Russian Hacker Wanted!

The arrest warrant for the Bundestag hacker represents a new German response to cyberattacks - and has potentially major implications

Thomas Reinhold 9 June 2020 Commentary

In May 2020, Germany's Federal Court of Justice issued an arrest warrant for a Russian citizen suspected of conducting the 2015 hack of the German Parliament's IT and communication system. This unprecedented move has attracted quite a bit of attention and represents, at least, a significant escalation, if not a complete shift, in Germany's strategic response to state-ordered cyberattacks.

In early May 2015, reports surfaced that a group of hackers had gained access to Parlakom, the internal computer system of the German Bundestag. Parlakom connects German parliamentarians and members of their staff with the local offices in their constituencies across Germany. The working hypothesis is that the attackers used spear phishing emails followed by malware to gradually access other network components. The malware was finally removed from the network permanently in late June 2015, but only after the Federal Cyber Security Authority, BSI, performed a complete restoration of the network and an almost total reset of the system. The entire system had to be switched off to stop the attack. According to media reports, up to 20,000 accounts were affected. Officially, it was confirmed that "isolated data outflows" occurred until June 2015. It was also confirmed that the type of attack and the malware samples found indicated that the attack was targeted, specifically designed to hit the Parlakom system, indicating a state-backed attacker.

The German magazine Der Spiegel also reported that the offices of 15 members of Parliament were compromised and that the hackers stole 16GB of internal emails, calendar data and other information. The breach forced the Parliament to choose between using a compromised IT system, making themselves vulnerable to further data breaches, and not using their central communication platform. The bill for restoring the Parlakom system amounted to 1.4 million euros, according to the Bundestag administration.

Germany Identifies the Culprit

Shortly after the 2015 incident, speculation began to swirl that Russian hackers were behind the attack. Multiple investigations later supported this theory, but it was never officially confirmed by the German authorities. The wheels of justice did not sleep, however.

In early 2016, the Federal Public Prosecutor General of the Federal Court of Justice (Generalbundesanwalt) launched an investigation against unknown persons on the suspicion of "an intelligence-led attack". Nearly five years after the incident, the Federal Court of Justice (Bundesgerichtshof) issued an arrest warrant for a Russian citizen named Dmitrij Badin.

Badin is a suspected agent of Russian military intelligence, the GRU. Specifically, he is believed to be a member of cyber unit 26165, better known as "Fancy Bear" or APT28 (Bellingcat has published an extensive profile of Badin). APT28 has also been linked to other significant political cyber operations, most prominently the 2016 hack of the US Democratic National Committee.

The issuance of the arrest warrant for Badin was unprecedented, as was Chancellor Merkel's clear finger pointing at Russia, while she declared that the attack was "unpleasant" and "outrageous". While the text of the indictment is not publicly available, media reports suggest that the warrant makes it abundantly clear that a foreign spy and member of a foreign military secret service committed the attack on the German Parliament. The judges made it clear that they consider this a "particularly serious case" of "state-ordered" espionage because it was "an attack on the parliament, and thus on the representative of the sovereign of the Federal Republic of Germany, the people, and the core area of German democracy. … A crime for which there has so far been no example".

Russia's Foreign Minister, Sergei Lavrov, rejected these allegations, claiming that there is no evidence that Russian hackers were behind the

attack. Russia has consistently rejected responsibility for cyber incidents in the past, sometimes even blaming such attacks on independent "patriotic hackers".

Legal Evolution or Political Revolution?

What implications does this indictment have for Germany's, and possibly the EU's, stance regarding malicious cyber activities against EU member states? While the United States has used criminal indictments to pursue hackers from other countries (in particular those associated with foreign intelligence agencies or their units) on several occasions, this approach is still novel in Europe. Until now, EU states have tried to abstain from instrumentalising criminal law for political aims.

In an official reaction to the arrest warrant, Chancellor Merkel reaffirmed the accusations and pointed out that the attack served to "disrupt a trusting cooperation". In the context of an already tense relationship, the warrant represented a departure from Germany's usual practice of trying to salvage communication channels with Russia, sending a clear and unambiguous signal that such malicious cyber activities would not be tolerated. In her statement, Chancellor Merkel emphasized that Russia's behaviour was perceived as and judged to be a strategy of "hybrid warfare" that, among other things, was intended to create "disorientation" and "distortion of facts". In a notable departure from her typically understated style of communication, she pointedly stated that the issue was no longer simply individual or an unpleasant incident, but Russian services' increasing aggressiveness and disregard for the rules of the game. And it didn't end there. Germany has also activated its European partners and started the political process to impose travel bans and asset freezes on Badin and his boss, Igor Kostyukov. Germany's directness in this response is surprising in some ways, given that it did not join in other countries' coordinated attribution of the cyberattacks against Georgia earlier this year. In the past, Germany's strategy has relied mostly on "backroom conversations" with

Russia and on subtly addressing its concerns through political communication, rather than direct accusations.

