A Conversation with General (Ret.) David H. Petraeus

Cyber operations are a perfect example of how efforts in one domain can affect virtually every aspect of a nations comprehensive security. The CDR was keenly interested in General David Petraeus' view of comprehensive security, its whole-of-government implications, and its critical importance to the United States. The interview was conducted via email during April and September of 2019.

The Cyber Defense Review (CDR): The 2018 DoD Cyber Strategy and GEN Paul Nakasone's February 2019 Congressional testimony describe a new, emerging strategic environment in cyberspace characterized by "great power competition" or "strategic competition" with China, Russia, and others. The dynamics of this new environment are perhaps most salient in cyberspace, with the US confronting near-peer and arguably even peer competitors, and where, due to the reliance of our economy and society on IT-connected infrastructure, the US is particularly vulnerable. This strategic competition extends well beyond cyberspace, to include political, military, and economic competitions across all other domains and instruments of power. How do you see strategic competition in cyberspace in relation to the other domains of warfare?

General (Ret.) David H. Petraeus: *Cyberspace is the newest domain of warfare, and is now very much front and center, joining land, air, sea, and space. It is also the domain in which "warfare" is already ongoing on a daily basis, as state and non-state actors probe our cyber defenses, conduct cyber reconnaissance of critical infrastructure control systems, try to inspire and direct extremist activities, seek to steal secrets and intellectual property, attempt to influence our debates and elections, and carry out criminal acts, among many other activities. Beyond that, any future military campaign inevitably will entail increasingly complex and important offensive and defensive cyberspace operations that complement operations in other domains, employing cyberspace capabilities to help defend our systems and also to degrade, disrupt, and defeat our adversaries' systems and networks that depend on cyber connectivity and other aspects of cyberspace.*

General David H. Petraeus (U.S. Army, Ret.) is a Partner with the global investment firm KKR and Chairman of the KKR Global Institute. He also serves on the boards of two KKR-owned companies, Optiv (a major cybersecurity firm) and OneStream (a leading business software provider), as well as the boards of a number of think tanks and numerous veterans service organizations. Additionally, he is a private venture capitalist with investments in well over a dozen startups. He previously served over 37 years in uniform and then was Director of the CIA. He culminated his military career with six consecutive commands, five in combat, including Command of the Multinational Force-Iraq during the "Surge," US Central Command, and the International Security Assistance Force in Afghanistan. A graduate, with distinction, from the U.S. Military Academy in 1974, General Petraeus later earned a Ph.D. from Princeton University in a multi-disciplinary program in international relations and economics. General Petraeus has held academic appointments at the U.S. Military Academy, the City University of New York's Honors College, the University of Southern California, and Harvard's Belfer Center. His numerous awards and decorations include four Defense Distinguished Service Medals, the Bronze Star Medal for Valor, the Combat Action Badge, the Ranger Tab, and Master Parachutist Wings. He has also been decorated by 13 foreign countries.

CDR: Your career has provided you with the unique opportunity to have an impact at senior levels in both the government and the private sector. Our adversaries carry out sophisticated cyber campaigns targeting the private sector; and the DoD has a mandate to "defend the Nation" in cyberspace, which includes the economic engines in the private sector. Given your experience, how can the U.S. Government and our private sector better collaborate to defend the Nation in cyberspace?

GEN (Ret.) Petraeus: *In recent years, the U.S. Government has taken many actions to improve our Nation's defenses (and offensive capabilities) in cyberspace, though clearly more work is required.*

Elevating U.S. Cyber Command (USCYBERCOM) to a fully-fledged combatant command in May 2018 was one (overdue) such action; and much more work needs to be done to fully define roles and missions of USCYBERCOM overall and the National Security Agency (NSA) and USCYBERCOM's other components individually, as well as its ultimate organizational architecture. Among these, the Department of Defense (DoD) still needs to resolve whether USCYBERCOM is, in essence, a military service (that recruits, trains, educates, equips, develops, etc.), a geographic combatant command (with cyberspace as its area of responsibility), or a functional combatant command (such as U.S. Special Operations Command)–or will perform tasks of all three, which I support, but which will also require in-depth conceptual work, as this in many respects would present a new paradigm for our military.

The establishment of the Cybersecurity and Critical Infrastructure Security Agency (CISA) within the Department of Homeland Security last fall was another positive step, one that many of us argued for some time ago. Nonetheless, much hard work is needed to build CISA concepts and capabilities, to recruit needed personnel, to enact enabling legislation, to build up required resources, and to implement the policies and regulations that will optimize our ability to operate in this newest warfare domain.

Finally, the establishment four years ago of the Cyber Threat Intelligence Integration Center in the Director of National Intelligence headquarters was another critical step, given that intelligence on state and non-state actors in cyberspace is so important to government cybersecurity activities, but also, through various methods of sharing, for private-sector cybersecurity firms and US companies, as well.

