Strategic Insights: Speed Kills—Enter an Age of Unbridled Hyperconnectivity

June 9, 2017 | Mr. Nathan P. Freier

This month, a team of U.S. Army War College (USAWC) researchers concluded a yearlong study on enterprise-level risk and risk assessment inside the Department of Defense (DoD). *At Our Own Peril: DoD Risk and Risk Assessment in a Post-Primacy World* argues for a new Department-level risk concept for describing, identifying, assessing, and communicating risk in an environment defined by sudden disruptive change. It suggests that a new concept should rest on four foundational principles: diversity, dynamism, persistent dialogue, and adaptation.[1]

Among *At Our Own Peril's* many insights, perhaps the most enlightening are those concerning the strategic environment and the complex hazards emerging from it. The report characterizes the contemporary environment as one of "post-primacy," where the United States remains a global power, but one that is commonly confronted by purposeful and contextual defense-relevant challenges that fall considerably outside of the DoD's dominant bias and convention.

The study suggests that the most transformative characteristic of the contemporary environment is the sudden onslaught of threats emerging from the dark underside of hyperconnectivity.[2] It is difficult to exaggerate the degree to which hyperconnectivity enables—according to the study's authors, researchers, and the defense-focused communities of interest and practice it consulted with—the following:

- Hostile or disruptive virtual mobilization worldwide;
- The collapse of privacy, secrecy, and operational security;

- Penetration, disruption, exploitation, and destruction of data storage and transmission, as well as the use of data and data-enabled systems; and finally,
- The unfettered manipulation of perceptions, material outcomes, and consequential strategic decisions through the strategic employment of various forms of information.

A New Appreciation for Information as an Instrument of Hostile Competition and War.

That which is loosely identified as the information sphere and—indeed often wrongly characterized exclusively as the cyber domain —has of late become the world's most contested and congested competitive space.[3] Indeed, while well-meaning strategists and planners work through the incredible complexity of cyber competition and conflict, the broader competitive space that revolves around information has rapidly transcended the challenges of ones and zeros alone.[4]

On the first, second, and third points, *At Our Own Peril* makes the following basic observations. First, the proliferation of portable communications and computing devices—matched with their inevitable interconnectedness—unavoidably increases the ability of purposeful actors at and below the state level to communicate, plan, agitate, and execute profoundly disruptive acts that range from the unprovoked and malicious to targeted and incredibly destructive.

Furthermore, the same connectivity also becomes a vehicle for the rapid, viral transmission of equally disruptive information, emerging more organically and triggering unanticipated, seemingly leaderless security challenges. The latter are literally unbounded, borderless, and virtually—at times—uncontrollable.[5] In the study team's view, the strategic significance of hyperconnectivity cannot be overstated. Currently, imagination is the only barrier to the worst possible manifestations of this increasingly complex challenge to U.S. interests and enduring defense objectives.

On the second point, it is clear that Americans (elite or otherwise) no longer benefit from an assumption of privacy to the extent that they are connected to the information grid. Virtually, anyone can be found, exposed, extorted, embarrassed, robbed, harmed, or intimidated from either open or anonymous sources as long as they remain "plugged in" and active on the worldwide web.[6] With the collapse of personal privacy comes the inevitable elimination of secrecy and operational security from a national security and defense

perspective as well. Wide uncontrolled access to technology that most now take for granted is rapidly undermining prior advantages of discrete, secret, or covert intentions, actions, or operations.[7]

The wide proliferation and use of cellular devices capable of high-definition recording matched to their capability for immediate transmission of sound, pictures, and written text is transforming both how the world gets its most up-to-date information, as well as fundamentally undermining the ability of the world's militaries and intelligence services to operate with a modicum of operational security. Furthermore, individuals, groups, and states are now able to access imagery and sensitive open source information that once was tightly controlled by governments. In the end, senior defense leaders should assume that all defense-related activity from minor tactical movements to major military operations would occur completely in the open from this point forward.[8]

On the third point, the secure storage, transmission, and use of data and data-enabled systems are under persistent assault. From a cyber perspective, unconnected or closed systems are frankly never completely closed.[9] Open systems are literally open to all. Finally, connected but encrypted systems are in fact first "connected" and then "encrypted." They are, therefore, neither closed nor unbreachable. Consequently, state secrets, sensitive or proprietary information, and information enabled technical systems face concerted efforts to penetrate, expose, and/or manipulate them for a variety of motives. The defense-related hazards are myriad in this regard.

A Different More Sophisticated Appreciation of Information as a Weapon.

Recent events indicate that hyperconnectivity as it relates to the fourth point—unfettered manipulation of perceptions, material outcomes, and consequential strategic decisions—may just be the most immediately consequential. Largely free riding on the back of a metastasizing global cyber superstructure, actors are increasingly weaponizing information, disinformation, and popular disaffection in order to bypass the traditional defenses of target states and institutions. Furthermore, the incidental or accidental weaponization of the same is increasingly creating unguided and unintended collateral effects from the strategic to tactical levels of decision and action. There are countless examples of these impacts in the contemporary environment.[10]

Now, as information literally travels at light speed, it is very difficult to limit its adverse effects. Sometimes the exposure or exploitation of high-impact information is **fact-free**. Sometimes it is **fact-inconvenient**. Still other times it is **fact-perilous**. Finally, there are times that it is **fact-toxic**.

