Statement for the Record

Richard Bejtlich

Chief Security Strategist

FireEye, Inc.

Before the

U.S. House of Representatives

Committee on Armed Services

Outside Perspectives

on the

Department of Defense Cyber Strategy

September 29, 2015

Chairman Thornberry, Ranking Member Smith, members of the Committee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. I am also a nonresident senior fellow at the Brookings Institution, and I am pursuing a PhD in war studies from King's College London. I began my security career as a military intelligence officer in 1997 at the Air Force Information Warfare Center.

My employer, FireEye, provides software to stop digital intruders, with 3,400 customers in 67 countries, including 250 of the Fortune 500. Our Mandiant consulting service, known for its 2013 report on Chinese PLA Unit 61398, helps companies identify and recover from intrusions. In 2014, we conducted hundreds of investigations in 13 countries.

As a private sector defense strategist and as a former military officer, I assess the new DoD cyber strategy as a transition document. Previous strategies emphasized DoD's role as protecting DoD networks from attack. The current document restates this role, and adds a new albeit limited mission: "defend the US homeland and vital interests from disruptive or destructive cyber attacks of significant consequence." Stepping outside the Beltway mentality, it might be natural to ask "what about OPM?" or even "what about Sony?" For these reasons I believe DoD's strategy is a step in the right direction, but one that needs to be augmented by additional measures.

Before listing my recommendations, I would like to briefly discuss four relevant topics: private sector security capabilities, attribution, hack-back, and acquisition.

In 2013 Mandiant published its APT1 report, exposing a Shanghai-based military unit that had attacked over 140 companies in a seven year period. Since then many other security companies and private research organizations have released reports describing a variety of hacking teams. Some organizations, like the Atlantic Council, have exposed the operations of Russian soldiers in Ukraine, again using open source media, tools, and techniques. These reports are part of a revolution in private sector intelligence.

Government and private parties each bring unique perspectives and capabilities to the attribution problem. Government analysts, using national technical means, can apply advanced signals, imagery, and human collection capabilities to hard targets, getting closer to the source of malicious activity.

Private companies and organizations can work more closely with the victims of malicious activity, often in ways not available to government agencies. Combining these two perspectives produces a more complete picture of adversary activity and enables more effective countermeasures.

The revolution in private sector capabilities has shattered the myth that attribution in cyber space is impossible. I recommend reading *Attributing Cyber Attacks* by Dr. Thomas Rid and Ben Buchanan to better appreciate the integration of political context with technical details. It is true that some national and criminal hacking teams are improving their operational security as a means to frustrate attribution work. However, the explosion in social media across the developed and developing world means the people behind the hacking continue to show more of their actions and personalities in public forums. Just last week two security companies combined forces to use social media and other online sources to expose a member of a military hacking unit in Kunming, China. I assess that improved information sharing will also drive forward the attribution capabilities of public and private teams.

Attribution matters because it contributes to verification and stability. Last week Presidents Obama and Xi stated that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." The success of this agreement rests on the ability of each party to identify malicious activity emanating from the other, and positively attribute it to the government-controlled and sanctioned teams operating on behalf of each party. This requires high levels of attribution on both sides, in the public and private spheres. Government attribution capabilities are important because they inform the quiet, inside advisors to decision makers. Private attribution matters because they are the louder, outside voice to the media and citizenry.

Consider the difference between "high" and "low" attribution capabilities. I define high attribution capabilities as the integration of technical and political analysis to detect and identify digital adversaries. Those lacking this skill are said to have "low" attribution capabilities. For an example of "high-high" attribution, imagine the US and Russia. For "high-low," imagine the US and China. For "low-low," imagine Vietnam and China. One way to measure attribution capabilities is to watch for private sector companies in the country of interest who can release high-quality security reports. In the US, we have

Mandiant and others. In Russia, Kaspersky. In China, Qihoo-360 is a rising star. None come to mind for Vietnam, for example.

When two opponents each possess high attribution capabilities, it becomes difficult for a malicious third party to run a "false flag" operation, trying to trick the opponents into escalating a conflict. Two parties with high attribution capabilities are also able to determine if attacks emanating from certain locations are the work of the nation state, or are the result of a third party hijacking computers in the hosting country.

When either one, or both, opponents possess low attribution capabilities, it is a less stable situation. This could be a problem with the agreement between China and the US. Private and public teams in the US can perform high levels of attribution on Chinese activity. Private and public teams in China do not share the same capabilities at present. China could therefore suspect that the US is behind certain hacks, although such activity could be caused by Russia or other actors. This is one reason to welcome the rise of private or nongovernment security companies in China, who may improve the country's attribution capabilities.

Despite my praise for the private sector, I do not advocate giving non-government parties the authority to conduct offensive operations, also known as "hack back." I worry that private sector offensive operations could invoke an escalatory spiral, for which the national government would be ultimately responsible. Also, despite my faith in private sector attribution, offensive operations require target knowledge that could exceed the capabilities of many private parties. Therefore, I recommend that the state retain the monopoly on violence by reserving for itself the right to hack-back.

