US Intel Vets Dispute Russia Hacking Claims

As the hysteria about Russia's alleged interference in the U.S. election grows, a key mystery is why U.S. intelligence would rely on "circumstantial evidence" when it has the capability for hard evidence, say U.S. intelligence veterans.

Veteran Intelligence Professionals for Sanity

MEMORANDUM

Allegations of Hacking Election Are Baseless

A *New York Times* report on Monday alluding to "overwhelming circumstantial evidence" leading the CIA to believe that Russian President Vladimir Putin "deployed computer hackers with the goal of tipping the election to Donald J. Trump" is, sadly, evidence-free. This is no surprise, because harder evidence of a technical nature points to an inside leak, not hacking – by Russians or anyone else.

Monday's *Washington Post* reports that Sen. James Lankford, R-Oklahoma, a member of the Senate Intelligence Committee, has joined other senators in calling for a bipartisan investigation of suspected cyber-intrusion by Russia. Reading our short memo could save the Senate from endemic partisanship, expense and unnecessary delay.

In what follows, we draw on decades of senior-level experience – with emphasis on cyber-intelligence and security – to cut through uninformed, largely partisan fog. Far from hiding behind anonymity, we are proud to speak out with the hope of gaining an audience appropriate to what we merit – given our long labors in government and other areas of technology. And corny though it may sound these days, our ethos as intelligence professionals remains, simply, to tell it like it is – without fear or favor.

We have gone through the various claims about hacking. For us, it is child's play to dismiss them. The email disclosures in question are the result of a leak, not a hack. Here's the difference between leaking and hacking:

Leak: When someone physically takes data out of an organization and gives it to some other person or organization, as Edward Snowden and Chelsea Manning did.

Hack: When someone in a remote location electronically penetrates operating systems, firewalls or any other cyber-protection system and then extracts data.

All signs point to leaking, not hacking. If hacking were involved, the National Security Agency would know it – and know both sender and recipient.

In short, since leaking requires physically removing data – on a thumb drive, for example – the only way such data can be copied and removed, with no electronic trace of what has left the server, is via a physical storage device.

Awesome Technical Capabilities

Again, NSA is able to identify both the sender and recipient when hacking is involved. Thanks largely to the material released by Edward Snowden, we can provide a full picture of NSA's extensive domestic data-collection network including Upstream programs like Fairview, Stormbrew and Blarney. These include at least 30 companies in the U.S. operating the fiber networks that carry the Public Switched Telephone Network as well as the World Wide Web. This gives NSA unparalleled access to data flowing within the U.S. and data going out to the rest of the world, as well as data transiting the U.S.

In other words, any data that is passed from the servers of the Democratic National Committee (DNC) or of Hillary Rodham Clinton (HRC) – or any other server in the U.S. – is collected by the NSA. These data transfers carry destination addresses in what are called packets, which enable the transfer to be traced and followed through the network.

Packets: Emails being passed across the World Wide Web are broken down into smaller segments called packets. These packets are passed into the network to be delivered to a recipient. This means the packets need to be reassembled at the receiving end.

To accomplish this, all the packets that form a message are assigned an identifying number that enables the receiving end to collect them for reassembly. Moreover, each packet carries the originator and ultimate receiver Internet protocol number (either IPV4 or IPV6) that enables the network to route data.

When email packets leave the U.S., the other "Five Eyes" countries (the U.K., Canada, Australia, and New Zealand) and the seven or eight additional countries participating with the U.S. in bulk-collection of everything on the planet would also have a record of where those email packets went after leaving the U.S.

These collection resources are extensive [see attached NSA slides 1, 2, 3, 4, 5]; they include hundreds of trace route programs that trace the path of packets going across the network and tens of thousands of hardware and software implants in switches and servers that manage the network. Any emails being extracted from one server going to another would be, at least in part, recognizable and

traceable by all these resources.

The bottom line is that the NSA would know where and how any “hacked” emails from the DNC, HRC or any other servers were routed through the network. This process can sometimes require a closer look into the routing to sort out intermediate clients, but in the end sender and recipient can be traced across the network.

The various ways in which usually anonymous spokespeople for U.S. intelligence agencies are equivocating – saying things like “our best guess” or “our opinion” or “our estimate” etc. – shows that the emails alleged to have been “hacked” cannot be traced across the network. Given NSA’s extensive trace capability, we conclude that DNC and HRC servers alleged to have been hacked were, in fact, not hacked.

The evidence that should be there is absent; otherwise, it would surely be brought forward, since this could be done without any danger to sources and methods. Thus, we conclude that the emails were *leaked by an insider* – as was the case with Edward Snowden and Chelsea Manning. Such an insider could be anyone in a government department or agency with access to NSA databases, or perhaps someone within the DNC.

As for the comments to the media as to what the CIA believes, the reality is that CIA is almost totally dependent on NSA for ground truth in the communications arena. Thus, it remains something of a mystery why the media is being fed strange stories about hacking that have no basis in fact. In sum, given what we know of NSA’s existing capabilities, it beggars belief that NSA would be unable to identify anyone – Russian or not – attempting to interfere in a U.S. election by hacking.

For the Steering Group, Veteran Intelligence Professionals for Sanity (VIPS)

William Binney, former Technical Director, World Geopolitical & Military Analysis, NSA; co-founder, SIGINT Automation Research Center (ret.)

Mike Gravel, former Adjutant, top secret control officer, Communications Intelligence Service; special agent of the Counter Intelligence Corps and former United States Senator

Larry Johnson, former CIA Intelligence Officer & former State Department Counter-Terrorism Official

Ray McGovern, former US Army infantry/intelligence officer & CIA analyst (ret.)

Elizabeth Murray, Deputy National Intelligence Officer for Middle East, CIA

(ret.)

Kirk Wiebe, former Senior Analyst, SIGINT Automation Research Center, NSA (ret.)