GRU 26165: The Russian cyber unit that hacks targets on-site

11/18/2022

By Justin Sherman

Russian hackers are not always breaching targets from afar, typing on their keyboards in Moscow bunkers or St. Petersburg apartment buildings. For some Russian government hackers, foreign travel is part of the game. They pack up their equipment, get on international flights, and covertly move around abroad to hack into computer systems.

Enter GRU Unit 26165 (of the military intelligence agency *Glavnoye Razvedyvatelnoye Upravlenie*), a military cyber unit with hackers operating remotely and on-site. Despite the security risks on-site cyber operations pose to governments and international organizations, and the questions they raise about how the West should track and combat Russian state hacking, Russia's activities in this realm are not receiving sufficient policy attention.

GRU Unit 26165, the 85th Main Special Communications Center

In March 2018, after the GRU tried to murder former Russian intelligence officer Sergei Skripal and his daughter Yulia in Salisbury, England using a Novichok nerve agent, the Kremlin came under international fire. British intelligence officials blamed the GRU, where Skripal used to work (and later became a British informant); the multinational Organization for the Prohibition of Chemical Weapons (OPCW), which enforces the Chemical Weapons Convention, launched an investigation; and in June of the same year, OPCW countries voted to let the body attribute chemical weapons attacks to particular actors. (A year later, the OPCW would formally ban Novichok nerve agents.) Additional journalistic investigations into the perpetrators, meanwhile, continued to point to the GRU's involvement.

Although the OPCW's investigation was not made public for months, the Russian government decided to move quickly against the organization, turning to a tactical cyber unit to do so.

OPCW Headquarters

On April 10, 2018, four Russian nationals landed at Amsterdam Schiphol Airport in the Netherlands. With diplomatic passports in hand, they were met by a member of the Russian embassy in The Hague. After loading a car with technical equipment—including a wireless network panel antenna to intercept traffic—the four individuals scouted the OPCW's headquarters in The Hague for days, taking photos and circling the building before being intercepted by the Dutch General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst* or AIVD) and sent back to Moscow. Seemingly, the plan had been for the operatives to hack into the OPCW's systems to disrupt investigations into the attempted GRU chemical weapon attack.

The Netherlands made all of this public on October 4, 2018, with Dutch intelligence identifying the four operators by name—Aleksei Sergeyevich Morenets and Evgenii Mikhaylovich Serebriakov were described as "cyber operators" and Oleg Mikhaylovich Sotnikov and Alexey Valerevich Minin were described as "HUMINT (human intelligence) support." The AIVD linked all of these individuals to Russia's GRU. A Department of Justice (DOJ) indictment issued on the same day went a step further, linking the hackers—Morenets and Serebriakov—to GRU Unit 26165.

Unit 26165, otherwise known as Fancy Bear, was already known for breaking into systems from afar, including the Democratic National Committee in 2016 and World Athletics (previously the International Amateur Athletic Federation) in 2017. Yet, the revelations around the attempted OPCW hack made clear that Unit 26165 does much more. The full DOJ indictment, subsequently published by the National Security Archive at The George Washington University, alleged that Morenets "was a member of a Unit 26165 team that traveled with technical equipment to locations around the world to conduct on-site hacking operations to target and maintain persistent access to WiFi networks used by victim organizations and personnel." Serebriakov also belonged to such a team. While Unit 26165 often conducts remote hacks from Russia, the indictment stated that "if the remote hack was unsuccessful or if it did not provide the conspirators with sufficient access to victims' networks," Unit 26165 would carry out "'on-site' or 'close access' hacking operations."

The OPCW incident was not the first time these particular hackers went abroad to conduct operations. According to the DOJ, Morenets traveled to Rio de Janeiro, Brazil, and Lausanne, Switzerland, in 2016 to breach the into WiFi networks used by people with access to the US Anti-Doping Agency, the World Anti-Doping Agency, and the Canadian Center for Ethics in Sport. Serebriakov, the indictment stated, also participated in these on-site hacking operations. Both individuals allegedly planned to target the Spiez Laboratory in Switzerland after the OPCW hack. The indictment alleged that Ivan Sergeyevich Yermakov, also part of GRU Unit 26165, provided remote reconnaissance support for his colleagues' on-site hacking operation against the OPCW.

Additionally, it is speculated that these on-site hackers were supported by another GRU unit, which is where the other two Russians caught in the Netherlands by the AIVD enter the picture. Sotnikov and Minin were described generically by the Dutch as HUMINT support for the two hackers, and as "Russian military intelligence officers" by the DOJ's full indictment. Neither of these government documents mentions a specific GRU unit associated with Sotnikov or Minin.

Published in tandem with the October 4, 2018 state disclosures was a new *Bellingcat* investigation linking Morenets' Russian car to the Unit 26165 building in Russia. It also linked Minin's car registration to the GRU "Conservatory." The Conservatory—formally numbered GRU Unit 22177—is the Russian Defense Ministry's Military Academy and a training site for the GRU, located in Moscow near GRU headquarters and other GRU training facilities. Due to Minin's connection to 22177 and the Dutch and US governments' vague references to Sotnikov and Minin as "HUMINT support" and "Russian military intelligence officers" separate from Unit 26165, numerous articles have speculated that operatives from another GRU unit were tasked to support the mission in The Hague.