The first proliferates in ways that undermine objective truth. In short, once fact-free information is deposited in or employed through the information sphere, the real story is lost in a sea of alternative realities. George F. Kennan was prescient in this regard when he observed, "the truth is sometimes a poor competitor in the market place of ideas—complicated, unsatisfying, full of dilemmas, always vulnerable to misinterpretation and abuse."[11]

Fact-inconvenient information exposes comprising details that by implication undermine legitimate authority and erode the relationships between governments and the governed. Fact-perilous data gives away the keys to the castle—exposing highly classified, sensitive, or proprietary information that can be used to accelerate a real loss of tactical, operational, or strategic advantage. Finally, exposed in the absence of context, fact-toxic information poisons important political discourse and fatally weakens foundational security at an international, regional, national, or personal level. Indeed, **fact-toxic** exposures are those likeliest to trigger viral or contagious insecurity across or within borders and between or among peoples.

Wake-Up! The Problem is Bigger than Cyber.

In light of all of this, securing computer networks and cyber lines of communication from the predations of opportunistic opponents remains a critical component of U.S. defense calculations. However, this is essential but also insufficient in the contemporary environment. Indeed, to date, American strategists have focused to the point of distraction on defense against the purposeful interruption or destruction of the U.S. information-focused connective tissue, as well as intrusion into and damage to sensitive information repositories. However, consequently, they have been less focused on the purposeful exploitation of the same architecture for the strategic manipulation of perceptions and its attendant influence on political and security outcomes.[12]

This idea of the grid as a vulnerability, a vector, and a weapon is an important future risk consideration for the DoD. Further, the ongoing revolution in connectivity will continue to transform how the DoD perceives and responds to hazards and calculates the risk factors related to all three considerations.

At Our Own Peril found a single core defense implication of hyperconnectivity—"speed kills." With hyperconnectivity comes a quantum increase in the velocity of change in strategic circumstances. It raises the specter of sudden, violent, or disruptive political contagions; rapid, unintended military escalation; as well as war prosecuted by alternative—even overtly non-violent—means at increasingly faster processing speeds. Furthermore, it enables virtual mobilization and distributed collective action under no centralized authority or control and at speeds that will outpace any 20th century bureaucracy's ability to adapt or respond.

When combined, these all add up to a much more complex and uncertain decision-making environment for senior defense and military leaders. The United States can clearly build more layered defenses against cyber-borne attacks on data and infrastructure. However, the most effective adversaries and adversarial forces have moved on to newer, more insidious methods. Human perceptions and the relative value of truth have increasingly become ripe territory for low risk/high impact manipulation of strategic outcomes, promising outsized strategic effect compared to relatively small investments in resources.

ENDNOTES

1. This "Strategic Insight" article is a synopsis of material from Nathan Freier *et al.*, *At Own Peril: DoD Risk and Risk Assessment in a Post-Primacy World*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, forthcoming.

2. Anabel Quan-Haase and Barry Wellman, "Networks of Distance and Media: A Case Study of a High-Tech Firm," paper presented at the "Trust and Communities Conference," Bielefeld, Germany, July 2003.

3. Louis Columbus, "Roundup Of Internet of Things Forecasts And Market Estimates, 2016," *Forbes*, November 27, 2016, available from *www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#bcaa1034ba55*, accessed January 10, 2017.

4. Colonel Joseph Felter, U.S. Army, Ret., "It's Not Just The Technology: Beyond Offset Strategies," *Strategika,* Iss. 39, March 15, 2017, available from *www.hoover.org/research/its-not-just-technology-beyond-offset-strategies*, accessed March 18, 2017.

5. "The Arab Spring: A Year of Revolution," *All Things Considered*, National Public Radio (NPR), December 17, 2011, transcript available from *www.npr.org/2011/12/17/143897126/the-arab-spring-a-year-of-revolution*, accessed March 21, 2017.

6. Nicole Perlroth, "Hackers Used New Weapons to Disrupt Major Websites Across U.S.," *The New York Times*, October 21, 2016, available from *https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html*, accessed December 18, 2016.

7. Columbus.

8. Patrick Tucker, "ISIS Has a Drone Strategy Too," *The Atlantic,* October 18, 2016, available from *www.theatlantic.com/technology/archive/2016/10/anti-drone/504479/*, accessed January 8, 2017.

9. Berndt Brehmer, "The Dynamic OODA Loop: "Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control," paper presented at 10th International Command and Control Symposium: The Future of C2, p. 2, available from *www.dodccrp.org/events/10th_ICCRTS/CD/papers/365.pdf*.

10. For example, "The Arab Spring: A Year Of Revolution," December 17, 2011.

11. George F. Kennan, *American Diplomacy*, Chicago: University of Chicago Press, 1984, p. 62.

12. Senator Rob Portman, "Senate Passes Major Portman-Murphy Counter-Propaganda Bill as Part of NDAA," December 8, 2016, available from *www.portman.senate.gov/public/index.cfm?p=press-releases&id=3765A225-B773-4F57-B21A-A265F4B5692C*.

*****