**SENATE ARMED SERVICES COMMITTEE**
**Subcommittee on Cybersecurity**

Dmitri Alperovitch
Co-Founder and Chief Technology Officer
CrowdStrike

Testimony on the Department of Defense's Cybersecurity Acquisition and Practices from the Private Sector

November 14, 2018

## Introduction

Chairman Rounds, Ranking Member Nelson, Senators of the Subcommittee: thank you for inviting me to testify at today's hearing.

I co-founded CrowdStrike more than 7 years ago with a mission to stop cyber breaches, including those caused by some of the most sophisticated adversaries. Today it is one of the world's leading cybersecurity firms and protects thousands of enterprise and government networks across over 100 countries. As part of our efforts, our endpoint security technology is deployed on IT systems and collects over a trillion security-related events every single week. On a daily basis we engage in virtual hand-to-hand combat with sophisticated adversaries from global criminal groups and nation-states such as China, Russia, Iran and North Korea seeking to compromise our customer networks. Our job is to hunt such adversaries and eject them rapidly from those networks before a breach occurs. We are exceptionally good at this job. I'm here to offer you a perspective based on this experience.

The Department of Defense (DoD) faces a similar challenge to that of the private sector. The very same threat actors targeting private industry today to steal intellectual property and sometimes carry out destructive attacks are trying to break into DoD networks to conduct espionage and degrade our warfighting capabilities.

In facing this threat, DoD has a number of advantages. In terms of experience, DoD deserves credit for having first defined, a generation ago, some of the concepts that still guide the field today in network defense. DoD's cybersecurity operators are every bit as talented and motivated as their private sector counterparts. In fact, some of the best people we have at CrowdStrike have backgrounds with the Department and our military services. And as a nation, we have applied significant resources to DoD cybersecurity. There likely is no organization on the planet that spends as much on cybersecurity as the Department.

Still, the private sector has the advantage of operating in the relatively unconstrained commercial environment. This environment has fostered agile responses to our shared threats that outpace DoD capabilities in some notable ways. The Department, of course, has some unique challenges in terms of the size of its IT enterprise and geographic dispersion. But I view scale as an advantage. The most capable private sector organizations have succeeded by maintaining a primary focus on rapidly detecting and ejecting adversaries from the networks which they are infiltrating on an almost constant basis.

I believe that applying a similar focus to DoD's defensive mission will advance the Department's ability to protect its enterprise and, thus, the security of our nation. The three most important strategies DoD should utilize to gain an upper hand in this fight are: hunting, cloud technologies, and the 1-10-60 rule.

### 1. Hunting

First, DoD needs to refocus on continuously hunting for adversaries on their networks. Much of what the Department does today is cyber hygiene. Implementing security controls is hygiene. Patching vulnerabilities is hygiene. Building an asset inventory is hygiene. All are important but are not sufficient to stop sophisticated breaches. No matter how good the Department gets at these tasks, they alone will not accomplish the most important mission: stopping foreign intelligence and military services from countries such as Russia and China from breaking into our networks. Let me reiterate this critical point – good cyber hygiene will not stop determined GRU or PLA cyber actors – just as having locks on the door of your house would not stop Navy Seals from getting in if they have a mission to do so. And too often these hygiene efforts come at the expense of hunting down and ejecting adversaries that are likely already in the network.

Hunting is assuming that adversaries are in your network and proactively searching for them by looking across your assets for indicators of malicious activity. Simply investigating alerts generated by security tools is not hunting. Good hunters have an offensive mindset and think like the adversary. They ask questions such as: if I were them, where would I hide? How would I move around this network? What trail would I likely leave? They also construct and test hypotheses about new attack activity based on previously observed adversary tactics, techniques, and procedures. They identify subtle distinctions among ostensibly legitimate behaviors or patterns. They understand the environment and how to concentrate their efforts, and adapt their process as adversaries demonstrate new capabilities.

Hunting is less labor-intensive than it may sound. For example, CrowdStrike's OverWatch service, which hunts 24x7 across thousands of networks and millions of machines around the world that make up our entire customer base – far larger in aggregate than the entire DoD enterprise – is comprised of approximately 20 people. We do have top-tier talent in these roles; our customer environments are well-instrumented; and we have architectures in place to support the mission. But DoD can use similar capabilities and ramp up their hunting operation without an enormous personnel mobilization effort.

### 2. Cloud technologies

Second, employing cloud technologies is essential to achieving these sorts of efficiencies. We must accept that DoD is – and will continue to be – burdened by obsolete infrastructure. For instance, it is challenging to upgrade IT systems on ships deployed at sea for months at a time. But the private sector grapples with the legacy infrastructure problem as well. Many of the largest financial services companies we work with still rely on mainframes from the 1970s. You accept such constraints where you must, and use forward-thinking acquisition strategies where you can. The presence of outdated IT infrastructure is not an insurmountable barrier to stopping our cyber enemies. Such thinking is not tolerated in the private sector, and DoD cannot accept it either.