Needless to say, government efforts are complemented in a very significant manner by a growing number of cybersecurity firms, products, capabilities, and integrators. And there is healthy collaboration among them, the intelligence community, U.S. executive departments that operate in this arena, and various national (especially the FBI as the lead federal agency for cybercrime investigation), state, and local law enforcement agencies.

Despite these actions and a number of others, I suspect that most individuals engaged in either government or private sector cybersecurity would acknowledge that the challenges continue to get ever more complex and sophisticated–and that it is hard just to keep pace with them conceptually, much less get the new legislation, resources, organizations, capabilities, policies, and regulations needed to cope with the evolving challenges in a timely manner. It would be accurate, I think, to observe that we need substantially to "pick up the pace" in this public-private partnership arena if we are to effectively counter the cyber threats we currently face, and which will inevitably grow in scope and complexity. (The NSA's newly announced Cybersecurity Directorate likely will help in this area.)

CDR: As the global strategic environment evolves in complexity, volatility, uncertainty, and ambiguity, it is critically important to analyze how the Army's talent management strategy recruits Soldiers for service in the future strategic cyber environment. What strategy should the Army install to attract cyber talent?

GEN (Ret.) Petraeus: *I think the Army has a reasonable sense of what is required to attract great cyber talent. That said, it needs to work very hard at this task. Being a cyber warrior clearly provides the extraordinary privilege of performing tasks that protect our country and way of life. That special privilege that will animate many. But recruiting great talent will also require special incentives in terms of compensation, fully-funded and cutting-edge training and education, opportunities with industry, and so forth. Of course, at the end of the day, there is always the intriguing reality that military cyber warriors can take actions in cyberspace that are not permissible in the private sector.*

Retention is another big challenge, of course, and one must recognize that even special compensation in uniform is unlikely to compete with Silicon Valley salaries; nonetheless, the opportunity, again, to perform missions larger than self together with others who also appreciate that opportunity, is very special. And, combining that motivation and the incentives I mention above has enabled NSA and the newer service cyber organizations to demonstrate an impressive ability to recruit and retain high quality cyber experts. Undoubtedly, though, recruiting and retention in this space will continue to be challenging.

CDR: The Russian and US information warfare capabilities seems to be growing at an alarming rate. Russians have successfully operationalized the Gerasimov Doctrine in Crimea and Ukraine, using information in conjunction with intelligence and special forces operations to achieve some strategic outcomes at relatively low cost. Likewise, as the DNI Report (January 6, 2017) confirmed, Russians manipulated social media platforms such as Facebook and Twitter during the 2016 US Presidential election. There is evidence that Russians also interfered in the UK's Brexit referendum. Despite Russian success in information warfare the Pentagon continues to think conventionally, such as hardening conventional forces in Poland to deter Putin. In your opinion, how does the US correct its course to compete in the information space?

GEN (Ret.) Petraeus: *The press in recent years has reported integration of U.S. military cyberspace operations with other warfare domain operations in ongoing campaigns against Islamist extremist organizations.*

For example, starting over three years ago, Task Force Ares activities complemented Coalition Joint Task Force actions on land and in the air, as well as our host nation partner's actions on the frontlines in Iraq and Syria that ultimately defeated the Islamic State in those countries (though disturbing remnants of IS remain). More recently, USCYBERCOM reportedly has exploited new authorities by taking offensive actions against foreign entities seeking to undermine democracy in the US, to include Russian entities seeking to interfere in the 2018 mid-term elections. The Department of Justice has pursued legal action in several cases against state and non-state actors, as well. And various diplomatic initiatives have also been pursued, including President Obama's pushback against China's theft of US intellectual property.

Those actions have been steps in the right direction. But it is clear that more needs to be done, employing every tool available to the US, our Government, and private sector, and that all government and private sector elements must collaborate better and accomplish more.

CDR: The DoD 2018 Cyber Strategy has adopted a more aggressive strategy of countering our adversaries in cyberspace with a policy of "Defend Forward," with an expanded focus of preventing and responding to cyberattacks that are below the threshold of military use of force. More recently, news reports have circulated that USCYBERCOM has engaged in its first such operation, taking offline a so-called Russian "troll farm" on election day in November 2018. Do you see this new development as an appropriate domain for the military since such operations will occur below the use of force threshold, and will likely be in defense of private entities and infrastructure?

GEN (Ret.) Petraeus: *I very much see it that way, and I strongly support the recent authorizations given to USCYBERCOM. But, as I noted in answering the previous question, I think the US will need to employ more aggressively all the capabilities available to us–legal, financial, diplomatic, cyber, and, in some cases, even military. As is often the case, a comprehensive, integrated approach is required. And inevitably, that will require overall coordination by the White House and executive branch departments and agencies, as has been seen in the current and past administrations, in particular. Going forward, in the years ahead, this coordination must be robustly resourced and maintained as one of our Nation's top priorities.*

GEN (Ret.) David Petraeus with West Point Cadets at the 2018 International Conference on Cyber Conflict in Tallinn, Estonia.