warned that the DHS program is suffering from low adoption rates: "Despite extensive outreach by DHS, the 'trickle down' of information to security administrators, analysts and operations staff has been limited."