THE CIPHER BRIEF CYBER ADVISORY BOARD:
NAVIGATING A NEW CYBER COMMAND

INTRODUCTION

The Cipher Brief Cyber Advisory Board convenes meetings with some of the most innovative thinkers across government and the private sector, tackling a range of cyber threats. Meetings are bi-monthly and are moderated by General Michael Hayden, former Director of the NSA and CIA, as well as a rotating list of guest moderators depending on the topic.

The Cipher Brief brought together a group of distinguished experts from military, intelligence, civil society, and private industry backgrounds for its Cyber Advisory Board Meeting on "Navigating a New Cyber Command" to discuss the growing challenges in engaging adversaries on the virtual battlefield.

KEY QUESTIONS:

- Are today's cyber warriors hampered by a lack of doctrine and if so - how can CYBERCOM address it?
- Should the future CYBERCOM model Special Operations Command or, given its role in the larger defense support to civilian authorities mission, would Northern Command serve as a better example?
- Does CYBERCOM need to proactively campaign to the American people and its industries – especially IT - on how it will effectively operate within the proper boundaries of a Title 10 organization?
- What triggers war in cyberspace, and are these areas that CYBERCOM is structured to fight and win in?

KEY FINDINGS

» The lack of doctrine is making fighting in cyberspace more difficult – but CYBERCOM's campaign against ISIS is creating the history and experience necessary to establish doctrine for America's cyberwarriors.

» CYBERCOM must be integrated with the private sector; the nation that best integrates with industry will have the most success in cyberspace.

» CYBERCOM faces two serious barriers to communicating its mission to the American people – a history of secrecy because of its affiliation with the National Security Agency, and the general public's lack of knowledge of cyber issues in general.

» There is no consensus about what constitutes an act of war in cyberspace, and norms are being established without significant input from the United States.

QUESTION 1: DOCTRINE

While the Army, Navy, and Air Force have years of combat history to study, analyze, and develop into doctrine, America's cyber warriors are not yet forged in the same way. And while the Navy devotes time and resources to understanding and preparing for what future conflict at sea will look like, according to one Cyber Advisor, the armed services are not dedicating the same amount of "cyber mindfulness" to understanding what future conflict in cyberspace entails.

"When you look at Russian doctrine in this space, it is far more elegant than anything American senior officers are doing," said General Michael Hayden, former Director of both the CIA and NSA and moderator of the Cyber Advisory Board. Our Board noted that even though technology has changed radically over the last four decades, the dynamics of cyber conflict have not changed; while the battlefield seems fluid, tactics have been the most affected – not strategy.

However, the U.S.' campaign against the Islamic State represents the first time CYBERCOM has publically entered the fight, and it has provided practice and experience that will help inform doctrine, training, and personnel structure. In a joint operation last November, Operation Glowing Symphony, the NSA and Cyber Command obtained access to ISIS administrator accounts and used them to block out members and delete content such as battlefield videos, how-to manuals, and recruitment forums.

Our experts agreed that CYBERCOM must be careful not to overlearn the lessons of this fight. Conventional warfare between near-peer adversaries will not be the same as engaging technically unsophisticated networks of individuals affiliated with ISIS. Generalizing knowledge gained fighting ISIS would be dangerous, in the mind of our Board, "because we have superiority over them that we are not going to have in many other cyber conflicts."

QUESTION 2: SOCOM OR NORTHCOM?

The 2016 National Defense Authorization Act directed the elevation of CYBERCOM using prescriptive language very similar to U.S. Special Operations Command's language, giving it service-like authorities: control over budgets, acquisition, work force development and training.

Though it would represent a major cultural shift for CYBERCOM, the Cyber Advisory Board considered the idea that a better model for its mission would be that of Northern Command, which is dedicated to defense support to civilian authorities and the protection of the contiguous United States. NORTHCOM, said one Advisor, is fully defensive in nature. In his eyes, CYBERCOM would have a hard time fulfilling a defense support to civilian authorities mission while so closely tied to the NSA. So,

> *"CYBERCOM needs to identify itself and its mission," noted General Hayden.*

No matter the model, CYBERCOM must be deeply integrated with the private sector. According to a leading academic in the space, there are few instances when the government was the deciding factor in a cyber crisis. Rather, the private sector has the expertise and agility to "bend cyberspace" and address attacks. The government, on the other hand, has other levers of power such as longevity, resources, and the authorities to leverage them. Therefore, success will be achieved by the nation that best integrates with the private sector.

QUESTION 3: HOW DOES CYBERCOM COMMUNICATE WITH THE AMERICAN PEOPLE?

CYBERCOM faces two serious barriers to communicating its mission to the American people – a history of secrecy because of its affiliation with the National Security Agency, and the general public's lack of knowledge of cyber issues in general. And, as a journalist in attendance brought up, the CYBERCOM campaign against ISIS was the first acknowledged military campaign in cyberspace, which served to "normalize" cyber as a weapon.

The NSA operates under Title 50 espionage authorities, while Cyber Command, as the country's cyber warfare and national defense combatant command, operates under Title 10 warmaking authorities. According to one former senior intelligence official on the Board, "The theory…was that both are constituted by traversing cyberspace, finding and fixing something in cyberspace, and then and only then will they decide if they will exploit it, attack it, or defend it." However, according to this view, that approach missed "the fact that the texture, the context, and the speed are profoundly different," between NSA and Cyber Command operations.

