Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Don't Rush To Judgment On Election Cyberattack Attribution

By **John Reed Stark** (October 23, 2020, 4:25 PM EDT)

John Reed Stark

When investigating a cyberattack, just because you have figured out the what, when and how does not mean you have figured out the who.

No doubt, after Election Day 2020, someone somewhere will allege that some form of cyberattack compromised the results.

Though it may be tempting to round up the usual suspects,[1] don't take the bait. While countries like Russia, China and North Korea certainly lack clean hands, they are not necessarily the perpetrators of every cyberattack targeting a U.S. organization or government entity.

Of course, aggressor nation-states and their proxies have been targeting U.S. institutions with cyberattacks for years. That fact is undisputed. Indeed, state-sponsored cyberespionage has spawned a new cyberarena for global warfare and societal disruption — a dangerous and unpredictable shifting of the battlefield paradigm, especially when it comes to U.S. elections.

Along these lines, the U.S. Department of Justice recently unsealed criminal charges[2] against six Russian intelligence officers in connection with some of the world's most damaging cyberattacks, including the disruption of Ukraine's power grid and release of a mock ransomware virus — NotPetya — that infected computers globally causing billions of dollars in damage.

But this recent DOJ case, which took years and a special prosecutor to investigate, is the exception and not the rule, because the perpetrators of most cyberattacks are rarely identified, let alone charged and actually brought to justice.

This article tackles the issue of attribution of cyberattacks head-on. Specifically, this article warns that before rushing to judgment regarding the attribution of the perpetrator of any cyberattack, especially pertaining to an election, consider the complex and intricate anatomy of data breaches; the subjectivity and circumstantial nature of digital forensic evidence; and the extraordinary level of guesswork, supposition and hypothesizing inherent in most attribution calculations.

Cyberattackers Leave No Crime Scene Investigation-Like Evidentiary Trail

After a cyberattack, there is rarely, if ever, a crime scene investigation-like or DNA evidentiary trail leading to the perpetrator. The cases are almost always circumstantial, and the digital forensic evidence rarely resides in plain view.

Evidence gleaned from a cyberattack can rest among disparate logs, if they even exist, volatile memory captures, server images, system registry entries, spoofed IP addresses, snarled network traffic, haphazard and uncorrelated timestamps, internet addresses, computer tags, malicious file names, system registry data, user account names, network protocols and a range of other suspicious activity.

Evidence can also become difficult to nail down — logs are destroyed or overwritten in the course of business; archives become corrupted; hardware is repurposed; and the list goes on.

In fact, the technological tidbits identified by digital forensic experts often lack enough of an evidentiary foundation to initiate a prosecution — especially when the intelligence becomes politicized. Moreover, like medical experts who disagree about a diagnosis or treatment, cybersecurity experts are notorious for disagreeing about attribution conclusions gleaned from the digital forensic remnants, residue, fragments and artifacts left behind in the aftermath of a data breach.

More Art Than Science

Attribution identification is far more art than science and too often contains a patchwork of hypothesizing, speculation, supposition and simple old-fashioned guesswork, rendering attribution conclusions overly subjective, skewed or even mistaken.

An online intruder can leave behind a digital crime scene akin to a ransacked home; a crime scene that is seemingly untouched and immaculate; or a crime scene that is somewhere in between. In order to reverse-engineer a cyberattack, forensic investigators, incident responders, security engineers and IT administrators employ an extensive array of practical skills to isolate malware that targets, accesses or otherwise infects a company's technological infrastructure.

The most effective cyberattack investigative methodology is often a tedious and exhaustive iterative process of digital forensics, malware reverse engineering, monitoring and scanning. When the analysis identifies any possible indicator of compromise, investigators examine network traffic and logs, in addition to scanning system hosts for these indicators of compromise.

When this effort reveals additional systems that may have been infiltrated, investigators will then forensically image and analyze those systems, and the process repeats itself. Armed with the information gathered during this lather, rinse and repeat phase, investigators can detect additional attempts by an attacker to regain access and begin to contain the attack.

But in stark contrast to the disciplined, iterative process and methodology of seeking indicators of compromise, determining attribution consists of a somewhat different and far less scientific approach.

