Government Business Council

DELL Software

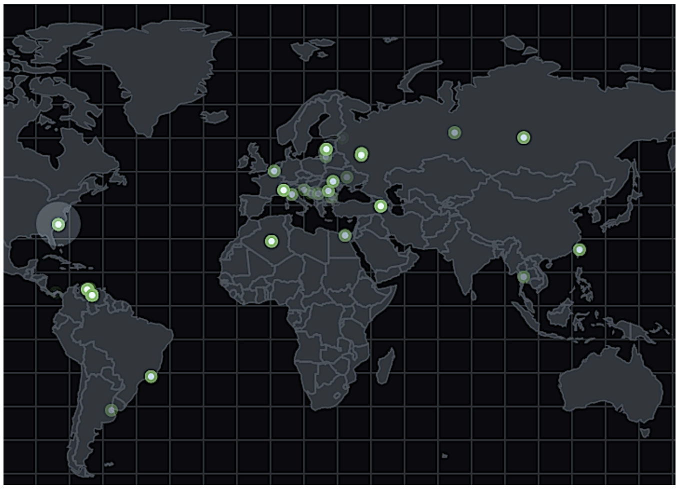
HOW THE PENTAGON CAN TACKLE THE CYBER ATTRIBUTION PROBLEM

TO EFFECTIVELY IDENTIFY THOSE RESPONSIBLE FOR CYBER ATTACKS, THE PENTAGON NEEDS A HOLISTIC ATTRIBUTION PROCESS THAT INTEGRATES TECHNICAL, OPERATIONAL, AND STRATEGIC LEVELS OF ANALYSIS

The November 2014 cyber attack on Sony® dramatically raised the profile of state-on-state cyber conflict after the FBI and President Obama publicly named North Korea as the source of the intrusion. Never before had the United States officially charged a foreign government with conducting a cyber attack on U.S. targets.[1] The incident demonstrates cyber attacks' capacity to inflict physical damage, adds to the growing list of significant inter-state cyber conflicts, and foreshadows the consequences of an expanding cyber arms race.

The Sony® hack was also significant in highlighting the importance of attribution in responding to such cyber attacks. The ability to identify perpetrators permits the U.S. to respond and goes a long way toward deterring further attacks. In fact, attribution is integral to the Department of Defense's cyber strategy. But identifying the sources of cyber attacks also poses an immense challenge.

To effectively identify those responsible for cyber attacks, DoD needs a holistic attribution process that integrates technical, operational, and strategic levels of analysis. As the foundational and perennially evolving aspect of cyber intrusion, the technical level currently represents DoD's largest concern.



The Pentagon's Attribution Challenge

Because it knows it will never be able to stop every cyber attack by foreign adversaries, DoD has held the view that deterrence is its best bet.[2] But achieving effective cyber deterrence is more difficult than more traditional forms of deterrence, such as that which the U.S. and the Soviet Union relied on to keep the Cold War from turning hot, because it is harder to identify perpetrators in cyberspace. As DoD's Cyberspace Policy Report from 2011 observes, "the same technical protocols of the Internet that have facilitated the explosive growth of cyberspace also provide some measure of anonymity. Our potential adversaries, both nations and non-state actors, clearly understand this dynamic and seek to use the challenge of attribution to their strategic advantage."[3]

The Pentagon has made progress enhancing its attribution capabilities in recent years, including standing up the Defense Cyber Crime Center, but the attribution challenge continues to weigh heavily. Increasing cooperation between state and non-state actor groups, in particular, further complicates attribution. When asked what concerns him most, Admiral Mike Rogers, head of both the NSA and Cyber Command, said in November 2014, "I'm watching some of these [nation-states and non-state actors] blur and create partnerships that make attribution more difficult. They clearly are intended to try to stymie attribution… this is going to require us to think a little differently."[4]

Underlining the need to enhance DoD's capacity for cyber deterrence, Frank Kendall, Undersecretary of Defense for Acquisition, Technology, and Logistics, established a Defense Science Board Task Force on Cyber Deterrence in October 2014. In particular, the task force is directed to study "methods for determining whether a cyber attack (versus cyber exploitation) is happening" and "means for rapid high-confidence attribution of attack."[5]

Outlining an Attribution Model

Attribution in cyberspace is not a black-or-white proposition. It is always a matter of degrees of certainty. So how can DoD optimize its attribution process to increase its level of certainty in responding to and deterring cyber adversaries? By adopting a three-pronged, common-sense analytical approach proposed by experts at the Department of War Studies at King's College in London in December 2014:[6]

Technical forensics - First and foremost, attribution requires understanding the incident in question at a technical level. The mechanics of what happened can yield essential clues for forming a hypothesis about the incident's source. Indicators of compromise, or the digital artifacts of a cyber intrusion, are generally the starting point of an investigation. Deciphering an attack's network penetration technique, targets, infrastructure, language of origin, pattern of life, and functionality, for example, can significantly narrow the list of suspects. Such technical evidence forms the basis of the entire attribution process.