Industry has demonstrated that cloud-based technologies can drive enormous efficiencies. DoD should continue adoption of these capabilities. It is encouraging to see significant movements toward the cloud government-wide, as mandated in the American Technology Council's 2017 IT Modernization Report.[1] Various initiatives in the Intelligence Community and across the defense enterprise are in some respects actually leading the way. But the key is ensuring that individual programs are designed with that approach. I see positive changes and hear the right things in high-level strategies, but change is slow to arrive and results on the ground are uneven.

In security, cloud-enabled technologies work because they flip the asymmetry between offense and defense. Modern security approaches take advantage of cloud resources by recording all computer security-related events in massive cloud-based data stores and perform advanced analytics and forensics on that data to uncover subtle adversary activity. Tracking trillions of events provides rich context for identifying suspicious patterns. What is more, once a threat is identified in one part of the network, cloud-based security technologies allow instantaneous distribution of protection against it across the entire ecosystem. With millions of endpoints under management, DoD can leverage cloud systems to turn its scale into a strength rather than a challenge.

### 3. The 1-10-60 Rule

Last, what DoD – and frankly, the Federal government as a whole – needs most is to define a new high-level defensive concept that drives measurable accountability. I suggest a model I developed at CrowdStrike called the 1-10-60 rule.[2] This rule is derived from the premise that to win a battle in cyberspace, speed is paramount. The only way you beat an adversary is by being faster than them.

[1] American Technology Council, *Report to the President on Federal IT Modernization*, December 2017. https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf.

[2] CrowdStrike, *Breakout Time: CrowdStrike CTO on How Long You Have to Detect, Analyze and Act to Stop a Breach*, May 1, 2018. https://www.youtube.com/watch?v=ujAVEGHr-uc.

The concept behind the rule is simple: to be successful at stopping breaches, an organization needs to detect, investigate, and remediate or contain the threat as quickly as possible. The very best private sector companies we work with strive to detect an intrusion on average within one minute, investigate it within 10 minutes, and isolate or remediate the problem within one hour. 1-10-60. That may sound impossible if you are accustomed to hearing about breaches that go undetected for months or years, but we work with private sector organizations that achieve that level of rapid response routinely.

We have to assume that persistent and dedicated adversaries will compromise individual machines periodically through exploitation of known or unknown vulnerabilities or through simple social engineering. The greatest vulnerability that every organization in the world has – and one that can never be patched – are the users. In our experience, in any enterprise with people, there will always be some who will open suspicious emails, click on random links and supply sensitive information to unknown websites. Cybersecurity training helps but will never completely eliminate this possibility. And when confronting foreign intelligence services, you also have to assume that the initial compromise vector may not even be cyber – but a malicious insider asset they have recruited inside the target organization.

So the important question to ask is not "Can you prevent the initial compromise?" – that may be an impossibility. Rather, you should ask "How long does it take for adversaries to take advantage of the initial machine they have established as their beachhead within the network, move laterally across the environment, and gain access to a sensitive resource?" Once adversaries are able to do that, what would have been a minor security event will turn into a full breach that requires a lengthy and complex incident response. If you stop the adversary before they achieve those objectives, you have prevented the breach.

In defining the 1-10-60 rule concept, CrowdStrike analyzed real intrusion data. We studied approximately 25,000 attempted breaches we detected last year across our customer networks and found that it took adversaries on average 1 hour and 58 minutes to move out from their initial beachhead – that first machine they had compromised on a network. We call this measure "breakout time,"[3] and from a defender's perspective, that is the time to beat.

I have strongly advocated that corporate Boards of Directors should also use the 1-10-60 rule as a primary accountability measure of their cybersecurity programs. This system drives clarity into the oversight process by enabling leadership to understand and measure performance. Not every organization can easily get to such fast reaction times, but even if you are not there, you can measure this performance on a monthly or quarterly basis and determine if the trend is going in the right direction. If it is not, you can hold your cybersecurity executives accountable for those results.

[3] CrowdStrike, *2018 Global Threat Report*, December 2017. p. 72. https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/.

## Conclusion

DoD must prevail in its mission to defend and secure its IT enterprise. Failure is not an option. Private industry is in some important ways outperforming DoD in cyber defense. But the challenges the Department faces in catching up are not insurmountable. A strong re-emphasis on hunting is the first step. Achieving economies of scale and other efficiencies through adoption of cloud-based security technologies where possible will make this easier and more sustainable over the long run.

It is also essential to have a clear ordering principle to inform staffing requirements and acquisition decisions. The 1-10-60 rule is a straightforward, metrics-driven approach based on adversary activity. Broad adoption of this approach will improve security by elevating the importance of speed in security operations, revealing performance gaps, and simplifying oversight. The result will be stronger accountability and better defense.

I have focused my testimony today on concepts rather than technologies. But everything I have described is achievable through practices and capabilities that are widely utilized in industry. DoD can adopt these capabilities, and by enhancing its own security posture, strengthen national defense.

Thank you again for inviting me to testify today. I look forward to your questions.

###