So what comes next? The actual consequences of Germany's actions will play out over the coming months, however, they will probably occur largely behind closed doors. But one thing is certain: Germany does not intend to tolerate Russia's meddling in national politics and its attacks on Germany's political institutions any longer. This is an important message a year ahead of the German federal elections. This new stance aligns Germany once again with other countries that have stood up to Russia's seemingly limitless cyber activities and interference in national matters, including disinformation campaigns and the undermining and de-authorisation of democratic values and institutions. Of course, now the genie is out of the bottle: German authorities will find it difficult to backtrack or soften their tone without losing political credibility on the international stage and at home.

Based on both the seriousness of the charges and the related political statement, it seems likely that Germany will handle similar incidents more assertively in the future and continue to use public attribution as a means of deterrence. This new approach also signals a clear shift from the communication strategy adopted in the past – such as when German government networks were breached in 2017 – towards a more risk-averse strategy that calls for a timely, decisive political response rather than one that is dependent on the outcome of a years-long investigation. This new approach also brings the EU a step closer to speaking with a common voice against similar interference.

Overall, pressure on Russia will now, presumably, increase. However, more pressure alone may have drawbacks. It may drive the country further into alienation (Abgrenzung) and lead to other unwelcome developments, such as Russia's decisions to establish independent IT backbone infrastructures and to support China's NewIP recommendations, thus further fracturing the international common ground. Acknowledging this, the German government

still emphasises the necessity of inter-state dialogues and is working to maintain communication channels.

An Opportunity for Germany

Germany's choice to opt for the criminal law path, and the accompanying political declarations, creates an opportunity to reinvigorate the debate about responsible state behaviour in cyberspace. Germany already actively participates in the UN-led processes devoted to those issues, such as the UN Group of Governmental Experts and the Open-Ended Working Group. For the moment, however, Germany – like the rest of the European states – has been caught between the United States and Russia as they compete to gain the upper hand in those debates – and unfortunately, they deal the cards. The two parallel UN processes are the best example of this competition. This should not prevent Germany – and the rest of the EU – from adopting a more assertive and stronger voice on this issue. Such a new position could be built on promoting and reinforcing three main commitments:

- Exposing the cyber activities of foreign state services targeting the IT systems of EU member states, regardless of where they originate from, and imposing consequences for them. This would require a pan-European debate about the US cyber strategy of persistent engagement. This strategy explicitly moves cyberdefence into the IT systems of adversaries by exerting constant pressure on their systems, leaving no operational space for cyberattacks. However, it also includes infiltrating the IT systems of allies when necessary.
- Promoting responsible vulnerability disclosure mechanisms that would support the objective of "demilitarisation" in cyberspace. Such mechanisms, adopted by, among others, the UK and the Netherlands, have been also proposed as a new norm by the Global Commission on Stability in Cyberspace and could help reduce the risk of malware infection waves like NotPetya or WannaCry.

- Promoting the international commitments accepted by states in the UN-GGE reports, including the commitment to prevent their territories from being used as launching pads for attacks and the commitment to provide assistance to countries that are the victims of such attacks. This will require establishing proper communication channels, to build confidence, and openly addressing key challenges to law enforcement and judicial cooperation. An expert dialogue between the EU and Russia – in line with the Russian proposal – might offer new insights into further operationalisation of such commitments.

The upcoming German Presidency of the Council offers a window of opportunity to move some of these conversations forward. What we need is the strong commitment to the existing rules that is binding for every state and every service.

Featured image: credits to Clint Patterson

Thomas Reinhold

Thomas Reinhold works in the research group ‘Science and Technology for Peace and Security’ at the University of Darmstadt. He is also a Non-Resident Fellow in Arms Control and Emerging Technologies at the Institute for Peace Research and Security Policy, Hamburg. Follow him on Twitter: @CyberPeace1.