Stepping back, assessing the picture

Policymakers should use this information as a case study for how Russian government hackers—and, theoretically, state hackers from other adversary countries—move around the world to break into systems. The use of on-site cyber operations abroad seems unique to this GRU team, with many possible motivations at play. It is unclear how high up the oversight chain these on-site operations go. What is clear, though, is that Western governments cannot restrict their hunt for Russian hackers to the digital sphere; they must also remember how Russian hacking fits into broader Russian intelligence activities, including overseas.

There are several takeaways and implications that result from this information. The on-site, overseas cyber operations of GRU Unit 26165 appears to stand out from other Russian government cyber units. Of course, cyber capabilities are a part of intelligence operations more broadly, and many human operations around the world leverage cyber reconnaissance on an ongoing basis. Nonetheless, when the United Kingdom (UK) released its own statement on Russian government cyber activity in October 2018, it clearly differentiated between the activities of Unit 26165 in the Netherlands, Brazil, and Switzerland and those of Unit 74455 (Sandworm), which it stressed "were carried out remotely—by GRU teams based within Russia." The DOJ indictment appears to suggest, although this is not totally clear, that hackers going abroad are part of at least one specific sub-team within the broader cyber unit. Further, the DOJ indictment lists numerous examples of on-site hacks or hack attempts, but publicly available information has not exposed the same kind of on-site operations by Russia's Foreign intelligence Service, the SVR.

The motivations behind the on-site operations of Unit 26165 are also a key question. Based on publicly available information, its proclivity for "close access" operations leans toward disrupting high-profile investigations into potentially embarrassing Russian government activity. The first set of reported hacks targeted international investigations into allegations of Russian doping at the Olympics; the second set of hacks targeted the international investigation into the attempted murder of the Skripals with chemical weapons. It is possible, therefore, that protecting the Kremlin's image is a high priority. Simultaneously, the DOJ indictment stated that Unit 26165 carries out on-site operations when remote operations are unsuccessful, suggesting a more functional, effects-oriented motive for sending hackers overseas.

However, there is another possibility: The GRU may simply be using on-site operations when it needs to draw attention away from its own failures. The botched attempt to murder Sergei and Yulia Skripal was carried out by GRU Unit 29155, a Russian military intelligence and assassination team with close relationships to the Signal Scientific Center federal research facility and the Ministry of Defense's State Institute for Experimental Military Medicine in St. Petersburg, entities suspected of managing Russia's Novichok program. GRU operatives are well-known for their high-risk appetites and sometimes overt violence, even relative to other Russian intelligence organs like the Federal Security Service (FSB), Russia's domestic security agency. (That said, the FSB is a violent organization, too, carrying out repressive tactics in Russia and, in 2019, assassinating a Georgian asylum seeker in Berlin.)

This tendency is playing out in cyberspace already, given that GRU teams are behind the NotPetya malware attack, shutdowns of Ukrainian power grids, and other more destructive, publicly visible operations. Such cyber activities, in line with broader intelligence cultures, stand in contrast to agencies like the SVR, which appears to place a premium on covertness, both online and offline. Wanting to frantically undermine an investigation into its own failed operation, it is not out of the question that the GRU sent Unit 26165 operatives overseas. That Unit 26165 hackers Morenets and Serebriakov may have had support from other parts of the GRU (HUMINT operators Sotbikov and Minin) in the OPCW plot suggests possible broader intra-agency coordination. But again, it is easy—and sometimes misguided—to assume there is more coordination within the Russian security services than actually occurs.

All of this raises a final and more interesting question always at play in the Russian cyber ecosystem: How far up the chain does oversight of on-site hacks go?

Cyber and information operations with high political sensitivity, which Moscow conceptualizes more cohesively than in the West, are more likely to be supervised by the Kremlin. The US intelligence community assessed, for example, that the influence actions targeting the 2016 US election were "approved at the highest levels of the Russian government," and a similar conclusion was reached vis-à-vis President Vladimir Putin and Russia's election interference in 2020. This may also be true for more traditional intelligence operations. When the UK finished its investigation into the murder of former Russian spy Alexander Litvinenko, who was killed on British soil with the

radioactive material Polonium-210, it concluded that Putin and Russian Security Council head Nikolai Patrushev "probably" approved the killing.

The GRU's botched murder attempt on the Skripals garnered significant international attention. At the time, Russian officials were already criticizing the OPCW's investigations into the Assad regime's use of chemical weapons in Syria —called an attempt "to make the OPCW draw hasty but at the same time far-reaching conclusions" by Russia's deputy foreign minister. When the investigation into the Skripal poisonings began, senior officials like Russian Foreign Minister Sergei Lavrov falsely claimed that a lab used by the OPCW picked up traces of a nerve agent possessed by NATO countries but not Russia. Putin, meanwhile, has always held particular contempt for people he perceives as betraying the Russian nation, once saying that "traitors always meet a bad end," suggesting a kind of personal anger directed at individuals like Sergei Skripal who became agents for the West. The Olympic doping investigations, too, proved an embarrassment for Moscow.

In this vein, it is quite possible that higher-level Kremlin officials may direct the GRU to act against investigations like OPCW's, prompting the GRU to deploy Unit 26165 hackers to the Netherlands. It is also plausible that the activities of Unit 26165 merely reflect broader intelligence collection priorities, spying on those trying to "hurt" Russia, such as investigators looking into Russian athlete doping. Since there are few publicly known cases of Unit 26165 conducting "close access" operations, perhaps these are not representative samples, with the GRU carrying out these activities on its own after all.

Regardless, the GRU is clearly sending hackers overseas to carry out operations. Going forward, Western intelligence and law enforcement personnel, as well as multinational organizations, would be wise to pay attention.

Image: OPCW Headquarters