Outgoing NSA official describes Russia's 2014 cyberattack on U.S. State Department as "hand-to-hand combat"

Insights into the changing cyber landscape

Cyber clash

- The November 2014 compromise of the State Department's unclassified computer system marked a new era of aggressiveness in Russian cyberattacks, according to officials who recently shed light on the incident
- Cybersecurity firms have traced the attack, which forced the State Department to briefly take its unclassified e-mail system offline, to Cozy Bear, the hacking collective linked to one of the two Russian spy agencies that would target the DNC and the 2016 U.S. presidential election
- Though not naming the Russians, NSA Deputy Director Richard Ledgett recently described the confrontation between the hackers and NSA defenders as 24 hours of cyber "hand-to-hand combat" The attack also demonstrated a new level of brazenness: whereas hackers would previously retreat once they had been discovered, in this instance the Russians remained inside the network, establishing new command and control stations after NSA and FBI officials destroyed existing ones

> **"That's a new level of interaction between a cyberattacker and a defender … It was a little bit of a game changer"**
>
> –NSA Deputy Director Richard Ledgett on Russia's 2014 tactics

China, Iran

- Senior officials from the current and previous administrations also added that China and Iran have displayed increasingly antagonistic cyber behavior, resisting attempts to expel them from U.S. networks. Though China's hacking for the purposes of economic espionage decreased following a September 2015 agreement between Presidents Obama and Xi, routine cyber intelligence gathering has continued unabated
- The intent behind these attacks, those officials said, goes beyond intelligence gathering to "sending a message that we have capabilities and that you are not the only player in town," as well as testing whether the U.S. is "willing to escalate … what is the U.S. government willing to do?"

Implications for the private sector

- Ledgett and others expect these aggressive cyber tactics to appear in attacks against the private sector, which will require more intelligence sharing from NSA and other government agencies. "We need to figure out," Ledgett recommended, "how do we leverage the private sector in a way that equips them with information that we have to make that a fair fight between them and the attacker?"

Sources: Ellen Nakashima, "New details emerge about 2014 Russian hack of the State Department: IT was 'hand to hand combat,'" The Washington Post, April 3, 2017; Joseph Marks, "Once stealthy, Russian hackers now go toe to toe with U.S. defenders," Nextgov, March 21, 2017; Images by Chameleon Design and Dev Patel, The Noun Project, April 2017.