The last hot topic is acquisition. DoD and other government agencies should adopt acquisition practices that seek best-value solutions, rather than lowest-cost providers. Too often we see DoD and other groups acquire products or solutions that meet narrow technical specifications, and succeed in frustrating only the most basic attacks. Congruent with Secretary Carter's efforts to involve Silicon Valley and foster innovation, it is crucial that DoD be open to testing and acquiring capabilities that can stand up to the worst adversaries. Furthermore, DoD must integrate a secure software development lifecycle approach to the weapons and systems it procures. Processes such as the Building Security In Maturity Model (BSIMM) should be incorporated such that DoD weapons and systems are as resilient as possible

to digital attack. Red teaming should also be applied at multiple stages of the development lifecycle, not simply when capabilities are in the field. It is much cheaper and more effective to discover and fix flaws when weapons and systems are being designed and built, rather than trying to remediate vulnerabilities near or on the battlefield.

Beyond the specifics of the DoD strategy, I would like to offer five recommendations to improve the nation's digital security. Three involve DoD and two involve the administration and other agencies.

First, I recommend DoD and the Intelligence Community modify the nature of offensive digital operations against national adversaries. According to open source intelligence tradecraft and stories published in open media, US government offensive digital activities currently focus on traditional espionage targets. These operations fulfill collection requirements such that US government decision makers can execute their duties, based on accurate and actionable intelligence. Foreign intelligence services also conduct these operations. However, foreign intelligence services, military units, and other teams also attack private sector companies, civil society organizations, and even individuals. US offensive digital capabilities should therefore be ordered to directly target the foreign teams that are attacking private US entities.

By putting pressure on these foreign teams, US victims would receive some relief from the relentless waves of foreign hacking campaigns. By "pressure" I mean low-level activities that introduce friction and uncertainty into the minds and processes of foreign hackers. For example, US offensive teams could quietly corrupt tools and infrastructure used by foreign teams against domestic targets. They could periodically crash foreign computers used to hack US targets, or degrade bandwidth used to transport malicious traffic. The idea is to introduce obstacles into foreign hacking operations, such that they are working uphill when trying to attack US victims.

Second, the DoD, the IC, and partners should consider indirect ways to help protect US private sector and associated targets. If government actors learn that private entities are being targeted by a foreign adversary, they should be more willing to warn of the attack before it happens. For the past eight years or so, the FBI and other intelligence organizations have provided valuable third party notification services. These are post-breach warnings to private US entities after the FBI or other agency determines that a foreign actor has stolen data from the private US entity.

In situations where the US is unwilling to directly disrupt foreign hacking activity, DoD or the IC should inform private entities about pending hacks. This concept, like the previous idea of putting direct pressure on foreign hacking teams, involves sensitive equities. Intelligence and cyber operators do not want to risk jeopardizing sources and methods by notifying victims of impending attacks. However, the government must do more than simply notify the private sector when they fall prey to advanced foreign hacking operations.

Third, Congress should sponsor studies, by a mix of government and private sector researchers, to determine the costs and benefits of creating an independent new digital military service, or Cyber Force. As a former captain who performed the computer network defense mission in the Air Force, I am pleased to see the existing military services improving the career paths and opportunities for today's troops. After speaking at an Army Cyber Institute event last week, I watched two Army captains explain how they would apply cyber tactics and tools to accomplish a simulated physical combat mission. Unfortunately, I was reminded of the challenges facing these young officers when an audience member warned the pair that their non-cyber colleagues might "think they were playing warrior," and that their makeshift technical solution might appear to be a toy.

These cultural barriers are real and inherent in each military service's ethos. My tentative proposal is that so-called tactical cyber missions, where digital tools support a physical mission, should remain with the existing services. Strategic cyber missions, where digital tools are the primary focus, should become the realm of a new Cyber Force. Each service thinks differently, and rewards different skills and accomplishments, and my sense is that we need a Cyber Force to recruit and retain the nation's most promising digital warriors. The Cyber Force could also pioneer the more flexible, agile, information-age acquisition, promotion, placement, and leadership practices advocated by Defense Secretary Carter and Under Secretary Carson.

Fourth, I recommend the President appoint a US Chief Information Security Officer (US CISO). The Executive Branch has a Chief Information Officer (CIO) and a Chief Technology Officer (CTO), but not a CISO. This is similar to the situation at many businesses prior to a breach, although the Federal government has repeatedly found itself in a post-breach situation. The US CISO should share the same rank as Megan Smith, current US CTO, who is an Assistant to the President. The US CISO should have

operational control of a Federal Computer Incident Response Team, or FedCIRT. The FedCIRT would be a joint, interagency team composed of representatives from across the government. The purpose of the FedCIRT would be to hunt for intruders in non-intelligence, non-defense networks, and conduct joint incident response and recovery operations with the affected departments and agencies. The US CISO should pay particular attention to government cloud infrastructure.

Fifth, the administration should develop the capability to take asymmetric actions that target adversary core interests, but in a way that leverages our strengths against their weaknesses. For example, in the case of China, the so-called Great Firewall is an important target. The Chinese government uses its Great Firewall to censor content it considers to be a threat to the Chinese Communist's Party control of the country. The New York Times published a story in early August describing how the administration was considering taking steps to undermine the Great Firewall as a response to the Office of Personnel Management breach. This action offers excellent flexibility that can be calibrated according to the signal and effects the government wishes to achieve. At the low end, the US could fund research to enable bypassing the Great Firewall. At the high end, the government could sponsor covert activity to enable censorship-free Internet access via satellite or mesh communications. Such actions would impose cost on the Chinese government in a way they would recognize and perceive as a reflection of core US interests, should the agreement between Presidents Obama and Xi not pan out. The ability to inflict asymmetric cost on adversaries is a core element of deterrence, which I believe plays a role in the digital arena.

I look forward to your questions.