But perhaps more difficult is the fact that the analogies society uses today to communicate about cyber issues are flawed. In the words of a Cyber Advisor from the intelligence community, "the reality is that no one understands how their computer works" and therefore, trying to speak a language that fits the frame of warfare makes everything more difficult.

QUESTION 4: WHAT TRIGGERS WAR IN CYBERSPACE?

The Cyber Advisory Board agreed that there is no consensus about what constitutes an act of war in cyberspace, and norms are being established without significant input from the United States. Recent events injected an entirely new vocabulary into the American lexicon: Russian troll farms, weaponized information, fake news, disinformation, bot armies and the darknet. But, do the use of these meet the threshold of an act of war?

The United States, in the eyes of our Cyber Advisory Board, is allowing cyber norms to be written around it. "One way to establish norms is to affirmatively declare doctrine, and another is to call out when folks cross what we would want to be normative lines," said a leading legal expert in the field of cybersecurity. But, many of our Cyber Advisors noted that other countries, such as Iran and North Korea, "are using the tools and creating norms and we aren't complaining about them." What's more, the near-peer adversaries that the United States could find itself in cyber conflict with in the future – most notably Russia – do not adhere to the same cyber warfare rules.

The Board also agreed that cyber is simply a tactical medium that enables traditional objectives, and technical superiority without strategy behind its application is insufficient. A private sector executive noted that often, too much emphasis is placed on cyber warfare, when in reality, the conflict involves hybrid warfare, of which cyber is merely a component: "you don't use every weapon you have in every battle."

The Cyber Advisory Board also agreed that technical superiority is not enough – rather, it is about "brain-to-brain superiority." A former leader of an intelligence agency added that cyber is a weapon with a shorter shelf-life and a smaller competitive advantage. "The technical capabilities matter less here. It is the maturity of the application," he said.

> *"The Russians are ten years ahead of us in that regard."*

WHERE OUR EXPERTS DISAGREE

» While many on the Board laid out the danger of developing doctrine out of an asymmetrical cyber fight such as the campaign against ISIS, others pointed out that no matter the service or weapon, the development of doctrine takes time, and this experience, alongside the elevation of the command, provides significant momentum in the right direction. How CYBERCOM categorizes its success and failures against ISIS will inform how it prepares and trains for future fights.

» The Board agreed that there is no consensus on **what** constitutes an act of war, but there was also disagreement about, **who**, or what entity, will ultimately make that decision. At a policy level, the United States may not want something to rise to the level of an act of war – but the policymakers may not be the ones who decide. Rather, businesses, courts – or another head of state - might make that decision before the U.S. can address the situation. However, a leading attorney in this field noted that a business simply cannot decide something is an act of war: rather, the private sector will put so much pressure on the government that it will be forced to make a decision. In General Hayden's words, without clear guidance, "answers will be created on our behalf."

» There is no agreed upon counter-narrative to misperceptions about CYBERCOM and the idea that the U.S. is "militarizing cyberspace." In a vacuum, the lack of a counter-narrative allows adversaries to spread misinformation. But, mixed messages from the government on the topic, in the eyes of one Cyber Advisor, has the potential to "undermine public confidence."

KEY QUESTIONS TO MOVE THE CONVERSATION FORWARD

» What does CYBERCOM's mission, personnel makeup, and acquisition requirements look like in an era of artificial intelligence and wars fought by algorithm?

» How can CYBERCOM be used as part of a comprehensive strategy, rather than an operational tool?

» How can CYBERCOM coordinate with other military components and integrate with commanders operating in other domains – land, air, sea, and space?

» What role does CYBERCOM have in developing the voice of the U.S. on norms regarding the militarization of cyberspace?

THE CYBER ADVISORY BOARD MEMBERS

General Michael Hayden
Former Director, CIA and NSA

Admiral James 'Sandy' Winnefeld
Former Vice Chairman, Joint Chiefs of Staff

Matthew Olsen
Former Director, National Counterterrorism Center

Chris Inglis
Former Deputy Director, National Security Agency

Rick Ledgett
Former Deputy Director, National Security Agency

Matt Devost
Managing Director, Accenture Security

Michael Sulmeyer
Director, Belfer Center's Cyber Security Project, Harvard University

Jason Healey
Senior Research Scholar, Columbia University

Lieutenant General Kevin McLaughlin
Former Deputy Director, U.S. Cyber Command

Jill Singer
Vice President, National Security, AT&T Global Public Sector

Raj De
Former General Counsel, National Security Agency

Bob Griffin
CEO, Ayasdi

Dmitri Alperovitch
Co-Founder and CTO, Crowdstrike

Neal Pollard
Principal, PricewaterhouseCoopers

Bob Gourley
Co-Founder and Partner, Cognitio

Nils Puhlmann
Co-Founder, Cloud Security Alliance

The Cipher Brief's Cyber Advisory Board is a community-based Board of leaders and influencers from both the public and private sectors who share their perspectives on today's most pressing cyber threats. If your company wants to take a proactive thought leadership position by becoming a sponsor of this public-private forum discussing emerging threats, vulnerabilities, and the policies to address them, please contact Brad Christian at bchristian@thecipherbrief.com.

Thank you to our sponsor Raytheon

Raytheon