The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russian Spycraft: How the Kremlin Hacked Its Way Into a Crisis

By Vladimir Frolov

October 11, 2016

Katerina Lobanova

Last Friday the U.S. Intelligence Community (USIC) publicly named the Russian government for directing "the recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations." It claimed that the disclosures of hacked emails "on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are intended to interfere with the U.S. election process", while "only Russia's most senior officials could have authorized these activities."

The hacking of the DNC computer networks was first disclosed in mid-June. CrowdStrike, a private cyber intelligence firm brought in by the DNC to investigate the hacks identified with a high degree of confidence two groups of hackers with links to Russia's intelligence services. COZY BEAR (CozyDuke or APT 29), ostensibly working for the FSB, Russia's domestic intelligence service, breached the networks in mid-2015 and had been collecting intelligence and personal data undetected until April 2016, when another group of hackers FANCY BEAR

(Sofacy or APT 29), purportedly working for GRU, Russia's military intelligence service, broke into the same network, unbeknown to the first group, and raised some flags for the system's security.

On July 22, on the eve of the Democratic Convention in Philadelphia, WikiLeaks released some 20,000 stolen emails showing top officials at the Democratic National Committee criticized and mocked Senator Bernie Sanders of Vermont, Hillary Clinton's rival during the primary campaign, even though the organization publicly insisted that it was neutral in the race. At that point it became a story about Russia trying to influence the outcome of the U.S. presidential election in favor of Donald Trump, who said he favored better U.S.-Russia ties. The timing of the leak was intended to cloud the Democratic convention in controversy, reignite party divisions, and motivate Sanders supporters not to vote for Clinton in November.

President Vladimir Putin in a recent interview to Bloomberg denied that Russia on a state level had anything to do with the email hacks, but his claim that "the important thing is the content that was given to the public, and not the search for who did it" suggested more than a cursory knowledge of the matter. His further claim that the Russian government did not possess the kind of sophisticated sense of U.S. domestic politics to pull off such a tricky game sounded lame. The Russian Foreign Ministry maintains a granular understanding of the intricate details of U.S. presidential and party politics. The Russian Embassy in Washington keeps about a dozen diplomats on the beat. It is not, as some claim, that the Russians suddenly discovered the DNC last year.

While the publicly available evidence linking Russian intelligence to the hacks is inconclusive and may even suggest a false flag operation to entangle Moscow in a brawl with Washington, the U.S. Intelligence Community had a high degree of confidence in Russian involvement even in July and the fact that they publicly named Russian intelligence as perpetrators suggests that they have definitive proof.

The question is what Moscow was really trying to accomplish. Cyber operations to collect intelligence are normal spycraft. The DNC and RNC are legitimate targets for Russian HUMINT and SIGINT operations, as are private email accounts and cell phones of key U.S. policy makers. You get intelligence by eavesdropping on people with access to real secrets.

Initially it appeared the Russian hacking was just about that, at least the COZY BEAR part of it in 2015. There were some notable scoops, like hacking the private email of former NATO Supreme Commander General Breedlove in early 2015 where he unsuccessfully lobbied the Obama administration for sending advanced anti-tank weapons to Ukraine (it was reassuring to know the White House was not serious about stopping the Russian armor in Eastern Ukraine), or a private audio by Hillary Clinton in which she opposed plans to develop a new nuclear cruise missile for U.S. strategic bombers. Otherwise the intelligence value of the trawl was small.

When the Russian hacking was discovered (due to the destructive rivalry between Russian intelligence services who failed to deconflict on the target), Moscow found itself sitting on a pile of Beltway gossip of limited intelligence value, but with some potential for influence operations. Perhaps, some "genius" suggested it should be made public to trash Hillary

Clinton whom the Kremlin intensely disliked for her public role in supporting the mass protests in Moscow in 2011. No thought was given to the likely impact on future U.S.-Russia relations, particularly if Clinton got elected, and what the U.S. response might be. As is custom with intelligence operations, the Foreign Ministry was not briefed on the plan.

It is unlikely that the Kremlin really hoped to influence the results of the U.S. presidential election or viewed Trump's victory as likely. This would have signaled a degree of incompetence that Moscow is still incapable of. Rather, the point of the exercise was to send a message that Russia mattered and could do bad things that the U.S., in Moscow's view, has been doing to Russia. It worked, but not exactly how Russia hoped. It made Russia a negative issue in the campaign.

Subsequent releases of hacked Clinton Campaign emails,▪including personal emails of her campaign chief John Podesta, reveal signs of a▪classic active measures campaign to smear Clinton and provide ammunition for▪Donald Trump attacks on his opponent in the race. They contained signs of▪falsification and doctoring typical of the active measures tactics while the▪timing of the release — the night the Washington post published a damaging▪audio with Trump discussing sexually assaulting women — suggests a tightly▪coordinated effort, with WikiLeaks playing an unsavory role.

It did not help Trump, but hurt Russia's relationship with▪the U.S. and the likely future American president — Hillary Clinton. This may no▪longer be the work of Russian intelligence services, as the Russian state media▪have mastered the art of active measures on a scale unimaginable by the KGB.▪For months, Russian state media have been running a character assassination▪campaign against Clinton highlighting every looney right-wing conspiracy on the▪market, including spurious assertions of Clinton's complicity in founding the Islamic State.▪This shows a glaring disconnect between Russia's foreign policy interests that require▪a workable and civil relationship with U.S. leaders and the interests of▪propaganda driven by personal ambition in detriment to the nation's large good.▪There is little that Russia has gained from this effort other than bad press.

The operation destroyed what little trust remained between the two countries at the sensitive moment of Kerry-Lavrov negotiations on Syria. It put U.S. President Barack Obama in an awkward position when not retaliating was politically unfeasible. Publicly naming Russia is just the first step. Economic and technology sanctions appear to be the most likely U.S. retaliation at this point, as Washington wants to maintain the option of re-engaging Russia on Syria and is wary of escalation by cyber attacks. Moscow needs to find a way to defuse the crisis. Offering secret talks on permissible rules of cyber warfare and cyber intelligence collection might be one way to do it. Better managing its intelligence services would be another.

Original url:
https://www.themoscowtimes.com/2016/10/11/russian-spycraft-how-kremlin-hacked-its-way-into-a-crisis-a55679