Correlating Cyberattack Modus Operandi

One oft-used methodology for determining cyberattack attribution is to draw conclusions by correlating a library of code similarities, shared tools and shared infrastructure and targets of known cyberattackers. But while matching modi operandi can certainly provide worthwhile intelligence fodder for U.S. government investigative teams and policymakers, pinpointing attribution to, and ascertaining the motives of, cyberattackers remains inherently subjective.

Moreover, today's online threat actors have begun eschewing custom tools in favor of using standard operating system features and off-the-shelf tools to compromise their targets. This

living-off-the land[3] hacking trend, where attackers make use of tools already installed on targeted computers or run simple scripts and shell code directly in memory, creates even more attribution challenges.

For instance, just before New Year's Eve in 2016, CNN's Jim Acosta reported that the Burlington, Vermont, electric utility had discovered Russian malware on one of its laptops, but, as many have since pointed out,[4] that malware was available for purchase online and hardly an inculpatory indicator of compromise of any particular government or other criminal actor.

Malware can come from anywhere and its mere presence does not necessarily indicate that a particular government hacking gang is involved — the infection could have come from something as simple as an employee visit to an infected website.[5] Attacks can also originate with disgruntled or former employees — so-called bad leavers[6] — which is why data breach response is a lengthy, tedious and holistic process exploring all possibilities of attack.

False Flag Cyberattacks

While some data security incidents may provide key evidence early on, most never do or, even worse, provide a series of false positives and other initial stumbling blocks. Thus, even if investigators can triangulate a common modus operandi among attackers, the entire criminal design could all be a false flag subterfuge, where one country's cybergang coopts the practices of another country's cybergang, to confuse, misdirect and lead astray.

From simply issuing false claims of responsibility to emulating the tools, techniques and even languages typically used by the group or country, false flag cyberattackers can hoodwink even the most seasoned cyberexperts. By interjecting chaos and confusion during a digital forensic investigation of a data breach, false flags make an already problematic undertaking even more byzantine.

For instance, in one of the more notorious examples of false flag attacks, Russian hackers[7] attempted to disrupt the South Korean Winter Olympics in 2018 by using code of a North Korean origin.

Along the same lines, a two-year probe by the U.K.'s National Cyber Security Centre and the U.S. National Security Agency[8] found that the Turla group purportedly linked to Russian intelligence carried out cyberattacks in 20 countries by hijacking the backdoors, tool sets and command control centers used by Oilrig, a hacker group purportedly linked to Iran.

False flags can also obfuscate motive. Election tampering, governmental destruction, espionage, terrorism, financial crime, insider trading, intellectual property thievery, trade secret pilfering, extortion and market manipulation, to name just a few, are all potential data beach objectives.

Ransomware-as-a-Service

To further confuse attribution efforts, some cyberattack tools, tactics, and even command and control centers can now be rented on the dark web, in essence allowing successful cyberattackers to franchise their criminal enterprises. These online organized crime syndicates can render attribution so multifaceted that pointing the finger at a perpetrator can become physically impossible.

For example, the increasingly popular ransomware-as-a-service model borrows from the software-as-a-service model, by providing a subscription-based malicious platform and toolset, enabling even the most novice threat actors to become affiliates and launch their own sophisticated

ransomware attacks.

By reducing the need to design cyberattacks and code malware, ransomware-as-a-service packages allow global criminals, including rogue nation-states, to carry out complex cyberattacks using another attacker's wares, thereby rendering themselves even more challenging to identify.

Looking Ahead

In some of the more infamous cyberattacks, the most compelling attribution evidence remains classified, so we are asked to take U.S. intelligence reports at their word. This is a big ask, and whether we should all blindly accept attribution-related conclusions of the U.S. intelligence agencies merits some deconstruction.

First, the typically invisible redactions and glaring omissions of government intelligence reports on cyberattacks can pack a double whammy. Skeletonized intelligence attribution reports released to the public intentionally exclude proof, more often offering strings of conclusions replete with troublesome hearsay and unsupported conclusory opinions.

In addition, U.S. intelligence assertions about cyberattacks, like those in most intelligence briefings and reports, allude to having a range of clandestine sources such as intercepted communications, foreign government agents and other covert origins.

Unfortunately, there exists no way to evaluate the evidence presented by, nor assess the credibility of, these deliberately naked conclusions and cloaked sources. We must therefore wholly rely upon the honesty, integrity and expertise of U.S. intelligence officials — a tough pill to swallow, especially for the more cynical or scientific.