ATTRIBUTION IN CYBERSPACE IS NOT A BLACK-OR-WHITE PROPOSITION. IT IS ALWAYS A MATTER OF DEGREES OF CERTAINTY

Operational analysis - By synthesizing technical information about an intrusion with non-technical and geopolitical analyses, a cyber-attack investigation can further shrink the list of possible perpetrators. Here, analysts explore the context of the attack, make more informed judgements about those responsible, and inform questions for strategic attribution analysis. DoD has a considerable advantage at the operational level because it already has extensive human and signals intelligence assets.

Strategic analysis - At the highest level, leaders digest operational analyses, probe for details, and make strategic decisions about who is responsible, why the attack was launched, and how to appropriately respond.

The Mandiant Intelligence Center's exposing of one of China's cyber espionage units offers an example of how these elements can be pieced together. Combining years of technical forensics work with operational analysis of the People's Liberation Army's cyber activities and intentions, Mandiant was able to attribute with high confidence a considerable amount of cyber espionage activity to a single PLA unit, Unit 61398, and even to specific individuals within that unit.[7] This aggregate analysis then contributed to the U.S. government's strategic decision to publicly respond. In May of 2014, the Department of Justice indicted five PLA officers without explicitly blaming Beijing as part of a calculated strategy to ratchet up pressure against Chinese cyber intrusions.[8]

Moving Forward

Each of the three levels of analysis represents a discrete challenge and requires unique capabilities and expertise. At present, the technical level of analysis is DoD's biggest variable for effective cyber attribution because it is the least developed.

Achieving a centralized, holistic view of DoD's cybersecurity architecture and network activity is therefore a key next step. Leveraging a comprehensive identity and access management (IAM) system that connects to all relevant business processes across DoD IT enterprises can allow for the kind of real-time, technical attribution analysis that is necessary for effective deterrence. By generating extensive audit trails of activity, such an IAM system can build a profile of a given attack and begin to inform operational and strategic attribution analyses.

For example, Kapersky Lab's investigation into the massive "Epic Turla" cyber-espionage campaign discovered technical evidence suggestive of Russian perpetrators.[9] An extensive review of the incursions' digital artifacts revealed that the hackers' command packages included searches for topics related to NATO and their code occasionally used Russian words. This is far from sufficient to attribute the campaign to the Russian government, but combined with existing human and signals intelligence on Russian cyber operations and a strategic understanding of the geopolitical context, it could spur a more formal attribution investigation.

Having sufficient visibility into a network as wide-ranging as DoD's is especially important when trying to identify malicious insiders and advanced persistent threats that penetrate the network utilizing stolen identity credentials. The most damaging cyber operations, like the Sony® hack and Epic Turla, often access networks using spear phishing and other social engineering techniques to set the stage for destructive attacks or simply collect valuable information indefinitely.

Attributing a hostile cyber intrusion with a high degree of certainty forms the cornerstone of effective DoD cyber deterrence. Determining the source of an attack will always be a political and subjective decision, but the best evidence about culpability will almost always be found at the technical level.

Sources

1. “N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say,” *New York Times*, December 2015.
2. “DoD to be More Transparent About Strategy to Deter Cyber Attacks,” *Federal News Radio*, October 2014.
3. Department of Defense Cyberspace Policy Report, Department of Defense, November 2011.
4. “Cyber Defense a Cooperative Effort, Rogers Says,” *DoD News*, Defense Media Activity, November 2014.
5. “Memorandum for Chairman - Defense Science Board,” Undersecretary of Defense for Acquisition, Technology, and Logistics, October 9, 2014.
6. “Attributing Cyber Attacks,” Thomas Rid and Ben Buchanan, *Journal of Strategic Studies*, December 2014.
7. *APT1: Exposing One of China’s Cyber Espionage Units*, Mandiant Intelligence Center, February 2013.
8. “Indictment of PLA Hackers is Part of Broad U.S. Strategy to Curb Chinese Cyberspying,” *Washington Post*, May 2014.
9. “The Epic Turla Operation,” *SecureList*, Kapersky Lab, August 2014.

Image Source: *Nextgov* Threatwatch (www.nextgov.com/cybersecurity/threatwatch)