Of course, the reasons for all of the secrecy make sense. Risking the compromise of critical intelligence sources is a matter of national security. In the end, perhaps a little blind faith is not too much to ask, especially given the bona fides of the many hard working U.S. experts battling the endless wave of computer crime.

These behind-the-scenes civil servants have dedicated their lives to pursuing the truth. I should know — I was once one of them. having spent almost 20 years in government service, most of the time investigating cybercrimes. Their conclusions, albeit subjective, can be of unique utility and value and should be extolled rather than derided.

On the other hand, history is littered with too many examples of the misguided application of so-called government intelligence. Of particular concern is when political appointees holding the higher ranks of government exploit the raw intelligence findings of career civil service underlings and recalibrate them for political gain, leading to dubious and tendentious attribution conclusions.

Given the limited chance that the U.S. government will identify, apprehend, arrest, extradite and bring to trial most cyberattackers, the real truth will always remain evasive. Even when the government has garnered enough evidence to warrant a bona fide indictment allegation, other roadblocks emerge, such as conflicting global sovereignty, clashing treaties and an overall lack of judicial comity.

Meanwhile, apprehending, let alone charging foreign perpetrators, also necessitates massive resources from a myriad of government agencies.

Consider the litany of public agencies, foreign governments and private companies that partook in the recent DOJ Russian hacking prosecution[9] — the global online dragnet was almost

unprecedented. Most federal law enforcement agencies lack the wherewithal to initiate more than just a few transnational investigations and prosecutions, let alone dedicate resources to a worldwide cyberhunt.

Hence, for politicians looking to advance their ideological interests; for reporters looking to generate headlines and clicks; and for cyberexperts looking to promote their services, it has become fashionable to make highly subjective, and sometimes wildly reckless, cyberattack attribution claims — especially those pertaining to elections.

After all, no one will ever really capture the perpetrators, and proving an attribution conclusion to be wrong, i.e., proving a negative is even more challenging than proving attribution in the first place. My take is that determining the identity of a cyberthreat actor for any attack, election-related or otherwise, has evolved into an unmanageable vortex and high-tech gumshoe guessing game.

So when the clock strikes midnight on election day, and the partisans, pundits and armchair analysts begin pointing fingers at state-sponsored hacking gangs, be sure to think twice — or even three times — before accepting their conclusions. Stop and weigh the evidence — there is rarely any smoking gun. Demand facts, seek truth, be objective and scrutinize the proof. Rushing to judgment not only disassembles and creates confusion, it also undermines the objectivity, candor and confidence that the public deserves.

John Reed Stark is president of John Reed Stark Consulting LLC. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as chief of its Office of Internet Enforcement.

[1] https://www.youtube.com/watch?v=HXuBnz6vtuI.

[2] "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (October 19,2020)" at https://www.justice.gov/opa/press-release/file/1328521/download.

[3] "Attackers Are Increasingly Living Off The Land," BroadCom, by Candid Wueest (July 12, 2017) at https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=6682c107-0172-4f4b-a528-616972fbfc19&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

[4] https://twitter.com/dellcam/status/815043480741408768.

[5] ''Fake News' And How The Washington Post Rewrote Its Story On Russian Hacking Of The Power Grid," Forbes, by Kalev Leetaru (January 1, 2017) at https://www.forbes.com/sites/kalevleetaru/2017/01/01/fake-news-and-how-the-washington-post-rewrote-its-story-on-russian-hacking-of-the-power-grid/#7cd145c97ad5.

[6] "The 21st Century Genesis of the Bad Leaver," BNA Privacy and Securities Law Report, by John Reed Stark (October 2011) at https://www.johnreedstark.com/wp-content/uploads/sites/180/2014/12/2011_BNA_21st-Century-Genesis-of-the-Bad-Leaver.pdf.

[7] "A Brief History of Russian Hackers' Evolving False Flags," Wired, by Andy Greenberg (October 21, 2019) at https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/.

[8] NSA and NCSC Release Joint Advisory on Turla Group Activity at https://us-cert.cisa.gov/ncas/current-activity/2019/10/21/nsa-and-ncsc-release-joint-advisory-turla-group-activity (October 21, 2019).

[9] Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (October 19, 2020) at https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.
